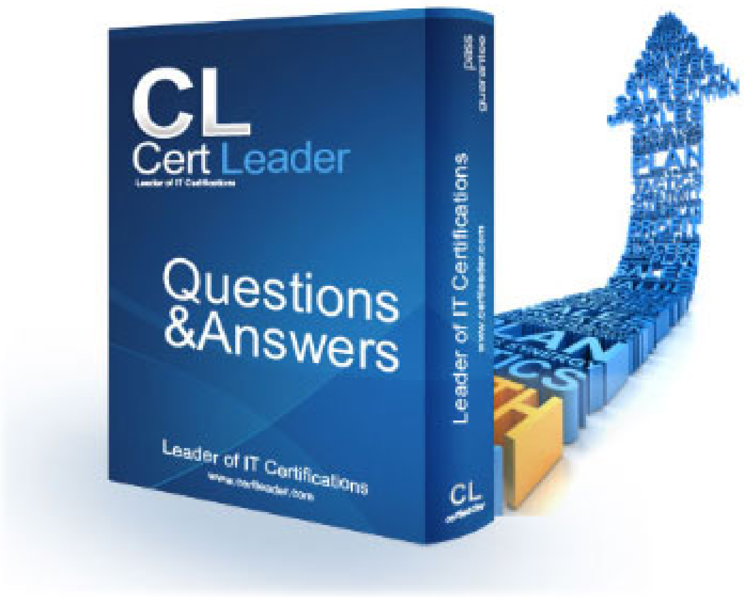
GSEC Dumps

GIAC Security Essentials Certification

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



NEW QUESTION 1
Which of the following protocols is used to send e-mails on the Internet?

A. SMTP
B. IMAP4
C. POP3
D. HTTP

Answer: A

NEW QUESTION 2
Which of the following is a Layer 3 device that will typically drop directed broadcast traffic?

A. Hubs
B. Bridges
C. Routers
D. Switches

Answer: C

NEW QUESTION 3
What is the maximum passphrase length in Windows 2000/XP/2003?

A. 255 characters
B. 127 characters
C. 95 characters
D. 63 characters

Answer: B

NEW QUESTION 4
Which class of IDS events occur when the IDS fails to alert on malicious data?

A. True Negative
B. True Positive
C. False Positive
D. False Negative

Answer: D

NEW QUESTION 5
Which of the following should be implemented to protect an organization from spam?

A. Auditing
B. System hardening
C. E-mail filtering
D. Packet filtering

Answer: C

NEW QUESTION 6
Which of the following radio frequencies is used by the IEEE 802.11a wireless network?

A. 3.7 GHz
B. 7.0 GHz
C. 2.4 GHz
D. 5.0 GHz

Answer: D

NEW QUESTION 7
During a scheduled evacuation training session the following events took place in this order:
* 1. Evacuation process began by triggering the building fire alarm.
* 2a. The meeting point leader arrived first at the designated meeting point and immediately began making note of who was and was not accounted for.
* 2b. Stairwell and door monitors made it to their designated position to leave behind a box of flashlights and prop the stairway doors open with a garbage can so employees can find exits and dispose of food and beverages.
2c. Special needs assistants performed their assigned responsibility to help employees out that require special assistance.
* 3. The safety warden communicated with the meeting point leader via walkie talkie to collect a list of missing personnel and communicated this information back to the searchers.
* 4. Searchers began checking each room and placing stick-it notes on the bottom of searched doors to designate which areas were cleared.
* 5. All special need assistants and their designated wards exited the building.
* 6. Searchers complete their assigned search pattern and exit with the Stairwell/door monitors.
Given this sequence of events, which role is in violation of its expected evacuation tasks?

A. Safety warden

B. Stairwell and door monitors
C. Meeting point leader
D. Searchers
E. Special needs assistants

Answer: B

NEW QUESTION 8
What database can provide contact information for Internet domains?

A. dig
B. who
C. who is
D. ns look up

Answer: C

NEW QUESTION 9
You work as a Network Administrator for Rick International. The company has a TCP/IP-based network. A user named Kevin wants to set an SSH terminal at home to connect to the company's network. You have to configure your company's router for it. By default, which of the following standard ports does the SSH protocol use for connection?

A. 443
B. 22
C. 21
D. 80

Answer: B

NEW QUESTION 10
Which of the following is a name, symbol, or slogan with which a product is identified?

A. Copyright
B. Trademark
C. Trade secret
D. Patent

Answer: B

NEW QUESTION 10
You work as a Network Administrator for Net World Inc. The company has a Linux-based network. You are optimizing performance and security on your Web server. You want to know the ports that are listening to FTP. Which of the following commands will you use?

