Exam Questions CEH-001

Certified Ethical Hacker (CEH)

https://www.2passeasy.com/dumps/CEH-001/

NEW QUESTION 1
- (Topic 1)
Cyber Criminals have long employed the tactic of masking their true identity. In IP spoofing, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine, by "spoofing" the IP address of that machine.
How would you detect IP spoofing?

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

Answer: D

NEW QUESTION 2
- (Topic 1)
What is a sniffing performed on a switched network called?

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

Answer: D

NEW QUESTION 3
- (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 4
- (Topic 1)
What port number is used by Kerberos protocol?

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

Answer: A

NEW QUESTION 5
- (Topic 1)
This tool is widely used for ARP Poisoning attack. Name the tool.

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

Answer: A

NEW QUESTION 6
- (Topic 1)
What does FIN in TCP flag define?

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

Answer: B

NEW QUESTION 7
- (Topic 1)
TCP SYN Flood attack uses the three-way handshake mechanism.
1. An attacker at system A sends a SYN packet to victim at system B.
2. System B sends a SYN/ACK packet to victim A.
3. As a normal three-way handshake mechanism system A should send an ACK packet to system B, however, system A does not send an ACK packet to system B. In this case client B is waiting for an ACK packet from client A.
This status of client B is called

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

Answer: B

NEW QUESTION 8
- (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 9
- (Topic 1)
What type of Virus is shown here?

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

Answer: E

NEW QUESTION 10
- (Topic 1)
Google uses a unique cookie for each browser used by an individual user on a computer. This cookie contains information that allows Google to identify records about that user on
its database. This cookie is submitted every time a user launches a Google search, visits a site using AdSense etc. The information stored in Google's database, identified by the cookie, includes
? Everything you search for using Google
? Every web page you visit that has Google Adsense ads

How would you prevent Google from storing your search keywords?

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

Answer: A

NEW QUESTION 10
- (Topic 1)
Web servers often contain directories that do not need to be indexed. You create a text file with search engine indexing restrictions and place it on the root directory of the Web Server.
User-agent: * Disallow: /images/ Disallow: /banners/ Disallow: /Forms/ Disallow: /Dictionary/ Disallow: /_borders/ Disallow: /_fpclass/ Disallow: /_overlay/ Disallow: /_private/ Disallow: /_themes/
What is the name of this file?

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

Answer: A

NEW QUESTION 15
- (Topic 1)
In Trojan terminology, what is required to create the executable file chess.exe as shown below?

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

Answer: C

NEW QUESTION 20
- (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 22
- (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 24
- (Topic 1)
You just purchased the latest DELL computer, which comes pre-installed with Windows 7, McAfee antivirus software and a host of other applications. You want to connect Ethernet wire to your cable modem and start using the computer immediately. Windows is dangerously insecure when unpacked from the box, and there are a few things that you must do before you use it.

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

Answer: ACDEF

NEW QUESTION 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 29
- (Topic 1)
XSS attacks occur on Web pages that do not perform appropriate bounds checking on data entered by users. Characters like < > that mark the beginning/end of a tag should be converted into HTML entities.

What is the correct code when converted to html entities?

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

Answer: D

NEW QUESTION 32
- (Topic 1)
Which of the following statement correctly defines ICMP Flood Attack? (Select 2 answers)

A. Bogus ECHO reply packets are flooded on the network spoofing the IP and MAC address
B. The ICMP packets signal the victim system to reply and the combination of traffic saturates the bandwidth of the victim's network
C. ECHO packets are flooded on the network saturating the bandwidth of the subnet causing denial of service
D. A DDoS ICMP flood attack occurs when the zombies send large volumes of ICMP_ECHO_REPLY packets to the victim system.

Answer: BD

NEW QUESTION 36
- (Topic 1)
Your computer is infected by E-mail tracking and spying Trojan. This Trojan infects the computer with a single file - emos.sys
Which step would you perform to detect this type of Trojan?

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

Answer: C

NEW QUESTION 40
- (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 44
- (Topic 1)
Which of the following type of scanning utilizes automated process of proactively identifying vulnerabilities of the computing systems present on a network?

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

Answer: D

NEW QUESTION 48
- (Topic 1)
What is the problem with this ASP script (login.asp)?

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

Answer: D

NEW QUESTION 53
- (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 56
- (Topic 2)
Which of the following encryption is NOT based on block cipher?

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

Answer: D

NEW QUESTION 57
- (Topic 2)
"Testing the network using the same methodologies and tools employed by attackers" Identify the correct terminology that defines the above statement.

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

Answer: B

NEW QUESTION 59
- (Topic 2)
File extensions provide information regarding the underlying server technology. Attackers can use this information to search vulnerabilities and launch attacks.
How would you disable file extensions in Apache servers?

A. Use disable-eXchange
B. Use mod_negotiation
C. Use Stop_Files
D. Use Lib_exchanges

Answer: B

NEW QUESTION 60
- (Topic 2)
While testing web applications, you attempt to insert the following test script into the search area on the company's web site:
<script>alert('Testing Testing Testing')</script>
Later, when you press the search button, a pop up box appears on your screen with the text "Testing Testing Testing". What vulnerability is detected in the web application here?

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

Answer: A

NEW QUESTION 63
- (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 68
- (Topic 2)
Bob was frustrated with his competitor, Brownies Inc., and decided to launch an attack that would result in serious financial losses. He planned the attack carefully and carried out the attack at the appropriate moment.
Meanwhile, Trent, an administrator at Brownies Inc., realized that their main financial transaction server had been attacked. As a result of the attack, the server crashed and Trent needed to reboot the system, as no one was able to access the resources of the company. This process involves human interaction to fix it.
What kind of Denial of Service attack was best illustrated in the scenario above?

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

Answer: C

NEW QUESTION 73
- (Topic 2)
You receive an e-mail like the one shown below. When you click on the link contained in
the mail, you are redirected to a website seeking you to download free Anti-Virus software. Dear valued customers,
We are pleased to announce the newest version of Antivirus 2010 for Windows which will probe you with total security against the latest spyware, malware, viruses, Trojans and other online threats. Simply visit the link below and enter your antivirus code:
Antivirus code: 5014 http://www.juggyboy/virus/virus.html
Thank you for choosing us, the worldwide leader Antivirus solutions. Mike Robertson
PDF Reader Support
Copyright Antivirus 2010 ?All rights reserved
If you want to stop receiving mail, please go to: http://www.juggyboy.com
or you may contact us at the following address: Media Internet Consultants, Edif. Neptuno, Planta Baja, Ave. Ricardo J. Alfaro, Tumba Muerto, n/a Panama
How will you determine if this is Real Anti-Virus or Fake Anti-Virus website?

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

Answer: C

NEW QUESTION 77
- (Topic 2)
Johnny is a member of the hacking group Orpheus1. He is currently working on breaking into the Department of Defense's front end Exchange Server. He was able to get into the server, located in a DMZ, by using an unused service account that had a very weak password that he was able to guess. Johnny wants to crack the administrator password, but does not have a lot of time to crack it. He wants to use a tool that already has the LM hashes computed for all possible permutations of the administrator password.
What tool would be best used to accomplish this?

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

Answer: D

NEW QUESTION 78
- (Topic 2)
LAN Manager Passwords are concatenated to 14 bytes, and split in half. The two halves are hashed individually. If the password is 7 characters or less, than the second half of the hash is always:

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

Answer: A

NEW QUESTION 79
- (Topic 2)
What type of Virus is shown here?

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

Answer: B

NEW QUESTION 81
- (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 83
- (Topic 2)
What type of encryption does WPA2 use?

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

Answer: B

NEW QUESTION 84
- (Topic 2)
In Trojan terminology, what is a covert channel?

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

Answer: A

NEW QUESTION 86
- (Topic 2)
One of the ways to map a targeted network for live hosts is by sending an ICMP ECHO request to the broadcast or the network address. The request would be broadcasted to all hosts on the targeted network. The live hosts will send an ICMP ECHO Reply to the attacker's source IP address.
You send a ping request to the broadcast address 192.168.5.255.
There are 40 computers up and running on the target network. Only 13 hosts send a reply while others do not. Why?

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

Answer: A

NEW QUESTION 88
- (Topic 2)
What is the IV key size used in WPA2?

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

Answer: D

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

master encryption keys and has a message integrity checking facility.

