GIAC.GCIH.v2022-05-19.q135

Exam Code:	GCIH
Exam Name:	GIAC Certified Incident Handler
Certification Provider:	GIAC
Free Question Number:	135
Version:	v2022-05-19
# of views:	712
# of Questions views:	13389
https://www.freecram.net/torrent/GIAC.GCIH.v2022-05-19.q135.html	

NEW QUESTION: 1
Which of the following penetration testing phases involves reconnaissance or data gathering?
A. Pre-attack phase
B. Out-attack phase
C. Post-attack phase
D. Attack phase
Answer: A (LEAVE A REPLY)

NEW QUESTION: 2
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 setting up a DMZ.
B. You cannot, you need an IDS.
C. By examining your domain controller server logs.
D. By examining your firewall logs.
Answer: (SHOW ANSWER)

NEW QUESTION: 3
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. Create incident checklists.
C. Create new sub-team to keep check.

D. Appoint someone else to check the procedures.
Answer: (SHOW ANSWER)

NEW QUESTION: 4
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. Vulnerabilities that allow a remote cracker to access sensitive data on a system
B. Vulnerabilities that allow a remote cracker to control sensitive data on a system
C. Vulnerabilities that help in Code injection attacks
D. Misconfiguration (e.g. open mail relay, missing patches, etc.)
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Which of the following tools is used for vulnerability scanning and calls Hydra to launch a dictionary attack?
A. Nessus
B. Whishker
C. Nmap
D. SARA
Answer: (SHOW ANSWER)

NEW QUESTION: 6
Which of the following is executed when a predetermined event occurs?
A. Logic bomb
B. Trojan horse
C. Worm
D. MAC
Answer: (SHOW ANSWER)

NEW QUESTION: 7
Which of the following is a version of netcat with integrated transport encryption capabilities?
A. Encat
B. Nikto
C. Socat
D. Cryptcat
Answer: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 8
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. 0xFFFFFFFFFFFF
B. 0xAAAAAAAAAA
C. 0x00000000000
D. 0xDDDDDDDDD
Answer: (SHOW ANSWER)

NEW QUESTION: 9
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. Cheops
B. Traceroute
C. Ettercap
D. NeoTrace
Answer: (SHOW ANSWER)

NEW QUESTION: 10
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. ARP spoofing
B. Cross-site scripting
C. Session fixation
D. Session sidejacking
Answer: (SHOW ANSWER)

NEW QUESTION: 11

Which of the following procedures is designed to enable security personnel to identify, mitigate, and recover from
malicious computer incidents, such as unauthorized access to a system or data, denialof-service, or unauthorized
changes to system hardware, software, or data?
A. Crisis Communication Plan
B. Disaster Recovery Plan
C. Cyber Incident Response Plan
D. Occupant Emergency Plan
Answer: (SHOW ANSWER)

NEW QUESTION: 12
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. SNMP enumeration
B. DNS zone transfer
C. NetBIOS NULL session
D. IIS buffer overflow
Answer: (SHOW ANSWER)

NEW QUESTION: 13
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: (SHOW ANSWER)

NEW QUESTION: 14
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. Security was not compromised as the webpage was hosted internally.
B. Security was compromised as keylogger is invisible for firewall.
C. The attack was social engineering and the firewall did not detect it.
D. The attack was Cross Site Scripting and the firewall blocked it.
Answer: (SHOW ANSWER)

NEW QUESTION: 15
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 User Name Mapping on the file servers in the network.
C. Configure ADRMS on the file servers in the network.
D. Enable the Network File System (NFS) component on the file servers in the network.
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Which of the following types of channels is used by Trojans for communication?
A. Loop channel
B. Open channel
C. Overt channel
D. Covert channel
Answer: (SHOW ANSWER)

NEW QUESTION: 17

Maria works as the Chief Security Officer for PassGuide 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. Public-key cryptography

B. Steganography

C. Encryption

D. RSA algorithm

Answer: (SHOW ANSWER)

NEW QUESTION: 18

US Garments wants all encrypted data communication between corporate office and remote location.

They want to achieve following results:

* I Authentication of users

* I Anti-replay

* I Anti-spoofing

* I IP packet encryption

They implemented IPSec using Authentication Headers (AHs). Which results does this solution provide?

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: (SHOW ANSWER)

Section: Volume C

NEW QUESTION: 19

What is the purpose of configuring a password protected screen saver on a computer?