A. netstat -a | grep FTP
B. FTP netstat -r
C. FTP netstat -a
D. netstat -r | grep FTP

Answer: A

NEW QUESTION 12
Which of the following choices accurately describes how PGP works when encrypting email?

A. PGP encrypts the message with the recipients public key, then encrypts this key with a random asymmetric ke
B. PGP creates a random asymmetric key that it uses to encrypt the message, then encrypts this key with the recipient's public key
C. PGP creates a random symmetric key that it uses to encrypt the message, then encrypts this key with the recipient's public key
D. PGP encrypts the message with the recipients public key, then encrypts this key with a random symmetric ke

Answer: B

NEW QUESTION 16
Which of the following protocols work at the Session layer of the OSI model? Each correct
answer represents a complete solution. Choose all that apply.

A. Border Gateway Multicast Protocol (BGMP)
B. Internet Security Association and Key Management Protocol (ISAKMP)
C. Trivial File Transfer Protocol (TFTP)
D. User Datagram Protocol (UDP)

Answer: AB

NEW QUESTION 17
Which of the following fields CANNOT be hashed by Authentication Header (AH) in transport mode?

A. Length

B. Source IP
C. TTL
D. Destination IP

Answer: C

NEW QUESTION 21
John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. John is working as a root user on the Linux operating system. He is currently working on his C based new traceroute program. Since, many processes are running together on the system, he wants to give the highest priority to the cc command process so that he can test his program, remove bugs, and submit it to the office in time. Which of the following commands will John use to give the highest priority to the cc command process?

A. nice -n 19 cc -c *.c &
B. nice cc -c *.c &
C. nice -n -20 cc -c *.c &
D. nice cc -c *.c

Answer: C

NEW QUESTION 23
When designing wireless networks, one strategy to consider is implementing security mechanisms at all layers of the OSI model. Which of the following protection mechanisms would protect layer 1?

A. Hardening applications
B. Limit RF coverage
C. Employing firewalls
D. Enabling strong encryption

Answer: B

NEW QUESTION 28
Which type of risk assessment results are typically categorized as low, medium, or high-risk events?

A. Technical
B. Qualitative
C. Management
D. Quantitative

Answer: B

NEW QUESTION 32
Which of the following protocols implements VPN using IPSec?

A. SLIP
B. PPP
C. L2TP
D. PPTP

Answer: C

NEW QUESTION 33
Which of the following best describes the level of risk associated with using proprietary crypto algorithms.?

A. Proprietary cryptographic algorithms are required by law to use shorter key lengths in the United States, so the risk is hig
B. Proprietary algorithms have not been subjected to public scrutiny, so they have been checked less throughly for vulnerabilitie
C. Proprietary algorithms are less likely be vulnerable than algorithms that have been publicly disclosed because of enhanced secrecy of the algorith
D. Proprietary algorithms are not known to generally be any more or less vulnerable than publicly scrutinized algorithm

Answer: B

NEW QUESTION 35
Which choice best describes the line below?
alert tcp any any -> 192.168.1.0/24 80 (content: /cgi-bin/test.cgi"; msg: "Attempted
CGI-BIN Access!!";)

A. Tcpdump filter
B. IP tables rule
C. Wire shark filter
D. Snort rule

Answer: D

NEW QUESTION 37
When discussing access controls, which of the following terms describes the process of determining the activities or functions that an Individual is permitted to perform?

A. Authentication
B. Identification
C. Authorization
D. Validation

Answer: C

NEW QUESTION 39
Which of the following applications would be BEST implemented with UDP instead of TCP?

A. A multicast streaming applicatio
B. A web browse
C. A DNS zone transfe
D. A file transfer applicatio

Answer: A

NEW QUESTION 42
Which Linux file lists every process that starts at boot time?

A. inetd
B. netsrv
C. initd
D. inittab

Answer: D

NEW QUESTION 45
What is the name of the Windows XP/2003 tool that you can use to schedule commands to be executed on remote systems during off-peak hours?

A. SCHTASKS.EXE
B. SCHEDULETSKS.EXE
C. SCHEDULR.EXE
D. SCHRUN.EXE

Answer: A

NEW QUESTION 48
Which of the following Unix syslog message priorities is the MOST severe?

A. err
B. emerg
C. crit
D. alert

Answer: B

NEW QUESTION 49
You work as a Network Administrator for McNeil Inc. The company has a Linux-based network. David, a Sales Manager, wants to know the name of the shell that he is currently using. Which of the following commands will he use to accomplish the task?

