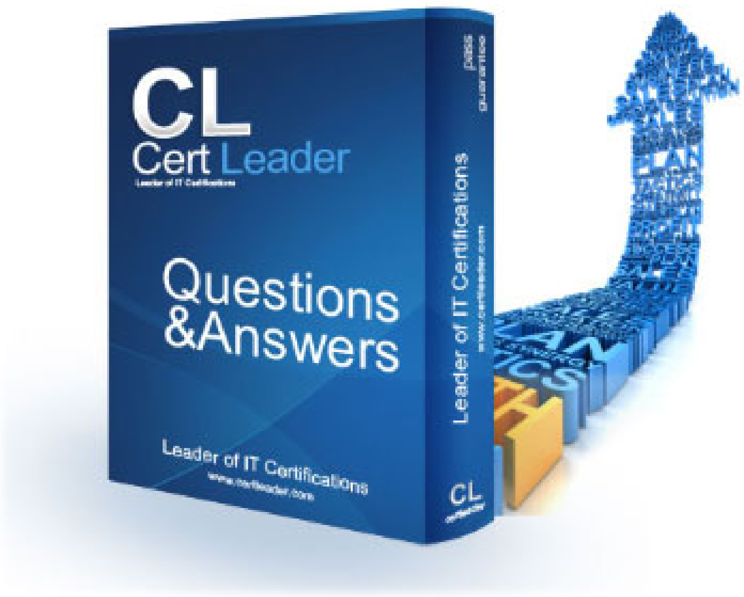
CEH-001 Dumps

Certified Ethical Hacker (CEH)

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



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

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

Answer: B

NEW QUESTION 2
- (Topic 1)
Lori is a Certified Ethical Hacker as well as a Certified Hacking Forensics Investigator working as an IT security consultant. Lori has been hired on by Kiley Innovators, a large marketing firm that recently underwent a string of thefts and corporate espionage incidents. Lori is told that a rival marketing company came out with an exact duplicate product right before Kiley Innovators was about to release it. The executive team believes that an employee is leaking information to the rival company. Lori questions all employees, reviews server logs, and firewall logs; after which she finds nothing. Lori is then given permission to search through the corporate email system. She searches by email being sent to and sent from the rival marketing company.
She finds one employee that appears to be sending very large email to this other marketing company, even though they should have no reason to be communicating with them. Lori tracks down the actual emails sent and upon opening them, only finds picture files attached to them. These files seem perfectly harmless, usually containing some kind of joke. Lori decides to use some special software to further examine the pictures and finds that each one had hidden text that was stored in each picture.
What technique was used by the Kiley Innovators employee to send information to the rival marketing company?

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

Answer: C

NEW QUESTION 3
- (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 4
- (Topic 1)
Shayla is an IT security consultant, specializing in social engineering and external penetration tests. Shayla has been hired on by Treks Avionics, a subcontractor for the Department of Defense. Shayla has been given authority to perform any and all tests necessary to audit the company's network security.
No employees for the company, other than the IT director, know about Shayla's work she will be doing. Shayla's first step is to obtain a list of employees through company website contact pages. Then she befriends a female employee of the company through an online chat website. After meeting with the female employee numerous times, Shayla is able to gain her trust and they become friends. One day, Shayla steals the employee's access badge and uses it to gain unauthorized access to the Treks Avionics offices.
What type of insider threat would Shayla be considered?

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

Answer: A

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

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

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

Answer: F

NEW QUESTION 6
- (Topic 1)
What is the correct command to run Netcat on a server using port 56 that spawns command shell when connected?

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

Answer: D

NEW QUESTION 7
- (Topic 1)
Annie has just succeeded in stealing a secure cookie via a XSS attack. She is able to replay the cookie even while the session is invalid on the server. Why do you think this is possible?

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

Answer: A

NEW QUESTION 8
- (Topic 1)

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

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

Answer: A

NEW QUESTION 9
- (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 10
- (Topic 1)
Attackers footprint target Websites using Google Hacking techniques. Google hacking is a term that refers to the art of creating complex search engine queries. It detects websites that are vulnerable to numerous exploits and vulnerabilities. Google operators are used to locate specific strings of text within the search results. The configuration file contains both a username and a password for an SQL database. Most sites with forums run a PHP message base. This file gives you the keys to that forum, including FULL ADMIN access to the database. WordPress uses config.php that stores the database Username and Password.
Which of the below Google search string brings up sites with "config.php" files?

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

Answer: C

NEW QUESTION 10
- (Topic 1)
Anonymizer sites access the Internet on your behalf, protecting your personal information from disclosure. An anonymizer protects all of your computer's identifying information while it surfs for you, enabling you to remain at least one step removed from the sites you visit.
You can visit Web sites without allowing anyone to gather information on sites visited by you. Services that provide anonymity disable pop-up windows and cookies, and conceal visitor's IP address.
These services typically use a proxy server to process each HTTP request. When the user requests a Web page by clicking a hyperlink or typing a URL into their browser, the service retrieves and displays the information using its own server. The remote server (where the requested Web page resides) receives information on the anonymous Web surfing service in place of your information.
In which situations would you want to use anonymizer? (Select 3 answers)

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

Answer: BCD

NEW QUESTION 14
- (Topic 1)
You receive an e-mail with the following text message.
"Microsoft and HP today warned all customers that a new, highly dangerous virus has been discovered which will erase all your files at midnight. If there's a file called hidserv.exe on your computer, you have been infected and your computer is now running a hidden server that allows hackers to access your computer.

Delete the file immediately. Please also pass this message to all your friends and colleagues as soon as possible."
You launch your antivirus software and scan the suspicious looking file hidserv.exe located in c:\windows directory and the AV comes out clean meaning the file is not infected. You view the file signature and confirm that it is a legitimate Windows system file "Human Interface Device Service".
What category of virus is this?

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

Answer: A

NEW QUESTION 16
- (Topic 1)
Which type of hacker represents the highest risk to your network?

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

Answer: C

NEW QUESTION 18
- (Topic 1)
How do you defend against DHCP Starvation attack?

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

Answer: B

NEW QUESTION 19
- (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 22
- (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 23
- (Topic 1)
One of the effective DoS/DDoS countermeasures is 'Throttling'. Which statement correctly defines this term?

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

Answer: A

NEW QUESTION 27
- (Topic 1)
Jimmy, an attacker, knows that he can take advantage of poorly designed input validation routines to create or alter SQL commands to gain access to private data or execute commands in the database. What technique does Jimmy use to compromise a database?

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

Answer: D

NEW QUESTION 30
- (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 32
- (Topic 1)
Lori was performing an audit of her company's internal Sharepoint pages when she came across the following codE. What is the purpose of this code?

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

Answer: C

NEW QUESTION 36
- (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 41
- (Topic 1)
This type of Port Scanning technique splits TCP header into several packets so that the packet filters are not able to detect what the packets intends to do.

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

Answer: B

NEW QUESTION 46
- (Topic 1)
BankerFox is a Trojan that is designed to steal users' banking data related to certain banking entities.
When they access any website of the affected banks through the vulnerable Firefox 3.5 browser, the Trojan is activated and logs the information entered by the user. All the information entered in that website will be logged by the Trojan and transmitted to the attacker's machine using covert channel.
BankerFox does not spread automatically using its own means. It needs an attacking user's intervention in order to reach the affected computer.