A. For preventing a system from a social engineering attack.

B. For preventing a system from a back door attack.

C. For preventing unauthorized access to a system.

D. For preventing a system from a Denial of Service (DoS) attack.

Answer: (SHOW ANSWER)

NEW QUESTION: 20

Which of the following attacks capture the secret value like a hash and reuse it later to gain access to a system without ever decrypting or decoding the hash?

A. Cross Site Scripting attack

B. Hashing attack

C. Rainbow attack
D. Replay attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 21
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 setting up a DMZ.
D. By examining your firewall logs.
Answer: (SHOW ANSWER)

NEW QUESTION: 22
Which of the following Nmap commands is used to perform a UDP port scan?
A. nmap -sS
B. nmap -sN
C. nmap -sY
D. nmap -sU
Answer: (SHOW ANSWER)

NEW QUESTION: 23
SIMULATION
Fill in the blank with the appropriate word.
StackGuard (as used by Immunix), ssp/ProPolice (as used by OpenBSD), and Microsoft's /GS option use
_____ defense against buffer overflow attacks.
Answer:
canary

NEW QUESTION: 24
Which of the following programs is used for bypassing normal authentication for securing remote access to a computer?
A. Spyware
B. Worm
C. Adware
D. Backdoor
Answer: (SHOW ANSWER)

NEW QUESTION: 25

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

A. Spoofing

B. Social engineering

C. OS Fingerprinting

D. Reconnaissance

Answer: (SHOW ANSWER)

NEW QUESTION: 26

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 Fair Credit Reporting Act (FCRA)

B. The Equal Credit Opportunity Act (ECOA)

C. The Electronic Communications Privacy Act of 1986 (ECPA)

D. Federal Information Security Management Act of 2002 (FISMA)

Answer: (SHOW ANSWER)

NEW QUESTION: 27

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. Trojan horse

C. Social Engineering

D. Session Hijacking

Answer: (SHOW ANSWER)

NEW QUESTION: 28

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 (LEAVE A REPLY)

Section: Volume A

NEW QUESTION: 29

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. Session Hijacking
B. Social Engineering
C. Dictionary attack
D. Trojan horse
Answer: (SHOW ANSWER)

NEW QUESTION: 30
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. Evil Twin
C. Virus
D. Denial of Service
Answer: (SHOW ANSWER)

NEW QUESTION: 31
Which of the following is a network worm that exploits the RPC sub-system vulnerability present in the Microsoft Windows operating system?
A. Win32/Agent
B. WMA/TrojanDownloader.GetCodec
C. Win32/PSW.OnLineGames
D. Win32/Conflicker
Answer: (SHOW ANSWER)

NEW QUESTION: 32
Which of the following tools can be used for network sniffing as well as for intercepting conversations through session hijacking?
A. IPChains
B. Tripwire
C. Hunt
D. Ethercap

Answer: (SHOW ANSWER)

NEW QUESTION: 33
Which of the following viruses/worms uses the buffer overflow attack?
A. Code red worm
B. Nimda virus
C. Klez worm
D. Chernobyl (CIH) virus
Answer: A (LEAVE A REPLY)

NEW QUESTION: 34
Which of the following characters will you use to check whether an application is vulnerable to an SQL injection
attack?
A. Semi colon (;)
B. Double quote (")
C. Dash (-)
D. Single quote (')
Answer: (SHOW ANSWER)

NEW QUESTION: 35
SIMULATION
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
Answer:
Egress filtering

NEW QUESTION: 36
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. Nessus
B. GFI LANguard
C. EtherApe
D. Pwdump
Answer: (SHOW ANSWER)

NEW QUESTION: 37
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. Grayware
B. Firmware
C. Melissa
D. Hardware
Answer: (SHOW ANSWER)

NEW QUESTION: 38
You want to measure the number of heaps used and overflows occurred at a point in time. Which of the following commands will you run to activate the appropriate monitor?
A. UPDATE DBM CONFIGURATION USING DFT_MON_TABLE
B. UPDATE DBM CONFIGURATION USING DFT_MON_BUFPOOL
C. UPDATE DBM CONFIGURATION DFT_MON_TIMESTAMP
D. UPDATE DBM CONFIGURATION USING DFT_MON_SORT
Answer: D (LEAVE A REPLY)

NEW QUESTION: 39
Which of the following applications is an example of a data-sending Trojan?
A. Senna Spy Generator
B. Firekiller 2000
C. eBlaster
D. SubSeven
Answer: C (LEAVE A REPLY)

NEW QUESTION: 40
Which of the following is a technique for creating Internet maps?
Each correct answer represents a complete solution. Choose two.

