Exam Questions CEH-001

Certified Ethical Hacker (CEH)

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

NEW QUESTION 1
- (Topic 1)
Which of the following countermeasure can specifically protect against both the MAC Flood and MAC Spoofing attacks?

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

Answer: A

NEW QUESTION 2
- (Topic 1)
Cyber Criminals have long employed the tactic of masking their true identity. In IP spoofing, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine, by "spoofing" the IP address of that machine.
How would you detect IP spoofing?

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

Answer: D

NEW QUESTION 3
- (Topic 1)
Ursula is a college student at a University in Amsterdam. Ursula originally went to college to study engineering but later changed to marine biology after spending a month at sea with her friends. These friends frequently go out to sea to follow and harass fishing fleets that illegally fish in foreign waters. Ursula eventually wants to put companies practicing illegal fishing out of business. Ursula decides to hack into the parent company's computers and destroy critical data knowing fully well that, if caught, she probably would be sent to jail for a very long time. What would Ursula be considered?

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

Answer: B

NEW QUESTION 4
- (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 5
- (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 6
- (Topic 1)
Bob has set up three web servers on Windows Server 2008 IIS 7.0. Bob has followed all the recommendations for securing the operating system and IIS. These servers are going to run numerous e-commerce websites that are projected to bring in thousands of dollars a day. Bob is still concerned about the security of these servers because of the potential for financial loss. Bob has asked his company's firewall administrator to set the firewall to
inspect all incoming traffic on ports 80 and 443 to ensure that no malicious data is getting into the network.
Why will this not be possible?

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

Answer: C

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

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

Answer: B

NEW QUESTION 8
- (Topic 1)
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 9
- (Topic 1)
In Buffer Overflow exploit, which of the following registers gets overwritten with return address of the exploit code?

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

Answer: D

NEW QUESTION 10
- (Topic 1)
Choose one of the following pseudo codes to describe this statement:
"If we have written 200 characters to the buffer variable, the stack should stop because it cannot hold any more data."

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

Answer: D

NEW QUESTION 10
- (Topic 1)
Jayden is a network administrator for her company. Jayden wants to prevent MAC spoofing on all the Cisco switches in the network. How can she accomplish

this?

A. Jayden can use the comman
B. ip binding set.
C. Jayden can use the comman
D. no ip spoofing.
E. She should use the comman
F. no dhcp spoofing.
G. She can use the comman
H. ip dhcp snooping binding.

Answer: D

NEW QUESTION 12
- (Topic 1)
Google uses a unique cookie for each browser used by an individual user on a computer. This cookie contains information that allows Google to identify records about that user on
its database. This cookie is submitted every time a user launches a Google search, visits a site using AdSense etc. The information stored in Google's database, identified by the cookie, includes
? Everything you search for using Google
? Every web page you visit that has Google Adsense ads
How would you prevent Google from storing your search keywords?

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

Answer: A

NEW QUESTION 14
- (Topic 1)
In Trojan terminology, what is required to create the executable file chess.exe as shown below?

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

Answer: C

NEW QUESTION 16
- (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 21
- (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 25
- (Topic 1)
This attack technique is used when a Web application is vulnerable to an SQL Injection but the results of the Injection are not visible to the attacker.

A. Unique SQL Injection

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

Answer: B

NEW QUESTION 29
- (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 32
- (Topic 1)
Which Steganography technique uses Whitespace to hide secret messages?

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

Answer: A

NEW QUESTION 35
- (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 40
- (Topic 1)
What type of session hijacking attack is shown in the exhibit?

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

Answer: D

NEW QUESTION 45
- (Topic 1)
Stephanie works as a records clerk in a large office building in downtown Chicago. On Monday, she went to a mandatory security awareness class (Security5) put on by her company's IT department. During the class, the IT department informed all employees that everyone's Internet activity was thenceforth going to be monitored.
Stephanie is worried that her Internet activity might give her supervisor reason to write her up, or worse get her fired. Stephanie's daily work duties only consume about four hours of her time, so she usually spends the rest of the day surfing the web. Stephanie really enjoys surfing the Internet but definitely does not want to get fired for it.
What should Stephanie use so that she does not get in trouble for surfing the Internet?

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

Answer: B

NEW QUESTION 46
- (Topic 1)
The SYN flood attack sends TCP connections requests faster than a machine can process them.
? Attacker creates a random source address for each packet
? SYN flag set in each packet is a request to open a new connection to the server from the spoofed IP address
? Victim responds to spoofed IP address, then waits for confirmation that never arrives (timeout wait is about 3 minutes)
? Victim's connection table fills up waiting for replies and ignores new connections
? Legitimate users are ignored and will not be able to access the server
How do you protect your network against SYN Flood attacks?

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

Answer: ABDE

NEW QUESTION 50
- (Topic 1)
Which type of scan does NOT open a full TCP connection?

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

Answer: A

NEW QUESTION 52
- (Topic 1)
Consider the following code:
URL:http://www.certified.com/search.pl? text=<script>alert(document.cookie)</script>
If an attacker can trick a victim user to click a link like this, and the Web application does not validate input, then the victim's browser will pop up an alert showing the users current set of cookies. An attacker can do much more damage, including stealing passwords, resetting your home page, or redirecting the user to another Web site.
What is the countermeasure against XSS scripting?

A. Create an IP access list and restrict connections based on port number
B. Replace "<" and ">" characters with "& l t;" and "& g t;" using server scripts
C. Disable Javascript in IE and Firefox browsers
D. Connect to the server using HTTPS protocol instead of HTTP

Answer: B

NEW QUESTION 53
- (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 54
- (Topic 1)
In what stage of Virus life does a stealth virus gets activated with the user performing certain actions such as running an infected program?

A. Design
B. Elimination
C. Incorporation
D. Replication
E. Launch
F. Detection

Answer: E

NEW QUESTION 56
- (Topic 1)
This IDS defeating technique works by splitting a datagram (or packet) into multiple fragments and the IDS will not spot the true nature of the fully assembled datagram. The datagram is not reassembled until it reaches its final destination. It would be a processor- intensive task for IDS to reassemble all fragments itself, and on a busy system the packet will slip through the IDS onto the network. What is this technique called?