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

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

Answer: E

NEW QUESTION 47
- (Topic 1)
Vulnerability scanners are automated tools that are used to identify vulnerabilities and misconfigurations of hosts. They also provide information regarding mitigating discovered vulnerabilities.

Which of the following statements is incorrect?

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

Answer: D

NEW QUESTION 48
- (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 53
- (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 54
- (Topic 1)
How do you defend against Privilege Escalation?

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

Answer: ABCE

NEW QUESTION 56
- (Topic 1)
Which Steganography technique uses Whitespace to hide secret messages?

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

Answer: A

NEW QUESTION 58
- (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 60
- (Topic 1)
SNMP is a connectionless protocol that uses UDP instead of TCP packets (True or False)

A. true
B. false

Answer: A

NEW QUESTION 62
- (Topic 1)
If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization.

How would you prevent such type of attacks?

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

Answer: C

NEW QUESTION 67
- (Topic 1)
Attacking well-known system defaults is one of the most common hacker attacks. Most software is shipped with a default configuration that makes it easy to install and setup the application. You should change the default settings to secure the system.
Which of the following is NOT an example of default installation?

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

Answer: D

NEW QUESTION 70
- (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 72
- (Topic 1)
What does ICMP (type 11, code 0) denote?

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

Answer: C

NEW QUESTION 74
- (Topic 1)
TCP/IP Session Hijacking is carried out in which OSI layer?

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

Answer: B

NEW QUESTION 76
- (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 81
- (Topic 1)
Which of the following tool would be considered as Signature Integrity Verifier (SIV)?

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

Answer: D

NEW QUESTION 86
- (Topic 2)
What type of attack is shown here?

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

Answer: D

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

NEW QUESTION 89
- (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 93
- (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 96
- (Topic 2)
What framework architecture is shown in this exhibit?

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

Answer: B

NEW QUESTION 101
- (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 105
- (Topic 2)
What is the correct order of steps in CEH System Hacking Cycle?

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

Answer: A

NEW QUESTION 110
- (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 111
- (Topic 2)
John the hacker is sniffing the network to inject ARP packets. He injects broadcast frames onto the wire to conduct MiTM attack. What is the destination MAC address of a broadcast frame?

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

Answer: A

NEW QUESTION 115
- (Topic 2)
In this type of Man-in-the-Middle attack, packets and authentication tokens are captured using a sniffer. Once the relevant information is extracted, the tokens are placed back on the network to gain access.

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

Answer: A

NEW QUESTION 119
- (Topic 2)
You establish a new Web browser connection to Google. Since a 3-way handshake is required for any TCP connection, the following actions will take place.

? DNS query is sent to the DNS server to resolve www.google.com
? DNS server replies with the IP address for Google?
? SYN packet is sent to Google.
? Google sends back a SYN/ACK packet
? Your computer completes the handshake by sending an ACK
? The connection is established and the transfer of data commences
Which of the following packets represent completion of the 3-way handshake?

A. 4th packet
B. 3rdpacket
C. 6th packet
D. 5th packet

Answer: D

NEW QUESTION 123
- (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 125
- (Topic 2)
In TCP communications there are 8 flags; FIN, SYN, RST, PSH, ACK, URG, ECE, CWR. These flags have decimal numbers assigned to them:
FIN = 1
SYN = 2
RST = 4
PSH = 8
ACK = 16
URG = 32
ECE = 64
CWR =128
Example: To calculate SYN/ACK flag decimal value, add 2 (which is the decimal value of the SYN flag) to 16 (which is the decimal value of the ACK flag), so the result would be 18.
Based on the above calculation, what is the decimal value for XMAS scan?

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

Answer: C

NEW QUESTION 128
- (Topic 2)
What is the default Password Hash Algorithm used by NTLMv2?

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

Answer: D

NEW QUESTION 133
- (Topic 2)
Jess the hacker runs L0phtCrack's built-in sniffer utility that grabs SMB password hashes and stores them for offline cracking. Once cracked, these passwords can provide easy access to whatever network resources the user account has access to. But Jess is not picking up hashes from the network. Why?

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

Answer: A

NEW QUESTION 136
- (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 138

- (Topic 2)
TCP packets transmitted in either direction after the initial three-way handshake will have which of the following bit set?

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

Answer: B

NEW QUESTION 140
- (Topic 2)
Which of the following is NOT part of CEH Scanning Methodology?

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

Answer: E

NEW QUESTION 143
- (Topic 2)
Within the context of Computer Security, which of the following statements describes Social Engineering best?

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

Answer: C

NEW QUESTION 144
- (Topic 2)
A digital signature is simply a message that is encrypted with the public key instead of the private key.

A. true
B. false

Answer: B

NEW QUESTION 146
- (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 148
- (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 150
- (Topic 2)
Which of the following Trojans would be considered 'Botnet Command Control Center'?

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

Answer: C

NEW QUESTION 154
- (Topic 2)
Study the snort rule given below and interpret the rule.
alert tcp any any --> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msG. "mountd access";)

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

Answer: D

NEW QUESTION 156
- (Topic 2)
When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN/ACK (synchronize acknowledge). The destination host must then hear an ACK (acknowledge) of the SYN/ACK before the connection is established. This is referred to as the "TCP three-way handshake." While waiting for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue typically empties quickly since the ACK is expected to arrive a few milliseconds after the SYN ACK. How would an attacker exploit this design by launching TCP SYN attack?

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

Answer: B

NEW QUESTION 158
- (Topic 2)
NetBIOS over TCP/IP allows files and/or printers to be shared over the network. You are trying to intercept the traffic from a victim machine to a corporate network printer. You are attempting to hijack the printer network connection from your laptop by sniffing the wire. Which port does SMB over TCP/IP use?

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

Answer: D

NEW QUESTION 161
- (Topic 2)
Bob is going to perform an active session hijack against Brownies Inc. He has found a target that allows session oriented connections (Telnet) and performs the sequence prediction on the target operating system. He manages to find an active session due to the high level of traffic on the network. What is Bob supposed to do next?

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

Answer: C

NEW QUESTION 162
- (Topic 2)
You are trying to break into a highly classified top-secret mainframe computer with highest security system in place at Merclyn Barley Bank located in Los Angeles. You know that conventional hacking doesn't work in this case, because organizations such as banks are generally tight and secure when it comes to protecting their systems. In other words you are trying to penetrate an otherwise impenetrable system. How would you proceed?

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

Answer: B

NEW QUESTION 165
- (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 167
- (Topic 2)
What is the command used to create a binary log file using tcpdump?

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

Answer: A

NEW QUESTION 172
- (Topic 3)
Which of the following statements are true regarding N-tier architecture? (Choose two.)

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

Answer: AC

NEW QUESTION 173
- (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 174
- (Topic 3)
You are the security administrator for a large network. You want to prevent attackers from running any sort of traceroute into your DMZ and discovering the internal structure of publicly accessible areas of the network. How can you achieve this?

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

Answer: A

NEW QUESTION 179
- (Topic 3)
Which of the following is a common Service Oriented Architecture (SOA) vulnerability?

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

Answer: D

NEW QUESTION 182
- (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 186
- (Topic 3)
You are performing a port scan with nmap. You are in hurry and conducting the scans at the fastest possible speed. However, you don't want to sacrifice reliability for speed. If stealth is not an issue, what type of scan should you run to get very reliable results?

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

Answer: B

NEW QUESTION 190
- (Topic 3)
During a wireless penetration test, a tester detects an access point using WPA2 encryption. Which of the following attacks should be used to obtain the key?