A. Active Probing
B. AS PATH Inference
C. Object Relational Mapping
D. Network Quota
Answer: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 41
Which of the following applications automatically calculates cryptographic hashes of all key system files that are to be monitored for modifications?
A. TCPView
B. Inzider
C. Tripwire
D. PrcView
Answer: (SHOW ANSWER)

NEW QUESTION: 42
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: (SHOW ANSWER)
Section: Volume C

NEW QUESTION: 43
Which of the following penetration testing phases involves reconnaissance or data gathering?
A. Pre-attack phase
B. Attack phase
C. Out-attack phase
D. Post-attack phase
Answer: (SHOW ANSWER)

NEW QUESTION: 44
In which of the following malicious hacking steps does email tracking come under?
A. Scanning
B. Maintaining Access
C. Gaining access
D. Reconnaissance
Answer: (SHOW ANSWER)

NEW QUESTION: 45
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: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 46
Which of the following attacks capture the secret value like a hash and reuse it later to gain access to a system without ever decrypting or decoding the hash?
A. Cross Site Scripting attack
B. Replay attack
C. Rainbow attack
D. Hashing attack
Answer: (SHOW ANSWER)
Section: Volume C

NEW QUESTION: 47
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. Attribute-based Access Control
B. Discretionary Access Control
C. Mandatory Access Control
D. Role-based Access Control
Answer: (SHOW ANSWER)

NEW QUESTION: 48
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. SYN scan
B. Nmap
C. IDLE scan

D. Host port scan
Answer: (SHOW ANSWER)

NEW QUESTION: 49
Fill in the blank with the appropriate term.
_____ is a technique used to make sure that incoming packets are actually from the networks that they claim to be from.
Answer:
Ingress filtering

NEW QUESTION: 50
Which of the following statements are true about netcat?
Each correct answer represents a complete solution. Choose all that apply.

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

NEW QUESTION: 51
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. Session hijacking
C. Man-in-the-middle
D. ARP spoofing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 52
Which of the following ensures that a party to a dispute cannot deny the authenticity of their signature on a
document or the sending of a message that they originated?
A. OS fingerprinting
B. Confidentiality
C. Reconnaissance
D. Non-repudiation
Answer: (SHOW ANSWER)

NEW QUESTION: 53
Which of the following are countermeasures to prevent unauthorized database access attacks?

Each correct answer represents a complete solution. Choose all that apply.

A. Session encryption

B. Applying strong firewall rules

C. Removing all stored procedures

D. Input sanitization

Answer: (SHOW ANSWER)

NEW QUESTION: 54

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 "PassGuide" - 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)

21.203 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

23.108 ms 14 0.so-4-1-0.TL1.ATL5.ALTER.NET (152.63.10.129) 37.894 ms 33.244 ms 33.910 ms 15 0.so-7-0-0.XL1.MIA4.ALTER.NET (152.63.86.189) 51.165 ms 49.935 ms 49.466 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 PassGuidegw1. customer.alter.net (65.195.239.14)

51.921 ms 51.571 ms 56.855 ms 19 www.PassGuide.com (65.195.239.22) 52.191 ms 52.571 ms 56.855 ms 20 www.PassGuide.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: (SHOW ANSWER)

Section: Volume A

NEW QUESTION: 55
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. Identification
B. Preparation
C. Recovery
D. Containment
Answer: (SHOW ANSWER)

NEW QUESTION: 56
Which of the following statements are true about tcp wrappers?
Each correct answer represents a complete solution. Choose all that apply.
A. tcp wrapper protects a Linux server from IP address spoofing.
B. 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.
C. tcp wrapper provides access control, host address spoofing, client username lookups, etc.
D. When a user uses a TCP wrapper, the inetd daemon runs the wrapper program tcpd instead of running the server
program directly.
Answer: (SHOW ANSWER)

NEW QUESTION: 57
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. Unused Sectors
B. Slack space
C. Hidden partition
D. Dumb space
Answer: (SHOW ANSWER)

NEW QUESTION: 58

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 PGIAC 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 mysql_real_escape_string() function for escaping input
B. Use the escapeshellarg() function
C. Use the escapeshellcmd() function
D. Use the session_regenerate_id() function
Answer: (SHOW ANSWER)

NEW QUESTION: 59
Which of the following attacks can be overcome by applying cryptography?
A. Buffer overflow
B. DoS
C. Sniffing
D. Web ripping
Answer: (SHOW ANSWER)

NEW QUESTION: 60
Which of the following Denial-of-Service (DoS) attacks employ IP fragmentation mechanism?
Each correct answer represents a complete solution. Choose two.