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

Answer: C

NEW QUESTION 58
- (Topic 1)
Which of the following statement correctly defines ICMP Flood Attack? (Select 2 answers)

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

Answer: BD

NEW QUESTION 61
- (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 66
- (Topic 1)
You are the Security Administrator of Xtrinity, Inc. You write security policies and conduct assessments to protect the company's network. During one of your

periodic checks to see how well policy is being observed by the employees, you discover an employee has attached cell phone 3G modem to his telephone line and workstation. He has used this cell phone 3G modem to dial in to his workstation, thereby bypassing your firewall. A security breach has occurred as a direct result of this activity. The employee explains that he used the modem because he had to download software for a department project. How would you resolve this situation?

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

Answer: B

NEW QUESTION 71
- (Topic 1)
Joel and her team have been going through tons of garbage, recycled paper, and other rubbish in order to find some information about the target they are attempting to penetrate. How would you call this type of activity?

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

Answer: A

NEW QUESTION 74
- (Topic 1)
What are the limitations of Vulnerability scanners? (Select 2 answers)

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

Answer: AC

NEW QUESTION 78
- (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 81
- (Topic 1)
Samuel is the network administrator of DataX Communications, Inc. He is trying to configure his firewall to block password brute force attempts on his network. He enables blocking the intruder's IP address for a period of 24 hours' time after more than three unsuccessful attempts. He is confident that this rule will secure his network from hackers on the Internet.
But he still receives hundreds of thousands brute-force attempts generated from various IP addresses around the world. After some investigation he realizes that the intruders are using a proxy somewhere else on the Internet which has been scripted to enable the random usage of various proxies on each request so as not to get caught by the firewall rule.
Later he adds another rule to his firewall and enables small sleep on the password attempt so that if the password is incorrect, it would take 45 seconds to return to the user to begin another attempt. Since an intruder may use multiple machines to brute force the password, he also throttles the number of connections that will be prepared to accept from a particular IP address. This action will slow the intruder's attempts.
Samuel wants to completely block hackers brute force attempts on his network.
What are the alternatives to defending against possible brute-force password attacks on his site?

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

Answer: D

NEW QUESTION 82
- (Topic 1)
You want to capture Facebook website traffic in Wireshark. What display filter should you use that shows all TCP packets that contain the word 'facebook'?

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

Answer: C

NEW QUESTION 86
- (Topic 1)
Bob waits near a secured door, holding a box. He waits until an employee walks up to the secured door and uses the special card in order to access the restricted area of the target company. Just as the employee opens the door, Bob walks up to the employee (still holding the box) and asks the employee to hold the door open so that he can enter. What is the best way to undermine the social engineering activity of tailgating?

A. Issue special cards to access secure doors at the company and provide a one-time only brief description of use of the special card
B. Educate and enforce physical security policies of the company to all the employees on a regular basis
C. Setup a mock video camera next to the special card reader adjacent to the secure door
D. Post a sign that states, "no tailgating" next to the special card reader adjacent to the secure door

Answer: B

NEW QUESTION 90
- (Topic 1)
While performing a ping sweep of a local subnet you receive an ICMP reply of Code 3/Type 13 for all the pings you have sent out. What is the most likely cause of this?

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

Answer: C

NEW QUESTION 94
- (Topic 1)
Jason works in the sales and marketing department for a very large advertising agency located in Atlanta. Jason is working on a very important marketing campaign for his company's largest client. Before the project could be completed and implemented, a competing advertising company comes out with the exact same marketing materials and advertising, thus rendering all the work done for Jason's client unusable. Jason is questioned about this and says he has no idea how all the material ended up in the hands of a competitor.
Without any proof, Jason's company cannot do anything except move on. After working on another high profile client for about a month, all the marketing and sales material again ends up in the hands of another competitor and is released to the public before Jason's company can finish the project. Once again, Jason says that he had nothing to do with it
and does not know how this could have happened. Jason is given leave with pay until they can figure out what is going on.
Jason's supervisor decides to go through his email and finds a number of emails that were sent to the competitors that ended up with the marketing material. The only items in the emails were attached jpg files, but nothing else. Jason's supervisor opens the picture files, but cannot find anything out of the ordinary with them.
What technique has Jason most likely used?

A. Stealth Rootkit Technique
B. ADS Streams Technique
C. Snow Hiding Technique
D. Image Steganography Technique

Answer: D

NEW QUESTION 96
- (Topic 1)
Attackers target HINFO record types stored on a DNS server to enumerate information. These are information records and potential source for reconnaissance. A network administrator has the option of entering host information specifically the CPU type and operating system when creating a new DNS record. An attacker can extract this type of information easily from a DNS server.
Which of the following commands extracts the HINFO record?

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

Answer: A

NEW QUESTION 101

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

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

Answer: D

NEW QUESTION 104
- (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 105
- (Topic 2)
Switches maintain a CAM Table that maps individual MAC addresses on the network to physical ports on the switch.

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

A. Switch then acts as hub by broadcasting packets to all machines on the network
B. The CAM overflow table will cause the switch to crash causing Denial of Service
C. The switch replaces outgoing frame switch factory default MAC address of FF:FF:FF:FF:FF:FF
D. Every packet is dropped and the switch sends out SNMP alerts to the IDS port

Answer: A

NEW QUESTION 108
- (Topic 2)
Every company needs a formal written document which spells out to employees precisely what they are allowed to use the company's systems for, what is prohibited, and what will happen to them if they break the rules. Two printed copies of the policy should be given to every employee as soon as possible after they join the organization. The employee should be asked to sign one copy, which should be safely filed by the company. No one should be allowed to use the company's computer systems until they have signed the policy in acceptance of its terms. What is this document called?

A. Information Audit Policy (IAP)
B. Information Security Policy (ISP)
C. Penetration Testing Policy (PTP)
D. Company Compliance Policy (CCP)

Answer: B

NEW QUESTION 110
- (Topic 2)

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

A. true
B. false

Answer: A

NEW QUESTION 113
- (Topic 2)
Which port, when configured on a switch receives a copy of every packet that passes through it?

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

Answer: C

NEW QUESTION 118
- (Topic 2)
Fred is the network administrator for his company. Fred is testing an internal switch. From an external IP address, Fred wants to try and trick this switch into thinking it already has established a session with his computer. How can Fred accomplish this?

A. Fred can accomplish this by sending an IP packet with the RST/SIN bit and the source address of his computer.
B. He can send an IP packet with the SYN bit and the source address of his computer.
C. Fred can send an IP packet with the ACK bit set to zero and the source address of the switch.
D. Fred can send an IP packet to the switch with the ACK bit and the source address of his machine.