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

Answer: A

NEW QUESTION 191
- (Topic 3)
Why attackers use proxy servers?

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

Answer: D

NEW QUESTION 196
- (Topic 3)
Which of the following types of firewall inspects only header information in network traffic?

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

Answer: A

NEW QUESTION 201
- (Topic 3)
A company is using Windows Server 2003 for its Active Directory (AD). What is the most efficient way to crack the passwords for the AD users?

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

Answer: C

NEW QUESTION 203
- (Topic 3)
Blake is in charge of securing all 20 of his company's servers. He has enabled hardware and software firewalls, hardened the operating systems, and disabled all unnecessary services on all the servers. Unfortunately, there is proprietary AS400 emulation software that must run on one of the servers that requires the telnet service to function properly. Blake is especially concerned about this since telnet can be a very large security risk in an organization. Blake is concerned about how this particular server might look to an outside attacker so he decides to perform some footprinting, scanning, and penetration tests on the server. Blake telnets into the server using Port 80 and types in the following command:
HEAD / HTTP/1.0
After pressing enter twice, Blake gets the following results: What has Blake just accomplished?

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

Answer: D

NEW QUESTION 205
- (Topic 3)
An attacker sniffs encrypted traffic from the network and is subsequently able to decrypt it. The attacker can now use which cryptanalytic technique to attempt to discover the encryption key?

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

Answer: D

NEW QUESTION 206
- (Topic 3)
A covert channel is a channel that _____

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

Answer: A

NEW QUESTION 211
- (Topic 3)
Blane is a security analyst for a law firm. One of the lawyers needs to send out an email to a client but he wants to know if the email is forwarded on to any other recipients. The client is explicitly asked not to re-send the email since that would be a violation of the lawyer's and client's agreement for this particular case. What can Blane use to accomplish this?

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

Answer: D

NEW QUESTION 213
- (Topic 3)
John runs a Web server, IDS and firewall on his network. Recently his Web server has been under constant hacking attacks. He looks up the IDS log files and sees no intrusion attempts but the Web server constantly locks up and needs rebooting due to various brute force and buffer overflow attacks but still the IDS alerts no intrusion whatsoever. John becomes suspicious and views the Firewall logs and he notices huge SSL connections constantly hitting his Web server. Hackers have been using the encrypted HTTPS protocol to send exploits to the Web server and that was the reason the IDS did not detect the intrusions. How would John protect his network from these types of attacks?

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

Answer: AC

NEW QUESTION 214
- (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 218
- (Topic 3)
If an attacker's computer sends an IPID of 24333 to a zombie (Idle Scanning) computer on
a closed port, what will be the response?

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

D. The zombie computer will respond with an IPID of 24335.

Answer: A

NEW QUESTION 221
- (Topic 3)
If an attacker's computer sends an IPID of 31400 to a zombie (Idle Scanning) computer on an open port, what will be the response?

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

Answer: B

Explanation:
31402 is the correct answer.

NEW QUESTION 224
- (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 225
- (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 230
- (Topic 3)
Hayden is the network security administrator for her company, a large finance firm based in Miami. Hayden just returned from a security conference in Las Vegas where they talked about all kinds of old and new security threats; many of which she did not know of. Hayden is worried about the current security state of her company's network so she decides to start scanning the network from an external IP address. To see how some of the hosts on her network react, she sends out SYN packets to an IP range. A number of IPs responds with a SYN/ACK response. Before the connection is established she sends RST packets to those hosts to stop the session. She does this to see how her intrusion detection system will log the traffic. What type of scan is Hayden attempting here?

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

Answer: D

NEW QUESTION 233
- (Topic 3)
On a Linux device, which of the following commands will start the Nessus client in the background so that the Nessus server can be configured?

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

Answer: C

NEW QUESTION 234
- (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 235
- (Topic 3)
Bill is a security analyst for his company. All the switches used in the company's office are Cisco switches. Bill wants to make sure all switches are safe from ARP poisoning. How can Bill accomplish this?

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

Answer: A

NEW QUESTION 239
- (Topic 3)
Wayne is the senior security analyst for his company. Wayne is examining some traffic logs on a server and came across some inconsistencies. Wayne finds some IP packets from a computer purporting to be on the internal network. The packets originate from 192.168.12.35 with a TTL of 15. The server replied to this computer and received a response from 192.168.12.35 with a TTL of 21. What can Wayne infer from this traffic log?

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

Answer: A

NEW QUESTION 243
- (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 244
- (Topic 3)
In the software security development life cyle process, threat modeling occurs in which phase?

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

Answer: A

NEW QUESTION 249
- (Topic 3)
Kevin is an IT security analyst working for Emerson Time Makers, a watch manufacturing company in Miami. Kevin and his girlfriend Katy recently broke up after a big fight. Kevin believes that she was seeing another person. Kevin, who has an online email account that he uses for most of his mail, knows that Katy has an account with that same company. Kevin logs into his email account online and gets the following URL after successfully logged in:
http://www.youremailhere.com/mail.asp?mailbox=Kevin&Smith=121%22 Kevin changes the URL to:
http://www.youremailhere.com/mail.asp?mailbox=Katy&Sanchez=121%22 Kevin is trying to access her email account to see if he can find out any information. What is Kevin attempting here to gain access to Katy's mailbox?

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

D. He is attempting a path-string attack to gain access to her mailbox

Answer: C

NEW QUESTION 252
- (Topic 3)
What do you call a pre-computed hash?

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

Answer: C

NEW QUESTION 256
- (Topic 3)
Keystroke logging is the action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.

How will you defend against hardware keyloggers when using public computers and Internet Kiosks? (Select 4 answers)

A. Alternate between typing the login credentials and typing characters somewhere else in the focus window
B. Type a wrong password first, later type the correct password on the login page defeating the keylogger recording
C. Type a password beginning with the last letter and then using the mouse to move the cursor for each subsequent letter.
D. The next key typed replaces selected text portio
E. E.
F. if the password is "secret", one could type "s", then some dummy keys "asdfsd".Then these dummies could be selected with mouse, and next character from the password "e" is typed, which replaces the dummies"asdfsd"
G. The next key typed replaces selected text portio
H. E.
I. if the password is "secret", one could type "s", then some dummy keys "asdfsd".Then these dummies could be selected with mouse, and next character from the password "e" is typed, which replaces the dummies"asdfsd"

Answer: ACDE

NEW QUESTION 260
- (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 264
- (Topic 3)
What is the main reason the use of a stored biometric is vulnerable to an attack?

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

Answer: D

NEW QUESTION 268
- (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 269
- (Topic 3)
Which of the following conditions must be given to allow a tester to exploit a Cross-Site Request Forgery (CSRF) vulnerable web application?

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

Answer: D

NEW QUESTION 270
- (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 271
- (Topic 4)
Which command line switch would be used in NMAP to perform operating system detection?

A. -OS
B. -sO
C. -sP
D. -O

Answer: D

NEW QUESTION 276
- (Topic 4)
Which tool can be used to silently copy files from USB devices?

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

Answer: B

NEW QUESTION 278
- (Topic 4)
Employees in a company are no longer able to access Internet web sites on their computers. The network administrator is able to successfully ping IP address of web servers on the Internet and is able to open web sites by using an IP address in place of the URL. The administrator runs the nslookup command for www.eccouncil.org and receives an error message stating there is no response from the server. What should the administrator do next?