A. Ping of Death attack
B. Teardrop attack
C. Land attack
D. SYN flood attack
Answer: (SHOW ANSWER)

NEW QUESTION: 61
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: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 62
You are responsible for security at a company that uses a lot of Web applications. You are most concerned about flaws in those applications allowing some attacker to get into your network. What method would be best for finding such flaws?
A. Manual penetration testing
B. Code review
C. Vulnerability scanning
D. Automated penetration testing
Answer: (SHOW ANSWER)

NEW QUESTION: 63
Which of the following applications automatically calculates cryptographic hashes of all key system files that are to be
monitored for modifications?
A. PrcView
B. TCPView
C. Inzider
D. Tripwire
Answer: (SHOW ANSWER)

NEW QUESTION: 64
What is the purpose of configuring a password protected screen saver on a computer?
A. For preventing a system from a back door attack.
B. For preventing unauthorized access to a system.
C. For preventing a system from a Denial of Service (DoS) attack.
D. For preventing a system from a social engineering attack.
Answer: (SHOW ANSWER)

NEW QUESTION: 65
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. Blue Pill
D. chkrootkit
Answer: (SHOW ANSWER)

NEW QUESTION: 66
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. Password cracking
C. Teardrop
D. IP address spoofing
Answer: (SHOW ANSWER)

NEW QUESTION: 67
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. mysql_real_escape_string()
B. regenerateid()
C. escapeshellarg()
D. escapeshellcmd()
Answer: (SHOW ANSWER)

NEW QUESTION: 68
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.
Which of the following types of attack has occurred?
A. Injection
B. Virus
C. Worm
D. Denial-of-service
Answer: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 69
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: (SHOW ANSWER)

NEW QUESTION: 70
Which of the following Trojans is used by attackers to modify the Web browser settings?
A. Trojan.Lodear
B. WMA/TrojanDownloader.GetCodec
C. Win32/Pacex.Gen
D. Win32/FlyStudio
Answer: (SHOW ANSWER)

NEW QUESTION: 71
Victor works as a professional Ethical Hacker for SecureEnet Inc. He wants to scan the wireless network of the
company. He uses a tool that is a free open-source utility for network exploration. The tool uses raw IP packets to
determine the following:
What ports are open on our network systems.
What hosts are available on the network.
Identify unauthorized wireless access points.
What services (application name and version) those hosts are offering.
What operating systems (and OS versions) they are running.
What type of packet filters/firewalls are in use.
Which of the following tools is Victor using?
A. Kismet
B. Nessus
C. Nmap
D. Sniffer
Answer: (SHOW ANSWER)

NEW QUESTION: 72
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. Gaining access

C. Reconnaissance

D. Covering tracks

Answer: (SHOW ANSWER)

NEW QUESTION: 73

Which of the following malicious software travels across computer networks without the assistance of a user?

A. Virus

B. Trojan horses

C. Worm

D. Hoax

Answer: (SHOW ANSWER)

NEW QUESTION: 74

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

A. escapeshellcmd()

B. strip_tags()

C. htmlentities()

D. escapeshellarg()

Answer: (SHOW ANSWER)

NEW QUESTION: 75

Adam, a malicious hacker is running a scan. Statistics of the scan is as follows:
Scan directed at open port: ClientServer
192.5.2.92:4079 ---------FIN--------->192.5.2.110:23192.5.2.92:4079 <----NO RESPONSE-----192.5.2.110:23
Scan directed at closed port:
ClientServer
192.5.2.92:4079 ---------FIN--------->192.5.2.110:23
192.5.2.92:4079<-----RST/ACK----------192.5.2.110:23
Which of the following types of port scan is Adam running?