Answer: D

NEW QUESTION 119
- (Topic 2)
What techniques would you use to evade IDS during a Port Scan? (Select 4 answers)

A. Use fragmented IP packets
B. Spoof your IP address when launching attacks and sniff responses from the server
C. Overload the IDS with Junk traffic to mask your scan
D. Use source routing (if possible)
E. Connect to proxy servers or compromised Trojaned machines to launch attacks

Answer: ABDE

NEW QUESTION 121
- (Topic 2)
You receive an e-mail like the one shown below. When you click on the link contained in
the mail, you are redirected to a website seeking you to download free Anti-Virus software. Dear valued customers,
We are pleased to announce the newest version of Antivirus 2010 for Windows which will probe you with total security against the latest spyware, malware, viruses, Trojans and other online threats. Simply visit the link below and enter your antivirus code:

Antivirus code: 5014 http://www.juggyboy/virus/virus.html
Thank you for choosing us, the worldwide leader Antivirus solutions. Mike Robertson
PDF Reader Support
Copyright Antivirus 2010 ?All rights reserved
If you want to stop receiving mail, please go to: http://www.juggyboy.com
or you may contact us at the following address: Media Internet Consultants, Edif. Neptuno, Planta Baja, Ave. Ricardo J. Alfaro, Tumba Muerto, n/a Panama
How will you determine if this is Real Anti-Virus or Fake Anti-Virus website?

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

Answer: C

NEW QUESTION 125
- (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 128
- (Topic 2)
This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.
<ahref="http://foobar.com/index.html?id=%3Cscript%20src=%22http://baddomain.com/bad script.js%22%3E%3C/script%3E">See foobar</a>
What is this attack?

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

D. Buffer Overflow attack

Answer: A

NEW QUESTION 132
- (Topic 2)
Finding tools to run dictionary and brute forcing attacks against FTP and Web servers is an easy task for hackers. They use tools such as arhontus or brutus to break into remote servers.

A command such as this, will attack a given 10.0.0.34 FTP and Telnet servers simultaneously with a list of passwords and a single login namE. linksys. Many FTP-specific password-guessing tools are also available from major security sites.
What defensive measures will you take to protect your network from these attacks?

A. Never leave a default password
B. Never use a password that can be found in a dictionary
C. Never use a password related to your hobbies, pets, relatives, or date of birth.
D. Use a word that has more than 21 characters from a dictionary as the password
E. Never use a password related to the hostname, domain name, or anything else that can be found with whois

Answer: ABCE

NEW QUESTION 135
- (Topic 2)
In this attack, a victim receives an e-mail claiming from PayPal stating that their account has been disabled and confirmation is required before activation. The attackers then scam to collect not one but two credit card numbers, ATM PIN number and other personal details.

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

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

Answer: D

NEW QUESTION 138
- (Topic 2)
You are gathering competitive intelligence on an organization. You notice that they have
jobs listed on a few Internet job-hunting sites. There are two jobs for network and system administrators. How can this help you in foot printing the organization?

A. To learn about the IP range used by the target network
B. To identify the number of employees working for the company
C. To test the limits of the corporate security policy enforced in the company
D. To learn about the operating systems, services and applications used on the network

Answer: D

NEW QUESTION 141
- (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 143
- (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 146
- (Topic 2)
Harold works for Jacobson Unlimited in the IT department as the security manager. Harold has created a security policy requiring all employees to use complex 14 character passwords. Unfortunately, the members of management do not want to have to use such long complicated passwords so they tell Harold's boss this new password policy should not apply to them. To comply with the management's wishes, the IT department creates
another Windows domain and moves all the management users to that domain. This new domain has a password policy only requiring 8 characters.
Harold is concerned about having to accommodate the managers, but cannot do anything about it. Harold is also concerned about using LanManager security on his network instead of NTLM or NTLMv2, but the many legacy applications on the network prevent using the more secure NTLM and NTLMv2. Harold pulls the SAM files from the DC's on the original domain and the new domain using Pwdump6.
Harold uses the password cracking software John the Ripper to crack users' passwords to make sure they are strong enough. Harold expects that the users' passwords in the original domain will take much longer to crack than the management's passwords in the new domain. After running the software, Harold discovers that the 14 character passwords only took a short time longer to crack than the 8 character passwords.
Why did the 14 character passwords not take much longer to crack than the 8 character passwords?

A. Harold should have used Dumpsec instead of Pwdump6
B. Harold's dictionary file was not large enough
C. Harold should use LC4 instead of John the Ripper
D. LanManger hashes are broken up into two 7 character fields

Answer: D

NEW QUESTION 148
- (Topic 2)
Blane is a network security analyst for his company. From an outside IP, Blane performs an XMAS scan using Nmap. Almost every port scanned does not illicit a response. What can he infer from this kind of response?

A. These ports are open because they do not illicit a response.
B. He can tell that these ports are in stealth mode.
C. If a port does not respond to an XMAS scan using NMAP, that port is closed.
D. The scan was not performed correctly using NMAP since all ports, no matter what their state, will illicit some sort of response from an XMAS scan.

Answer: A

NEW QUESTION 150
- (Topic 2)
Attackers send an ACK probe packet with random sequence number, no response means port is filtered (Stateful firewall is present) and RST response means the port is not filtered. What type of Port Scanning is this?

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

Answer: D

NEW QUESTION 154
- (Topic 2)
E-mail tracking is a method to monitor and spy the delivered e-mails to the intended recipient.

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

A. When the e-mail was received and read

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

Answer: H

NEW QUESTION 155
- (Topic 2)
A Trojan horse is a destructive program that masquerades as a benign application. The software initially appears to perform a desirable function for the user prior to installation
and/or execution, but in addition to the expected function steals information or harms the system.

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

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

Answer: B

NEW QUESTION 159
- (Topic 2)
You are footprinting an organization and gathering competitive intelligence. You visit the company's website for contact information and telephone numbers but do not find them listed there. You know they had the entire staff directory listed on their website 12 months ago but now it is not there. Is there any way you can retrieve information from a website that is outdated?

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

Answer: C

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

NEW QUESTION 164
- (Topic 2)
Identify SQL injection attack from the HTTP requests shown below:

A. http://www.myserver.c0m/search.asp? lname=smith%27%3bupdate%20usertable%20set%20passwd%3d%27hAx0r%27%3b--%00
B. http://www.myserver.c0m/script.php?mydata=%3cscript%20src=%22
C. http%3a%2f%2fwww.yourserver.c0m%2fbadscript.js%22%3e%3c%2fscript%3e
D. http://www.victim.com/example accountnumber=67891&creditamount=999999999

Answer: A

NEW QUESTION 165
- (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 169
- (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 172
- (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 177
- (Topic 2)
Fred is scanning his network to ensure it is as secure as possible. Fred sends a TCP probe packet to a host with a FIN flag and he receives a RST/ACK response. What does this mean?

