# GAQM

## Exam Questions CEH-001

Certified Ethical Hacker (CEH)

# About Exambible

***Your Partner of IT Exam***

# Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

# Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

**NEW QUESTION 1**
- (Topic 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**
- (Topic 1)
A rootkit is a collection of tools (programs) that enable administrator-level access to a computer. This program hides itself deep into an operating system for malicious activity and is extremely difficult to detect. The malicious software operates in a stealth fashion by hiding its files, processes and registry keys and may be used to create a hidden directory or folder designed to keep out of view from a user's operating system and security software.

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

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

**Answer:** D

**NEW QUESTION 3**
- (Topic 1)
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 4**
- (Topic 1)
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 5**
- (Topic 1)
Peter extracts the SID list from Windows 2008 Server machine using the hacking tool "SIDExtracter". Here is the output of the SIDs:

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 6**
- (Topic 1)

An attacker finds a web page for a target organization that supplies contact information for the company. Using available details to make the message seem authentic, the attacker drafts e-mail to an employee on the contact page that appears to come from an individual who might reasonably request confidential information, such as a network administrator.
The email asks the employee to log into a bogus page that requests the employee's user name and password or click on a link that will download spyware or other malicious programming.
Google's Gmail was hacked using this technique and attackers stole source code and sensitive data from Google servers. This is highly sophisticated attack using zero-day exploit vectors, social engineering and malware websites that focused on targeted individuals working for the company.
What is this deadly attack called?

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

**Answer:** A

**NEW QUESTION 7**
- (Topic 1)
The following script shows a simple SQL injection. The script builds an SQL query by concatenating hard-coded strings together with a string entered by the user:

The user is prompted to enter the name of a city on a Web form. If she enters Chicago, the query assembled by the script looks similar to the following:
SELECT * FROM OrdersTable WHERE ShipCity = 'Chicago'
How will you delete the OrdersTable from the database using SQL Injection?

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

**Answer:** A

**NEW QUESTION 8**
- (Topic 1)
Attackers footprint target Websites using Google Hacking techniques. Google hacking is a term that refers to the art of creating complex search engine queries. It detects websites that are vulnerable to numerous exploits and vulnerabilities. Google operators are used to locate specific strings of text within the search results. The configuration file contains both a username and a password for an SQL database. Most sites with forums run a PHP message base. This file gives you the keys to that forum, including FULL ADMIN access to the database. WordPress uses config.php that stores the database Username and Password.
Which of the below Google search string brings up sites with "config.php" files?

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

**Answer:** C

**NEW QUESTION 9**
- (Topic 1)
Jack Hacker wants to break into Brown Co.'s computers and obtain their secret double fudge cookie recipe. Jack calls Jane, an accountant at Brown Co., pretending to be an administrator from Brown Co. Jack tells Jane that there has been a problem with some accounts and asks her to verify her password with him "just to double check our records." Jane does not suspect anything amiss, and parts with her password. Jack can now access Brown Co.'s computers with a valid user name and password, to steal the cookie recipe. What kind of attack is being illustrated here?

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

**Answer:** C

**NEW QUESTION 10**
- (Topic 1)
In Buffer Overflow exploit, which of the following registers gets overwritten with return address of the exploit code?

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

**Answer:** D

**NEW QUESTION 10**
- (Topic 1)
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 11**
- (Topic 1)
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 14**
- (Topic 1)
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 19**
- (Topic 1)
You want to hide a secret.txt document inside c:\windows\system32\tcpip.dll kernel library using ADS streams. How will you accomplish this?

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

**Answer:** B

**NEW QUESTION 24**
- (Topic 1)
In the context of password security: a simple dictionary attack involves loading a dictionary file (a text file full of dictionary words) into a cracking application such as L0phtCrack or John the Ripper, and running it against user accounts located by the application. The larger the word and word fragment selection, the more effective the dictionary attack is. The brute force method is the most inclusive - though slow. Usually, it tries every possible letter and number combination in its automated exploration. If you would use both brute force and dictionary combined together to have variations of words, what would you call such an attack?

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

**Answer:** C

**NEW QUESTION 26**
- (Topic 1)
Which of the following statements would NOT be a proper definition for a Trojan Horse?

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

**Answer:** A

**NEW QUESTION 27**
- (Topic 1)
Maintaining a secure Web server requires constant effort, resources, and vigilance from an organization. Securely administering a Web server on a daily basis is an essential aspect of Web server security.
Maintaining the security of a Web server will usually involve the following steps:
1. Configuring, protecting, and analyzing log files
2. Backing up critical information frequently
3. Maintaining a protected authoritative copy of the organization's Web content
4. Establishing and following procedures for recovering from compromise
5. Testing and applying patches in a timely manner
6. Testing security periodically.
In which step would you engage a forensic investigator?

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

**Answer:** D

**NEW QUESTION 32**
- (Topic 1)
How do you defend against ARP Spoofing? Select three.

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

**Answer:** ACD

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

**NEW QUESTION 34**
- (Topic 1)
If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization.

How would you prevent such type of attacks?

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

**Answer:** C

**NEW QUESTION 39**
- (Topic 1)
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 43**
- (Topic 1)
You are the Security Administrator of Xtrinity, Inc. You write security policies and conduct assessments to protect the company's network. During one of your periodic checks to see how well policy is being observed by the employees, you discover an employee has attached cell phone 3G modem to his telephone line and workstation. He has used this cell phone 3G modem to dial in to his workstation, thereby bypassing your firewall. A security breach has occurred as a direct result of this activity. The employee explains that he used the modem because he had to download software for a department project. How would you resolve this situation?

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

**Answer:** B

**NEW QUESTION 47**
- (Topic 1)
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 49**
- (Topic 1)
Attackers target HINFO record types stored on a DNS server to enumerate information. These are information records and potential source for reconnaissance. A network administrator has the option of entering host information specifically the CPU type and operating system when creating a new DNS record. An attacker can extract this type of information easily from a DNS server.
Which of the following commands extracts the HINFO record?

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

**Answer:** A

**NEW QUESTION 50**
- (Topic 1)
What type of attack is shown in the following diagram?

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

**Answer:** A

**NEW QUESTION 53**
- (Topic 1)
An attacker has successfully compromised a remote computer. Which of the following comes as one of the last steps that should be taken to ensure that the compromise cannot be traced back to the source of the problem?

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

**Answer:** D

**NEW QUESTION 56**
- (Topic 1)
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.

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 60**
- (Topic 1)
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 64**
- (Topic 2)
What type of attack is shown here?

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

**Answer:** D

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

**NEW QUESTION 66**
- (Topic 2)
Data is sent over the network as clear text (unencrypted) when Basic Authentication is configured on Web Servers.

A. true
B. false

**Answer:** A

**NEW QUESTION 68**
- (Topic 2)
What framework architecture is shown in this exhibit?

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

**Answer:** B

**NEW QUESTION 73**
- (Topic 2)
Joseph has just been hired on to a contractor company of the Department of Defense as their Senior Security Analyst. Joseph has been instructed on the company's strict security policies that have been implemented, and the policies that have yet to be put in place. Per the Department of Defense, all DoD users and the users of their contractors must use two- factor authentication to access their networks. Joseph has been delegated the task of researching and implementing the best two-factor authentication method for his company. Joseph's supervisor has told him that they would like to use some type of hardware device in tandem with a security or identifying pin number. Joseph's company has already researched using smart cards and all the resources needed to implement them, but found the smart cards to not be cost effective. What type of device should Joseph use for two- factor authentication?

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

**Answer:** D

**NEW QUESTION 74**
- (Topic 2)
What type of session hijacking attack is shown in the exhibit?

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

**Answer:** A

**NEW QUESTION 79**
- (Topic 2)
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 81**
- (Topic 2)
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 83**
- (Topic 2)
You are the CIO for Avantes Finance International, a global finance company based in Geneva. You are responsible for network functions and logical security throughout the entire corporation. Your company has over 250 servers running Windows Server, 5000 workstations running Windows Vista, and 200 mobile users working from laptops on Windows 7.
Last week, 10 of your company's laptops were stolen from salesmen while at a conference in Amsterdam. These laptops contained proprietary company information. While doing damage assessment on the possible public relations nightmare this may become, a news story leaks about the stolen laptops and also that sensitive information from those computers was posted to a blog online.
What built-in Windows feature could you have implemented to protect the sensitive information on these laptops?

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

**Answer:** D

**NEW QUESTION 88**
- (Topic 2)
What is the default Password Hash Algorithm used by NTLMv2?

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

**Answer:** D

**NEW QUESTION 93**
- (Topic 2)
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 98**
- (Topic 2)
Finding tools to run dictionary and brute forcing attacks against FTP and Web servers is an easy task for hackers. They use tools such as arhontus or brutus to break into remote servers.

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 100**
- (Topic 2)
Within the context of Computer Security, which of the following statements describes Social Engineering best?

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

**Answer:** C

**NEW QUESTION 105**
- (Topic 2)
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 107**
- (Topic 2)
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 110**
- (Topic 2)
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 113**
- (Topic 2)
You are footprinting an organization and gathering competitive intelligence. You visit the company's website for contact information and telephone numbers but do not find them listed there. You know they had the entire staff directory listed on their website 12 months ago but now it is not there. Is there any way you can retrieve information from a website that is outdated?

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

**Answer:** C

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

**NEW QUESTION 117**
- (Topic 2)
Which of the following Trojans would be considered 'Botnet Command Control Center'?

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

**Answer:** C

**NEW QUESTION 122**
- (Topic 2)
NetBIOS over TCP/IP allows files and/or printers to be shared over the network. You are trying to intercept the traffic from a victim machine to a corporate network printer. You are attempting to hijack the printer network connection from your laptop by sniffing the wire. Which port does SMB over TCP/IP use?

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

**Answer:** D

**NEW QUESTION 123**
- (Topic 2)
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 124**
- (Topic 2)
The programmers on your team are analyzing the free, open source software being used to run FTP services on a server in your organization. They notice that there is excessive number of functions in the source code that might lead to buffer overflow. These C++ functions do not check bounds. Identify the line in the source code that might lead to buffer overflow?