NEW QUESTION 93
- (Topic 2)
Frederickson Security Consultants is currently conducting a security audit on the networks of Hawthorn Enterprises, a contractor for the Department of Defense. Since Hawthorn Enterprises conducts business daily with the federal government, they must abide by very stringent security policies. Frederickson is testing all of Hawthorn's physical and logical security measures including biometrics, passwords, and permissions. The federal government requires that all users must utilize random, non-dictionary passwords that must take at least 30 days to crack. Frederickson has confirmed that all Hawthorn employees use a random password generator for their network passwords. The Frederickson consultants have saved off numerous SAM files from Hawthorn's servers using Pwdump6 and are going to try and crack the network passwords. What method of attack is best suited to crack these passwords in the shortest amount of time?

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

Answer: A

NEW QUESTION 94
- (Topic 2)
E-mail tracking is a method to monitor and spy the delivered e-mails to the intended recipient.

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

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

Answer: H

NEW QUESTION 95
- (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 96
- (Topic 2)
You are programming a buffer overflow exploit and you want to create a NOP sled of 200 bytes in the program exploit.c

What is the hexadecimal value of NOP instruction?

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

Answer: D

NEW QUESTION 98

- (Topic 2)
Fred is scanning his network to ensure it is as secure as possible. Fred sends a TCP probe packet to a host with a FIN flag and he receives a RST/ACK response. What does this mean?

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

Answer: D

NEW QUESTION 103
- (Topic 2)
How do you defend against MAC attacks on a switch?

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

Answer: D

NEW QUESTION 104
- (Topic 3)
Jane wishes to forward X-Windows traffic to a remote host as well as POP3 traffic. She is worried that adversaries might be monitoring the communication link and could inspect captured traffic. She would like to tunnel the information to the remote end but does not have VPN capabilities to do so. Which of the following tools can she use to protect the link?

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

Answer: D

NEW QUESTION 106
- (Topic 3)
Lauren is performing a network audit for her entire company. The entire network is comprised of around 500 computers. Lauren starts an ICMP ping sweep by sending one IP packet to the broadcast address of the network, but only receives responses from around five hosts. Why did this ping sweep only produce a few responses?

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

Answer: C

NEW QUESTION 108
- (Topic 3)
SOAP services use which technology to format information?

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

Answer: C

NEW QUESTION 112
- (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 115
- (Topic 3)
You are trying to hijack a telnet session from a victim machine with IP address 10.0.0.5 to Cisco router at 10.0.0.1. You sniff the traffic and attempt to predict the sequence and acknowledgement numbers to successfully hijack the telnet session.
Here is the captured data in tcpdump.

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

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

Answer: A

NEW QUESTION 118
- (Topic 3)
A security engineer is attempting to map a company’s internal network. The engineer enters in the following NMAP commanD.
NMAP –n –sS –P0 –p 80 ***.***.**.** What type of scan is this?

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

Answer: C

NEW QUESTION 123
- (Topic 3)
Which of the following processes evaluates the adherence of an organization to its stated security policy?

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

Answer: D

NEW QUESTION 124
- (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 127
- (Topic 3)
WWW wanderers or spiders are programs that traverse many pages in the World Wide Web by recursively retrieving linked pages. Search engines like Google, frequently spider web pages for indexing. How will you stop web spiders from crawling certain directories on your website?

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

Answer: A

NEW QUESTION 129
- (Topic 3)
You ping a target IP to check if the host is up. You do not get a response. You suspect ICMP is blocked at the firewall. Next you use hping2 tool to ping the target host and you get a response. Why does the host respond to hping2 and not ping packet?

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

Answer: D

NEW QUESTION 130
- (Topic 3)
Which type of scan measures a person's external features through a digital video camera?

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

Answer: C

NEW QUESTION 134
- (Topic 3)
Which of the following techniques can be used to mitigate the risk of an on-site attacker from connecting to an unused network port and gaining full access to the network? (Choose three.)

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

Answer: ACE

NEW QUESTION 139
- (Topic 3)
Least privilege is a security concept that requires that a user is

A. limited to those functions required to do the job.

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

Answer: A

NEW QUESTION 142
- (Topic 3)
One way to defeat a multi-level security solution is to leak data via

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

Answer: C

NEW QUESTION 147
- (Topic 3)
Simon is security analyst writing signatures for a Snort node he placed internally that captures all mirrored traffic from his border firewall. From the following signature, what will Snort look for in the payload of the suspected packets?
alert tcp $EXTERNAL_NET any -> $HOME_NET 27374 (msG. "BACKDOOR SIG -
SubSseven 22";flags: A+; content: "|0d0a5b52504c5d3030320d0a|"; reference:arachnids, 485;) alert

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

Answer: B

NEW QUESTION 152
- (Topic 3)
A company has made the decision to host their own email and basic web services. The administrator needs to set up the external firewall to limit what protocols should be allowed to get to the public part of the company's network. Which ports should the administrator open? (Choose three.)

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

Answer: CDE

NEW QUESTION 155
- (Topic 3)
Which tool is used to automate SQL injections and exploit a database by forcing a given web application to connect to another database controlled by a hacker?

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

Answer: D

Explanation:
Mole is an automatic SQL Injection exploitation tool. Only by providing a vulnerable URL and a valid string on the site it can detect the injection and exploit it, either by using the union technique or a Boolean query based technique. The Mole uses a command based interface, allowing the user to indicate the action he wants to perform easily

NEW QUESTION 159
- (Topic 3)
What type of port scan is represented here.

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

Answer: A

NEW QUESTION 162
- (Topic 3)
Which type of antenna is used in wireless communication?

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

Answer: A

NEW QUESTION 163
- (Topic 3)
Which of the following items of a computer system will an anti-virus program scan for viruses?

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

Answer: A

NEW QUESTION 165
- (Topic 3)
Which type of password cracking technique works like dictionary attack but adds some numbers and symbols to the words from the dictionary and tries to crack the password?

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

Answer: C

NEW QUESTION 166
- (Topic 3)
Which of the following are valid types of rootkits? (Choose three.)

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

Answer: ACD

NEW QUESTION 171
- (Topic 3)
Here is the ASCII Sheet.

You want to guess the DBO username juggyboy (8 characters) using Blind SQL Injection technique.
What is the correct syntax?

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

Answer: A

NEW QUESTION 175
- (Topic 4)
An attacker has been successfully modifying the purchase price of items purchased on the company's web site. The security administrators verify the web server and Oracle database have not been compromised directly. They have also verified the Intrusion Detection
System (IDS) logs and found no attacks that could have caused this. What is the mostly likely way the attacker has been able to modify the purchase price?

A. By using SQL injection
B. By changing hidden form values
C. By using cross site scripting
D. By utilizing a buffer overflow attack

Answer: B

NEW QUESTION 179
- (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 180
- (Topic 4)
The use of technologies like IPSec can help guarantee the followinG. authenticity, integrity, confidentiality and

A. non-repudiation.
B. operability.
C. security.
D. usability.

Answer: A

NEW QUESTION 183
- (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 185
- (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 187
- (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 189
- (Topic 4)
The intrusion detection system at a software development company suddenly generates multiple alerts regarding attacks against the company's external webserver, VPN concentrator, and DNS servers. What should the security team do to determine which alerts to check first?

A. Investigate based on the maintenance schedule of the affected systems.
B. Investigate based on the service level agreements of the systems.
C. Investigate based on the potential effect of the incident.
D. Investigate based on the order that the alerts arrived in.

Answer: C

NEW QUESTION 192
- (Topic 4)
Which of the following tools will scan a network to perform vulnerability checks and compliance auditing?

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

Answer: C

NEW QUESTION 194
- (Topic 4)
Which of the following is an example of IP spoofing?

A. SQL injections
B. Man-in-the-middle
C. Cross-site scripting
D. ARP poisoning

Answer: B

NEW QUESTION 195
- (Topic 4)
A security consultant is trying to bid on a large contract that involves penetration testing and reporting. The company accepting bids wants proof of work so the consultant prints out several audits that have been performed. Which of the following is likely to occur as a result?

A. The consultant will ask for money on the bid because of great work.
B. The consultant may expose vulnerabilities of other companies.
C. The company accepting bids will want the same type of format of testing.
D. The company accepting bids will hire the consultant because of the great work performed.