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

Answer: D

NEW QUESTION 178
- (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 181
- (Topic 2)
One of the most common and the best way of cracking RSA encryption is to begin to derive the two prime numbers, which are used in the RSA PKI mathematical process. If the two numbers p and q are discovered through a process, then the private key can be derived.

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

Answer: A

NEW QUESTION 186
- (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 188
- (Topic 2)
Nathan is testing some of his network devices. Nathan is using Macof to try and flood the ARP cache of these switches. If these switches' ARP cache is successfully flooded, what will be the result?

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

Answer: A

NEW QUESTION 193
- (Topic 2)
The programmers on your team are analyzing the free, open source software being used to run FTP services on a server in your organization. They notice that there is excessive number of functions in the source code that might lead to buffer overflow. These C++ functions do not check bounds. Identify the line in the source code that might lead to buffer overflow?

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

Answer: B

NEW QUESTION 196
- (Topic 3)
A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed. Which security policy must the security analyst check to see if dial-out modems are allowed?

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

Answer: C

NEW QUESTION 197
- (Topic 3)
An attacker is attempting to telnet into a corporation's system in the DMZ. The attacker doesn't want to get caught and is spoofing his IP address. After numerous tries he remains unsuccessful in connecting to the system. The attacker rechecks that the target system is
actually listening on Port 23 and he verifies it with both nmap and hping2. He is still unable to connect to the target system. What could be the reason?

A. The firewall is blocking port 23 to that system
B. He needs to use an automated tool to telnet in
C. He cannot spoof his IP and successfully use TCP
D. He is attacking an operating system that does not reply to telnet even when open

Answer: C

NEW QUESTION 198
- (Topic 3)
You are writing security policy that hardens and prevents Footprinting attempt by Hackers. Which of the following countermeasures will NOT be effective against this attack?

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

Answer: F

NEW QUESTION 199
- (Topic 3)
In order to show improvement of security over time, what must be developed?

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

Answer: C

NEW QUESTION 203
- (Topic 3)
SOAP services use which technology to format information?

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

Answer: C

NEW QUESTION 205
- (Topic 3)
Harold just got home from working at Henderson LLC where he works as an IT technician. He was able to get off early because they were not too busy. When he walks into his home office, he notices his teenage daughter on the computer, apparently chatting with someone online. As soon as she hears Harold enter the room, she closes all her windows and tries to act like she was playing a game. When Harold asks her what she was doing, she acts very nervous and does not give him a straight answer. Harold is very concerned because he does not want his daughter to fall victim to online predators and the sort. Harold doesn't necessarily want to install any programs that will restrict the sites his daughter goes to, because he doesn't want to alert her to his trying to figure out what she is doing. Harold wants to use some kind of program that will track her activities online, and send Harold an email of her activity once a day so he can see what she has been up to. What kind of software could Harold use to accomplish this?

A. Install hardware Keylogger on her computer
B. Install screen capturing Spyware on her computer
C. Enable Remote Desktop on her computer
D. Install VNC on her computer

Answer: B

NEW QUESTION 207
- (Topic 3)
Which vital role does the U.S. Computer Security Incident Response Team (CSIRT) provide?

A. Incident response services to any user, company, government agency, or organization in partnership with the Department of Homeland Security
B. Maintenance of the nation’s Internet infrastructure, builds out new Internet infrastructure, and decommissions old Internet infrastructure
C. Registration of critical penetration testing for the Department of Homeland Security and public and private sectors
D. Measurement of key vulnerability assessments on behalf of the Department of Defense (DOD) and State Department, as well as private sectors

Answer: A

NEW QUESTION 208
- (Topic 3)
The traditional traceroute sends out ICMP ECHO packets with a TTL of one, and increments the TTL until the destination has been reached. By printing the gateways that generate ICMP time exceeded messages along the way, it is able to determine the path packets take to reach the destination.
The problem is that with the widespread use of firewalls on the Internet today, many of the packets that traceroute sends out end up being filtered, making it impossible to completely trace the path to the destination.

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

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

Answer: A

NEW QUESTION 212
- (Topic 3)
A security engineer is attempting to map a company’s internal network. The engineer enters in the following NMAP commanD.
NMAP –n –sS –P0 –p 80 ***.***.**.** What type of scan is this?

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

Answer: C

NEW QUESTION 217
- (Topic 3)
John is the network administrator of XSECURITY systems. His network was recently compromised. He analyzes the log files to investigate the attack. Take a look at the following Linux log file snippet. The hacker compromised and "owned" a Linux machine. What is the hacker trying to accomplish here?

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

Answer: D

NEW QUESTION 219
- (Topic 3)
Which of the following processes evaluates the adherence of an organization to its stated security policy?

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

Answer: D

NEW QUESTION 223
- (Topic 3)
Which type of scan measures a person's external features through a digital video camera?

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

Answer: C

NEW QUESTION 225
- (Topic 3)
Which of the following techniques can be used to mitigate the risk of an on-site attacker from connecting to an unused network port and gaining full access to the network? (Choose three.)

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

Answer: ACE

NEW QUESTION 229
- (Topic 3)
Which tool would be used to collect wireless packet data?

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

Answer: A

NEW QUESTION 232
- (Topic 3)
Which of the following can take an arbitrary length of input and produce a message digest output of 160 bit?

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

Answer: A

NEW QUESTION 233
- (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 237
- (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 242
- (Topic 3)
Bank of Timbuktu is a medium-sized, regional financial institution in Timbuktu. The bank has deployed a new Internet-accessible Web application recently. Customers can access their account balances, transfer money between accounts, pay bills and conduct online financial business using a Web browser.
John Stevens is in charge of information security at Bank of Timbuktu. After one month in production, several customers have complained about the Internet enabled banking application. Strangely, the account balances of many of the bank's customers had been changed! However, money hasn't been removed from the bank; instead, money was transferred between accounts. Given this attack profile, John Stevens reviewed the Web application's logs and found the following entries:

What kind of attack did the Hacker attempt to carry out at the bank?