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

**Answer:** B

**NEW QUESTION 129**
- (Topic 3)
Which of the following statements are true regarding N-tier architecture? (Choose two.)

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

**Answer:** AC

**NEW QUESTION 132**
- (Topic 3)
How do you defend against ARP Poisoning attack? (Select 2 answers)

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

**Answer:** AC

**NEW QUESTION 134**
- (Topic 3)
During a penetration test, the tester conducts an ACK scan using NMAP against the external interface of the DMZ firewall. NMAP reports that port 80 is unfiltered. Based on this response, which type of packet inspection is the firewall conducting?

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

**Answer:** C

**NEW QUESTION 136**
- (Topic 3)
John is the network administrator of XSECURITY systems. His network was recently compromised. He analyzes the log files to investigate the attack. Take a look at the following Linux log file snippet. The hacker compromised and "owned" a Linux machine. What is the hacker trying to accomplish here?

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

**Answer:** D

**NEW QUESTION 139**
- (Topic 3)
The GET method should never be used when sensitive data such as credit card is being sent to a CGI program. This is because any GET command will appear in the URL, and will be logged by any servers. For example, let's say that you've entered your credit card information into a form that uses the GET method. The URL may appear like this:
https://www.xsecurity-bank.com/creditcard.asp?cardnumber=453453433532234
The GET method appends the credit card number to the URL. This means that anyone with access to a server log will be able to obtain this information. How would you protect from this type of attack?

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

**Answer:** C

**NEW QUESTION 144**
- (Topic 3)
Perimeter testing means determining exactly what your firewall blocks and what it allows. To conduct a good test, you can spoof source IP addresses and source ports. Which of the following command results in packets that will appear to originate from the system at 10.8.8.8? Such a packet is useful for determining whether the firewall is allowing random packets in or out of your network.

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

**Answer:** D

**NEW QUESTION 147**
- (Topic 3)
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 151**
- (Topic 3)
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 154**
- (Topic 3)
Which tool would be used to collect wireless packet data?

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

**Answer:** A

**NEW QUESTION 157**
- (Topic 3)
Which of the following can take an arbitrary length of input and produce a message digest output of 160 bit?

A. SHA-1
B. MD5

C. HAVAL
D. MD4

**Answer:** A

**NEW QUESTION 162**
- (Topic 3)
On a Linux device, which of the following commands will start the Nessus client in the background so that the Nessus server can be configured?

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

**Answer:** C

**NEW QUESTION 167**
- (Topic 3)
Which of the following Exclusive OR transforms bits is NOT correct?

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

**Answer:** C

**NEW QUESTION 168**
- (Topic 3)
Jacob is looking through a traffic log that was captured using Wireshark. Jacob has come across what appears to be SYN requests to an internal computer from a spoofed IP address. What is Jacob seeing here?

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

**Answer:** B

**NEW QUESTION 173**
- (Topic 3)
In the software security development life cyle process, threat modeling occurs in which phase?

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

**Answer:** A

**NEW QUESTION 178**
- (Topic 3)
Which of the following represent weak password? (Select 2 answers)

A. Passwords that contain letters, special characters, and numbers Exampl
B. ap1$%##f@52
C. Passwords that contain only numbers Exampl
D. 23698217
E. Passwords that contain only special characters Exampl
F. &*#@!(%)
G. Passwords that contain letters and numbers Exampl
H. meerdfget123
I. Passwords that contain only letters Exampl
J. QWERTYKLRTY
K. Passwords that contain only special characters and numbers Exampl
L. 123@$45
M. Passwords that contain only letters and special characters Exampl
N. bob@&ba
O. Passwords that contain Uppercase/Lowercase from a dictionary list Exampl
P. OrAnGe

**Answer:** EH

**NEW QUESTION 182**
- (Topic 3)
When does the Payment Card Industry Data Security Standard (PCI-DSS) require organizations to perform external and internal penetration testing?

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

**Answer:** A

**NEW QUESTION 184**
- (Topic 3)
A company has five different subnets: 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0 and 192.168.5.0. How can NMAP be used to scan these adjacent Class C networks?

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

**Answer:** A

**NEW QUESTION 189**
- (Topic 3)
You are trying to package a RAT Trojan so that Anti-Virus software will not detect it. Which of the listed technique will NOT be effective in evading Anti-Virus scanner?

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

**Answer:** A

**NEW QUESTION 192**
- (Topic 3)
Which of the following conditions must be given to allow a tester to exploit a Cross-Site Request Forgery (CSRF) vulnerable web application?

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

**Answer:** D

**NEW QUESTION 194**
- (Topic 4)
Which of the following processes of PKI (Public Key Infrastructure) ensures that a trust relationship exists and that a certificate is still valid for specific operations?

A. Certificate issuance
B. Certificate validation
C. Certificate cryptography
D. Certificate revocation

**Answer:** B

**NEW QUESTION 195**
- (Topic 4)
Which results will be returned with the following Google search query?
site:target.com -site:Marketing.target.com accounting

A. Results matching all words in the query
B. Results matching “accounting” in domain target.com but not on the site Marketing.target.com
C. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting
D. Results for matches on target.com and Marketing.target.com that include the word “accounting”

**Answer:** B

**NEW QUESTION 197**
- (Topic 4)
Which of the following parameters enables NMAP's operating system detection feature?

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

**Answer:** D

**NEW QUESTION 202**
- (Topic 4)
A security policy will be more accepted by employees if it is consistent and has the support of

A. coworkers.
B. executive management.
C. the security officer.
D. a supervisor.

**Answer:** B

**NEW QUESTION 207**
- (Topic 4)
One advantage of an application-level firewall is the ability to

A. filter packets at the network level.
B. filter specific commands, such as http:post.
C. retain state information for each packet.
D. monitor tcp handshaking.

**Answer:** B

**NEW QUESTION 208**
- (Topic 4)
An engineer is learning to write exploits in C++ and is using the exploit tool Backtrack. The engineer wants to compile the newest C++ exploit and name it calc.exe. Which command would the engineer use to accomplish this?

A. g++ hackersExploit.cpp -o calc.exe
B. g++ hackersExploit.py -o calc.exe
C. g++ -i hackersExploit.pl -o calc.exe
D. g++ --compile –i hackersExploit.cpp -o calc.exe

**Answer:** A

**NEW QUESTION 210**
- (Topic 4)
A Security Engineer at a medium-sized accounting firm has been tasked with discovering how much information can be obtained from the firm's public facing web servers. The engineer decides to start by using netcat to port 80.
The engineer receives this output:
HTTP/1.1 200 OK
Server: Microsoft-IIS/6
Expires: Tue, 17 Jan 2011 01:41:33 GMT
DatE. Mon, 16 Jan 2011 01:41:33 GMT
Content-TypE. text/html Accept-Ranges: bytes
Last-ModifieD. Wed, 28 Dec 2010 15:32:21 GMT
ETaG. "b0aac0542e25c31:89d" Content-Length: 7369
Which of the following is an example of what the engineer performed?

A. Cross-site scripting
B. Banner grabbing
C. SQL injection
D. Whois database query

**Answer:** B

**NEW QUESTION 211**
- (Topic 4)
What type of OS fingerprinting technique sends specially crafted packets to the remote OS and analyzes the received response?

A. Passive
B. Reflective
C. Active
D. Distributive

**Answer:** C

**NEW QUESTION 215**
- (Topic 4)
How can telnet be used to fingerprint a web server?

A. telnet webserverAddress 80 HEAD / HTTP/1.0
B. telnet webserverAddress 80 PUT / HTTP/1.0
C. telnet webserverAddress 80 HEAD / HTTP/2.0
D. telnet webserverAddress 80 PUT / HTTP/2.0

**Answer:** A

**NEW QUESTION 220**
- (Topic 4)
A hacker is attempting to use nslookup to query Domain Name Service (DNS). The hacker uses the nslookup interactive mode for the search. Which command should the hacker type into the command shell to request the appropriate records?

A. Locate type=ns
B. Request type=ns
C. Set type=ns
D. Transfer type=ns

**Answer:** C

**NEW QUESTION 221**
- (Topic 4)
When creating a security program, which approach would be used if senior management is supporting and enforcing the security policy?

A. A bottom-up approach
B. A top-down approach
C. A senior creation approach
D. An IT assurance approach

**Answer:** B

**NEW QUESTION 224**
- (Topic 4)
Which method can provide a better return on IT security investment and provide a thorough and comprehensive assessment of organizational security covering policy, procedure design, and implementation?

A. Penetration testing
B. Social engineering
C. Vulnerability scanning
D. Access control list reviews

**Answer:** A

**NEW QUESTION 228**
- (Topic 4)
Which type of intrusion detection system can monitor and alert on attacks, but cannot stop them?

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

**Answer:** B

**NEW QUESTION 233**
- (Topic 4)
Bluetooth uses which digital modulation technique to exchange information between paired devices?

A. PSK (phase-shift keying)
B. FSK (frequency-shift keying)
C. ASK (amplitude-shift keying)
D. QAM (quadrature amplitude modulation)

**Answer:** A

**NEW QUESTION 235**
- (Topic 4)
When using Wireshark to acquire packet capture on a network, which device would enable the capture of all traffic on the wire?

A. Network tap
B. Layer 3 switch
C. Network bridge
D. Application firewall

**Answer:** A

**NEW QUESTION 238**
- (Topic 4)
A company firewall engineer has configured a new DMZ to allow public systems to be located away from the internal network. The engineer has three security zones set:
Untrust (Internet) – (Remote network = 217.77.88.0/24) DMZ (DMZ) – (11.12.13.0/24)
Trust (Intranet) – (192.168.0.0/24)
The engineer wants to configure remote desktop access from a fixed IP on the remote network to a remote desktop server in the DMZ. Which rule would best fit this requirement?