Answer: B

NEW QUESTION 199
- (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 203
- (Topic 4)
While testing the company's web applications, a tester attempts to insert the following test script into the search area on the company's web sitE.
<script>alert(" Testing Testing Testing ")</script>
Afterwards, when the tester presses the search button, a pop-up box appears on the screen with the text: "Testing Testing Testing". Which vulnerability has been detected in the web application?

A. Buffer overflow
B. Cross-site request forgery
C. Distributed denial of service

D. Cross-site scripting

Answer: D

NEW QUESTION 204
- (Topic 4)
When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's computer to update the router configuration. What type of an alert is this?

A. False positive
B. False negative
C. True positve
D. True negative

Answer: A

NEW QUESTION 207
- (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 209
- (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 214
- (Topic 4)
Which of the following items is unique to the N-tier architecture method of designing software applications?

A. Application layers can be separated, allowing each layer to be upgraded independently from other layers.
B. It is compatible with various databases including Access, Oracle, and SQL.
C. Data security is tied into each layer and must be updated for all layers when any upgrade is performed.
D. Application layers can be written in C, ASP.NET, or Delphi without any performance loss.

Answer: A

NEW QUESTION 218
- (Topic 4)
A consultant has been hired by the V.P. of a large financial organization to assess the company's security posture. During the security testing, the consultant comes across child pornography on the V.P.'s computer. What is the consultant's obligation to the financial organization?

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

Answer: B

NEW QUESTION 220
- (Topic 4)
Which of the following is an example of an asymmetric encryption implementation?

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

Answer: B

NEW QUESTION 222
- (Topic 4)

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

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

Answer: D

NEW QUESTION 226
- (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 230
- (Topic 4)
Which of the following is an application that requires a host application for replication?

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

Answer: D

NEW QUESTION 235
- (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 236
- (Topic 4)
To reduce the attack surface of a system, administrators should perform which of the following processes to remove unnecessary software, services, and insecure configuration settings?

A. Harvesting
B. Windowing
C. Hardening
D. Stealthing

Answer: C

NEW QUESTION 239
- (Topic 4)
Which NMAP feature can a tester implement or adjust while scanning for open ports to avoid detection by the network’s IDS?

A. Timing options to slow the speed that the port scan is conducted
B. Fingerprinting to identify which operating systems are running on the network
C. ICMP ping sweep to determine which hosts on the network are not available
D. Traceroute to control the path of the packets sent during the scan

Answer: A

NEW QUESTION 240
- (Topic 4)
Which types of detection methods are employed by Network Intrusion Detection Systems (NIDS)? (Choose two.)

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

Answer: AB

NEW QUESTION 244
- (Topic 4)
A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

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

Answer: B

NEW QUESTION 245
- (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 246
- (Topic 4)
A network administrator received an administrative alert at 3:00 a.m. from the intrusion detection system. The alert was generated because a large number of packets were coming into the network over ports 20 and 21. During analysis, there were no signs of attack on the FTP servers. How should the administrator classify this situation?

A. True negatives
B. False negatives
C. True positives
D. False positives

Answer: D

NEW QUESTION 248
- (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 251
- (Topic 4)
What is the main difference between a “Normal” SQL Injection and a “Blind” SQL Injection vulnerability?

A. The request to the web server is not visible to the administrator of the vulnerable application.
B. The attack is called “Blind” because, although the application properly filters user input, it is still vulnerable to code injection.
C. The successful attack does not show an error message to the administrator of the affected application.
D. The vulnerable application does not display errors with information about the injection results to the attacker.

Answer: D

NEW QUESTION 255
- (Topic 5)
A newly discovered flaw in a software application would be considered which kind of security vulnerability?

A. Input validation flaw
B. HTTP header injection vulnerability
C. 0-day vulnerability
D. Time-to-check to time-to-use flaw

Answer: C

NEW QUESTION 256
- (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 260
- (Topic 5)
Which of the following descriptions is true about a static NAT?

A. A static NAT uses a many-to-many mapping.
B. A static NAT uses a one-to-many mapping.
C. A static NAT uses a many-to-one mapping.
D. A static NAT uses a one-to-one mapping.

Answer: D

NEW QUESTION 262
- (Topic 5)
Which security control role does encryption meet?

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

Answer: A

NEW QUESTION 265
- (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 267
- (Topic 5)
Which of the following is used to indicate a single-line comment in structured query language (SQL)?

A. --
B. ||
C. %%
D. "

Answer: A

NEW QUESTION 271
- (Topic 5)
A Certificate Authority (CA) generates a key pair that will be used for encryption and decryption of email. The integrity of the encrypted email is dependent on the security of which of the following?

A. Public key
B. Private key
C. Modulus length
D. Email server certificate

Answer: B

NEW QUESTION 276
- (Topic 5)
Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results? TCP port 21 – no response TCP port 22 – no response TCP port 23 – Time-to-live
exceeded

A. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host.
B. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server.
C. The scan on port 23 passed through the filtering devic
D. This indicates that port 23 was not blocked at the firewall.
E. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error.

Answer: C

NEW QUESTION 280
- (Topic 5)
Pentest results indicate that voice over IP traffic is traversing a network. Which of the following tools will decode a packet capture and extract the voice conversations?

A. Cain
B. John the Ripper
C. Nikto
D. Hping

Answer: A

NEW QUESTION 281
- (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 284
- (Topic 5)
Which of the following describes the characteristics of a Boot Sector Virus?

A. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR
B. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR
C. Modifies directory table entries so that directory entries point to the virus code instead of the actual program
D. Overwrites the original MBR and only executes the new virus code

Answer: B

NEW QUESTION 286
- (Topic 5)
A company has hired a security administrator to maintain and administer Linux and Windows-based systems. Written in the nightly report file is the followinG. Firewall log files are at the expected value of 4 MB. The current time is 12am. Exactly two hours later the size has decreased considerably. Another hour goes by and the log files have shrunk in size again.
Which of the following actions should the security administrator take?

A. Log the event as suspicious activity and report this behavior to the incident response team immediately.
B. Log the event as suspicious activity, call a manager, and report this as soon as possible.
C. Run an anti-virus scan because it is likely the system is infected by malware.
D. Log the event as suspicious activity, continue to investigate, and act according to the site's security policy.

Answer: D

NEW QUESTION 289
- (Topic 5)
A tester has been using the msadc.pl attack script to execute arbitrary commands on a Windows NT4 web server. While it is effective, the tester finds it tedious to perform extended functions.
On further research, the tester come across a perl script that runs the following msadc functions:system("perl msadc.pl -h $host -C \"echo open $your >testfile\"");

Which exploit is indicated by this script?

A. A buffer overflow exploit
B. A chained exploit
C. A SQL injection exploit
D. A denial of service exploit

Answer: B

NEW QUESTION 294
- (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 299
- (Topic 5)
Which of the following techniques does a vulnerability scanner use in order to detect a vulnerability on a target service?

A. Port scanning
B. Banner grabbing
C. Injecting arbitrary data
D. Analyzing service response

Answer: D

NEW QUESTION 302
- (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 305
- (Topic 5)
What is the primary drawback to using advanced encryption standard (AES) algorithm with a 256 bit key to share sensitive data?

A. Due to the key size, the time it will take to encrypt and decrypt the message hinders
B. efficient communication.
C. To get messaging programs to function with this algorithm requires complex configurations.
D. It has been proven to be a weak cipher; therefore, should not be trusted to protect sensitive data.
E. It is a symmetric key algorithm, meaning each recipient must receive the key through a different channel than the message.

Answer: D

NEW QUESTION 308
- (Topic 5)
Which of the following does proper basic configuration of snort as a network intrusion detection system require?

A. Limit the packets captured to the snort configuration file.
B. Capture every packet on the network segment.
C. Limit the packets captured to a single segment.
D. Limit the packets captured to the /var/log/snort directory.

Answer: A

NEW QUESTION 311
- (Topic 5)
When analyzing the IDS logs, the system administrator notices connections from outside of the LAN have been sending packets where the Source IP address and Destination IP address are the same. There have been no alerts sent via email or logged in the IDS. Which type of an alert is this?

A. False positive
B. False negative
C. True positive
D. True negative

Answer: B

NEW QUESTION 316
- (Topic 6)
Which address translation scheme would allow a single public IP address to always correspond to a single machine on an internal network, allowing "server publishing"?