A. Brute force attack in which the Hacker attempted guessing login ID and password from password cracking tools.
B. The Hacker attempted Session hijacking, in which the Hacker opened an account with the bank, then logged in to receive a session ID, guessed the next ID and took over Jason's session.
C. The Hacker used a generator module to pass results to the Web server and exploited Web application CGI vulnerability.
D. The Hacker first attempted logins with suspected user names, then used SQL Injection to gain access to valid bank login IDs.

Answer: D

NEW QUESTION 244
- (Topic 3)
What command would you type to OS fingerprint a server using the command line?

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

Answer: C

NEW QUESTION 245

- (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 249
- (Topic 3)
Which of the following is a hashing algorithm?

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

Answer: A

NEW QUESTION 254
- (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 257
- (Topic 3)
You generate MD5 128-bit hash on all files and folders on your computer to keep a baseline check for security reasons?

What is the length of the MD5 hash?

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

Answer: A

NEW QUESTION 259
- (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 262
- (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 267
- (Topic 3)

A hacker, who posed as a heating and air conditioning specialist, was able to install a
sniffer program in a switched environment network. Which attack could the hacker use to sniff all of the packets in the network?

A. Fraggle
B. MAC Flood
C. Smurf
D. Tear Drop

Answer: B

NEW QUESTION 270
- (Topic 3)
Which of the following Exclusive OR transforms bits is NOT correct?

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

Answer: C

NEW QUESTION 274
- (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 278
- (Topic 3)
Passive reconnaissance involves collecting information through which of the following?

A. Social engineering
B. Network traffic sniffing
C. Man in the middle attacks
D. Publicly accessible sources

Answer: D

NEW QUESTION 283
- (Topic 3)
To see how some of the hosts on your network react, Winston sends out SYN packets to an IP range. A number of IPs respond with a SYN/ACK response. Before the connection is established he sends RST packets to those hosts to stop the session. Winston has done this to see how his intrusion detection system will log the traffic. What type of scan is Winston attempting here?

A. Winston is attempting to find live hosts on your company's network by using an XMAS scan.
B. He is utilizing a SYN scan to find live hosts that are listening on your network.
C. This type of scan he is using is called a NULL scan.
D. He is using a half-open scan to find live hosts on your network.

Answer: D

NEW QUESTION 286
- (Topic 3)
Some passwords are stored using specialized encryption algorithms known as hashes. Why is this an appropriate method?

A. It is impossible to crack hashed user passwords unless the key used to encrypt them is obtained.
B. If a user forgets the password, it can be easily retrieved using the hash key stored by administrators.

C. Hashing is faster compared to more traditional encryption algorithms.
D. Passwords stored using hashes are non-reversible, making finding the password much more difficult.

Answer: D

NEW QUESTION 287
- (Topic 3)
Which of the following describes a component of Public Key Infrastructure (PKI) where a copy of a private key is stored to provide third-party access and to facilitate recovery operations?

A. Key registry
B. Recovery agent
C. Directory
D. Key escrow

Answer: D

NEW QUESTION 288
- (Topic 3)
A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a new document that allowed the forms to be completed, the student decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted.
Which cryptography attack is the student attempting?

A. Man-in-the-middle attack
B. Brute-force attack
C. Dictionary attack
D. Session hijacking

Answer: C

NEW QUESTION 293
- (Topic 3)
A company has five different subnets: 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0 and 192.168.5.0. How can NMAP be used to scan these adjacent Class C networks?

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

Answer: A

NEW QUESTION 294
- (Topic 3)
You are trying to package a RAT Trojan so that Anti-Virus software will not detect it. Which of the listed technique will NOT be effective in evading Anti-Virus scanner?

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

Answer: A

NEW QUESTION 297
- (Topic 4)
A security policy will be more accepted by employees if it is consistent and has the support of

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

Answer: B

NEW QUESTION 301
- (Topic 4)
One advantage of an application-level firewall is the ability to

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

Answer: B

NEW QUESTION 303
- (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 305
- (Topic 4)
What type of OS fingerprinting technique sends specially crafted packets to the remote OS and analyzes the received response?

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

Answer: C

NEW QUESTION 307
- (Topic 4)
While testing the company's web applications, a tester attempts to insert the following test script into the search area on the company's web sitE.
<script>alert(" Testing Testing Testing ")</script>
Afterwards, when the tester presses the search button, a pop-up box appears on the screen with the text: "Testing Testing Testing". Which vulnerability has been detected in the web application?

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

Answer: D

NEW QUESTION 311
- (Topic 4)
Which of the following problems can be solved by using Wireshark?

A. Tracking version changes of source code
B. Checking creation dates on all webpages on a server
C. Resetting the administrator password on multiple systems
D. Troubleshooting communication resets between two systems

Answer: D

NEW QUESTION 316
- (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 321
- (Topic 4)
A hacker was able to sniff packets on a company's wireless network. The following information was discovereD.
The Key 10110010 01001011
The Cyphertext 01100101 01011010
Using the Exlcusive OR, what was the original message?

A. 00101000 11101110
B. 11010111 00010001
C. 00001101 10100100
D. 11110010 01011011

Answer: B

NEW QUESTION 323
- (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 327
- (Topic 4)
Which of the following items is unique to the N-tier architecture method of designing software applications?

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

Answer: A

NEW QUESTION 332
- (Topic 4)
Which NMAP command combination would let a tester scan every TCP port from a class C network that is blocking ICMP with fingerprinting and service detection?

A. NMAP -PN -A -O -sS 192.168.2.0/24
B. NMAP -P0 -A -O -p1-65535 192.168.0/24
C. NMAP -P0 -A -sT -p0-65535 192.168.0/16
D. NMAP -PN -O -sS -p 1-1024 192.168.0/8

Answer: B

NEW QUESTION 335
- (Topic 4)
For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. While using a digital signature, the message digest is encrypted with which key?

A. Sender's public key
B. Receiver's private key
C. Receiver's public key
D. Sender's private key

Answer: D

NEW QUESTION 339
- (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 344
- (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 347
- (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 349
- (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 350
- (Topic 4)
How can rainbow tables be defeated?

A. Password salting
B. Use of non-dictionary words
C. All uppercase character passwords
D. Lockout accounts under brute force password cracking attempts

Answer: A

NEW QUESTION 351
- (Topic 4)
Which method can provide a better return on IT security investment and provide a thorough and comprehensive assessment of organizational security covering policy, procedure design, and implementation?

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

Answer: A

NEW QUESTION 355
- (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 358
- (Topic 4)
Which of the following is an application that requires a host application for replication?