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

Answer: A

NEW QUESTION 280
- (Topic 4)
Which of the statements concerning proxy firewalls is correct?

A. Proxy firewalls increase the speed and functionality of a network.
B. Firewall proxy servers decentralize all activity for an application.
C. Proxy firewalls block network packets from passing to and from a protected network.
D. Computers establish a connection with a proxy firewall which initiates a new network connection for the client.

Answer: D

NEW QUESTION 285
- (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 289
- (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 292
- (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 296
- (Topic 4)
Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Which of the following is the correct bit size of the Diffie-Hellman (DH) group 5?

A. 768 bit key
B. 1025 bit key
C. 1536 bit key
D. 2048 bit key

Answer: C

NEW QUESTION 298
- (Topic 4)
A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed. Considering the NMAP result below, which of the following is likely to be installed on the target machine by the OS?

```
Starting NMAP 5.21 at 2011-03-15 11:06
NMAP scan report for 172.16.40.65 Host is up (1.00s latency).
Not shown: 993 closed ports PORT STATE SERVICE
21/tcp open ftp 23/tcp open telnet 80/tcp open http
139/tcp open netbios-ssn 515/tcp open
631/tcp open ipp 9100/tcp open
MAC Address: 00:00:48:0D:EE:89
```

A. The host is likely a Windows machine.
B. The host is likely a Linux machine.
C. The host is likely a router.
D. The host is likely a printer.

Answer: D

NEW QUESTION 299
- (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 302
- (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 303
- (Topic 4)
There is a WEP encrypted wireless access point (AP) with no clients connected. In order to crack the WEP key, a fake authentication needs to be performed. What information is needed when performing fake authentication to an AP? (Choose two.)

A. The IP address of the AP
B. The MAC address of the AP
C. The SSID of the wireless network
D. A failed authentication packet

Answer: BC

NEW QUESTION 304
- (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 308
- (Topic 4)
Which command lets a tester enumerate alive systems in a class C network via ICMP using native Windows tools?

A. ping 192.168.2.
B. ping 192.168.2.255
C. for %V in (1 1 255) do PING 192.168.2.%V
D. for /L %V in (1 1 254) do PING -n 1 192.168.2.%V | FIND /I "Reply"

Answer: D

NEW QUESTION 313
- (Topic 4)
Which of the following programs is usually targeted at Microsoft Office products?

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

Answer: C

NEW QUESTION 317
- (Topic 4)
Which of the following ensures that updates to policies, procedures, and configurations are made in a controlled and documented fashion?

A. Regulatory compliance
B. Peer review
C. Change management
D. Penetration testing

Answer: C

NEW QUESTION 319
- (Topic 4)
What is the most secure way to mitigate the theft of corporate information from a laptop that was left in a hotel room?

A. Set a BIOS password.
B. Encrypt the data on the hard drive.
C. Use a strong logon password to the operating system.
D. Back up everything on the laptop and store the backup in a safe place.

Answer: B

NEW QUESTION 322
- (Topic 4)
Which type of access control is used on a router or firewall to limit network activity?

A. Mandatory
B. Discretionary
C. Rule-based
D. Role-based

Answer: C

NEW QUESTION 327
- (Topic 4)
Which of the following scanning tools is specifically designed to find potential exploits in Microsoft Windows products?

A. Microsoft Security Baseline Analyzer
B. Retina
C. Core Impact
D. Microsoft Baseline Security Analyzer

Answer: D

NEW QUESTION 330
- (Topic 4)
A network security administrator is worried about potential man-in-the-middle attacks when users access a corporate web site from their workstations. Which of the following is the best remediation against this type of attack?

A. Implementing server-side PKI certificates for all connections
B. Mandating only client-side PKI certificates for all connections
C. Requiring client and server PKI certificates for all connections
D. Requiring strong authentication for all DNS queries

Answer: C

NEW QUESTION 332
- (Topic 4)
A corporation hired an ethical hacker to test if it is possible to obtain users' login credentials using methods other than social engineering. Access to offices and to a network node is granted. Results from server scanning indicate all are adequately patched and physical access is denied, thus, administrators have access only through Remote Desktop. Which technique could be used to obtain login credentials?

A. Capture every users' traffic with Ettercap.
B. Capture LANMAN Hashes and crack them with LC6.
C. Guess passwords using Medusa or Hydra against a network service.
D. Capture administrators RDP traffic and decode it with Cain and Abel.

Answer: D

NEW QUESTION 337
- (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 339
- (Topic 4)
A security consultant decides to use multiple layers of anti-virus defense, such as end user desktop anti-virus and E-mail gateway. This approach can be used to mitigate which kind of attack?

A. Forensic attack
B. ARP spoofing attack
C. Social engineering attack
D. Scanning attack

Answer: C

NEW QUESTION 344
- (Topic 4)
Which of the following is a characteristic of Public Key Infrastructure (PKI)?

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

Answer: B

NEW QUESTION 346
- (Topic 4)
After gaining access to the password hashes used to protect access to a web based application, knowledge of which cryptographic algorithms would be useful to gain access to the application?

A. SHA1
B. Diffie-Helman
C. RSA
D. AES

Answer: A

NEW QUESTION 350
- (Topic 4)
How do employers protect assets with security policies pertaining to employee surveillance activities?

A. Employers promote monitoring activities of employees as long as the employees demonstrate trustworthiness.
B. Employers use informal verbal communication channels to explain employee monitoring activities to employees.
C. Employers use network surveillance to monitor employee email traffic, network access, and to record employee keystrokes.
D. Employers provide employees written statements that clearly discuss the boundaries of monitoring activities and consequences.

Answer: D

NEW QUESTION 352
- (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 353
- (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 355
- (Topic 4)
When comparing the testing methodologies of Open Web Application Security Project (OWASP) and Open Source Security Testing Methodology Manual (OSSTMM) the main difference is

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

C. OWASP addresses controls and OSSTMM does not.
D. OSSTMM addresses controls and OWASP does not.

Answer: D

NEW QUESTION 356
- (Topic 4)
A penetration tester was hired to perform a penetration test for a bank. The tester began searching for IP ranges owned by the bank, performing lookups on the bank's DNS servers, reading news articles online about the bank, watching what times the bank employees come into work and leave from work, searching the bank's job postings (paying special attention to IT related jobs), and visiting the local dumpster for the bank's corporate office. What phase of the penetration test is the tester currently in?

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

Answer: D

NEW QUESTION 358
- (Topic 4)
Which type of scan is used on the eye to measure the layer of blood vessels?

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

Answer: B

NEW QUESTION 362
- (Topic 4)
Which type of security document is written with specific step-by-step details?

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

Answer: B

NEW QUESTION 365
- (Topic 4)
How does an operating system protect the passwords used for account logins?

A. The operating system performs a one-way hash of the passwords.
B. The operating system stores the passwords in a secret file that users cannot find.
C. The operating system encrypts the passwords, and decrypts them when needed.
D. The operating system stores all passwords in a protected segment of non-volatile memory.

Answer: A

NEW QUESTION 368
- (Topic 4)
A security administrator notices that the log file of the company`s webserver contains suspicious entries:

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

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

Answer: B

NEW QUESTION 372
- (Topic 4)
What statement is true regarding LM hashes?

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

Answer: D

NEW QUESTION 377
- (Topic 4)
Windows file servers commonly hold sensitive files, databases, passwords and more. Which of the following choices would be a common vulnerability that usually exposes them?