A. Permit 217.77.88.0/24 11.12.13.0/24 RDP 3389
B. Permit 217.77.88.12 11.12.13.50 RDP 3389
C. Permit 217.77.88.12 11.12.13.0/24 RDP 3389
D. Permit 217.77.88.0/24 11.12.13.50 RDP 3389

**Answer:** B

**NEW QUESTION 239**
- (Topic 4)
What is the purpose of conducting security assessments on network resources?

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

**Answer:** B

**NEW QUESTION 241**
- (Topic 4)
What is the outcome of the comm”nc -l -p 2222 | nc 10.1.0.43 1234"?

A. Netcat will listen on the 10.1.0.43 interface for 1234 seconds on port 2222.
B. Netcat will listen on port 2222 and output anything received to a remote connection on 10.1.0.43 port 1234.
C. Netcat will listen for a connection from 10.1.0.43 on port 1234 and output anything received to port 2222.
D. Netcat will listen on port 2222 and then output anything received to local interface 10.1.0.43.

**Answer:** B

**NEW QUESTION 245**
- (Topic 4)
A developer for a company is tasked with creating a program that will allow customers to update their billing and shipping information. The billing address field used is limited to 50 characters. What pseudo code would the developer use to avoid a buffer overflow attack on the billing address field?

A. if (billingAddress = 50) {update field} else exit
B. if (billingAddress != 50) {update field} else exit
C. if (billingAddress >= 50) {update field} else exit
D. if (billingAddress <= 50) {update field} else exit

**Answer:** D

**NEW QUESTION 246**
- (Topic 4)
Which of the following is a characteristic of Public Key Infrastructure (PKI)?

A. Public-key cryptosystems are faster than symmetric-key cryptosystems.
B. Public-key cryptosystems distribute public-keys within digital signatures.
C. Public-key cryptosystems do not require a secure key distribution channel.
D. Public-key cryptosystems do not provide technical non-repudiation via digital signatures.

**Answer:** B

**NEW QUESTION 250**
- (Topic 4)
Which Open Web Application Security Project (OWASP) implements a web application full of known vulnerabilities?

A. WebBugs
B. WebGoat
C. VULN_HTML
D. WebScarab

**Answer:** B

**NEW QUESTION 251**
- (Topic 4)
If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

A. Hping
B. Traceroute
C. TCP ping
D. Broadcast ping

**Answer:** A

**NEW QUESTION 255**

- (Topic 4)
Which of the following is a detective control?

A. Smart card authentication
B. Security policy
C. Audit trail
D. Continuity of operations plan

**Answer:** C

**NEW QUESTION 258**
- (Topic 4)
When comparing the testing methodologies of Open Web Application Security Project (OWASP) and Open Source Security Testing Methodology Manual (OSSTMM) the main difference is

A. OWASP is for web applications and OSSTMM does not include web applications.
B. OSSTMM is gray box testing and OWASP is black box testing.
C. OWASP addresses controls and OSSTMM does not.
D. OSSTMM addresses controls and OWASP does not.

**Answer:** D

**NEW QUESTION 260**
- (Topic 4)
A penetration tester was hired to perform a penetration test for a bank. The tester began searching for IP ranges owned by the bank, performing lookups on the bank's DNS servers, reading news articles online about the bank, watching what times the bank employees come into work and leave from work, searching the bank's job postings (paying special attention to IT related jobs), and visiting the local dumpster for the bank's corporate office. What phase of the penetration test is the tester currently in?

A. Information reporting
B. Vulnerability assessment
C. Active information gathering
D. Passive information gathering

**Answer:** D

**NEW QUESTION 265**
- (Topic 4)
Which type of scan is used on the eye to measure the layer of blood vessels?

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

**Answer:** B

**NEW QUESTION 270**
- (Topic 4)
A security administrator notices that the log file of the company`s webserver contains suspicious entries:

Based on source code analysis, the analyst concludes that the login.php script is vulnerable to

A. command injection.
B. SQL injection.
C. directory traversal.
D. LDAP injection.

**Answer:** B

**NEW QUESTION 272**
- (Topic 4)
What statement is true regarding LM hashes?

A. LM hashes consist in 48 hexadecimal characters.
B. LM hashes are based on AES128 cryptographic standard.
C. Uppercase characters in the password are converted to lowercase.
D. LM hashes are not generated when the password length exceeds 15 characters.

**Answer:** D

**NEW QUESTION 276**
- (Topic 4)
A computer technician is using a new version of a word processing software package when it is discovered that a special sequence of characters causes the entire computer to crash. The technician researches the bug and discovers that no one else experienced the problem. What is the appropriate next step?

A. Ignore the problem completely and let someone else deal with it.

B. Create a document that will crash the computer when opened and send it to friends.
C. Find an underground bulletin board and attempt to sell the bug to the highest bidder.
D. Notify the vendor of the bug and do not disclose it until the vendor gets a chance to issue a fix.

**Answer:** D

**NEW QUESTION 280**
- (Topic 4)
Which of the following is a protocol that is prone to a man-in-the-middle (MITM) attack and maps a 32-bit address to a 48-bit address?

A. ICPM
B. ARP
C. RARP
D. ICMP

**Answer:** B

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

**NEW QUESTION 281**
- (Topic 5)
Which United States legislation mandates that the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) must sign statements verifying the completeness and accuracy of financial reports?

A. Sarbanes-Oxley Act (SOX)
B. Gramm-Leach-Bliley Act (GLBA)
C. Fair and Accurate Credit Transactions Act (FACTA)
D. Federal Information Security Management Act (FISMA)

**Answer:** A

**NEW QUESTION 285**
- (Topic 5)
How can a policy help improve an employee's security awareness?

A. By implementing written security procedures, enabling employee security training, and promoting the benefits of security
B. By using informal networks of communication, establishing secret passing procedures, and immediately terminating employees
C. By sharing security secrets with employees, enabling employees to share secrets, and establishing a consultative help line
D. By decreasing an employee's vacation time, addressing ad-hoc employment clauses, and ensuring that managers know employee strengths

**Answer:** A

**NEW QUESTION 290**
- (Topic 5)
Which statement best describes a server type under an N-tier architecture?

A. A group of servers at a specific layer
B. A single server with a specific role
C. A group of servers with a unique role
D. A single server at a specific layer

**Answer:** C

**NEW QUESTION 295**
- (Topic 5)
Which of the following network attacks takes advantage of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?

A. Teardrop
B. SYN flood
C. Smurf attack
D. Ping of death

**Answer:** A

**NEW QUESTION 297**
- (Topic 5)
Which of the following cryptography attack methods is usually performed without the use of a computer?

A. Ciphertext-only attack
B. Chosen key attack
C. Rubber hose attack
D. Rainbow table attack

**Answer:** C

**NEW QUESTION 298**
- (Topic 5)
The precaution of prohibiting employees from bringing personal computing devices into a facility is what type of security control?

A. Physical
B. Procedural
C. Technical
D. Compliance

**Answer:** B

**NEW QUESTION 303**
- (Topic 5)
A penetration tester is hired to do a risk assessment of a company's DMZ. The rules of engagement states that the penetration test be done from an external IP address with no prior knowledge of the internal IT systems. What kind of test is being performed?

A. white box
B. grey box
C. red box
D. black box

**Answer:** D

**NEW QUESTION 304**
- (Topic 5)
WPA2 uses AES for wireless data encryption at which of the following encryption levels?

A. 64 bit and CCMP
B. 128 bit and CRC
C. 128 bit and CCMP
D. 128 bit and TKIP

**Answer:** C

**NEW QUESTION 306**
- (Topic 5)
The following is a sample of output from a penetration tester's machine targeting a machine with the IP address of 192.168.1.106:

What is most likely taking place?

A. Ping sweep of the 192.168.1.106 network
B. Remote service brute force attempt
C. Port scan of 192.168.1.106
D. Denial of service attack on 192.168.1.106

**Answer:** B

**NEW QUESTION 309**
- (Topic 5)
Advanced encryption standard is an algorithm used for which of the following?

A. Data integrity
B. Key discovery
C. Bulk data encryption
D. Key recovery

**Answer:** C

**NEW QUESTION 311**
- (Topic 5)
While checking the settings on the internet browser, a technician finds that the proxy server settings have been checked and a computer is trying to use itself as a proxy server. What specific octet within the subnet does the technician see?

A. 10.10.10.10
B. 127.0.0.1
C. 192.168.1.1
D. 192.168.168.168

**Answer:** B

**NEW QUESTION 314**
- (Topic 5)
Fingerprinting VPN firewalls is possible with which of the following tools?

A. Angry IP
B. Nikto
C. Ike-scan
D. Arp-scan

**Answer:** C

**NEW QUESTION 316**
- (Topic 5)
An NMAP scan of a server shows port 69 is open. What risk could this pose?

A. Unauthenticated access
B. Weak SSL version
C. Cleartext login
D. Web portal data leak

**Answer:** A

**NEW QUESTION 317**
- (Topic 5)
A Network Administrator was recently promoted to Chief Security Officer at a local university. One of employee's new responsibilities is to manage the implementation of an RFID card access system to a new server room on campus. The server room will house student enrollment information that is securely backed up to an off-site location.
During a meeting with an outside consultant, the Chief Security Officer explains that he is concerned that the existing security controls have not been designed properly. Currently, the Network Administrator is responsible for approving and issuing RFID card access to the server room, as well as reviewing the electronic access logs on a weekly basis.
Which of the following is an issue with the situation?

A. Segregation of duties
B. Undue influence
C. Lack of experience
D. Inadequate disaster recovery plan

**Answer:** A

**NEW QUESTION 322**
- (Topic 5)
Which of the following network attacks relies on sending an abnormally large packet size that exceeds TCP/IP specifications?

A. Ping of death
B. SYN flooding
C. TCP hijacking
D. Smurf attack

**Answer:** A

**NEW QUESTION 324**
- (Topic 5)
Which of the following programming languages is most vulnerable to buffer overflow attacks?

A. Perl
B. C++
C. Python
D. Java

**Answer:** B

**NEW QUESTION 325**
- (Topic 5)
What are the three types of compliance that the Open Source Security Testing Methodology Manual (OSSTMM) recognizes?

A. Legal, performance, audit
B. Audit, standards based, regulatory
C. Contractual, regulatory, industry
D. Legislative, contractual, standards based

**Answer:** D

**NEW QUESTION 327**
- (Topic 5)
A security engineer has been asked to deploy a secure remote access solution that will allow employees to connect to the company’s internal network. Which of the following can be implemented to minimize the opportunity for the man-in-the-middle attack to occur?