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

Answer: D

NEW QUESTION 363
- (Topic 4)
A company firewall engineer has configured a new DMZ to allow public systems to be located away from the internal network. The engineer has three security zones set:
Untrust (Internet) – (Remote network = 217.77.88.0/24) DMZ (DMZ) – (11.12.13.0/24)
Trust (Intranet) – (192.168.0.0/24)
The engineer wants to configure remote desktop access from a fixed IP on the remote network to a remote desktop server in the DMZ. Which rule would best fit this requirement?

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

Answer: B

NEW QUESTION 367
- (Topic 4)
What is the purpose of conducting security assessments on network resources?

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

Answer: B

NEW QUESTION 368
- (Topic 4)
What is the outcome of the comm"nc -l -p 2222 | nc 10.1.0.43 1234"?

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

Answer: B

NEW QUESTION 373
- (Topic 4)
A developer for a company is tasked with creating a program that will allow customers to update their billing and shipping information. The billing address field used is limited to 50 characters. What pseudo code would the developer use to avoid a buffer overflow attack on the billing address field?

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

Answer: D

NEW QUESTION 374
- (Topic 4)
To reduce the attack surface of a system, administrators should perform which of the following processes to remove unnecessary software, services, and insecure configuration settings?

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

Answer: C

NEW QUESTION 378
- (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 381
- (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 386
- (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 388
- (Topic 4)
Which of the following guidelines or standards is associated with the credit card industry?

A. Control Objectives for Information and Related Technology (COBIT)
B. Sarbanes-Oxley Act (SOX)
C. Health Insurance Portability and Accountability Act (HIPAA)
D. Payment Card Industry Data Security Standards (PCI DSS)

Answer: D

NEW QUESTION 393
- (Topic 4)
A penetration tester is attempting to scan an internal corporate network from the internet without alerting the border sensor. Which is the most efficient technique should the tester consider using?

A. Spoofing an IP address
B. Tunneling scan over SSH
C. Tunneling over high port numbers
D. Scanning using fragmented IP packets

Answer: B

NEW QUESTION 396
- (Topic 4)
If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

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

Answer: A

NEW QUESTION 401
- (Topic 4)
Smart cards use which protocol to transfer the certificate in a secure manner?

A. Extensible Authentication Protocol (EAP)
B. Point to Point Protocol (PPP)
C. Point to Point Tunneling Protocol (PPTP)
D. Layer 2 Tunneling Protocol (L2TP)

Answer: A

NEW QUESTION 405
- (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 406
- (Topic 4)
What is the main difference between a “Normal” SQL Injection and a “Blind” SQL Injection vulnerability?

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

Answer: D

NEW QUESTION 409
- (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 412
- (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 415
- (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 420
- (Topic 4)
A computer technician is using a new version of a word processing software package when it is discovered that a special sequence of characters causes the entire computer to crash. The technician researches the bug and discovers that no one else experienced the problem. What is the appropriate next step?

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

Answer: D

NEW QUESTION 421
- (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 426
- (Topic 5)
Which of the following are variants of mandatory access control mechanisms? (Choose two.)

A. Two factor authentication

B. Acceptable use policy
C. Username / password
D. User education program
E. Sign in register

Answer: AC

NEW QUESTION 427
- (Topic 5)
While performing data validation of web content, a security technician is required to restrict malicious input. Which of the following processes is an efficient way of restricting malicious input?

A. Validate web content input for query strings.
B. Validate web content input with scanning tools.
C. Validate web content input for type, length, and range.
D. Validate web content input for extraneous queries.

Answer: C

NEW QUESTION 428
- (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 429
- (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 434
- (Topic 5)
A penetration tester is hired to do a risk assessment of a company's DMZ. The rules of engagement states that the penetration test be done from an external IP address with no prior knowledge of the internal IT systems. What kind of test is being performed?

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

Answer: D

NEW QUESTION 437
- (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 440
- (Topic 5)
What is the main advantage that a network-based IDS/IPS system has over a host-based solution?

A. They do not use host system resources.
B. They are placed at the boundary, allowing them to inspect all traffic.
C. They are easier to install and configure.
D. They will not interfere with user interfaces.

Answer: A

NEW QUESTION 444
- (Topic 5)
Which security control role does encryption meet?

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

Answer: A

NEW QUESTION 448
- (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 452
- (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 457
- (Topic 5)
What results will the following command yielD. 'NMAP -sS -O -p 123-153 192.168.100.3'?

A. A stealth scan, opening port 123 and 153
B. A stealth scan, checking open ports 123 to 153
C. A stealth scan, checking all open ports excluding ports 123 to 153
D. A stealth scan, determine operating system, and scanning ports 123 to 153

Answer: D

NEW QUESTION 461
- (Topic 5)
Which of the following is a hardware requirement that either an IDS/IPS system or a proxy server must have in order to properly function?

A. Fast processor to help with network traffic analysis
B. They must be dual-homed
C. Similar RAM requirements
D. Fast network interface cards

Answer: B

NEW QUESTION 462
- (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 463
- (Topic 5)
An NMAP scan of a server shows port 25 is open. What risk could this pose?

A. Open printer sharing
B. Web portal data leak
C. Clear text authentication
D. Active mail relay

Answer:

D

NEW QUESTION 467
- (Topic 5)
An NMAP scan of a server shows port 69 is open. What risk could this pose?

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

Answer: A

NEW QUESTION 472
- (Topic 5)
Which of the following tools would be the best choice for achieving compliance with PCI Requirement 11?

A. Truecrypt
B. Sub7
C. Nessus
D. Clamwin

Answer: C

NEW QUESTION 477
- (Topic 5)
A recently hired network security associate at a local bank was given the responsibility to perform daily scans of the internal network to look for unauthorized devices. The employee decides to write a script that will scan the network for unauthorized devices every morning at 5:00 am.
Which of the following programming languages would most likely be used?

A. PHP
B. C#
C. Python
D. ASP.NET

Answer: C

NEW QUESTION 481
- (Topic 5)
During a penetration test, a tester finds a target that is running MS SQL 2000 with default credentials. The tester assumes that the service is running with Local System account. How can this weakness be exploited to access the system?