A. Cross-site scripting
B. SQL injection
C. Missing patches
D. CRLF injection

Answer: C

NEW QUESTION 378
- (Topic 5)
Which of the following is a preventive control?

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

Answer: A

NEW QUESTION 382
- (Topic 5)
What are common signs that a system has been compromised or hacked? (Choose three.)

A. Increased amount of failed logon events
B. Patterns in time gaps in system and/or event logs
C. New user accounts created
D. Consistency in usage baselines
E. Partitions are encrypted
F. Server hard drives become fragmented

Answer: ABC

NEW QUESTION 385
- (Topic 5)
The precaution of prohibiting employees from bringing personal computing devices into a facility is what type of security control?

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

Answer: B

NEW QUESTION 390
- (Topic 5)
A botnet can be managed through which of the following?

A. IRC
B. E-Mail
C. Linkedin and Facebook
D. A vulnerable FTP server

Answer: A

NEW QUESTION 392
- (Topic 5)
Which of the following is a client-server tool utilized to evade firewall inspection?

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

Answer: A

NEW QUESTION 394
- (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 396
- (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 399
- (Topic 5)
Which cipher encrypts the plain text digit (bit or byte) one by one?

A. Classical cipher
B. Block cipher
C. Modern cipher
D. Stream cipher

Answer: D

NEW QUESTION 403
- (Topic 5)
Advanced encryption standard is an algorithm used for which of the following?

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

Answer: C

NEW QUESTION 405
- (Topic 5)
While checking the settings on the internet browser, a technician finds that the proxy server settings have been checked and a computer is trying to use itself as a proxy server. What specific octet within the subnet does the technician see?

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

Answer: B

NEW QUESTION 406
- (Topic 5)
Fingerprinting VPN firewalls is possible with which of the following tools?

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

Answer: C

NEW QUESTION 407
- (Topic 5)
What are the three types of authentication?

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

Answer: B

NEW QUESTION 409
- (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 411
- (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 413
- (Topic 5)
Which of the following is a component of a risk assessment?

A. Physical security
B. Administrative safeguards
C. DMZ
D. Logical interface

Answer: B

NEW QUESTION 414
- (Topic 5)
Which of the following algorithms provides better protection against brute force attacks by using a 160-bit message digest?

A. MD5
B. SHA-1

C. RC4
D. MD4

Answer: B

NEW QUESTION 419
- (Topic 5)
What is the best defense against privilege escalation vulnerability?

A. Patch systems regularly and upgrade interactive login privileges at the system administrator level.
B. Run administrator and applications on least privileges and use a content registry for tracking.
C. Run services with least privileged accounts and implement multi-factor authentication and authorization.
D. Review user roles and administrator privileges for maximum utilization of automation services.

Answer: C

NEW QUESTION 422
- (Topic 5)
Which of the following programming languages is most vulnerable to buffer overflow attacks?

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

Answer: B

NEW QUESTION 423
- (Topic 5)
Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

A. Cavity virus
B. Polymorphic virus
C. Tunneling virus
D. Stealth virus

Answer: D

NEW QUESTION 424
- (Topic 5)
Which of the following defines the role of a root Certificate Authority (CA) in a Public Key Infrastructure (PKI)?

A. The root CA is the recovery agent used to encrypt data when a user's certificate is lost.
B. The root CA stores the user's hash value for safekeeping.
C. The CA is the trusted root that issues certificates.
D. The root CA is used to encrypt email messages to prevent unintended disclosure of data.

Answer: C

NEW QUESTION 428
- (Topic 5)
ICMP ping and ping sweeps are used to check for active systems and to check

A. if ICMP ping traverses a firewall.
B. the route that the ICMP ping took.
C. the location of the switchport in relation to the ICMP ping.
D. the number of hops an ICMP ping takes to reach a destination.

Answer: A

NEW QUESTION 431
- (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 436
- (Topic 5)

A tester has been hired to do a web application security test. The tester notices that the site is dynamic and must make use of a back end database.
In order for the tester to see if SQL injection is possible, what is the first character that the tester should use to attempt breaking a valid SQL request?

A. Semicolon
B. Single quote
C. Exclamation mark
D. Double quote

Answer: B

NEW QUESTION 440
- (Topic 5)
A consultant is hired to do physical penetration testing at a large financial company. In the first day of his assessment, the consultant goes to the company`s building dressed like an electrician and waits in the lobby for an employee to pass through the main access gate,
then the consultant follows the employee behind to get into the restricted area. Which type of attack did the consultant perform?

A. Man trap
B. Tailgating
C. Shoulder surfing
D. Social engineering

Answer: B

NEW QUESTION 442
- (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 447
- (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 450
- (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 451
- (Topic 5)
A pentester is using Metasploit to exploit an FTP server and pivot to a LAN. How will the pentester pivot using Metasploit?

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

Answer: D

NEW QUESTION 453
- (Topic 5)
Which of the following are advantages of adopting a Single Sign On (SSO) system? (Choose two.)

A. A reduction in password fatigue for users because they do not need to know multiple passwords when accessing multiple applications
B. A reduction in network and application monitoring since all recording will be completed at the SSO system
C. A reduction in system administration overhead since any user login problems can be resolved at the SSO system
D. A reduction in overall risk to the system since network and application attacks can only happen at the SSO point

Answer: AC

NEW QUESTION 458
- (Topic 5)
Which system consists of a publicly available set of databases that contain domain name registration contact information?

A. WHOIS
B. IANA
C. CAPTCHA
D. IETF

Answer: A

NEW QUESTION 462
- (Topic 5)
Which security strategy requires using several, varying methods to protect IT systems against attacks?

A. Defense in depth
B. Three-way handshake
C. Covert channels
D. Exponential backoff algorithm

Answer: A

NEW QUESTION 464
- (Topic 5)
If an e-commerce site was put into a live environment and the programmers failed to remove the secret entry point that was used during the application development, what is this secret entry point known as?

A. SDLC process
B. Honey pot
C. SQL injection
D. Trap door

Answer: D

NEW QUESTION 469
- (Topic 6)
A company is legally liable for the content of email that is sent from its systems, regardless of whether the message was sent for private or business-related purposes. This could lead to prosecution for the sender and for the company's directors if, for example, outgoing email was found to contain material that was pornographic, racist, or likely to incite someone to commit an act of terrorism. You can always defend yourself by "ignorance of the law" clause.

A. true
B. false

Answer: B

NEW QUESTION 470
- (Topic 6)
Which of the following LM hashes represents a password of less than 8 characters?

A. 0182BD0BD4444BF836077A718CCDF409
B. 44EFCE164AB921CQAAD3B435B51404EE
C. BA810DBA98995F1817306D272A9441BB
D. CEC52EB9C8E3455DC2265B23734E0DAC
E. B757BF5C0D87772FAAD3B435B51404EE
F. E52CAC67419A9A224A3B108F3FA6CB6D

Answer: BE

Explanation:
Any password that is shorter than 8 characters will result in the hashing of 7 null bytes, yielding the constant value of 0xAAD3B435B51404EE, hence making it easy to identify short passwords on sight.

NEW QUESTION 472
- (Topic 6)
To what does "message repudiation" refer to what concept in the realm of email security?

A. Message repudiation means a user can validate which mail server or servers a message was passed through.
B. Message repudiation means a user can claim damages for a mail message that damaged their reputation.
C. Message repudiation means a recipient can be sure that a message was sent from a particular person.
D. Message repudiation means a recipient can be sure that a message was sent from a certain host.
E. Message repudiation means a sender can claim they did not actually send a particular message.