A. SSL
B. Mutual authentication
C. IPSec
D. Static IP addresses

**Answer:** C

**NEW QUESTION 329**
- (Topic 5)
During a penetration test, a tester finds that the web application being analyzed is vulnerable to Cross Site Scripting (XSS). Which of the following conditions must be met to exploit this vulnerability?

A. The web application does not have the secure flag set.
B. The session cookies do not have the HttpOnly flag set.
C. The victim user should not have an endpoint security solution.
D. The victim's browser must have ActiveX technology enabled.

**Answer:** B

**NEW QUESTION 331**
- (Topic 5)
Which technical characteristic do Ethereal/Wireshark, TCPDump, and Snort have in common?

A. They are written in Java.
B. They send alerts to security monitors.
C. They use the same packet analysis engine.
D. They use the same packet capture utility.

**Answer:** D

**NEW QUESTION 335**
- (Topic 5)
What information should an IT system analysis provide to the risk assessor?

A. Management buy-in
B. Threat statement
C. Security architecture
D. Impact analysis

**Answer:** C

**NEW QUESTION 340**
- (Topic 5)
A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?

A. The gateway is not routing to a public IP address.
B. The computer is using an invalid IP address.
C. The gateway and the computer are not on the same network.
D. The computer is not using a private IP address.

**Answer:** A

**NEW QUESTION 345**
- (Topic 5)
Which of the following levels of algorithms does Public Key Infrastructure (PKI) use?

A. RSA 1024 bit strength
B. AES 1024 bit strength
C. RSA 512 bit strength
D. AES 512 bit strength

**Answer:** A

**NEW QUESTION 350**
- (Topic 5)
What technique is used to perform a Connection Stream Parameter Pollution (CSPP) attack?

A. Injecting parameters into a connection string using semicolons as a separator
B. Inserting malicious Javascript code into input parameters
C. Setting a user's session identifier (SID) to an explicit known value
D. Adding multiple parameters with the same name in HTTP requests

**Answer:** A

**NEW QUESTION 353**
- (Topic 5)
A hacker is attempting to see which ports have been left open on a network. Which NMAP switch would the hacker use?

A. -sO
B. -sP
C. -sS
D. -sU

**Answer:** A

**NEW QUESTION 358**
- (Topic 5)
A certified ethical hacker (CEH) is approached by a friend who believes her husband is cheating. She offers to pay to break into her husband's email account in order to find proof so she can take him to court. What is the ethical response?

A. Say no; the friend is not the owner of the account.
B. Say yes; the friend needs help to gather evidence.
C. Say yes; do the job for free.
D. Say no; make sure that the friend knows the risk she’s asking the CEH to take.

**Answer:** A

**NEW QUESTION 360**
- (Topic 5)
From the two screenshots below, which of the following is occurring?

A. 10.0.0.253 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.
B. 10.0.0.253 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2.
C. 10.0.0.2 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.
D. 10.0.0.252 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2.

**Answer:** A

**NEW QUESTION 364**
- (Topic 5)
A pentester is using Metasploit to exploit an FTP server and pivot to a LAN. How will the pentester pivot using Metasploit?

A. Issue the pivot exploit and set the meterpreter.
B. Reconfigure the network settings in the meterpreter.
C. Set the payload to propagate through the meterpreter.
D. Create a route statement in the meterpreter.

**Answer:** D

**NEW QUESTION 368**
- (Topic 6)
What is the following command used for? net use \targetipc$ "" /u:""

A. Grabbing the etc/passwd file
B. Grabbing the SAM
C. Connecting to a Linux computer through Samba.
D. This command is used to connect as a null session
E. Enumeration of Cisco routers

**Answer:** D

**Explanation:**
The null session is one of the most debilitating vulnerabilities faced by Windows. Null sessions can be established through port 135, 139, and 445.

**NEW QUESTION 371**
- (Topic 6)
What flags are set in a X-MAS scan?(Choose all that apply.

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

**Answer:** CDF

**Explanation:**
FIN, URG, and PSH are set high in the TCP packet for a X-MAS scan

**NEW QUESTION 376**
- (Topic 6)
What are the two basic types of attacks? (Choose two.

A. DoS
B. Passive
C. Sniffing
D. Active
E. Cracking

**Answer:** BD

**Explanation:**
Passive and active attacks are the two basic types of attacks.

**NEW QUESTION 380**
- (Topic 6)
According to the CEH methodology, what is the next step to be performed after footprinting?

A. Enumeration
B. Scanning
C. System Hacking
D. Social Engineering
E. Expanding Influence

**Answer:** B

**Explanation:**
Once footprinting has been completed, scanning should be attempted next. Scanning should take place on two distinct levels: network and host.

**NEW QUESTION 385**
- (Topic 6)
The use of alert thresholding in an IDS can reduce the volume of repeated alerts, but introduces which of the following vulnerabilities?

A. An attacker, working slowly enough, can evade detection by the IDS.
B. Network packets are dropped if the volume exceeds the threshold.
C. Thresholding interferes with the IDS' ability to reassemble fragmented packets.
D. The IDS will not distinguish among packets originating from different sources.

**Answer:** A

**NEW QUESTION 387**
- (Topic 6)
Why would an attacker want to perform a scan on port 137?

A. To discover proxy servers on a network
B. To disrupt the NetBIOS SMB service on the target host
C. To check for file and print sharing on Windows systems
D. To discover information about a target host using NBTSTAT

**Answer:** D

**Explanation:**
Microsoft encapsulates netbios information within TCP/Ip using ports 135- 139.It is trivial for an attacker to issue the following command:
nbtstat -A (your Ip address)
From their windows machine and collect information about your windows machine (if you
are not blocking traffic to port 137 at your borders).

**NEW QUESTION 390**
- (Topic 6)
Which of the following systems would not respond correctly to an nmap XMAS scan?

A. Windows 2000 Server running IIS 5
B. Any Solaris version running SAMBA Server
C. Any version of IRIX
D. RedHat Linux 8.0 running Apache Web Server

**Answer:** A

**Explanation:**
When running a XMAS Scan, if a RST packet is received, the port is considered closed, while no response means it is open|filtered. The big downside is that not all systems follow RFC 793 to the letter. A number of systems send RST responses to the probes regardless of whether the port is open or not. This causes all of the ports to be labeled closed. Major operating systems that do this are Microsoft Windows, many Cisco devices, BSDI, and IBM OS/400.

**NEW QUESTION 395**
- (Topic 6)
What ICMP message types are used by the ping command?

A. Timestamp request (13) and timestamp reply (14)
B. Echo request (8) and Echo reply (0)
C. Echo request (0) and Echo reply (1)

D. Ping request (1) and Ping reply (2)

**Answer:** B

**Explanation:**
ICMP Type 0 = Echo Reply, ICMP Type 8 = Echo

**NEW QUESTION 397**
- (Topic 6)
Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security-related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position. Harold is currently trying to run a Sniffer on the agency's network to get an idea of what kind of traffic is being passed around, but the program he is using does not seem to be capturing anything. He pours through the Sniffer's manual, but cannot find anything that directly relates to his problem. Harold decides to ask the network administrator if he has any thoughts on the problem. Harold is told that the Sniffer was not working because the agency's network is a switched network, which cannot be sniffed by some programs without some tweaking. What technique could Harold use to sniff his agency's switched network?

A. ARP spoof the default gateway
B. Conduct MiTM against the switch
C. Launch smurf attack against the switch
D. Flood the switch with ICMP packets

**Answer:** A

**NEW QUESTION 398**
- (Topic 6)
Neil notices that a single address is generating traffic from its port 500 to port 500 of several other machines on the network. This scan is eating up most of the network bandwidth and Neil is concerned. As a security professional, what would you infer from this scan?

A. It is a network fault and the originating machine is in a network loop
B. It is a worm that is malfunctioning or hardcoded to scan on port 500
C. The attacker is trying to detect machines on the network which have SSL enabled
D. The attacker is trying to determine the type of VPN implementation and checking for IPSec

**Answer:** D

**Explanation:**
Port 500 is used by IKE (Internet Key Exchange). This is typically used for IPSEC-based VPN software, such as Freeswan, PGPnet, and various vendors of in-a-box VPN solutions such as Cisco. IKE is used to set up the session keys. The actual session is usually sent with ESP (Encapsulated Security Payload) packets, IP protocol 50 (but some in-a-box VPN's such as Cisco are capable of negotiating to send the encrypted tunnel over a UDP channel, which is useful for use across firewalls that block IP protocols other than TCP or UDP).

**NEW QUESTION 399**
- (Topic 6)
One of your team members has asked you to analyze the following SOA record. What is the TTL?
Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600
3600 604800 2400.

A. 200303028
B. 3600
C. 604800
D. 2400
E. 60
F. 4800

**Answer:** D

**Explanation:**
The SOA includes a timeout value. This value can tell an attacker how long any DNS "poisoning" would last. It is the last set of numbers in the record.

**NEW QUESTION 403**
- (Topic 6)
Which of the following commands runs snort in packet logger mode?

A. ./snort -dev -h ./log
B. ./snort -dev -l ./log
C. ./snort -dev -o ./log
D. ./snort -dev -p ./log

**Answer:** B

**Explanation:**
Note: If you want to store the packages in binary mode for later analysis use
./snort -l ./log -b

**NEW QUESTION 408**
- (Topic 6)

_____ is found in all versions of NTFS and is described as the ability to fork file data into existing files without affecting their functionality, size, or display to traditional file browsing utilities like dir or Windows Explorer

A. Alternate Data Streams
B. Merge Streams
C. Steganography
D. NetBIOS vulnerability

**Answer:** A

**NEW QUESTION 411**
- (Topic 6)
What does a type 3 code 13 represent?(Choose two.

A. Echo request
B. Destination unreachable
C. Network unreachable
D. Administratively prohibited
E. Port unreachable
F. Time exceeded

**Answer:** BD

**Explanation:**
Type 3 code 13 is destination unreachable administratively prohibited. This type of message is typically returned from a device blocking a port.