A. Using the Metasploit psexec module setting the SA / Admin credential
B. Invoking the stored procedure xp_shell to spawn a Windows command shell
C. Invoking the stored procedure cmd_shell to spawn a Windows command shell
D. Invoking the stored procedure xp_cmdshell to spawn a Windows command shell

Answer: D

NEW QUESTION 483
- (Topic 5)
A Network Administrator was recently promoted to Chief Security Officer at a local university. One of employee's new responsibilities is to manage the implementation of an RFID card access system to a new server room on campus. The server room will house student enrollment information that is securely backed up to an off-site location.
During a meeting with an outside consultant, the Chief Security Officer explains that he is concerned that the existing security controls have not been designed properly. Currently, the Network Administrator is responsible for approving and issuing RFID card access to the server room, as well as reviewing the electronic access logs on a weekly basis.
Which of the following is an issue with the situation?

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

Answer: A

NEW QUESTION 488
- (Topic 5)
A tester is attempting to capture and analyze the traffic on a given network and realizes that the network has several switches. What could be used to successfully sniff the traffic on this switched network? (Choose three.)

A. ARP spoofing
B. MAC duplication
C. MAC flooding
D. SYN flood
E. Reverse smurf attack
F. ARP broadcasting

Answer: ABC

NEW QUESTION 490
- (Topic 5)
Which of the following network attacks relies on sending an abnormally large packet size that exceeds TCP/IP specifications?

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

Answer: A

NEW QUESTION 495
- (Topic 5)
A hacker searches in Google for filetype:pcf to find Cisco VPN config files. Those files may contain connectivity passwords that can be decoded with which of the following?

A. Cupp
B. Nessus
C. Cain and Abel
D. John The Ripper Pro

Answer: C

NEW QUESTION 498
- (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 501
- (Topic 5)
Which of the following techniques will identify if computer files have been changed?

A. Network sniffing
B. Permission sets
C. Integrity checking hashes
D. Firewall alerts

Answer: C

NEW QUESTION 506
- (Topic 5)
A security engineer has been asked to deploy a secure remote access solution that will allow employees to connect to the company's internal network. Which of the following can be implemented to minimize the opportunity for the man-in-the-middle attack to occur?

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

Answer: C

NEW QUESTION 510
- (Topic 5)
Pentest results indicate that voice over IP traffic is traversing a network. Which of the following tools will decode a packet capture and extract the voice conversations?

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

Answer: A

NEW QUESTION 514
- (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 515
- (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 519
- (Topic 5)
Which property ensures that a hash function will not produce the same hashed value for two different messages?

A. Collision resistance
B. Bit length
C. Key strength
D. Entropy

Answer: A

NEW QUESTION 524
- (Topic 5)
An IT security engineer notices that the company's web server is currently being hacked. What should the engineer do next?

A. Unplug the network connection on the company's web server.
B. Determine the origin of the attack and launch a counterattack.
C. Record as much information as possible from the attack.
D. Perform a system restart on the company's web server.

Answer: C

NEW QUESTION 528
- (Topic 5)
Which technical characteristic do Ethereal/Wireshark, TCPDump, and Snort have in common?

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

Answer: D

NEW QUESTION 529
- (Topic 5)
Which of the following levels of algorithms does Public Key Infrastructure (PKI) use?

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

Answer: A

NEW QUESTION 532
- (Topic 5)
Which set of access control solutions implements two-factor authentication?

A. USB token and PIN
B. Fingerprint scanner and retina scanner
C. Password and PIN
D. Account and password

Answer: A

NEW QUESTION 536

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

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

Answer: A

NEW QUESTION 538
- (Topic 5)
A certified ethical hacker (CEH) is approached by a friend who believes her husband is cheating. She offers to pay to break into her husband's email account in order to find proof so she can take him to court. What is the ethical response?

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

Answer: A

NEW QUESTION 540
- (Topic 5)
Which protocol and port number might be needed in order to send log messages to a log analysis tool that resides behind a firewall?

A. UDP 123
B. UDP 541
C. UDP 514
D. UDP 415

Answer: C

NEW QUESTION 543
- (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 544
- (Topic 5)
Which of the following does proper basic configuration of snort as a network intrusion detection system require?

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

Answer: A

NEW QUESTION 548
- (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 550
- (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 551
- (Topic 6)
One of your team members has asked you to analyze the following SOA record. What is the version?
Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600
3600 604800 2400.

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

Answer: A

Explanation:
The SOA starts with the format of YYYYMMDDVV where VV is the version.

NEW QUESTION 554
- (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 557
- (Topic 6)
What is the proper response for a NULL scan if the port is closed?

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

Answer: E

Explanation:
Closed ports respond to a NULL scan with a reset.

NEW QUESTION 558
- (Topic 6)
What are the two basic types of attacks? (Choose two.

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

Answer: BD

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

NEW QUESTION 560
- (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 561
- (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 566
- (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 569
- (Topic 6)
According to the CEH methodology, what is the next step to be performed after footprinting?

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

Answer: B

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

NEW QUESTION 574
- (Topic 6)
Where should a security tester be looking for information that could be used by an attacker against an organization? (Select all that apply)

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

Answer: ABCDEF

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

NEW QUESTION 575
- (Topic 6)
MX record priority increases as the number increases. (True/False.

A. True
B. False

Answer: B

Explanation:

The highest priority MX record has the lowest number.

NEW QUESTION 579
- (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 583
- (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 584
- (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 588
- (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 589
- (Topic 6)
Which of the following systems would not respond correctly to an nmap XMAS scan?

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

Answer: A

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

NEW QUESTION 593
- (Topic 6)
What ICMP message types are used by the ping command?

A. Timestamp request (13) and timestamp reply (14)
B. Echo request (8) and Echo reply (0)
C. Echo request (0) and Echo reply (1)
D. Ping request (1) and Ping reply (2)

Answer: B

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

NEW QUESTION 597
- (Topic 6)
Which type of Nmap scan is the most reliable, but also the most visible, and likely to be picked up by and IDS?

A. SYN scan
B. ACK scan
C. RST scan
D. Connect scan
E. FIN scan

Answer: D

Explanation:
The TCP full connect (-sT) scan is the most reliable.

NEW QUESTION 598
- (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 600
- (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 601
- (Topic 6)
Name two software tools used for OS guessing? (Choose two.

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

Answer: AC

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

NEW QUESTION 606
- (Topic 6)
Neil notices that a single address is generating traffic from its port 500 to port 500 of several other machines on the network. This scan is eating up most of the network bandwidth and Neil is concerned. As a security professional, what would you infer from this scan?