A. Overloading Port Address Translation
B. Dynamic Port Address Translation
C. Dynamic Network Address Translation
D. Static Network Address Translation

Answer: D

Explanation:

Mapping an unregistered IP address to a registered IP address on a one-to- one basis. Particularly useful when a device needs to be accessible from outside the network.

NEW QUESTION 319
- (Topic 6)
Bob is acknowledged as a hacker of repute and is popular among visitors of “underground” sites. Bob is willing to share his knowledge with those who are willing to learn, and many have expressed their interest in learning from him. However, this knowledge has a risk associated with it, as it can be used for malevolent attacks as well.
In this context, what would be the most affective method to bridge the knowledge gap between the “black” hats or crackers and the “white” hats or computer security professionals? (Choose the test answer)

A. Educate everyone with books, articles and training on risk analysis, vulnerabilities and safeguards.
B. Hire more computer security monitoring personnel to monitor computer systems and networks.
C. Make obtaining either a computer security certification or accreditation easier to achieve so more individuals feel that they are a part of something larger than life.
D. Train more National Guard and reservist in the art of computer security to help out in times of emergency or crises.

Answer: A

Explanation:
Bridging the gap would consist of educating the white hats and the black hats equally so that their knowledge is relatively the same. Using books, articles, the internet, and professional training seminars is a way of completing this goal.

NEW QUESTION 321
- (Topic 6)
At a Windows Server command prompt, which command could be used to list the running services?

A. Sc query type= running
B. Sc query \\servername
C. Sc query
D. Sc config

Answer: C

NEW QUESTION 325
- (Topic 6)
____ is one of the programs used to wardial.

A. DialIT
B. Netstumbler
C. TooPac
D. Kismet
E. ToneLoc

Answer: E

Explanation:
ToneLoc is one of the programs used to wardial. While this is considered an "old school" technique, it is still effective at finding backdoors and out of band network entry points.

NEW QUESTION 330
- (Topic 6)
Sandra has been actively scanning the client network on which she is doing a vulnerability assessment test. While conducting a port scan she notices open ports in the range of 135 to 139. What protocol is most likely to be listening on those ports?

A. Finger
B. FTP
C. Samba
D. SMB

Answer: D

Explanation:
The SMB (Server Message Block) protocol is used among other things for file sharing in Windows NT / 2000. In Windows NT it ran on top of NBT (NetBIOS over TCP/IP), which used the famous ports 137, 138 (UDP) and 139 (TCP). In Windows 2000, Microsoft added the possibility to run SMB directly over TCP/IP, without the extra layer of NBT. For this they use TCP port 445.

NEW QUESTION 332
- (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 334
- (Topic 6)
Where should a security tester be looking for information that could be used by an attacker against an organization? (Select all that apply)

A. CHAT rooms
B. WHOIS database
C. News groups
D. Web sites
E. Search engines
F. Organization's own web site

Answer: ABCDEF

Explanation:
A Security tester should search for information everywhere that he/she can access. You never know where you find that small piece of information that could penetrate a strong defense.

NEW QUESTION 339
- (Topic 6)
What port scanning method is the most reliable but also the most detectable?

A. Null Scanning
B. Connect Scanning
C. ICMP Scanning
D. Idlescan Scanning
E. Half Scanning
F. Verbose Scanning

Answer: B

Explanation:
A TCP Connect scan, named after the Unix connect() system call is the most accurate scanning method. If a port is open the operating system completes the TCP three- way handshake, and the port scanner immediately closes the connection.

NEW QUESTION 344
- (Topic 6)
An Nmap scan shows the following open ports, and nmap also reports that the OS guessing results to match too many signatures hence it cannot reliably be identified:
21 ftp
23 telnet
80 http
443 https
What does this suggest?

A. This is a Windows Domain Controller
B. The host is not firewalled
C. The host is not a Linux or Solaris system
D. The host is not properly patched

Answer: C

NEW QUESTION 347
- (Topic 6)
You have initiated an active operating system fingerprinting attempt with nmap against a target system:

What operating system is the target host running based on the open ports shown above?

A. Windows XP
B. Windows 98 SE
C. Windows NT4 Server
D. Windows 2000 Server

Answer: D

Explanation:
The system is reachable as an active directory domain controller (port 389, LDAP)

NEW QUESTION 351
- (Topic 6)
Name two software tools used for OS guessing? (Choose two.

A. Nmap
B. Snadboy
C. Queso
D. UserInfo

E. NetBus

Answer: AC

Explanation:
Nmap and Queso are the two best-known OS guessing programs. OS guessing software has the ability to look at peculiarities in the way that each vendor implements the RFC's. These differences are compared with its database of known OS fingerprints. Then a best guess of the OS is provided to the user.

NEW QUESTION 352
- (Topic 6)
Your XYZ trainee Sandra asks you which are the four existing Regional Internet Registry (RIR's)?

A. APNIC, PICNIC, ARIN, LACNIC
B. RIPE NCC, LACNIC, ARIN, APNIC
C. RIPE NCC, NANIC, ARIN, APNIC
D. RIPE NCC, ARIN, APNIC, LATNIC

Answer: B

Explanation:
All other answers include non existing organizations (PICNIC, NANIC, LATNIC). See http://www.arin.net/library/internet_info/ripe.html

NEW QUESTION 354
- (Topic 6)
While attempting to discover the remote operating system on the target computer, you receive the following results from an nmap scan:

Remote operating system guess: Too many signatures match to reliably guess the OS. Nmap run completed -- 1 IP address (1 host up) scanned in 277.483 seconds
What should be your next step to identify the OS?

A. Perform a firewalk with that system as the target IP
B. Perform a tcp traceroute to the system using port 53
C. Run an nmap scan with the -v-v option to give a better output
D. Connect to the active services and review the banner information

Answer: D

Explanation:
Most people don’t care about changing the banners presented by applications listening to open ports and therefore you should get fairly accurate information when grabbing banners from open ports with, for example, a telnet application.

NEW QUESTION 357
- (Topic 6)
Which of the following command line switch would you use for OS detection in Nmap?

A. -D
B. -O
C. -P
D. -X

Answer: B

Explanation:
OS DETECTION:
-O: Enable OS detection (try 2nd generation w/fallback to 1st)
-O2: Only use the new OS detection system (no fallback)
-O1: Only use the old (1st generation) OS detection system
--osscan-limit: Limit OS detection to promising targets
--osscan-guess: Guess OS more aggressively

NEW QUESTION 358
- (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 361
- (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 365
- (Topic 6)
Which of the following tools are used for footprinting? (Choose four)

A. Sam Spade
B. NSLookup
C. Traceroute
D. Neotrace
E. Cheops

Answer: ABCD

Explanation:
All of the tools listed are used for footprinting except Cheops.

NEW QUESTION 369
- (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 374
- (Topic 7)
You have retrieved the raw hash values from a Windows 2000 Domain Controller. Using social engineering, you come to know that they are enforcing strong passwords. You understand that all users are required to use passwords that are at least 8 characters in length. All passwords must also use 3 of the 4 following categories: lower case letters, capital letters, numbers and special characters.
With your existing knowledge of users, likely user account names and the possibility that they will choose the easiest passwords possible, what would be the fastest type of password cracking attack you can run against these hash values and still get results?

A. Online Attack
B. Dictionary Attack
C. Brute Force Attack
D. Hybrid Attack

Answer: D

Explanation:
A dictionary attack will not work as strong passwords are enforced, also the minimum length of 8 characters in the password makes a brute force attack time consuming. A hybrid attack where you take a word from a dictionary and exchange a number of letters with numbers and special characters will probably be the fastest way to crack the passwords.

NEW QUESTION 375
- (Topic 7)
Which of the following is the primary objective of a rootkit?

A. It opens a port to provide an unauthorized service
B. It creates a buffer overflow

C. It replaces legitimate programs
D. It provides an undocumented opening in a program

Answer: C

Explanation:
Actually the objective of the rootkit is more to hide the fact that a system has been compromised and the normal way to do this is by exchanging, for example, ls to a version that doesn't show the files and process implanted by the attacker.