Answer: E

Explanation:
A quality that prevents a third party from being able to prove that a communication between two other parties ever took place. This is a desirable quality if you do not want your communications to be traceable.
Non-repudiation is the opposite quality—a third party can prove that a communication between two other parties took place. Non-repudiation is desirable if you want to be able to trace your communications and prove that they occurred. Repudiation – Denial of message submission or delivery.

NEW QUESTION 475
- (Topic 6)
A XYZ security System Administrator is reviewing the network system log files.
He notes the following:
? Network log files are at 5 MB at 12:00 noon.
? At 14:00 hours, the log files at 3 MB.
What should he assume has happened and what should he do about the situation?

A. He should contact the attacker's ISP as soon as possible and have the connection disconnected.
B. He should log the event as suspicious activity, continue to investigate, and take further steps according to site security policy.
C. He should log the file size, and archive the information, because the router crashed.
D. He should run a file system check, because the Syslog server has a self correcting file system problem.
E. He should disconnect from the Internet discontinue any further unauthorized use, because an attack has taken place.

Answer: B

Explanation:
You should never assume a host has been compromised without verification. Typically, disconnecting a server is an extreme measure and should only be done when it is confirmed there is a compromise or the server contains such sensitive data that the loss of service outweighs the risk. Never assume that any administrator or automatic process is making changes to a system. Always investigate the root cause of the change on the system and follow your organizations security policy.

NEW QUESTION 477
- (Topic 6)
What is the proper response for a FIN scan if the port is closed?

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

Answer: E

Explanation:
Closed ports respond to a FIN scan with a RST.

NEW QUESTION 482
- (Topic 6)
What are the default passwords used by SNMP? (Choose two.)

A. Password
B. SA
C. Private
D. Administrator
E. Public
F. Blank

Answer: CE

Explanation:
Besides the fact that it passes information in clear text, SNMP also uses well-known passwords. Public and private are the default passwords used by SNMP.

NEW QUESTION 487
- (Topic 6)
Which of the following Nmap commands would be used to perform a stack fingerprinting?

A. Nmap -O -p80 <host(s.>
B. Nmap -hU -Q<host(s.>
C. Nmap -sT -p <host(s.>
D. Nmap -u -o -w2 <host>
E. Nmap -sS -0p target

Answer: A

Explanation:
This option activates remote host identification via TCP/IP fingerprinting. In other words, it uses a bunch of techniques to detect subtlety in the underlying operating system network stack of the computers you are scanning. It uses this information to create a "fingerprint" which it compares with its database of known OS fingerprints (the nmap-os- fingerprints file. to decide what type of system you are scanning.

NEW QUESTION 489
- (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 493
- (Topic 6)
Who is an Ethical Hacker?

A. A person who hacks for ethical reasons
B. A person who hacks for an ethical cause
C. A person who hacks for defensive purposes
D. A person who hacks for offensive purposes

Answer: C

Explanation:
The Ethical hacker is a security professional who applies his hacking skills for defensive purposes.

NEW QUESTION 495
- (Topic 6)
Bob has been hired to perform a penetration test on XYZ.com. He begins by looking at IP address ranges owned by the company and details of domain name registration. He then goes to News Groups and financial web sites to see if they are leaking any sensitive information of have any technical details online.
Within the context of penetration testing methodology, what phase is Bob involved with?

A. Passive information gathering
B. Active information gathering
C. Attack phase
D. Vulnerability Mapping

Answer: A

Explanation:
He is gathering information and as long as he doesn’t make contact with any of the targets systems he is considered gathering this information in a passive mode.

NEW QUESTION 500
- (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 502
- (Topic 6)
A specific site received 91 ICMP_ECHO packets within 90 minutes from 47 different sites. 77 of the ICMP_ECHO packets had an ICMP ID:39612 and Seq:57072. 13 of the ICMP_ECHO packets had an ICMP ID:0 and Seq:0. What can you infer from this information?

A. The packets were sent by a worm spoofing the IP addresses of 47 infected sites
B. ICMP ID and Seq numbers were most likely set by a tool and not by the operating system
C. All 77 packets came from the same LAN segment and hence had the same ICMP ID and Seq number
D. 13 packets were from an external network and probably behind a NAT, as they had an ICMP ID 0 and Seq 0

Answer: B

NEW QUESTION 506
- (Topic 6)
Which of the following ICMP message types are used for destinations unreachables?

A. 3
B. 11
C. 13
D. 17

Answer: B

Explanation:
Type 3 messages are used for unreachable messages. 0 is Echo Reply, 8 is Echo request, 11 is time exceeded, 13 is timestamp and 17 is subnet mask request. Learning these would
be advisable for the test.

NEW QUESTION 507
- (Topic 6)
What type of port scan is shown below?

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

Answer: C

Explanation:
An Xmas port scan is variant of TCP port scan. This type of scan tries to obtain information about the state of a target port by sending a packet which has multiple TCP flags set to 1 - "lit as an Xmas tree". The flags set for Xmas scan are FIN, URG and PSH. The purpose is to confuse and bypass simple firewalls. Some stateless firewalls only check against security policy those packets which have the SYN flag set (that is, packets that initiate connection according to the standards). Since Xmas scan packets are different, they can pass through these simple systems and reach the target host.

NEW QUESTION 509
- (Topic 6)
War dialing is a very old attack and depicted in movies that were made years ago. Why would a modem security tester consider using such an old technique?

A. It is cool, and if it works in the movies it must work in real life.
B. It allows circumvention of protection mechanisms by being on the internal network.
C. It allows circumvention of the company PBX.
D. A good security tester would not use such a derelict technique.

Answer: B

Explanation:
If you are lucky and find a modem that answers and is connected to the target network, it usually is less protected (as only employees are supposed to know of its existence) and once connected you don't need to take evasive actions towards any firewalls or IDS.

NEW QUESTION 511
- (Topic 6)

Your lab partner is trying to find out more information about a competitors web site. The site has a .com extension. She has decided to use some online whois tools and look in one of the regional Internet registrys. Which one would you suggest she looks in first?

A. LACNIC
B. ARIN
C. APNIC
D. RIPE
E. AfriNIC

Answer: B

Explanation:
Regional registries maintain records from the areas from which they govern. ARIN is responsible for domains served within North and South America and therefore, would be a good starting point for a .com domain.

NEW QUESTION 514
- (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 517
- (Topic 6)
Paul has just finished setting up his wireless network. He has enabled numerous security features such as changing the default SSID, enabling WPA encryption, and enabling MAC filtering on his wireless router. Paul notices that when he uses his wireless connection, the speed is sometimes 54 Mbps and sometimes it is only 24Mbps or less. Paul connects to his wireless router's management utility and notices that a machine with an unfamiliar name is connected through his wireless connection. Paul checks the router's logs and notices that the unfamiliar machine has the same MAC address as his laptop. What is Paul seeing here?

A. MAC spoofing
B. Macof
C. ARP spoofing
D. DNS spoofing

Answer: A

NEW QUESTION 521
- (Topic 6)
John has scanned the web server with NMAP. However, he could not gather enough information to help him identify the operating system running on the remote host accurately.
What would you suggest to John to help identify the OS that is being used on the remote web server?

A. Connect to the web server with a browser and look at the web page.
B. Connect to the web server with an FTP client.
C. Telnet to port 8080 on the web server and look at the default page code.
D. Telnet to an open port and grab the banner.