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

Answer: D

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

NEW QUESTION 611
- (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 613
- (Topic 6)
John is using a special tool on his Linux platform that has a signature database and is therefore able to detect hundred of vulnerabilities in UNIX, Windows, and commonly-used web CGI scripts. Additionally, the database detects DDoS zombies and Trojans. What would be the name of this multifunctional tool?

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

Answer: C

Explanation:
Nessus is the world's most popular vulnerability scanner, estimated to be used by over 75, 000 organizations world-wide. Nmap is mostly used for scanning, not for detecting vulnerabilities. Hping is a free packet generator and analyzer for the TCP/IP protocol and make is used to automatically build large applications on the *nix plattform.

NEW QUESTION 614
- (Topic 6)
When Nmap performs a ping sweep, which of the following sets of requests does it send to the target device?

A. ICMP ECHO_REQUEST & TCP SYN
B. ICMP ECHO_REQUEST & TCP ACK
C. ICMP ECHO_REPLY & TFP RST
D. ICMP ECHO_REPLY & TCP FIN

Answer: B

Explanation:
The default behavior of NMAP is to do both an ICMP ping sweep (the usual kind of ping) and a TCP port 80 ACK ping sweep. If an admin is logging these this will be fairly characteristic of NMAP.

NEW QUESTION 615
- (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 618
- (Topic 6)
Botnets are networks of compromised computers that are controlled remotely and surreptitiously by one or more cyber criminals. How do cyber criminals infect a victim's computer with bots? (Select 4 answers)

A. Attackers physically visit every victim's computer to infect them with malicious software
B. Home computers that have security vulnerabilities are prime targets for botnets
C. Spammers scan the Internet looking for computers that are unprotected and use these "open-doors" to install malicious software
D. Attackers use phishing or spam emails that contain links or attachments
E. Attackers use websites to host the bots utilizing Web Browser vulnerabilities

Answer: BCDE

Explanation:
New Questions

NEW QUESTION 621
- (Topic 6)
You are scanning into the target network for the first time. You find very few conventional ports open. When you attempt to perform traditional service identification by connecting to the open ports, it yields either unreliable or no results. You are unsure of which protocols are being used. You need to discover as many different protocols as possible.
Which kind of scan would you use to achieve this? (Choose the best answer)

A. Nessus scan with TCP based pings.
B. Nmap scan with the –sP (Ping scan) switch.
C. Netcat scan with the –u –e switches.
D. Nmap with the –sO (Raw IP packets) switch.

Answer: D

Explanation:
Running Nmap with the –sO switch will do a IP Protocol Scan. The IP protocol scan is a bit different than the other nmap scans. The IP protocol scan is searching for additional IP protocols in use by the remote station, such as ICMP, TCP, and UDP. If a router is scanned, additional IP protocols such as EGP or IGP may be identified.

NEW QUESTION 625
- (Topic 6)
What port scanning method involves sending spoofed packets to a target system and then looking for adjustments to the IPID on a zombie system?

A. Blind Port Scanning
B. Idle Scanning
C. Bounce Scanning
D. Stealth Scanning
E. UDP Scanning

Answer: B

Explanation:
From NMAP:
-sI <zombie host[:probeport]> Idlescan: This advanced scan method allows for a truly blind
TCP port scan of the target (meaning no packets are sent to the tar- get from your real IP address). Instead, a unique side-channel attack exploits predictable "IP fragmentation ID" sequence generation on the zombie host to glean information about the open ports on the target.

NEW QUESTION 626
- (Topic 6)
_____ is found in all versions of NTFS and is described as the ability to fork file data into existing files without affecting their functionality, size, or display to traditional file browsing utilities like dir or Windows Explorer

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

Answer: A

NEW QUESTION 629
- (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 632
- (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 636
- (Topic 6)
A very useful resource for passively gathering information about a target company is:

A. Host scanning
B. Whois search
C. Traceroute
D. Ping sweep

Answer: B

Explanation:
A, C & D are "Active" scans, the question says: "Passively"

NEW QUESTION 639
- (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 640
- (Topic 6)
Doug is conducting a port scan of a target network. He knows that his client target network has a web server and that there is a mail server also which is up and running. Doug has been sweeping the network but has not been able to elicit any response from the remote target. Which of the following could be the most likely cause behind this lack of response? Select 4.

A. UDP is filtered by a gateway
B. The packet TTL value is too low and cannot reach the target
C. The host might be down
D. The destination network might be down
E. The TCP windows size does not match
F. ICMP is filtered by a gateway

Answer: ABCF

Explanation:
If the destination host or the destination network is down there is no way to get an answer and if TTL (Time To Live) is set too low the UDP packets will "die" before reaching the host because of too many hops between the scanning computer and the target. The TCP receive window size is the amount of received data (in bytes) that can be buffered during a connection. The sending host can send only that amount of data before it must wait for an acknowledgment and window update from the receiving host and ICMP is mainly used for echo requests and not in port scans.

NEW QUESTION 642

- (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 647
- (Topic 6)
Peter extracts the SIDs list from Windows 2000 Server machine using the hacking tool “SIDExtractor”. Here is the output of the SIDs:

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

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

Answer: F

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

NEW QUESTION 648
- (Topic 6)
What is the proper response for a X-MAS scan if the port is closed?

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

Answer: E

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

NEW QUESTION 651
- (Topic 6)
Because UDP is a connectionless protocol: (Select 2)

A. UDP recvfrom() and write() scanning will yield reliable results
B. It can only be used for Connect scans
C. It can only be used for SYN scans
D. There is no guarantee that the UDP packets will arrive at their destination

E. ICMP port unreachable messages may not be returned successfully

Answer: DE

Explanation:
Neither UDP packets, nor the ICMP errors are guaranteed to arrive, so UDP scanners must also implement retransmission of packets that appear to be lost (or you will get a bunch of false positives).

NEW QUESTION 655
- (Topic 7)
Exhibit:

Study the following log extract and identify the attack.

A. Hexcode Attack
B. Cross Site Scripting
C. Multiple Domain Traversal Attack
D. Unicode Directory Traversal Attack

Answer: D

Explanation:
The “Get /msadc/……/……/……/winnt/system32/cmd.exe?” shows that a Unicode Directory Traversal Attack has been performed.

NEW QUESTION 657
- (Topic 7)
Which of the following is not considered to be a part of active sniffing?

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

Answer: C

NEW QUESTION 659
- (Topic 7)
What is the proper response for a NULL scan if the port is open?

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

Answer: F

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

NEW QUESTION 662
- (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 667
......