NEW QUESTION 376
- (Topic 7)
A denial of Service (DoS) attack works on the following principle:

A. MS-DOS and PC-DOS operating system utilize a weaknesses that can be compromised and permit them to launch an attack easily.
B. All CLIENT systems have TCP/IP stack implementation weakness that can be compromised and permit them to lunch an attack easily.
C. Overloaded buffer systems can easily address error conditions and respond appropriately.
D. Host systems cannot respond to real traffic, if they have an overwhelming number of incomplete connections (SYN/RCVD State).
E. A server stops accepting connections from certain networks one those network become flooded.

Answer: D

Explanation:
Denial-of-service (often abbreviated as DoS) is a class of attacks in which an attacker attempts to prevent legitimate users from accessing an Internet service, such as a web site.This can be done by exercising a software bug that causes the software running the service to fail (such as the "Ping of Death" attack against Windows NT systems), sending enough data to consume all available network bandwidth (as in the May, 2001 attacks against Gibson Research), or sending data in such a way as to consume a particular resource needed by the service.

NEW QUESTION 377
- (Topic 7)
What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?

A. Copy the system files from a known good system
B. Perform a trap and trace
C. Delete the files and try to determine the source
D. Reload from a previous backup
E. Reload from known good media

Answer: E

Explanation:
If a rootkit is discovered, you will need to reload from known good media. This typically means performing a complete reinstall.

NEW QUESTION 380
- (Topic 7)
Which tool/utility can help you extract the application layer data from each TCP connection from a log file into separate files?

A. Snort
B. argus
C. TCPflow
D. Tcpdump

Answer: C

Explanation:
Tcpflow is a program that captures data transmitted as part of TCP connections (flows), and stores the data in a way that is convenient for protocol analysis or debugging. A program like 'tcpdump' shows a summary of packets seen on the wire, but usually doesn't store the data that's actually being transmitted. In contrast, tcpflow reconstructs the actual data streams and stores each flow in a separate file for later analysis.

NEW QUESTION 384
- (Topic 7)
What happens when one experiences a ping of death?

A. This is when an IP datagram is received with the "protocol" field in the IP header set to 1 (ICMP) and the "type" field in the ICMP header is set to 18 (Address Mask Reply).
B. This is when an IP datagram is received with the "protocol" field in the IP header set to 1 (ICMP), the Last Fragment bit is set, and (IP offset ' 8) + (IP data length) >65535.In other words, the IP offset (which represents the starting position of this fragment in the original packet, and which is in 8-byte units) plus the rest of the packet is greater than the maximum size for an IP packet.
C. This is when an IP datagram is received with the "protocol" field in the IP header set to 1 (ICMP) and the source equal to destination address.
D. This is when an the IP header is set to 1 (ICMP) and the "type" field in the ICMP header is set to 5 (Redirect).

Answer: B

Explanation:
A hacker can send an IP packet to a vulnerable machine such that the lastfragment contains an offest where (IP offset *8) + (IP data length)>65535.This means that when the packet is reassembled, its total length is largerthan the legal limit, causing buffer overruns in the machine's OS (becousethe buffer sizes are defined only to accomodate the maximum allowed size ofthe packet based on RFC 791)...IDS can generally recongize such attacks bylooking for packet fragments that have the IP header's protocol field set to1 (ICMP), the last bit set, and (IP offset *8) +(IP data length)>65535" CCIE Professional Development Network Security Principles and Practices by Saadat Malik pg 414 "Ping of Death" attacks cause systems to react in an unpredictable fashion when receiving oversized IP packets.

TCP/IP allows for a maximum packet size of up to 65536 octets (1 octet = 8 bits of data), containing aminimum of 20 octets of IP header information and zero or more octets ofoptional information, with the rest of the packet being data. Ping of Deathattacks can cause crashing, freezing, and rebooting.

NEW QUESTION 389
- (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 390
- (Topic 7)
In the context of password security, a simple dictionary attack involves loading a dictionary file (a text file full of dictionary words) into a cracking application such as L0phtCrack or John the Ripper, and running it against user accounts located by the application. The larger the word and word fragment selection, the more effective the dictionary attack is. The brute force method is the most inclusive, although slow. It usually tries every possible letter and number combination in its automated exploration.
If you would use both brute force and dictionary methods combined together to have variation of words, what would you call such an attack?

A. Full Blown
B. Thorough
C. Hybrid
D. BruteDics

Answer: C

Explanation:
A combination of Brute force and Dictionary attack is called a Hybrid attack or Hybrid dictionary attack.

NEW QUESTION 394
- (Topic 7)
Under what conditions does a secondary name server request a zone transfer from a primary name server?

A. When a primary SOA is higher that a secondary SOA
B. When a secondary SOA is higher that a primary SOA
C. When a primary name server has had its service restarted
D. When a secondary name server has had its service restarted
E. When the TTL falls to zero

Answer: A

Explanation:
Understanding DNS is critical to meeting the requirements of the CEH. When the serial number that is within the SOA record of the primary server is higher than the Serial number within the SOA record of the secondary DNS server, a zone transfer will take place.

NEW QUESTION 395
- (Topic 7)
When discussing passwords, what is considered a brute force attack?

A. You attempt every single possibility until you exhaust all possible combinations or discover the password
B. You threaten to use the rubber hose on someone unless they reveal their password
C. You load a dictionary of words into your cracking program
D. You create hashes of a large number of words and compare it with the encrypted passwords
E. You wait until the password expires

Answer: A

Explanation:
Brute force cracking is a time consuming process where you try every possible combination of letters, numbers, and characters until you discover a match.

NEW QUESTION 396
- (Topic 7)
In the following example, which of these is the "exploit"?
Today, Microsoft Corporation released a security notice. It detailed how a person could bring down the Windows 2003 Server operating system, by sending malformed packets to it. They detailed how this malicious process had been automated using basic scripting. Even worse, the new automated method for bringing down the server has already been used to perform denial of service attacks on many large commercial websites.
Select the best answer.

A. Microsoft Corporation is the exploit.
B. The security "hole" in the product is the exploit.
C. Windows 2003 Server
D. The exploit is the hacker that would use this vulnerability.

E. The documented method of how to use the vulnerability to gain unprivileged access.

Answer: E

Explanation:
Explanations:
Microsoft is not the exploit, but if Microsoft documents how the vulnerability can be used to gain unprivileged access, they are creating the exploit. If they just say that there is a hole in the product, then it is only a vulnerability. The security "hole" in the product is called the "vulnerability". It is documented in a way that shows how to use the vulnerability to gain unprivileged access, and it then becomes an "exploit". In the example given, Windows 2003 Server is the TOE (Target of Evaluation). A TOE is an IT System, product or component that requires security evaluation or is being identified. The hacker that would use this vulnerability is exploiting it, but the hacker is not the exploit. The documented method of how to use the vulnerability to gain unprivileged access is the correct answer.

NEW QUESTION 401
- (Topic 7)
Joseph was the Web site administrator for the Mason Insurance in New York, who's main Web site was located at www.masonins.com. Joseph uses his laptop computer regularly to administer the Web site.
One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker's message "Hacker Message: You are dead! Freaks!
From his office, which was directly connected to Mason Insurance's internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact. No changes were apparent. Joseph called a friend of his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So, while Smith and his friend could see the defaced page, Joseph saw the intact Mason Insurance web site. To help make sense of this problem, Joseph decided to access the Web site using his dial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith.
After his modem connected, he quickly typed www.masonins.com in his browser to reveal the following web page:
H@cker Mess@ge:
Y0u @re De@d! Fre@ks!
After seeing the defaced Web site, he disconnected his dial-up line, reconnected to the internal network, and used Secure Shell (SSH) to log in directly to the Web server. He ran Tripwire against the entire Web site, and determined that every system file and all the Web content on the server were intact.
How did the attacker accomplish this hack?

A. ARP spoofing
B. SQL injection
C. DNS poisoning
D. Routing table injection

Answer: C

Explanation:
External calls for the Web site has been redirected to another server by a successful DNS poisoning.

NEW QUESTION 406
- (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 409
- (Topic 7)
What is the algorithm used by LM for Windows2000 SAM?