A. XMAS scan

B. FIN scan

C. Idle scan

D. ACK scan

Answer: (SHOW ANSWER)

NEW QUESTION: 76
Which of the following is used to determine the operating system on the remote computer in a network
environment?
A. Social engineering
B. OS Fingerprinting
C. Reconnaissance
D. Spoofing
Answer: (SHOW ANSWER)

NEW QUESTION: 77
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: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 78
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: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 79
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. Port scanning
B. Setting up a honey pot
C. Vulnerability scanning
D. Setting up IDS
Answer: (SHOW ANSWER)

NEW QUESTION: 80
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. SubSeven
B. eBlaster
C. NetBus
D. Qaz
Answer: (SHOW ANSWER)

NEW QUESTION: 81
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: B,D (LEAVE A REPLY)

NEW QUESTION: 82
Which of the following types of skills are required in the members of an incident handling team? Each correct answer represents a complete solution. Choose all that apply.

A. Diplomatic skills
B. Technical skills
C. Organizational skills
D. Methodical skills
Answer: (SHOW ANSWER)

NEW QUESTION: 83
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: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 84
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. Reconnaissance
B. Mutual authentication
C. Role-based access control
D. Multi-factor authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 85
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: (SHOW ANSWER)
Section: Volume C
Explanation

NEW QUESTION: 86
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. Session Hijacking
B. Denial of Service
C. Spyware
D. Ping Flood
Answer: (SHOW ANSWER)

NEW QUESTION: 87
Which of the following applications is NOT used for passive OS fingerprinting?

A. p0f
B. Satori
C. Networkminer
D. Nmap
Answer: (SHOW ANSWER)

NEW QUESTION: 88
Which of the following is used to gather information about a remote network protected by a firewall?

A. Wardialing
B. Firechalking
C. Warchalking
D. Firewalking
Answer: (SHOW ANSWER)

NEW QUESTION: 89
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: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 90
Which of the following penetration testing phases involves reconnaissance or data gathering?

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

D. Out-attack phase
Answer: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 91
You work as a Network Administrator for InformSec Inc. You find that the TCP port number 23476 is open on your server. You suspect that there may be a Trojan named Donald Dick installed on your server. Now you want to verify whether Donald Dick is installed on it or not. For this, you want to know the process running on port 23476, as well as the process id, process name, and the path of the process on your server. Which of the following applications will you most likely use to accomplish the task?
A. Tripwire
B. SubSeven
C. Netstat
D. Fport
Answer: (SHOW ANSWER)
Section: Volume A
Explanation/Reference:

NEW QUESTION: 92
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: (SHOW ANSWER)
Section: Volume A

NEW QUESTION: 93
Which of the following is the process of comparing cryptographic hash functions of system executables and configuration files?
A. Reconnaissance
B. Shoulder surfing
C. Spoofing
D. File integrity auditing
Answer: (SHOW ANSWER)

NEW QUESTION: 94
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 target site should authenticate in GET and POST parameters, not only cookies.
C. The target site should have limited lifetime authentication cookies.
D. The attacker must target a site that doesn't check the referrer header.
Answer: (SHOW ANSWER)

NEW QUESTION: 95
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 escapeshellcmd() function
B. Use the session_regenerate_id() function
C. Use the mysql_real_escape_string() function for escaping input
D. Use the escapeshellarg() function
Answer: (SHOW ANSWER)

NEW QUESTION: 96
You work as a System Administrator in SunSoft Inc. You are running a virtual machine on Windows Server
2003. The virtual machine is protected by DPM. Now, you want to move the virtual machine to another host.
Which of the following steps can you use to accomplish the task?
Each correct answer represents a part of the solution. Choose all that apply.
A. Remove the original virtual machine from the old server and stop the protection for the original virtual machine.

B. Run consistency check.
C. Add the copied virtual machine to a protection group.
D. Copy the virtual machine to the new server.
Answer: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 97
Which of the following types of rootkits replaces regular application binaries with Trojan fakes and modifies the
behavior of existing applications using hooks, patches, or injected code?
A. Boot loader rootkit
B. Kernel level rootkit
C. Hypervisor rootkit
D. Application level rootkit
Answer: (SHOW ANSWER)

NEW QUESTION: 98
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?
Each correct answer represents a complete solution. Choose all that apply.
A. Authentication of users
B. IP packet encryption
C. Anti-spoofing
D. Anti-replay
Answer: (SHOW ANSWER)

NEW QUESTION: 99
You want to perform passive footprinting against we-are-secure Inc. Web server. Which of the following tools will you use?
A. Nmap
B. Ethereal
C. Ettercap
D. Netcraft
Answer: (SHOW ANSWER)

Section: Volume B

NEW QUESTION: 100

In which of the following methods does an hacker use packet sniffing to read network traffic between two parties to steal the session cookies?