A. mv $shell
B. echo $shell
C. rm $shell
D. ls $shell

Answer: B

NEW QUESTION 54
An organization monitors the hard disks of its employees' computers from time to time. Which policy does this pertain to?

A. Privacy policy
B. Backup policy
C. User password policy
D. Network security policy

Answer: A

NEW QUESTION 59
You ask your system administrator to verify user compliance with the corporate policies on password strength, namely that all passwords will have at least one numeral, at least one letter, at least one special character and be 15 characters long. He comes to you with a set of compliance tests for use with an offline password cracker. They are designed to examine the following parameters of the password:
* they contain only numerals
* they contain only letters
* they contain only special characters

* they contain only letters and numerals
" they contain only letters and special characters
* they contain only numerals and special characters
Of the following, what is the benefit to using this set of tests?

A. They are focused on cracking passwords that use characters prohibited by the password policy
B. They find non-compliant passwords without cracking compliant password
C. They are focused on cracking passwords that meet minimum complexity requirements
D. They crack compliant and non-compliant passwords to determine whether the current policy is strong enough

Answer: B

NEW QUESTION 63
Which of the following monitors program activities and modifies malicious activities on a system?

A. Back door
B. HIDS
C. NIDS
D. RADIUS

Answer: B

NEW QUESTION 65
An employee is currently logged into the corporate web server, without permission. You log into the web server as 'admin" and look for the employee's username: "dmaul" using the "who" command. This is what you get back:

A. The contents of the /var/log/messages file has been altered
B. The contents of the bash history file has been altered
C. The contents of the utmp file has been altered
D. The contents of the http logs have been altered

Answer: B

NEW QUESTION 68
What is the term for a game in which for every win there must be an equivalent loss?

A. Asymmetric
B. Untenable
C. Zero-sum
D. Gain-oriented

Answer: C

NEW QUESTION 71
Which of the following is a benefit to utilizing Cygwin for Windows?

A. The ability to install a complete Red Hat operating system Install on Window
B. The ability to bring much more powerful scripting capabilities to Window
C. The ability to run a production Apache serve
D. The ability to install a complete Ubuntu operating system install on Window

Answer: A

NEW QUESTION 74
While building multiple virtual machines on a single host operating system, you have determined that each virtual machine needs to work on the network as a

separate entity with its own unique IP address on the same logical subnet. You also need to limit each guest operating system to how much system resources it has access to. Which of the following correctly identifies steps that must be taken towards setting up these virtual environments?

A. The virtual machine software must define a separate virtual network Interface to each virtual machine and then define which unique logical hard drive partition should be available to the guest operating syste
B. The virtual machine software must define a separate virtual network interface since each system needs to have an IP address on the same logical subnet requiring they use the same physical interface on the host operating syste
C. The virtual machine software must define a separate virtual network interface to each virtual machine as well as how much RAM should be available to each virtual machin
D. The virtual machine software establishes the existence of the guest operating systems and the physical system resources to be used by that system will be configured from within the guest operating syste
E. The virtual machine software must define a separate physical network interface to each virtual machine so that the guest operating systems can have unique IP addresses and then define how much of the systems RAM is available to the guest operating syste

Answer: E

NEW QUESTION 78
Which of the following classes of fire comes under Class C fire?

A. Paper or wood fire
B. Oil fire
C. Combustible metals fire
D. Electronic or computer fire

Answer: D

NEW QUESTION 82
Which of the following statements regarding the Secure Sockets Layer (SSL) security model are true?
Each correct answer represents a complete solution. Choose two.

A. The client can optionally authenticate the serve
B. The client always authenticates the serve
C. The server always authenticates the clien
D. The server can optionally authenticate the clien

Answer: BD

NEW QUESTION 87
You are an Intrusion Detection Analyst and the system has alerted you to an Event of Interest (EOI) that appears to be activity generated by a worm. You investigate and find that the network traffic was normal. How would this type of alert be categorized?

A. False Positive
B. True Negative
C. True Positive
D. False Negative

Answer: A

NEW QUESTION 88
Which of the following is required to be backed up on a domain controller to recover Active Directory?

A. System state data
B. Operating System files
C. User's personal data
D. Installed third party application's folders

Answer: A

NEW QUESTION 89
What is the key difference between Electronic Codebook mode and other block cipher modes like Cipher Block Chaining, Cipher-Feedback and Output-Feedback?