A. MD4
B. DES
C. SHA
D. SSL

Answer: B

Explanation:
Okay, this is a tricky question. We say B, DES, but it could be A “MD4” depending on what their asking - Windows 2000/XP keeps users passwords not "apparently", but as hashes, i.e. actually as "check sum" of the passwords. Let's go into the passwords keeping at large. The most interesting structure of the complex SAM-file building is so called V-block. It's size is 32 bytes and it includes hashes of the password for the local entering: NT Hash of 16-byte length, and hash used during the authentication of access to the common resources of other computers LanMan Hash, or simply LM Hash, of the same 16-byte length. Algorithms of the formation of these hashes are following:
NT Hash formation:
1. User password is being generated to the Unicode-line.
2. Hash is being generated based on this line using MD4 algorithm.
3. Gained hash in being encoded by the DES algorithm, RID (i.e. user identifier) had been used as a key. It was necessary for gaining variant hashes for users who have equal passwords. You remember that all users have different RIDs (RID of the Administrator's built in account is 500, RID of the Guest's built in account is 501, all other users get RIDs equal 1000, 1001, 1002, etc.).
LM Hash formation:
1. User password is being shifted to capitals and added by nulls up to 14-byte length.

2. Gained line is divided on halves 7 bytes each, and each of them is being encoded separately using DES, output is 8-byte hash and total 16-byte hash.
3. Then LM Hash is being additionally encoded the same way as it had been done in the NT Hash formation algorithm step 3.

NEW QUESTION 410
- (Topic 7)
Which of the following keyloggers cannot be detected by anti-virus or anti-spyware products?

A. Covert keylogger
B. Stealth keylogger
C. Software keylogger
D. Hardware keylogger

Answer: D

Explanation:
As the hardware keylogger never interacts with the Operating System it is undetectable by anti-virus or anti-spyware products.

NEW QUESTION 412
- (Topic 7)
A file integrity program such as Tripwire protects against Trojan horse attacks by:

A. Automatically deleting Trojan horse programs
B. Rejecting packets generated by Trojan horse programs
C. Using programming hooks to inform the kernel of Trojan horse behavior
D. Helping you catch unexpected changes to a system utility file that might indicate it had been replaced by a Trojan horse

Answer: D

Explanation:
Tripwire generates a database of the most common files and directories on your system. Once it is generated, you can then check the current state of your system against the original database and get a report of all the files that have been modified, deleted or added. This comes in handy if you allow other people access to your machine and even if you don't, if someone else does get access, you'll know if they tried to modify
files such as /bin/login etc.

NEW QUESTION 413
- (Topic 7)
The follows is an email header. What address is that of the true originator of the message?

A. 19.25.19.10
B. 51.32.123.21
C. 168.150.84.123
D. 215.52.220.122
E. 8.10.2/8.10.2

Answer: C

Explanation:
Spoofing can be easily achieved by manipulating the "from" name field, however, it is much more difficult to hide the true source address. The "received from" IP address 168.150.84.123 is the true source of the

NEW QUESTION 416
- (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 418
- (Topic 7)
You have the SOA presented below in your Zone. Your secondary servers have not been able to contact your primary server to synchronize information. How long will the secondary servers attempt to contact the primary server before it considers that zone is dead and stops responding to queries?
collegae.edu.SOA, cikkye.edu ipad.college.edu. (200302028 3600 3600 604800 3600)

A. One day
B. One hour
C. One week
D. One month

Answer: C

Explanation:
The numbers represents the following values: 200302028; se = serial number
3600; ref = refresh = 1h 3600; ret = update retry = 1h 604800; ex = expiry = 1w
3600; min = minimum TTL = 1h

NEW QUESTION 422
- (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 424
- (Topic 8)
What is the expected result of the following exploit?

A. Opens up a telnet listener that requires no username or password.
B. Create a FTP server with write permissions enabled.
C. Creates a share called “sasfile” on the target system.
D. Creates an account with a user name of Anonymous and a password of noone@nowhere.com.

Answer: A

Explanation:
The script being depicted is in perl (both msadc.pl and the script their using as a wrapper) -
- $port, $your, $user, $pass, $host are variables that hold the port # of a DNS server, an IP, username, and FTP password. $host is set to argument variable 0 (which means the string typed directly after the command). Essentially what happens is it connects to an FTP server and downloads nc.exe (the TCP/IP swiss-army knife -- netcat) and uses nc to open a TCP port spawning cmd.exe (cmd.exe is the Win32 DOS shell on NT/2000/2003/XP), cmd.exe when spawned requires NO username or password and has the permissions of the username it is being executed as (probably guest in this instance, although it could be administrator).
The #'s in the script means the text following is a comment, notice the last line in particular, if the # was removed the script would spawn a connection to itself, the host system it was running on.

NEW QUESTION 426
- (Topic 8)
What do you conclude from the nmap results below? Staring nmap V. 3.10ALPHA0 (www.insecure.org/map/)
(The 1592 ports scanned but not shown below are in state: closed)
Port State Service 21/tcp open ftp 25/tcp open smtp 80/tcp open http 443/tcp open https
Remote operating system guess: Too many signatures match the reliability guess the OS. Nmap run completed – 1 IP address (1 host up) scanned in 91.66 seconds

A. The system is a Windows Domain Controller.
B. The system is not firewalled.
C. The system is not running Linux or Solaris.
D. The system is not properly patched.

Answer: B

Explanation:
There is no reports of any ports being filtered.

NEW QUESTION 429
- (Topic 8)
If you come across a sheepdip machine at your client’s site, what should you do?

A. A sheepdip computer is used only for virus-checking.
B. A sheepdip computer is another name for a honeypot
C. A sheepdip coordinates several honeypots.
D. A sheepdip computers defers a denial of service attack.

Answer: A

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 431
- (Topic 8)
What is the advantage in encrypting the communication between the agent and the monitor in an Intrusion Detection System?

A. Encryption of agent communications will conceal the presence of the agents
B. The monitor will know if counterfeit messages are being generated because they will not be encrypted
C. Alerts are sent to the monitor when a potential intrusion is detected
D. An intruder could intercept and delete data or alerts and the intrusion can go undetected

Answer: B

NEW QUESTION 434
- (Topic 8)
Which one of the following attacks will pass through a network layer intrusion detection system undetected?

A. A teardrop attack
B. A SYN flood attack
C. A DNS spoofing attack
D. A test.cgi attack

Answer: D

Explanation:
Because a network-based IDS reviews packets and headers, it can also detect denial of service (DoS) attacks
Not A or B:
The following sections discuss some of the possible DoS attacks available. Smurf
Fraggle SYN Flood Teardrop
DNS DoS Attacks”

NEW QUESTION 437
- (Topic 8)
Which of the following is not an effective countermeasure against replay attacks?

A. Digital signatures
B. Time Stamps
C. System identification
D. Sequence numbers

Answer: C

Explanation:
A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. Effective countermeasures should be anything that makes it hard to delay or replay the packet (time stamps and sequence numbers) or anything that prove the package is received as it was sent from the original sender (digital signature)

NEW QUESTION 438
- (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 441
- (Topic 8)
In which of the following should be performed first in any penetration test?

A. System identification
B. Intrusion Detection System testing
C. Passive information gathering
D. Firewall testing

Answer: C

NEW QUESTION 443
- (Topic 8)
Jacob would like your advice on using a wireless hacking tool that can save him time and get him better results with lesser packets. You would like to recommend a tool that uses KoreK's implementation. Which tool would you recommend from the list below?

A. Kismet
B. Shmoo
C. Aircrack
D. John the Ripper

Answer: C

Explanation:
Implementing KoreK's attacks as well as improved FMS, aircrack provides the fastest and most effective statistical attacks available.John the Ripper is a password cracker, Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system, and

NEW QUESTION 447
- (Topic 8)
Derek has stumbled upon a wireless network and wants to assess its security. However, he does not find enough traffic for a good capture. He intends to use AirSnort on the captured traffic to crack the WEP key and does not know the IP address range or the AP. How can he generate traffic on the network so that he can capture enough packets to crack the WEP key?

A. Use any ARP requests found in the capture
B. Derek can use a session replay on the packets captured
C. Derek can use KisMAC as it needs two USB devices to generate traffic
D. Use Ettercap to discover the gateway and ICMP ping flood tool to generate traffic

Answer: D

Explanation:
By forcing the network to answer to a lot of ICMP messages you can gather
enough packets to crack the WEP key.

NEW QUESTION 449
- (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 454
- (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 459
- (Topic 8)
Peter is a Network Admin. He is concerned that his network is vulnerable to a smurf attack. What should Peter do to prevent a smurf attack?

Select the best answer.