A. Cross-site scripting
B. Physical accessing
C. Session fixation
D. Session sidejacking
Answer: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 101

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 Wireshark.
B. You will use the ftp service.
C. You will use CryptCat instead of NetCat.
D. You will use brutus.
Answer: (SHOW ANSWER)

NEW QUESTION: 102

Which of the following are types of access control attacks?
Each correct answer represents a complete solution. Choose all that apply.
A. Spoofing
B. Brute force attack
C. Dictionary attack
D. Mail bombing
Answer: (SHOW ANSWER)

Section: Volume A

NEW QUESTION: 103
Which of the following techniques is used when a system performs the penetration testing with the objective of accessing unauthorized information residing inside a computer?
A. Phreaking
B. Port scanning
C. Biometrician
D. Van Eck Phreaking
Answer: (SHOW ANSWER)

NEW QUESTION: 104
When you conduct the XMAS scanning using Nmap, you find that most of the ports scanned do not give a response. What can be the state of these ports?
A. Filtered
B. Open
C. Closed
Answer: (SHOW ANSWER)
Section: Volume C
Explanation

NEW QUESTION: 105
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: (SHOW ANSWER)
Section: Volume A

NEW QUESTION: 106
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. Place a honey pot in the DMZ.
B. Implement network based antivirus.
C. Shorten the timeout for connection attempts.
D. Implement a strong password policy.
Answer: (SHOW ANSWER)

NEW QUESTION: 107
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 (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 108
You work as a Network Administrator for InformSec Inc. You find that the TCP port number 23476 is open on your server. You suspect that there may be a Trojan named Donald Dick installed on your server. Now you want to verify whether Donald Dick is installed on it or not. For this, you want to know the process running on port 23476, as well as the process id, process name, and the path of the process on your server. Which of the following applications will you most likely use to accomplish the task?
A. Tripwire
B. SubSeven
C. Netstat
D. Fport
Answer: D (LEAVE A REPLY)
Section: Volume A
Explanation

NEW QUESTION: 109
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: (SHOW ANSWER)

NEW QUESTION: 110

Which of the following tools can be used to detect the steganography?

A. Dskprobe

B. Blindside

C. ImageHide

D. Snow

Answer: (SHOW ANSWER)

Section: Volume A

NEW QUESTION: 111

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. Keystroke logging

C. Hacking

D. Session hijacking

Answer: (SHOW ANSWER)

NEW QUESTION: 112

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:

* Information gathering
* Determining network range
* Identifying active machines
* Finding open ports and applications
* OS fingerprinting
* 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. Cheops
C. NeoTrace
D. Traceroute
Answer: (SHOW ANSWER)

NEW QUESTION: 113
You work as a System Administrator in SunSoft Inc. You are running a virtual machine on Windows Server 2003. The
virtual machine is protected by DPM. Now, you want to move the virtual machine to another host. Which of the
following steps can you use to accomplish the task?
Each correct answer represents a part of the solution. Choose all that apply.
A. Remove the original virtual machine from the old server and stop the protection for the original virtual machine.
B. Run consistency check.
C. Add the copied virtual machine to a protection group.
D. Copy the virtual machine to the new server.
Answer: (SHOW ANSWER)

NEW QUESTION: 114
Adam works as a Network Administrator for PassGuide Inc. He wants to prevent the network from DOS attacks. Which of the following is most useful against DOS attacks?
A. Honey Pot
B. Distributive firewall
C. SPI
D. Internet bot
Answer: C (LEAVE A REPLY)

NEW QUESTION: 115
Which of the following are based on malicious code?
Each correct answer represents a complete solution. Choose two.
A. Denial-of-Service (DoS)
B. Biometrics
C. Trojan horse
D. Worm
Answer: (SHOW ANSWER)
Section: Volume C

NEW QUESTION: 116

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. Virus

B. Smurf

C. Denial of Service

D. Evil Twin

Answer: (SHOW ANSWER)

NEW QUESTION: 117

Which of the following commands can be used for port scanning?

A. nc -g

B. nc -w

C. nc -t

D. nc -z

Answer: (SHOW ANSWER)

NEW QUESTION: 118

Against which of the following does SSH provide protection?

Each correct answer represents a complete solution. Choose two.