**NEW QUESTION 413**
- (Topic 6)
Which of the following activities will NOT be considered as passive footprinting?

A. Go through the rubbish to find out any information that might have been discarded.
B. Search on financial site such as Yahoo Financial to identify assets.
C. Scan the range of IP address found in the target DNS database.
D. Perform multiples queries using a search engine.

**Answer:** C

**Explanation:**
Passive footprinting is a method in which the attacker never makes contact with the target systems. Scanning the range of IP addresses found in the target DNS is considered making contact to the systems behind the IP addresses that is targeted by the scan.

**NEW QUESTION 417**
- (Topic 6)
You receive an email with the following message: Hello Steve,
We are having technical difficulty in restoring user database record after the recent blackout. Your account data is corrupted. Please logon to the SuperEmailServices.com and change your password.
http://www.supermailservices.com@0xde.0xad.0xbe.0xef/support/logon.htm
If you do not reset your password within 7 days, your account will be permanently disabled locking you out from our e-mail services.
Sincerely, Technical Support
SuperEmailServices
From this e-mail you suspect that this message was sent by some hacker since you have been using their e-mail services for the last 2 years and they have never sent out an e-mail such as this. You also observe the URL in the message and confirm your suspicion about 0xde.0xad.0xbde.0xef which looks like hexadecimal numbers. You immediately enter the following at Windows 2000 command prompt:
Ping 0xde.0xad.0xbe.0xef
You get a response with a valid IP address.
What is the obstructed IP address in the e-mail URL?

A. 222.173.190.239
B. 233.34.45.64
C. 54.23.56.55
D. 199.223.23.45

**Answer:** A

**Explanation:**
0x stands for hexadecimal and DE=222, AD=173, BE=190 and EF=239

**NEW QUESTION 420**
- (Topic 6)
An nmap command that includes the host specification of 202.176.56-57.* will scan
_____ number of hosts.

A. 2
B. 256
C. 512
D. Over 10, 000

**Answer:** C

**Explanation:**
The hosts with IP address 202.176.56.0-255 & 202.176.56.0-255 will be scanned (256+256=512)

**NEW QUESTION 422**
- (Topic 6)
What are two things that are possible when scanning UDP ports? (Choose two.

A. A reset will be returned
B. An ICMP message will be returned
C. The four-way handshake will not be completed
D. An RFC 1294 message will be returned
E. Nothing

**Answer:** BE

**Explanation:**
Closed UDP ports can return an ICMP type 3 code 3 message. No response can mean the port is open or the packet was silently dropped.

**NEW QUESTION 426**
- (Topic 6)
Exhibit

(Note: the student is being tested on concepts learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.)
Snort has been used to capture packets on the network. On studying the packets, the penetration tester finds it to be abnormal. If you were the penetration tester, why would you find this abnormal?
What is odd about this attack? Choose the best answer.

A. This is not a spoofed packet as the IP stack has increasing numbers for the three flags.
B. This is back orifice activity as the scan comes form port 31337.
C. The attacker wants to avoid creating a sub-carries connection that is not normally valid.
D. These packets were crafted by a tool, they were not created by a standard IP stack.

**Answer:** B

**Explanation:**
Port 31337 is normally used by Back Orifice. Note that 31337 is hackers spelling of ‘elite’, meaning ‘elite hackers’.

**NEW QUESTION 427**
- (Topic 6)
A person approaches a network administrator and wants advice on how to send encrypted email from home. The end user does not want to have to pay for any license fees or manage server services. Which of the following is the most secure encryption protocol that the network administrator should recommend?

A. IP Security (IPSEC)
B. Multipurpose Internet Mail Extensions (MIME)
C. Pretty Good Privacy (PGP)
D. Hyper Text Transfer Protocol with Secure Socket Layer (HTTPS)

**Answer:** C

**NEW QUESTION 429**
- (Topic 6)
Peter extracts the SIDs list from Windows 2000 Server machine using the hacking tool “SIDExtractor”. Here is the output of the SIDs:

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

**Explanation:**
The SID of the built-in administrator will always follow this example: S-1-5- domain-500

**NEW QUESTION 431**
- (Topic 6)
What is the proper response for a X-MAS scan if the port is closed?

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

F. No response

**Answer:** E

**Explanation:**
Closed ports respond to a X-MAS scan with a RST.

**NEW QUESTION 435**
- (Topic 7)
Which of the following is not considered to be a part of active sniffing?

A. MAC Flooding
B. ARP Spoofing
C. SMAC Fueling
D. MAC Duplicating

**Answer:** C

**NEW QUESTION 439**
- (Topic 7)
What is the proper response for a NULL scan if the port is open?

A. SYN
B. ACK
C. FIN
D. PSH
E. RST
F. No response

**Answer:** F

**Explanation:**
A NULL scan will have no response if the port is open.

**NEW QUESTION 440**
- (Topic 7)
Jason's Web server was attacked by a trojan virus. He runs protocol analyzer and notices that the trojan communicates to a remote server on the Internet. Shown below is the standard "hexdump" representation of the network packet, before being decoded. Jason wants to identify the trojan by looking at the destination port number and mapping to a trojan-port number database on the Internet. Identify the remote server's port number by decoding the packet?

A. Port 1890 (Net-Devil Trojan)
B. Port 1786 (Net-Devil Trojan)
C. Port 1909 (Net-Devil Trojan)
D. Port 6667 (Net-Devil Trojan)

**Answer:** D

**Explanation:**
From trace, 0x1A0B is 6667, IRC Relay Chat, which is one port used. Other ports are in the 900's.

**NEW QUESTION 445**
- (Topic 7)
Samantha was hired to perform an internal security test of XYZ. She quickly realized that all networks are making use of switches instead of traditional hubs. This greatly limits her ability to gather information through network sniffing.
Which of the following techniques can she use to gather information from the switched network or to disable some of the traffic isolation features of the switch? (Choose two)

A. Ethernet Zapping
B. MAC Flooding
C. Sniffing in promiscuous mode
D. ARP Spoofing

**Answer:** BD

**Explanation:**
In a typical MAC flooding attack, a switch is flooded with packets, each containing different source MAC addresses. The intention is to consume the limited memory set aside in the switch to store the MAC address-to-physical port translation table.The result of this attack causes the switch to enter a state called failopen mode, in which all incoming packets are broadcast out on all ports (as with a hub), instead of just down the correct port as per normal operation. The principle of ARP spoofing is to send
fake, or 'spoofed', ARP messages to an Ethernet LAN. These frames contain false MAC addresses, confusing network devices, such as network switches. As a result frames intended for one machine can be mistakenly sent to another (allowing the packets to be sniffed) or an unreachable host (a denial of service attack).

**NEW QUESTION 448**
- (Topic 7)
ARP poisoning is achieved in steps

A. 1

B. 2
C. 3
D. 4

**Answer:** B

**Explanation:**
The hacker begins by sending a malicious ARP "reply" (for which there was no previous request) to your router, associating his computer's MAC address with your IP Address. Now your router thinks the hacker's computer is your computer. Next, the hacker sends a malicious ARP reply to your computer, associating his MAC Address with the routers IP Address. Now your machine thinks the hacker's computer is your router. The hacker has now used ARP poisoning to accomplish a MitM attack.

**NEW QUESTION 450**
- (Topic 7)
How would you describe a simple yet very effective mechanism for sending and receiving unauthorized information or data between machines without alerting any firewalls and IDS's on a network?

A. Covert Channel
B. Crafted Channel
C. Bounce Channel
D. Deceptive Channel

**Answer:** A

**Explanation:**
A covert channel is described as: "any communication channel that can be exploited by a process to transfer information in a manner that violates the systems security policy." Essentially, it is a method of communication that is not part of an actual computer system design, but can be used to transfer information to users or system processes that normally would not be allowed access to the information.

**NEW QUESTION 455**
- (Topic 7)
Which of the following Netcat commands would be used to perform a UDP scan of the lower 1024 ports?

A. Netcat -h -U
B. Netcat -hU <host(s.>
C. Netcat -sU -p 1-1024 <host(s.>
D. Netcat -u -v -w2 <host> 1-1024
E. Netcat -sS -O target/1024

**Answer:** D

**Explanation:**
The proper syntax for a UDP scan using Netcat is "Netcat -u -v -w2 <host> 1-1024". Netcat is considered the Swiss-army knife of hacking tools because it is so versatile.

**NEW QUESTION 457**
- (Topic 7)
Exhibit:

The following is an entry captured by a network IDS.You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You figure that the attacker is attempting a buffer overflow attack. You also notice "/bin/sh" in the ASCII part of the output. As an analyst what would you conclude about the attack?

A. The buffer overflow attack has been neutralized by the IDS
B. The attacker is creating a directory on the compromised machine
C. The attacker is attempting a buffer overflow attack and has succeeded
D. The attacker is attempting an exploit that launches a command-line shell

**Answer:** D

**Explanation:**
This log entry shows a hacker using a buffer overflow to fill the data buffer and trying to insert the execution of /bin/sh into the executable code part of the thread. It is probably an existing exploit that is used, or a directed attack with a custom built buffer overflow with the “payload” that launches the command shell.

**NEW QUESTION 461**
- (Topic 7)
This kind of password cracking method uses word lists in combination with numbers and special characters:

A. Hybrid
B. Linear
C. Symmetric
D. Brute Force

**Answer:** A

**Explanation:**
A Hybrid (or Hybrid Dictionary) Attack uses a word list that it modifies slightly to find passwords that are almost from a dictionary (like St0pid)

**NEW QUESTION 464**
- (Topic 7)
Which DNS resource record can indicate how long any "DNS poisoning" could last?

A. MX
B. SOA
C. NS
D. TIMEOUT

**Answer:** B

**Explanation:**
The SOA contains information of secondary servers, update intervals and expiration times.

**NEW QUESTION 469**
- (Topic 7)
Why would you consider sending an email to an address that you know does not exist within the company you are performing a Penetration Test for?

A. To determine who is the holder of the root account
B. To perform a DoS
C. To create needless SPAM
D. To illicit a response back that will reveal information about email servers and how they treat undeliverable mail
E. To test for virus protection

**Answer:** D

**Explanation:**
Sending a bogus email is one way to find out more about internal servers. Also, to gather additional IP addresses and learn how they treat mail.