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 523
- (Topic 6)
What is the essential difference between an ‘Ethical Hacker’ and a ‘Cracker’?

A. The ethical hacker does not use the same techniques or skills as a cracker.
B. The ethical hacker does it strictly for financial motives unlike a cracker.
C. The ethical hacker has authorization from the owner of the target.
D. The ethical hacker is just a cracker who is getting paid.

Answer: C

Explanation:
The ethical hacker uses the same techniques and skills as a cracker and the motive is to find the security breaches before a cracker does. There is nothing that says that a cracker does not get paid for the work he does, a ethical hacker has the owners authorization and will get paid even if he does not succeed to penetrate the target.

NEW QUESTION 527
- (Topic 6)
Snort has been used to capture packets on the network. On studying the packets, the penetration tester finds it to be abnormal. If you were the penetration tester, why would you find this abnormal?
05/20-17:0645.061034 192.160.13.4:31337 --> 172.16.1.101:1
TCP TTL:44 TOS:0x10 ID:242
***FRP** Seq:0xA1D95 Ack:0x53 Win: 0x400
What is odd about this attack? (Choose the most appropriate statement)

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

Answer: B

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

NEW QUESTION 532
- (Topic 6)
You are conducting a port scan on a subnet that has ICMP blocked. You have discovered 23 live systems and after scanning each of them you notice that they all show port 21 in closed state.
What should be the next logical step that should be performed?

A. Connect to open ports to discover applications.
B. Perform a ping sweep to identify any additional systems that might be up.
C. Perform a SYN scan on port 21 to identify any additional systems that might be up.
D. Rescan every computer to verify the results.

Answer: C

Explanation:
As ICMP is blocked you’ll have trouble determining which computers are up and running by using a ping sweep. As all the 23 computers that you had discovered earlier had port 21 closed, probably any additional, previously unknown, systems will also have port 21 closed. By running a SYN scan on port 21 over the target network you might get replies from additional systems.

NEW QUESTION 533
- (Topic 6)
What are two types of ICMP code used when using the ping command?

A. It uses types 0 and 8.
B. It uses types 13 and 14.
C. It uses types 15 and 17.
D. The ping command does not use ICMP but uses UDP.

Answer: A

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

NEW QUESTION 536
- (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 537
- (Topic 6)
Study the log below and identify the scan type.

A. nmap -sR 192.168.1.10
B. nmap -sS 192.168.1.10
C. nmap -sV 192.168.1.10
D. nmap -sO -T 192.168.1.10

Answer: D

NEW QUESTION 539
- (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 543
- (Topic 6)
A distributed port scan operates by:

A. Blocking access to the scanning clients by the targeted host
B. Using denial-of-service software against a range of TCP ports
C. Blocking access to the targeted host by each of the distributed scanning clients
D. Having multiple computers each scan a small number of ports, then correlating the results

Answer: D

Explanation:
Think of dDoS (distributed Denial of Service) where you use a large number of computers to create simultaneous traffic against a victim in order to shut them down.

NEW QUESTION 546
- (Topic 6)
Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security-related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position. Harold is currently trying to run a Sniffer on the agency's network to get an idea of what kind of

traffic is being passed around, but the program he is using does not seem to be capturing anything. He pours through the Sniffer's manual, but cannot find anything that directly relates to his problem. Harold decides to ask the network administrator if he has any thoughts on the problem. Harold is told that the Sniffer was not working because the agency's network is a switched network, which cannot be sniffed by some programs without some tweaking. What technique could Harold use to sniff his agency's switched network?

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

Answer: A

NEW QUESTION 547
- (Topic 6)
What is the disadvantage of an automated vulnerability assessment tool?

A. Ineffective
B. Slow
C. Prone to false positives
D. Prone to false negatives
E. Noisy

Answer: E

Explanation:
Vulnerability assessment tools perform a good analysis of system vulnerabilities; however, they are noisy and will quickly trip IDS systems.

NEW QUESTION 550
- (Topic 6)
What is "Hacktivism"?

A. Hacking for a cause
B. Hacking ruthlessly
C. An association which groups activists
D. None of the above

Answer: A

Explanation:
The term was coined by author/critic Jason Logan King Sack in an article about media artist Shu Lea Cheang. Acts of hacktivism are carried out in the belief that proper use of code will have leveraged effects similar to regular activism or civil disobedience.

NEW QUESTION 551
- (Topic 6)
Which of the following commands runs snort in packet logger mode?

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

Answer: B

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

NEW QUESTION 554
- (Topic 6)
Which one of the following is defined as the process of distributing incorrect Internet Protocol (IP) addresses/names with the intent of diverting traffic?

A. Network aliasing
B. Domain Name Server (DNS) poisoning
C. Reverse Address Resolution Protocol (ARP)
D. Port scanning

Answer: B

Explanation:
This reference is close to the one listed DNS poisoning is the correct answer.
This is how DNS DOS attack can occur. If the actual DNS records are unattainable to the attacker for him to alter in this fashion, which they should be, the attacker can insert this data into the cache of there server instead of replacing the actual records, which is referred to as cache poisoning.

NEW QUESTION 556
- (Topic 6)
What does a type 3 code 13 represent?(Choose two.

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

Answer: BD

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

NEW QUESTION 557
- (Topic 6)
Destination unreachable administratively prohibited messages can inform the hacker to what?

A. That a circuit level proxy has been installed and is filtering traffic
B. That his/her scans are being blocked by a honeypot or jail
C. That the packets are being malformed by the scanning software
D. That a router or other packet-filtering device is blocking traffic
E. That the network is functioning normally

Answer: D

Explanation:
Destination unreachable administratively prohibited messages are a good way to discover that a router or other low-level packet device is filtering traffic. Analysis of the ICMP message will reveal the IP address of the blocking device and the filtered port. This further adds the to the network map and information being discovered about the network and hosts.

NEW QUESTION 558
- (Topic 6)
While performing ping scans into a target network you get a frantic call from the organization’s security team. They report that they are under a denial of service attack. When you stop your scan, the smurf attack event stops showing up on the organization’s IDS monitor. How can you modify your scan to prevent triggering this event in the IDS?

A. Scan more slowly.
B. Do not scan the broadcast IP.
C. Spoof the source IP address.
D. Only scan the Windows systems.

Answer: B

Explanation:
Scanning the broadcast address makes the scan target all IP addresses on that subnet at the same time.

NEW QUESTION 560
- (Topic 6)
You receive an email with the following message: Hello Steve,
We are having technical difficulty in restoring user database record after the recent blackout. Your account data is corrupted. Please logon to the SuperEmailServices.com and change your password.
http://www.supermailservices.com@0xde.0xad.0xbe.0xef/support/logon.htm
If you do not reset your password within 7 days, your account will be permanently disabled locking you out from our e-mail services.
Sincerely, Technical Support
SuperEmailServices
From this e-mail you suspect that this message was sent by some hacker since you have been using their e-mail services for the last 2 years and they have never sent out an e-mail such as this. You also observe the URL in the message and confirm your suspicion about 0xde.0xad.0xbde.0xef which looks like hexadecimal numbers. You immediately enter the following at Windows 2000 command prompt:
Ping 0xde.0xad.0xbe.0xef
You get a response with a valid IP address.
What is the obstructed IP address in the e-mail URL?

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

Answer: A

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

NEW QUESTION 565
- (Topic 6)
Which of the following tools can be used to perform a zone transfer?