A. Password sniffing

B. Broadcast storm

C. IP spoofing

D. DoS attack

Answer: (SHOW ANSWER)

NEW QUESTION: 119

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

A. rsync

B. smbclient

C. mutt

D. scp

Answer: (SHOW ANSWER)

NEW QUESTION: 120

An attacker sends a large number of packets to a target computer that causes denial of service.
Which of the following type of attacks is this?

A. Flooding

B. Snooping

C. Spoofing

D. Phishing

Answer: (SHOW ANSWER)

NEW QUESTION: 121
Which of the following rootkits adds additional code or replaces portions of an operating system, including both the kernel and associated device drivers?
A. Hypervisor rootkit
B. Kernel level rootkit
C. Library rootkit
D. Boot loader rootkit
Answer: (SHOW ANSWER)

NEW QUESTION: 122
Adam works as an Incident Handler for Umbrella Inc. He is informed by the senior authorities that the server of the
marketing department has been affected by a malicious hacking attack. Supervisors are also claiming that some
sensitive data are also stolen.
Adam immediately arrived to the server room of the marketing department and identified the event as an incident.
He isolated the infected network from the remaining part of the network and started preparing to image the entire
system. He captures volatile data, such as running process, ram, and network connections.
Which of the following steps of the incident handling process is being performed by Adam?
A. Identification
B. Recovery
C. Containment
D. Eradication
Answer: (SHOW ANSWER)

NEW QUESTION: 123
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 create a snapshot of the virtual machine.
B. Use the Virtualization Management Console to save the state of the virtual machine.
C. Use the Edit Virtual Hard Disk Wizard to copy the virtual hard disk of the virtual machine.
D. Log on to the virtual host and create a new dynamically expanding virtual hard disk.
Answer: (SHOW ANSWER)

NEW QUESTION: 124
Which of the following tools combines two programs, and also encrypts the resulting package in an attempt to foil antivirus programs?
A. Tiny
B. Trojan Man
C. NetBus
D. EliteWrap
Answer: (SHOW ANSWER)

NEW QUESTION: 125
Fill in the blank with the appropriate name of the rootkit.
A _____ rootkit uses device or platform firmware to create a persistent malware image.
Answer:
firmware

NEW QUESTION: 126
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. strcat()
B. strlength()
C. printf()
D. strcpy()
Answer: (SHOW ANSWER)

NEW QUESTION: 127

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 CryptCat instead of NetCat.
C. You will use Wireshark.
D. You will use brutus.
Answer: (SHOW ANSWER)

NEW QUESTION: 128
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 perform banner grabbing to the hosts given in the IP address list.
B. You want to perform port scanning to the hosts given in the IP address list.
C. You want to put nmap in the listen mode 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: (SHOW ANSWER)

NEW QUESTION: 129
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 Emergency Management System (NEMS)
C. National Disaster Management System (NDMS)
D. National Incident Management System (NIMS)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 130
You want to create an SSH tunnel for POP and SMTP protocols. Which of the following commands will you run?

A. ssh -L 110:mailhost:110 -L 25:mailhost:25 -1
B. ssh -L 110:mailhost:110 -L 25
C. ssh -L 25:mailhost:110 -L 110
D. ssh -L 110:mailhost:110 -L 25:mailhost:25 -1 user -N mailhost
Answer: (SHOW ANSWER)

NEW QUESTION: 131
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 is still vulnerable to ping sweep attack.
B. Network is now vulnerable to Ping of death attack.
C. Network turns completely immune from the ping sweep attacks.
D. Network is protected from the ping sweep attack until the next reboot of the server.
Answer: (SHOW ANSWER)

NEW QUESTION: 132
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 PATH Inference
B. Path MTU discovery (PMTUD)
C. AS Route Inference
D. Firewalking
Answer: (SHOW ANSWER)

NEW QUESTION: 133
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 (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 134
Adam works as a Security Analyst for Umbrella Inc. CEO of the company ordered him to implement two-factor authentication for the employees to access their networks. He has told him that he would like to use some type of hardware device in tandem with a security or identifying pin number. Adam decides to implement smart cards but they are not cost effective.
Which of the following types of hardware devices will Adam use to implement two-factor authentication?
A. Biometric device
B. Security token
C. Proximity cards
D. One Time Password
Answer: (SHOW ANSWER)
Section: Volume C

NEW QUESTION: 135
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: (SHOW ANSWER)
Section: Volume C