**NEW QUESTION 473**
- (Topic 7)
Exhibit:

Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?

A. har.txt
B. SAM file
C. wwwroot
D. Repair file

**Answer:** B

**Explanation:**
He is actually trying to get the file har.txt but this file contains a copy of the SAM file.

**NEW QUESTION 474**
- (Topic 7)
Null sessions are un-authenticated connections (not using a username or password.) to an NT or 2000 system. Which TCP and UDP ports must you filter to check null sessions on your network?

A. 137 and 139
B. 137 and 443
C. 139 and 443
D. 139 and 445

**Answer:** D

**Explanation:**
NULL sessions take advantage of “features” in the SMB (Server Message Block) protocol that exist primarily for trust relationships. You can establish a NULL session with a Windows host by logging on with a NULL user name and password. Primarily the following ports are vulnerable if they are accessible:

C:\Documents and Settings\user-nwz\Desktop\1.JPG

**NEW QUESTION 479**
- (Topic 7)
Tess King, the evil hacker, is purposely sending fragmented ICMP packets to a remote target. The total size of this ICMP packet once reconstructed is over 65, 536 bytes. From the information given, what type of attack is Tess King attempting to perform?

A. Syn flood
B. Smurf
C. Ping of death
D. Fraggle

**Answer:** C

**Explanation:**
Reference: http://insecure.org/sploits/ping-o-death.html

**NEW QUESTION 483**
- (Topic 7)
After an attacker has successfully compromised a remote computer, what would be one of the last steps that would be taken to ensure that the compromise is not traced back to the source of the problem?

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

**Answer:** C

**Explanation:**
As a hacker you don't want to leave any traces that could lead back to you.

**NEW QUESTION 485**
- (Topic 7)
What happens during a SYN flood attack?

A. TCP connection requests floods a target machine is flooded with randomized source address & ports for the TCP ports.
B. A TCP SYN packet, which is a connection initiation, is sent to a target machine, giving the target host's address as both source and destination, and is using the same port on the target host as both source and destination.
C. A TCP packet is received with the FIN bit set but with no ACK bit set in the flags field.
D. A TCP packet is received with both the SYN and the FIN bits set in the flags field.

**Answer:** A

**NEW QUESTION 488**
- (Topic 7)
Fingerprinting an Operating System helps a cracker because:

A. It defines exactly what software you have installed
B. It opens a security-delayed window based on the port being scanned
C. It doesn't depend on the patches that have been applied to fix existing security holes
D. It informs the cracker of which vulnerabilities he may be able to exploit on your system

**Answer:** D

**Explanation:**
When a cracker knows what OS and Services you use he also knows which exploits might work on your system. If he would have to try all possible exploits for all possible Operating Systems and Services it would take too long time and the possibility of being detected increases.

**NEW QUESTION 493**
- (Topic 7)
Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform SNMP enquires over the network. Which of these tools would do the SNMP enumeration he is looking for?
Select the best answers.

A. SNMPUtil
B. SNScan
C. SNMPScan
D. Solarwinds IP Network Browser
E. NMap

**Answer:** ABD

**Explanation:**
Explanations:
SNMPUtil is a SNMP enumeration utility that is a part of the Windows 2000 resource kit. With SNMPUtil, you can retrieve all sort of valuable information through SNMP. SNScan is a SNMP network scanner by Foundstone. It does SNMP scanning to find open SNMP ports. Solarwinds IP Network Browser is a SNMP enumeration tool with a graphical tree- view of the remote machine's SNMP data.

**NEW QUESTION 496**
- (Topic 7)
Exhibit:

You have captured some packets in Ethereal. You want to view only packets sent from 10.0.0.22. What filter will you apply?

A. ip = 10.0.0.22
B. ip.src == 10.0.0.22
C. ip.equals 10.0.0.22
D. ip.address = 10.0.0.22

**Answer:** B

**Explanation:**
ip.src tells the filter to only show packets with 10.0.0.22 as the source.

**NEW QUESTION 499**
- (Topic 7)
What hacking attack is challenge/response authentication used to prevent?

A. Replay attacks
B. Scanning attacks
C. Session hijacking attacks
D. Password cracking attacks

**Answer:** A

**Explanation:**
A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it. With a challenge/response authentication you ensure that captured packets can't be retransmitted without a new authentication.

**NEW QUESTION 503**
- (Topic 7)
Which of the following are well know password-cracking programs?(Choose all that apply.

A. L0phtcrack
B. NetCat
C. Jack the Ripper
D. Netbus
E. John the Ripper

**Answer:** AE

**Explanation:**
L0phtcrack and John the Ripper are two well know password-cracking programs. Netcat is considered the Swiss-army knife of hacking tools, but is not used for password cracking

**NEW QUESTION 504**
- (Topic 7)
What is a Trojan Horse?

A. A malicious program that captures your username and password
B. Malicious code masquerading as or replacing legitimate code
C. An unauthorized user who gains access to your user database and adds themselves as a user
D. A server that is to be sacrificed to all hacking attempts in order to log and monitor the hacking activity

**Answer:** B

**Explanation:**
A Trojan Horse is an apparently useful and innocent program containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data.

**NEW QUESTION 507**
- (Topic 8)
Bill has successfully executed a buffer overflow against a Windows IIS web server. He has been able to spawn an interactive shell and plans to deface the main web page. He first attempts to use the "Echo" command to simply overwrite index.html and remains unsuccessful. He then attempts to delete the page and achieves no progress. Finally, he tries to overwrite it with another page again in vain.
What is the probable cause of Bill's problem?

A. The system is a honeypot.
B. There is a problem with the shell and he needs to run the attack again.
C. You cannot use a buffer overflow to deface a web page.
D. The HTML file has permissions of ready only.

**Answer:** D

**Explanation:**
The question states that Bill had been able to spawn an interactive shell.By this statement we can tell that the buffer overflow and its corresponding code was enough to spawn a shell. Any shell should make it possible to change the webpage.So we either don't have sufficient privilege to change the webpage (answer D) or it's a honeypot (answer A). We think the preferred answer is D

**NEW QUESTION 512**
- (Topic 8)
Rebecca is a security analyst and knows of a local root exploit that has the ability to enable local users to use available exploits to gain root privileges. This vulnerability exploits a condition in the Linux kernel within the execve() system call. There is no known workaround that exists for this vulnerability. What is the correct action to be taken by Rebecca in this situation as a recommendation to management?

A. Rebecca should make a recommendation to disable the () system call
B. Rebecca should make a recommendation to upgrade the Linux kernel promptly
C. Rebecca should make a recommendation to set all child-process to sleep within the execve()
D. Rebecca should make a recommendation to hire more system administrators to monitor all child processes to ensure that each child process can't elevate privilege

**Answer:** B

**NEW QUESTION 514**
- (Topic 8)
ETHER: Destination address : 0000BA5EBA11 ETHER: Source address :

An employee wants to defeat detection by a network-based IDS application. He does not want to attack the system containing the IDS application. Which of the following strategies can be used to defeat detection by a network-based IDS application?

A. Create a SYN flood
B. Create a network tunnel
C. Create multiple false positives
D. Create a ping flood

**Answer:** B

**Explanation:**
Certain types of encryption presents challenges to network-based intrusion detection and may leave the IDS blind to certain attacks, where a host-based IDS analyzes the data after it has been decrypted.

**NEW QUESTION 517**
- (Topic 8)
Exhibit

Study the log given in the exhibit,
Precautionary measures to prevent this attack would include writing firewall rules. Of these firewall rules, which among the following would be appropriate?

A. Disallow UDP 53 in from outside to DNS server
B. Allow UDP 53 in from DNS server to outside
C. Disallow TCP 53 in form secondaries or ISP server to DNS server
D. Block all UDP traffic

**Answer:** B

**Explanation:**
You only want your or your ISP's outside DNS to be able to contact your inside DNS. All other traffic should be directed against the outside DNS.

**NEW QUESTION 518**
- (Topic 8)
When working with Windows systems, what is the RID of the true administrator account?

A. 500
B. 501
C. 1000
D. 1001
E. 1024
F. 512

**Answer:** A

**Explanation:**
Because of the way in which Windows functions, the true administrator account always has a RID of 500.

**NEW QUESTION 523**
- (Topic 8)
Symmetric encryption algorithms are known to be fast but present great challenges on the key management side. Asymmetric encryption algorithms are slow but allow communication with a remote host without having to transfer a key out of band or in person. If we combine the strength of both crypto systems where we use the symmetric algorithm to encrypt the bulk of the data and then use the asymmetric encryption system to encrypt the symmetric key, what would this type of usage be known as?

A. Symmetric system
B. Combined system
C. Hybrid system
D. Asymmetric system

**Answer:** C

**Explanation:**
Because of the complexity of the underlying problems, most public-key algorithms involve operations such as modular multiplication and exponentiation, which are much more computationally expensive than the techniques used in most block ciphers, especially with typical key sizes. As a result, public-key cryptosystems are

commonly "hybrid" systems, in which a fast symmetric-key encryption algorithm is used for the message itself, while the relevant symmetric key is sent with the message, but encrypted using a public-key algorithm. Similarly, hybrid signature schemes are often used, in which a cryptographic hash function is computed, and only the resulting hash is digitally signed.

**NEW QUESTION 527**
- (Topic 8)
If you send a SYN to an open port, what is the correct response?(Choose all correct answers.

A. SYN
B. ACK
C. FIN
D. PSH

**Answer:** AB

**Explanation:**
The proper response is a SYN / ACK. This technique is also known as half- open scanning.

**NEW QUESTION 531**
- (Topic 8)
Once an intruder has gained access to a remote system with a valid username and password, the attacker will attempt to increase his privileges by escalating the used account to one that has increased privileges. such as that of an administrator. What would be the best countermeasure to protect against escalation of priveges?

A. Give users tokens
B. Give user the least amount of privileges
C. Give users two passwords
D. Give users a strong policy document

**Answer:** B

**Explanation:**
With less privileges it is harder to increase the privileges.

**NEW QUESTION 534**
- (Topic 8)
Which is the right sequence of packets sent during the initial TCP three way handshake?

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

**Answer:** D

**Explanation:**
A TCP connection always starts with a request for synchronization, a SYN, the reply to that would be another SYN together with a ACK to acknowledge that the last package was delivered successfully and the last part of the three way handshake should be only an ACK to acknowledge that the SYN reply was recived.