A. NSLookup
B. Finger
C. Dig
D. Sam Spade

E. Host
F. Netcat
G. Neotrace

Answer: ACDE

Explanation:
There are a number of tools that can be used to perform a zone transfer. Some of these include: NSLookup, Host, Dig, and Sam Spade.

NEW QUESTION 567
- (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 569
- (Topic 6)
What does an ICMP (Code 13) message normally indicates?

A. It indicates that the destination host is unreachable
B. It indicates to the host that the datagram which triggered the source quench message will need to be re-sent
C. It indicates that the packet has been administratively dropped in transit
D. It is a request to the host to cut back the rate at which it is sending traffic to the Internet destination

Answer: C

Explanation:
CODE 13 and type 3 is destination unreachable due to communication administratively prohibited by filtering hence maybe they meant "code 13", therefore would be C).
Note:
A - Type 3 B - Type 4
C - Type 3 Code 13 D - Typ4 4

NEW QUESTION 572
- (Topic 6)
Which of the following is an automated vulnerability assessment tool?

A. Whack a Mole
B. Nmap
C. Nessus
D. Kismet
E. Jill32

Answer: C

Explanation:
Nessus is a vulnerability assessment tool.

NEW QUESTION 577
- (Topic 6)
Exhibit

Joe Hacker runs the hping2 hacking tool to predict the target host’s sequence numbers in one of the hacking session.
What does the first and second column mean? Select two.

A. The first column reports the sequence number
B. The second column reports the difference between the current and last sequence number
C. The second column reports the next sequence number
D. The first column reports the difference between current and last sequence number

Answer: AB

NEW QUESTION 580
- (Topic 6)
What two things will happen if a router receives an ICMP packet, which has a TTL value of 1, and the destination host is several hops away? (Select 2 answers)

A. The router will discard the packet
B. The router will decrement the TTL value and forward the packet to the next router on the path to the destination host

C. The router will send a time exceeded message to the source host
D. The router will increment the TTL value and forward the packet to the next router on the path to the destination host.
E. The router will send an ICMP Redirect Message to the source host

Answer: AC

NEW QUESTION 583
- (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 585
- (Topic 6)
Exhibit

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

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

Answer: B

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

NEW QUESTION 589
- (Topic 6)
A person approaches a network administrator and wants advice on how to send encrypted email from home. The end user does not want to have to pay for any license fees or manage server services. Which of the following is the most secure encryption protocol that the network administrator should recommend?

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

Answer: C

NEW QUESTION 594
- (Topic 7)
Study the snort rule given below:

From the options below, choose the exploit against which this rule applies.

A. WebDav
B. SQL Slammer
C. MS Blaster
D. MyDoom

Answer: C

Explanation:
MS Blaster scans the Internet for computers that are vulnerable to its attack. Once found, it tries to enter the system through the port 135 to create a buffer overflow. TCP ports 139 and 445 may also provide attack vectors.

NEW QUESTION 597
- (Topic 7)
Jason's Web server was attacked by a trojan virus. He runs protocol analyzer and notices that the trojan communicates to a remote server on the Internet. Shown below is the standard "hexdump" representation of the network packet, before being decoded. Jason wants to identify the trojan by looking at the destination port number and mapping to a trojan-port number database on the Internet. Identify the remote server's port number by decoding the packet?

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

Answer: D

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

NEW QUESTION 599
- (Topic 7)
_____ is the process of converting something from one representation to the simplest form. It deals with the way in which systems convert data from one form to another.

A. Canonicalization
B. Character Mapping
C. Character Encoding
D. UCS transformation formats

Answer: A

Explanation:
Canonicalization (abbreviated c14n) is the process of converting data that has more than one possible representation into a "standard" canonical representation. This can be done to compare different representations for equivalence, to count the number of distinct data structures (e.g., in combinatorics), to improve the efficiency of various algorithms by eliminating repeated calculations, or to make it possible to impose a meaningful sorting order.

NEW QUESTION 600
- (Topic 7)
Erik notices a big increase in UDP packets sent to port 1026 and 1027 occasionally. He enters the following at the command prompt.
$ nc -l -p 1026 -u -v
In response, he sees the following message.
cell(?(c)????STOPALERT77STOP! WINDOWS REQUIRES IMMEDIATE ATTENTION.
Windows has found 47 Critical Errors. To fix the errors please do the following:
1. Download Registry Repair from: www.reg-patch.com
2. Install Registry Repair
3. Run Registry Repair
4. Reboot your computer
1. FAILURE TO ACT NOW MAY LEAD TO DATA LOSS AND CORRUPTION!
What would you infer from this alert?

A. The machine is redirecting traffic to www.reg-patch.com using adware
B. It is a genuine fault of windows registry and the registry needs to be backed up
C. An attacker has compromised the machine and backdoored ports 1026 and 1027
D. It is a messenger spa
E. Windows creates a listener on one of the low dynamic ports from 1026 to 1029 and the message usually promotes malware disguised as legitimate utilities

Answer: D

Explanation:
The "net send" Messenger service can be used by unauthorized users of your computer, without gaining any kind of privileged access, to cause a pop-up window to appear on your computer. Lately, this feature has been used by unsolicited commercial advertisers to inform many campus users about a "university diploma service"...

NEW QUESTION 604
- (Topic 7)
Which of the following algorithms can be used to guarantee the integrity of messages being sent, in transit, or stored? (Choose the best answer)

A. symmetric algorithms
B. asymmetric algorithms

C. hashing algorithms
D. integrity algorithms

Answer: C

Explanation:
In cryptography, a cryptographic hash function is a hash function with certain additional security properties to make it suitable for use as a primitive in various information security applications, such as authentication and message integrity. A hash function takes a long string (or 'message') of any length as input and produces a fixed length string as output, sometimes termed a message digest or a digital fingerprint.

NEW QUESTION 606
- (Topic 7)
How would you describe a simple yet very effective mechanism for sending and receiving unauthorized information or data between machines without alerting any firewalls and IDS's on a network?

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

Answer: A

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

NEW QUESTION 608
- (Topic 7)
Exhibit:
ettercap –NCLzs --quiet
What does the command in the exhibit do in “Ettercap”?

A. This command will provide you the entire list of hosts in the LAN
B. This command will check if someone is poisoning you and will report its IP.
C. This command will detach from console and log all the collected passwords from the network to a file.
D. This command broadcasts ping to scan the LAN instead of ARP request of all the subnet IPs.

Answer: C

Explanation:
-N = NON interactive mode (without ncurses)
-C = collect all users and passwords
-L = if used with -C (collector) it creates a file with all the password sniffed in the session in the form "YYYYMMDD-collected-pass.log"
-z = start in silent mode (no arp storm on start up)
-s = IP BASED sniffing
--quiet = "demonize" ettercap. Useful if you want to log all data in background.

NEW QUESTION 609
- (Topic 7)
Sniffing is considered an active attack.

A. True
B. False

Answer: B

Explanation:
Sniffing is considered a passive attack.

NEW QUESTION 613
- (Topic 7)
Which of the following display filters will you enable in Ethereal to view the three-way handshake for a connection from host 192.168.0.1?

A. ip == 192.168.0.1 and tcp.syn
B. ip.addr = 192.168.0.1 and syn = 1
C. ip.addr==192.168.0.1 and tcp.flags.syn
D. ip.equals 192.168.0.1 and syn.equals on

Answer: C

NEW QUESTION 615
......