A. He should disable unicast on all routers
B. Disable multicast on the router
C. Turn off fragmentation on his router
D. Make sure all anti-virus protection is updated on all systems
E. Make sure his router won't take a directed broadcast

Answer: E

Explanation:
Explanations:
Unicasts are one-to-one IP transmissions, by disabling this he would disable most network transmissions but still not prevent the smurf attack. Turning of multicast or fragmentation on the router has nothing to do with Peter's concerns as a smurf attack uses broadcast, not multicast and has nothing to do with fragmentation. Anti-virus protection will not help prevent a smurf attack. A smurf attack is a broadcast from a spoofed source. If directed broadcasts are enabled on the destination all the computers at the destination will respond to the spoofed source, which is really the victim. Disabling directed broadcasts on a router can prevent the attack.

NEW QUESTION 463
- (Topic 8)
After studying the following log entries, what is the attacker ultimately trying to achieve as inferred from the log sequence?
1. mkdir -p /etc/X11/applnk/Internet/.etc
2. mkdir -p /etc/X11/applnk/Internet/.etcpasswd
3. touch -acmr /etc/passwd /etc/X11/applnk/Internet/.etcpasswd
4. touch -acmr /etc /etc/X11/applnk/Internet/.etc
5. passwd nobody -d
6. /usr/sbin/adduser dns -d/bin -u 0 -g 0 -s/bin/bash
7. passwd dns -d
8. touch -acmr /etc/X11/applnk/Internet/.etcpasswd /etc/passwd
9. touch -acmr /etc/X11/applnk/Internet/.etc /etc

A. Change password of user nobody
B. Extract information from a local directory
C. Change the files Modification Access Creation times
D. Download rootkits and passwords into a new directory

Answer: C

NEW QUESTION 467
- (Topic 8)
RC4 is known to be a good stream generator. RC4 is used within the WEP standard on wireless LAN. WEP is known to be insecure even if we are using a stream cipher that is known to be secured.
What is the most likely cause behind this?

A. There are some flaws in the implementation.
B. There is no key management.
C. The IV range is too small.
D. All of the above.
E. None of the above.

Answer: D

Explanation:
Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit IV, there is a 50% probability
the same IV will repeat after 5000 packets.
Many WEP systems require a key in hexadecimal format. Some users choose keys that spell words in the limited 0-9, A-F hex character set, for example C0DE C0DE C0DE C0DE. Such keys are often easily guessed.

NEW QUESTION 469
- (Topic 8)
Network Intrusion Detection systems can monitor traffic in real time on networks.
Which one of the following techniques can be very effective at avoiding proper detection?

A. Fragmentation of packets.
B. Use of only TCP based protocols.
C. Use of only UDP based protocols.
D. Use of fragmented ICMP traffic only.

Answer: A

Explanation:
If the default fragmentation reassembly timeout is set to higher on the client than on the IDS then the it is possible to send an attack in fragments that will never be reassembled in the IDS but they will be reassembled and read on the client computer acting victim.

NEW QUESTION 474
- (Topic 8)
This kind of attack will let you assume a users identity at a dynamically generated web page or site:

A. SQL Injection
B. Cross Site Scripting
C. Session Hijacking
D. Zone Transfer

Answer: B

Explanation:
Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users. Examples of such code include HTML code and client-side scripts. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy.

NEW QUESTION 479
- (Topic 8)
You want to carry out session hijacking on a remote server. The server and the client are communicating via TCP after a successful TCP three way handshake. The server has just received packet #120 from the client. The client has a receive window of 200 and the server has a receive window of 250.
Within what range of sequence numbers should a packet, sent by the client fall in order to be accepted by the server?

A. 200-250
B. 121-371
C. 120-321
D. 121-231
E. 120-370

Answer: B

Explanation:
Package number 120 have already been received by the server and the window is 250 packets, so any package number from 121 (next in sequence) to 371 (121+250).

NEW QUESTION 480
- (Topic 8)
You perform the above traceroute and notice that hops 19 and 20 both show the same IP address.

This probably indicates what?

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

Answer: C

NEW QUESTION 484
- (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 487
- (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 490
- (Topic 8)
What are the main drawbacks for anti-virus software?

A. AV software is difficult to keep up to the current revisions.
B. AV software can detect viruses but can take no action.
C. AV software is signature driven so new exploits are not detected.
D. It's relatively easy for an attacker to change the anatomy of an attack to bypass AV systems
E. AV software isn't available on all major operating systems platforms.
F. AV software is very machine (hardware) dependent.

Answer: C

Explanation:
Although there are functions like heuristic scanning and sandbox technology, the Antivirus program is still mainly depending of signature databases and can only find already known viruses.

NEW QUESTION 495
- (Topic 8)
Jim's organization has just completed a major Linux roll out and now all of the organization's systems are running the Linux 2.5 kernel. The roll out expenses has posed constraints on purchasing other essential security equipment and software. The organization requires an option to control network traffic and also perform stateful inspection of traffic going into and out of the DMZ.
Which built-in functionality of Linux can achieve this?

A. IP Tables
B. IP Chains
C. IP Sniffer
D. IP ICMP

Answer: A

Explanation:
iptables is a user space application program that allows a system administrator to configure the netfilter tables, chains, and rules (described above). Because iptables requires elevated privileges to operate, it must be executed by user root, otherwise it fails to function. On most Linux systems, iptables is installed as /sbin/iptables. IP Tables performs stateful inspection while the older IP Chains only performs stateless inspection.

NEW QUESTION 497
- (Topic 8)
There are two types of honeypots- high and low interaction. Which of these describes a low interaction honeypot? Select the best answers.

A. Emulators of vulnerable programs
B. More likely to be penetrated
C. Easier to deploy and maintain
D. Tend to be used for production
E. More detectable
F. Tend to be used for research

Answer: ACDE

Explanation:
Explanations:
A low interaction honeypot would have emulators of vulnerable programs, not the real programs.
A high interaction honeypot is more likely to be penetrated as it is running the real program and is more vulnerable than an emulator.
Low interaction honeypots are easier to deploy and maintain. Usually you would just use a program that is already available for download and install it. Hackers don't usually crash or destroy these types of programs and it would require little maintenance.
A low interaction honeypot tends to be used for production.
Low interaction honeypots are more detectable because you are using emulators of the real programs. Many hackers will see this and realize that they are in a honeypot.
A low interaction honeypot tends to be used for production. A high interaction honeypot tends to be used for research.

NEW QUESTION 502
- (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 503
- (Topic 8)
When referring to the Domain Name Service, what is denoted by a ‘zone’?

A. It is the first domain that belongs to a company.
B. It is a collection of resource records.
C. It is the first resource record type in the SOA.
D. It is a collection of domains.

Answer: B

Explanation:
A reasonable definition of a zone would be a portion of the DNS namespace where responsibility has been delegated.

NEW QUESTION 504
- (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 in which also he remains unsuccessful. What is the probable cause of Bill's problem?

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

Answer: C

NEW QUESTION 506
- (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%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%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 511
- (Topic 8)
Peter is a Linux network admin. As a knowledgeable security consultant, he turns to you to look for help on a firewall. He wants to use Linux as his firewall and use the latest freely available version that is offered. What do you recommend?
Select the best answer.

A. Ipchains
B. Iptables
C. Checkpoint FW for Linux
D. Ipfwadm

Answer: B

Explanation:
Explanations:
Ipchains was improved over ipfwadm with its chaining mechanism so that it can have multiple rulesets. However, it isn't the latest version of a free Linux firewall.
Iptables
replaced ipchains and is the latest of the free Linux firewall tools. Any Checkpoint firewall is not going to meet Jason's desire to have a free firewall. Ipfwadm is used to build Linux firewall rules prior to 2.2.0. It is a outdated version.