**NEW QUESTION 535**
- (Topic 8)
An employee wants to defeat detection by a network-based IDS application. He does not want to attack the system containing the IDS application.
Which of the following strategies can be used to defeat detection by a network-based IDS application? (Choose the best answer)

A. Create a network tunnel.
B. Create a multiple false positives.
C. Create a SYN flood.
D. Create a ping flood.

**Answer:** A

**Explanation:**
Certain types of encryption presents challenges to network-based intrusion detection and may leave the IDS blind to certain attacks, where a host-based IDS analyzes the data after it has been decrypted.

**NEW QUESTION 536**
- (Topic 8)
Which of the following snort rules look for FTP root login attempts?

A. alert tcp -> any port 21 (msg:"user root";)
B. alert tcp -> any port 21 (message:"user root";)
C. alert ftp -> ftp (content:"user password root";)
D. alert tcp any any -> any any 21 (content:"user root";)

**Answer:** D

**Explanation:**
The snort rule header is built by defining action (alert), protocol (tcp), from IP subnet port (any any), to IP subnet port (any any 21), Payload Detection Rule Options (content:"user root";)

**NEW QUESTION 538**
- (Topic 8)
Which of the following is one of the key features found in a worm but not seen in a virus?

A. The payload is very small, usually below 800 bytes.
B. It is self replicating without need for user intervention.
C. It does not have the ability to propagate on its own.
D. All of them cannot be detected by virus scanners.

**Answer:** B

**Explanation:**
A worm is similar to a virus by its design, and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any help from a person. A worm takes advantage of file or information transport features on your system, which allows it to travel unaided.

**NEW QUESTION 540**
- (Topic 8)
Say that "abigcompany.com" had a security vulnerability in the javascript on their website in the past. They recently fixed the security vulnerability, but it had been there for many months. Is there some way to 4go back and see the code for that error?
Select the best answer.

A. archive.org
B. There is no way to get the changed webpage unless you contact someone at the company
C. Usenet
D. Javascript would not be in their html so a service like usenet or archive wouldn't help you

**Answer:** A

**Explanation:**
Explanations:
Archive.org is a website that periodically archives internet content. They have archives of websites over many years. It could be used to go back and look at the javascript as javascript would be in the HTML code.

**NEW QUESTION 544**
- (Topic 8)
You have performed the traceroute below and notice that hops 19 and 20 both show the same IP address.
What can be inferred from this output?

A. An application proxy firewall
B. A stateful inspection firewall
C. A host based IDS
D. A Honeypot

**Answer:** B

**NEW QUESTION 545**
- (Topic 8)
What is Form Scalpel used for?

A. Dissecting HTML Forms
B. Dissecting SQL Forms
C. Analysis of Access Database Forms
D. Troubleshooting Netscape Navigator
E. Quatro Pro Analysis Tool

**Answer:** A

**Explanation:**
Form Scalpel automatically extracts forms from a given web page and splits up all fields for editing and manipulation.

**NEW QUESTION 546**
- (Topic 8)
What is a sheepdip?

A. It is another name for Honeynet
B. It is a machine used to coordinate honeynets
C. It is the process of checking physical media for virus before they are used in a computer
D. None of the above

**Answer:** C

**Explanation:**
Also known as a footbath, a sheepdip is the process of checking physical media, such as floppy disks or CD-ROMs, for viruses before they are used in a computer. Typically, a computer that sheepdips is used only for that process and nothing else and is isolated from the other computers, meaning it is not connected to the network. Most sheepdips use at least two different antivirus programs in order to increase effectiveness.

**NEW QUESTION 548**
- (Topic 8)
Clive is conducting a pen-test and has just port scanned a system on the network. He has identified the operating system as Linux and been able to elicit responses from ports 23, 25 and 53. He infers port 23 as running Telnet service, port 25 as running SMTP service and port 53 as running DNS service. The client confirms these findings and attests to the current availability of the services. When he tries to telnet to port 23 or 25, he gets a blank screen in response. On typing other commands, he sees only blank spaces or underscores symbols on the screen. What are you most likely to infer from this?

A. The services are protected by TCP wrappers
B. There is a honeypot running on the scanned machine
C. An attacker has replaced the services with trojaned ones
D. This indicates that the telnet and SMTP server have crashed

**Answer:** A

**Explanation:**
TCP Wrapper is a host-based network ACL system, used to filter network access to Internet protocol services run on (Unix-like) operating systems such as Linux or
BSD. It allows host or subnetwork IP addresses, names and/or ident query replies, to be used as tokens on which to filter for access control purposes.

**NEW QUESTION 549**
- (Topic 8)
On a default installation of Microsoft IIS web server, under which privilege does the web server software execute?

A. Everyone
B. Guest
C. System
D. Administrator

**Answer:** C

**Explanation:**
If not changed during the installation, IIS will execute as Local System with way to high privileges.

**NEW QUESTION 552**
- (Topic 8)
After studying the following log entries, how many user IDs can you identify that the attacker has tampered with?
1. mkdir -p /etc/X11/applnk/Internet/.etc
2. mkdir -p /etc/X11/applnk/Internet/.etcpasswd
3. touch -acmr /etc/passwd /etc/X11/applnk/Internet/.etcpasswd
4. touch -acmr /etc /etc/X11/applnk/Internet/.etc
5. passwd nobody -d
6. /usr/sbin/adduser dns -d/bin -u 0 -g 0 -s/bin/bash
7. passwd dns -d
1. 8. touch -acmr /etc/X11/applnk/Internet/.etcpasswd /etc/passwd

9. touch -acmr /etc/X11/applnk/Internet/.etc /etc

A. IUSR_
B. acmr, dns
C. nobody, dns
D. nobody, IUSR_

**Answer:** C

**Explanation:**
Passwd is the command used to modify a user password and it has been used together with the usernames nobody and dns.

**NEW QUESTION 554**
- (Topic 8)
When working with Windows systems, what is the RID of the true administrator account?

A. 500
B. 501
C. 512
D. 1001
E. 1024
F. 1000

**Answer:** A

**Explanation:**
The built-in administrator account always has a RID of 500.

**NEW QUESTION 555**
- (Topic 8)
You have just received an assignment for an assessment at a company site. Company's management is concerned about external threat and wants to take appropriate steps to insure security is in place. Anyway the management is also worried about possible threats coming from inside the site, specifically from employees belonging to different Departments. What kind of assessment will you be performing ?

A. Black box testing
B. Black hat testing
C. Gray box testing
D. Gray hat testing
E. White box testing
F. White hat testing

**Answer:** C

**Explanation:**
Internal Testing is also referred to as Gray-box testing.

**NEW QUESTION 557**
- (Topic 8)
What type of cookies can be generated while visiting different web sites on the Internet?

A. Permanent and long term cookies.
B. Session and permanent cookies.
C. Session and external cookies.
D. Cookies are all the same, there is no such thing as different type of cookies.

**Answer:** B

**Explanation:**
There are two types of cookies: a permanent cookie that remains on a visitor's computer for a given time and a session cookie the is temporarily saved in the visitor's computer memory during the time that the visitor is using the Web site. Session cookies disappear when you close your Web browser.

**NEW QUESTION 562**
- (Topic 8)
Why would an ethical hacker use the technique of firewalking?

A. It is a technique used to discover wireless network on foot.
B. It is a technique used to map routers on a network link.
C. It is a technique used to discover the nature of rules configured on a gateway.
D. It is a technique used to discover interfaces in promiscuous mode.

**Answer:** C

**Explanation:**
Firewalking uses a traceroute-like IP packet analysis to determine whether or not a particular packet can pass from the attacker’s host to a destination host through a packet-filtering device. This technique can be used to map ‘open’ or ‘pass through’ ports on a gateway. More over, it can determine whether packets with various control information can pass through a given gateway.

**NEW QUESTION 566**
- (Topic 8)
You are the security administrator for a large network. You want to prevent attackers from running any sort of traceroute into your DMZ and discover the internal structure of publicly accessible areas of the network.
How can you achieve this?

A. Block ICMP at the firewall.
B. Block UDP at the firewall.
C. Both A and B.
D. There is no way to completely block doing a trace route into this area.

**Answer:** D

**Explanation:**
When you run a traceroute to a target network address, you send a UDP packet with one time to live (TTL) to the target address. The first router this packet hits decreases the TTL to 0 and rejects the packet. Now the TTL for the packet is expired. The router sends back an ICMP message type 11 (Exceeded) code 0 (TTL--Exceeded) packet to your system with a source address. Your system displays the round-trip time for that first hop and sends out the next UDP packet with a TTL of 2.
This process continues until you receive an ICMP message type 3 (Unreachable) code 3 (Port--Unreachable) from the destination system. Traceroute is completed when your machine receives a Port-Unreachable message.
If you receive a message with three asterisks [* * *] during the traceroute, a router in the path doesn't return ICMP messages. Traceroute will continue to send UDP packets until the destination is reached or the maximum number of hops is exceeded.

**NEW QUESTION 567**
- (Topic 8)
Take a look at the following attack on a Web Server using obstructed URL:
http://www.example.com/script.ext?template%2e%2e%2e%2e%2e%2f%2e%2f%65%74% 63%2f%70%61%73%73%77%64
The request is made up of:
%2e%2e%2f%2e%2e%2f%2e%2f% = ../../../
%65%74%63 = etc
%2f = /
%70%61%73%73%77%64 = passwd
How would you protect information systems from these attacks?

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

**Answer:** B

**Explanation:**
This is a typical Unicode attack. By configuring your IDS to trigger on strange Unicode requests you can protect your web-server from this type of attacks.

**NEW QUESTION 572**
- (Topic 8)
Bill is attempting a series of SQL queries in order to map out the tables within the database that he is trying to exploit.
Choose the attack type from the choices given below.

A. Database Fingerprinting
B. Database Enumeration
C. SQL Fingerprinting
D. SQL Enumeration

**Answer:** A

**Explanation:**
He is trying to create a view of the characteristics of the target database, he is taking it’s fingerprints

**NEW QUESTION 574**
- (Topic 8)
You have been called to investigate a sudden increase in network traffic at XYZ. It seems that the traffic generated was too heavy that normal business functions could no longer be rendered to external employees and clients. After a quick investigation, you find that the computer has services running attached to TFN2k and Trinoo software. What do you think was the most likely cause behind this sudden increase in traffic?

A. A distributed denial of service attack.
B. A network card that was jabbering.
C. A bad route on the firewall.
D. Invalid rules entry at the gateway.

**Answer:** A

**Explanation:**
In computer security, a denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users. Typically the targets are high- profile web servers, and the attack attempts to make the hosted web pages unavailable on the Internet. It is a computer crime that violates the Internet proper use policy as indicated by the Internet Architecture Board (IAB). TFN2K and Trinoo are tools used for conducting DDos attacks.

**NEW QUESTION 579**
- (Topic 8)

Bubba has just accessed he preferred ecommerce web site and has spotted an item that he would like to buy. Bubba considers the price a bit too steep. He looks at the source code of the webpage and decides to save the page locally, so that he can modify the page variables. In the context of web application security, what do you think Bubba has changes?

A. A hidden form field value.
B. A hidden price value.
C. An integer variable.
D. A page cannot be changed locally, as it is served by a web server.

**Answer:** A

**NEW QUESTION 581**
- (Topic 8)
Which of the following statements best describes the term Vulnerability?

A. A weakness or error that can lead to a compromise
B. An agent that has the potential to take advantage of a weakness
C. An action or event that might prejudice security
D. The loss potential of a threat.

**Answer:** A

**Explanation:**
Vulnerabilities are all weaknesses that can be exploited.

**NEW QUESTION 585**
- (Topic 8)
Why do you need to capture five to ten million packets in order to crack WEP with AirSnort?

A. All IVs are vulnerable to attack
B. Air Snort uses a cache of packets
C. Air Snort implements the FMS attack and only encrypted packets are counted
D. A majority of weak IVs transmitted by access points and wireless cards are not filtered by contemporary wireless manufacturers

**Answer:** C

**Explanation:**
Since the summer of 2001, WEP cracking has been a trivial but time consuming process. A few tools, AirSnort perhaps the most famous, that implement the Fluhrer-Mantin-Shamir (FMS) attack were released to the security community -- who until then were aware of the problems with WEP but did not have practical penetration testing tools. Although simple to use, these tools require a very large number of packets to be gathered before being able to crack a WEP key. The AirSnort web site estimates the total number of packets at five to ten million, but the number actually required may be higher than you think.

**NEW QUESTION 590**
- (Topic 8)
Pandora is used to attack network operating systems.

A. Windows
B. UNIX
C. Linux
D. Netware
E. MAC OS

**Answer:** D

**Explanation:**
While there are not lots of tools available to attack Netware, Pandora is one that can be used.

**NEW QUESTION 595**
- (Topic 8)
Bob reads an article about how insecure wireless networks can be. He gets approval from his management to implement a policy of not allowing any wireless devices on the network. What other steps does Bob have to take in order to successfully implement this? (Select 2 answer.)

A. Train users in the new policy.
B. Disable all wireless protocols at the firewall.
C. Disable SNMP on the network so that wireless devices cannot be configured.
D. Continuously survey the area for wireless devices.

**Answer:** AD

**Explanation:**
If someone installs a access point and connect it to the network there is no way to find it unless you are constantly surveying the area for wireless devices. SNMP and firewalls can not prevent the installation of wireless devices on the corporate network.

**NEW QUESTION 597**
- (Topic 8)
Sandra is conducting a penetration test for XYZ.com. She knows that XYZ.com is using wireless networking for some of the offices in the building right down the street. Through social engineering she discovers that they are using 802.11g. Sandra knows that 802.11g uses the same 2.4GHz frequency range as 802.11b.

Using NetStumbler and her 802.11b wireless NIC, Sandra drives over to the building to map the wireless networks. However, even though she repositions herself around the building several times, Sandra is not able to detect a single AP.
What do you think is the reason behind this?

A. Netstumbler does not work against 802.11g.
B. You can only pick up 802.11g signals with 802.11a wireless cards.
C. The access points probably have WEP enabled so they cannot be detected.
D. The access points probably have disabled broadcasting of the SSID so they cannot be detected.
E. 802.11g uses OFDM while 802.11b uses DSSS so despite the same frequency and 802.11b card cannot see an 802.11g signal.
F. Sandra must be doing something wrong, as there is no reason for her to not see the signals.

**Answer:** E

**NEW QUESTION 600**
- (Topic 8)
_____ ensures that the enforcement of organizational security policy does not rely on voluntary web application user compliance. It secures information by assigning sensitivity labels on information and comparing this to the level of security a user is operating at.

A. Mandatory Access Control
B. Authorized Access Control
C. Role-based Access Control
D. Discretionary Access Control

**Answer:** A

**Explanation:**
In computer security, mandatory access control (MAC) is a kind of access control, defined by the TCSEC as "a means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity."

**NEW QUESTION 603**
- (Topic 8)
In order to attack a wireless network, you put up an access point and override the signal of the real access point. As users send authentication data, you are able to capture it. What kind of attack is this?

A. WEP attack
B. Drive by hacking
C. Rogue access point attack
D. Unauthorized access point attack

**Answer:** C

**Explanation:**
The definition of a Rogue access point is:
1. A wireless access point (AP) installed by an employee without the consent of the IT department. Without the proper security configuration, users have exposed their company's network to the outside world.
2. An access point (AP) set up by an attacker outside a facility with a wireless network. Also called an "evil twin, " the rogue AP picks up beacons (signals that advertise its presence) from the company's legitimate AP and transmits identical beacons, which some client machines inside the building associate with.

**NEW QUESTION 607**
- (Topic 8)
A client has approached you with a penetration test requirements. They are concerned with the possibility of external threat, and have invested considerable resources in protecting their Internet exposure. However, their main concern is the possibility of an employee elevating his/her privileges and gaining access to information outside of their respective department.
What kind of penetration test would you recommend that would best address the client's concern?

A. A Black Box test
B. A Black Hat test
C. A Grey Box test
D. A Grey Hat test
E. A White Box test
F. A White Hat test

**Answer:** C

**NEW QUESTION 609**
- (Topic 8)
Kevin has been asked to write a short program to gather user input for a web application. He likes to keep his code neat and simple. He chooses to use printf(str) where he should have ideally used printf(?s? str). What attack will his program expose the web application to?

A. Cross Site Scripting
B. SQL injection Attack
C. Format String Attack
D. Unicode Traversal Attack

**Answer:** C

**Explanation:**
Format string attacks are a new class of software vulnerability discovered around 1999, previously thought harmless. Format string attacks can be used to crash a

program or to execute harmful code. The problem stems from the use of unfiltered user input as the format string parameter in certain C functions that perform formatting, such as printf(). A malicious user may use the %s and %x format tokens, among others, to print data from the stack or possibly other locations in memory. One may also write arbitrary data to arbitrary locations using the %n format token, which commands printf() and similar functions to write back the number of bytes formatted to the same argument to printf(), assuming that the corresponding argument exists, and is of type int * .

**NEW QUESTION 610**
- (Topic 8)
Clive has been monitoring his IDS and sees that there are a huge number of ICMP Echo Reply packets that are being received on the external gateway interface. Further inspection reveals that they are not responses from the internal hosts' requests but simply responses coming from the Internet.
What could be the most likely cause?

A. Someone has spoofed Clive's IP address while doing a smurf attack.
B. Someone has spoofed Clive's IP address while doing a land attack.
C. Someone has spoofed Clive's IP address while doing a fraggle attack.
D. Someone has spoofed Clive's IP address while doing a DoS attack.

**Answer:** A

**Explanation:**
The smurf attack, named after its exploit program, is a denial-of-service attack that uses spoofed broadcast ping messages to flood a target system. In such an attack, a perpetrator sends a large amount of ICMP echo (ping) traffic to IP broadcast addresses, all of it having a spoofed source address of the intended victim. If the routing device delivering traffic to those broadcast addresses performs the IP broadcast to layer 2 broadcast function, most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply, multiplying the traffic by the number of hosts responding. On a multi-access broadcast network, hundreds of machines might reply to each packet.

**NEW QUESTION 611**
- (Topic 8)
While examining a log report you find out that an intrusion has been attempted by a machine whose IP address is displayed as 0xde.0xad.0xbe.0xef. It looks to you like a hexadecimal number. You perform a ping 0xde.0xad.0xbe.0xef. Which of the following IP addresses will respond to the ping and hence will likely be responsible for the intrusion?

A. 192.10.25.9
B. 10.0.3.4
C. 203.20.4.5
D. 222.273.290.239

**Answer:** D

**Explanation:**
Convert the hex number to binary and then to decimal.

**NEW QUESTION 612**
- (Topic 8)
There is some dispute between two network administrators at your company. Your boss asks you to come and meet with the administrators to set the record straight. Which of these are true about PKI and encryption?
Select the best answers.

A. PKI provides data with encryption, compression, and restorability.
B. Public-key encryption was invented in 1976 by Whitfield Diffie and Martin Hellman.
C. When it comes to eCommerce, as long as you have authenticity, and authenticity, you do not need encryption.
D. RSA is a type of encryption.

**Answer:** BD

**Explanation:**
PKI provides confidentiality, integrity, and authenticity of the messages exchanged between these two types of systems. The 3rd party provides the public key and the receiver verifies the message with a combination of the private and public key. Public- key encryption WAS invented in 1976 by Whitfield Diffie and Martin Hellman. The famous hashing algorithm Diffie-Hellman was named after them. The RSA Algorithm is created by the RSA Security company that also has created other widely used encryption algorithms.

**NEW QUESTION 616**
.....

# Relate Links

**100% Pass Your CEH-001 Exam with Exambible Prep Materials**

https://www.exambible.com/CEH-001-exam/

# Contact us

**We are proud of our high-quality customer service, which serves you around the clock 24/7.**

**Viste -** https://www.exambible.com/