NEW QUESTION 516
- (Topic 8)
Exhibit:
TCP TTL:50 TOS:0×0 ID:53476 DF
*****PA* Seq: 0x33BC72AD Ack: 0x110CE81E Win: 0x7D78 TCP Options => NOP NOP TS: 126045057 105803098
50 41 53 53 20 90 90 90 90 90 90 90 90 90 90 90 PASS ………..
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 …………….
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 …………….
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 …………….
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 …………….
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 …………….
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 …………….
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 …………….
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 …………….
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 …………….
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 …………….
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 …………….
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 …………….
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 …………….
90 90 90 90 90 90 90 31 C0 31 DB 31 C9 B0 46 CD …….1.1.1..F.
80 31 C0 31 DB 43 89 D9 41 B0 3F CD 80 EB 6B 5E .1.1.C..A.?…k^
31 C0 31 C9 8D 5E 01 88 46 04 66 B9 FF FF 01 B0 1.1..^..F.f…..
27 CD 80 31 C0 8D 5E 01 B0 3D CD 80 31 C0 31 DB '..1..^..=..1.1.
8D 5E 08 89 43 02 31 C9 FE C9 31 C0 8D 5E 08 B0 .^..C.1…1..^..
0C CD 80 FE C9 75 F3 31 C0 88 46 09 8D 5E 08 B0 …..u.1..F..^..
3D CD 80 FE 0E B0 30 FE C8 88 46 04 31 C0 88 46 =…..0…F.1..F
07 89 76 08 89 46 0C 89 F3 8D 4E 08 8D 56 0C B0 ..v..F….N..V..
0B CD 80 31 C0 31 DB B0 01 CD 80 E8 90 FF FF FF …1.1……….
FF FF FF 30 62 69 6E 30 73 68 31 2E 2E 31 31 76 …0bin0sh1..11v
65 6E 67 6C 69 6E 40 6B 6F 63 68 61 6D 2E 6B 61 englin@kocham.ka
73 69 65 2E 63 6F 6D 0D 0A sie.com..
=+ 12/09-01:22:31.169534 172.16.1.104:21 -> 207.219.207.240:1882
TCP TTL:63 TOS:0×10 ID:48231 DF
*****PA* Seq: 0x110CE81E Ack: 0x33BC7446 Win: 0x7D78 TCP Options => NOP NOP TS: 105803113 126045057
35 33 30 20 4C 6F 67 69 6E 20 69 6E 63 6F 72 72 530 Login incorr
65 63 74 2E 0D 0A ect…
=+ 12/09-01:22:39.878150 172.16.1.104:21 -> 207.219.207.240:1882 TCP TTL:63 TOS:0×10
ID:48233 DF
*****PA* Seq: 0x110CE834 Ack: 0x33BC7447 Win: 0x7D78 TCP Options => NOP NOP TS: 105803984 126045931
32 32 31 20 59 6F 75 20 63 6F 75 6C 64 20 61 74 221 You could at
20 6C 65 61 73 74 20 73 61 79 20 67 6F 6F 64 62 least say goodb
79 65 2E 0D 0A ye…
=+ 12/09-01:22:39.880154 172.16.1.104:21 -> 207.219.207.240:1882
TCP TTL:63 TOS:0×10 ID:48234 DF
***F**A* Seq: 0x110CE859 Ack: 0x33BC7447 Win: 0x7D78 TCP Options => NOP NOP TS: 105803984 126045931
Given the following extract from the snort log on a honeypot, what service is being exploited? :

A. FTP
B. SSH
C. Telnet
D. SMTP

Answer: A

Explanation:
The connection is done to 172.16.1.104:21.

NEW QUESTION 517
- (Topic 8)
When a malicious hacker identifies a target and wants to eventually compromise this target, what would be among the first steps that he would perform? (Choose the best answer)

A. Cover his tracks by eradicating the log files and audit trails.
B. Gain access to the remote computer in order to conceal the venue of attacks.
C. Perform a reconnaissance of the remote target for identical of venue of attacks.
D. Always begin with a scan in order to quickly identify venue of attacks.

Answer: C

Explanation:
A hacker always starts with a preparatory phase (Reconnaissance) where he
seeks to gather as much information as possible about the target of evaluation prior to launching an attack. The reconnaissance can be either passive or active (or both).

NEW QUESTION 522
- (Topic 8)
Which of the following is NOT a valid NetWare access level?

A. Not Logged in

B. Logged in
C. Console Access
D. Administrator

Answer: D

Explanation:
Administrator is an account not a access level.

NEW QUESTION 523
- (Topic 8)
On wireless networks, SSID is used to identify the network. Why are SSID not considered to be a good security mechanism to protect a wireless networks?

A. The SSID is only 32 bits in length.
B. The SSID is transmitted in clear text.
C. The SSID is the same as the MAC address for all vendors.
D. The SSID is to identify a station, not a network.

Answer: B

Explanation:
The SSID IS constructed to identify a network, it IS NOT the same as the MAC address and SSID's consists of a maximum of 32 alphanumeric characters.

NEW QUESTION 524
- (Topic 8)
While probing an organization you discover that they have a wireless network. From your attempts to connect to the WLAN you determine that they have deployed MAC filtering by using ACL on the access points. What would be the easiest way to circumvent and communicate on the WLAN?

A. Attempt to crack the WEP key using Airsnort.
B. Attempt to brute force the access point and update or delete the MAC ACL.
C. Steel a client computer and use it to access the wireless network.
D. Sniff traffic if the WLAN and spoof your MAC address to one that you captured.

Answer: D

Explanation:
The easiest way to gain access to the WLAN would be to spoof your MAC address to one that already exists on the network.

NEW QUESTION 529
- (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 533
- (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 536
- (Topic 8)
You are attempting to map out the firewall policy for an organization. You discover your target system is one hop beyond the firewall. Using hping2, you send SYN packets with the exact TTL of the target system starting at port 1 and going up to port 1024. What is this process known as?

A. Footprinting

B. Firewalking
C. Enumeration
D. Idle scanning

Answer: B

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 541
- (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 545
- (Topic 8)
John is discussing security with Jane. Jane had mentioned to John earlier that she suspects an LKM has been installed on her server. She believes this is the reason that the server has been acting erratically lately. LKM stands for Loadable Kernel Module.
What does this mean in the context of Linux Security?

A. Loadable Kernel Modules are a mechanism for adding functionality to a file system without requiring a kernel recompilation.
B. Loadable Kernel Modules are a mechanism for adding functionality to an operating- system kernel after it has been recompiled and the system rebooted.
C. Loadable Kernel Modules are a mechanism for adding auditing to an operating-system kernel without requiring a kernel recompilation.
D. Loadable Kernel Modules are a mechanism for adding functionality to an operating- system kernel without requiring a kernel recompilation.

Answer: D

Explanation:
Loadable Kernel Modules, or LKM, are object files that contain code to extend the running kernel, or so-called base kernel, without the need of a kernel recompilation. Operating systems other than Linux, such as BSD systems, also provide support for LKM's. However, the Linux kernel generally makes far greater and more versatile use of LKM's than other systems. LKM's are typically used to add support for new hardware, filesystems or for adding system calls. When the functionality provided by an LKM is no longer required, it can be unloaded, freeing memory.

NEW QUESTION 546
- (Topic 8)
Snort is an open source Intrusion Detection system. However, it can also be used for a few other purposes as well.
Which of the choices below indicate the other features offered by Snort?

A. IDS, Packet Logger, Sniffer
B. IDS, Firewall, Sniffer
C. IDS, Sniffer, Proxy
D. IDS, Sniffer, content inspector

Answer: A

Explanation:
Snort is a free software network intrusion detection and prevention system capable of performing packet logging & real-time traffic analysis, on IP networks. Snort was written by Martin Roesch but is now owned and developed by Sourcefire

NEW QUESTION 550
- (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 551
- (Topic 8)
The Slammer Worm exploits a stack-based overflow that occurs in a DLL implementing the Resolution Service.
Which of the following Database Server was targeted by the slammer worm?

A. Oracle
B. MSSQL
C. MySQL
D. Sybase
E. DB2

Answer: B

Explanation:
W32.Slammer is a memory resident worm that propagates via UDP Port 1434 and exploits a vulnerability in SQL Server 2000 systems and systems with MSDE 2000 that have not applied the patch released by Microsoft Security Bulletin MS02-039.

NEW QUESTION 554
- (Topic 8)
What does black box testing mean?

A. You have full knowledge of the environment
B. You have no knowledge of the environment
C. You have partial knowledge of the environment

Answer: B

Explanation:
Black box testing is conducted when you have no knowledge of the environment. It is more time consuming and expensive.

NEW QUESTION 556
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CEH-001 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CEH-001 Product From:

https://www.2passeasy.com/dumps/CEH-001/

Money Back Guarantee

CEH-001 Practice Exam Features:

* CEH-001 Questions and Answers Updated Frequently

* CEH-001 Practice Questions Verified by Expert Senior Certified Staff

* CEH-001 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CEH-001 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year