A. Plaintext patterns are concealed by XO Ring with previous cipher text block but input to the block cipher is not randomize
B. Plaintext patterns are concealed and input to the block cipher is randomized by XO Ring with previous cipher text bloc
C. Plaintext patterns encrypted with the same key will always generate the same Cipher text pattern
D. Plaintext patterns are not concealed but input to the block cipher is randomized by XO Ring with previous cipher text bloc

Answer: C

NEW QUESTION 93
John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. He is working as a root user on the Linux operating system. He wants to delete his private.txt file from his operating system. He knows that the deleted file can be recovered easily. Hence, he wants to delete the file securely. He wants to hide the shredding, and so he desires to add a final overwrite of the file private.txt with zero. Which of the following commands will John use to accomplish his task?

A. rmdir -v private.txt
B. shred -vfu private.txt
C. shred -vfuz private.txt

D. rm -vf private.txt

Answer: C

NEW QUESTION 95
When a host on a remote network performs a DNS lookup of www.google.com, which of the following is likely to provide an Authoritative reply?

A. The local DNS server
B. The top-level DNS server for .com
C. The DNS server for google.com
D. The root DNS server

Answer: A

NEW QUESTION 97
The process of enumerating all hosts on a network defines which of the following activities?

A. Port scanning
B. Vulnerability scanning
C. GPS mapping
D. Network mapping

Answer: D

NEW QUESTION 101
Which of the following is an UDP based protocol?

A. telnet
B. SNMP
C. IMAP
D. LDAP

Answer: B

NEW QUESTION 105
Which of the following protocols describes the operation of security In H.323? A. H.239

A. H.245
B. H.235
C. H.225

Answer: C

NEW QUESTION 108
Which of the following is NOT typically used to mitigate the war dialing threat?

A. Setting up monitored modems on special phone numbers
B. Setting modems to auto-answer mode
C. Proactively scanning your own phone numbers
D. Monitoring call logs at the switch

Answer: B

NEW QUESTION 110
A sensor that uses a light beam and a detecting plate to alarm if the light beam is obstructed is most commonly used to identify which of the following threats?

A. Power
B. Smoke
C. Natural Gas
D. Water
E. Toxins

Answer: B

NEW QUESTION 111
What protocol is a WAN technology?

A. 802.11
B. 802.3
C. Ethernet
D. Frame Relay

Answer: D

NEW QUESTION 115
Which common firewall feature can be utilized to generate a forensic trail of evidence and to identify attack trends against your network?

A. NAT
B. State Table
C. Logging
D. Content filtering

Answer: C

NEW QUESTION 120
What is the first thing that should be done during the containment step of incident handling?

A. Change all the passwords
B. Secure the area
C. Prepare the Jump bag
D. Notify management
E. Prepare a report

Answer: B

NEW QUESTION 121
Which of the following attack vectors are addressed by Xinetd and TCP Wrappers?

A. Outsider attack from network
B. Outsider attack from a telephone
C. Insider attack from local network
D. Attack from previously installed malicious code
E. A and B
F. A and C
G. B and D
H. C and D

Answer: B

NEW QUESTION 125
Which of the following areas of a network contains DNS servers and Web servers for Internet users?

A. VPN
B. MMZ
C. VLAN
D. DMZ

Answer: D

NEW QUESTION 129
Which of the following is more commonly used for establishing high-speed backbones that interconnect smaller networks and can carry signals over significant distances?

A. Bluetooth
B. Ethernet
C. Token ring
D. Asynchronous Transfer Mode (ATM)

Answer: D

NEW QUESTION 130
You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network. You have configured a firewall on the network. A filter has been applied to block all the ports. You want to enable sending and receiving of emails on the network. Which of the following ports will you open?
Each correct answer represents a complete solution. Choose two.

A. 80
B. 25
C. 20
D. 110

Answer: BD

NEW QUESTION 135
You work as a Network Administrator for Tech2tech Inc. You have configured a network-based IDS for your company. You have physically installed sensors at all key positions throughout the network such that they all report to the command console.
What will be the key functions of the sensors in such a physical layout?
Each correct answer represents a complete solution. Choose all that apply.

A. To collect data from operating system logs
B. To notify the console with an alert if any intrusion is detected

C. To analyze for known signatures
D. To collect data from Web servers

Answer: BC

NEW QUESTION 137
There are three key factors in selecting a biometric mechanism. What are they?

A. Reliability, encryption strength, and cost
B. Encryption strength, authorization method, and cost
C. Reliability, user acceptance, and cost
D. User acceptance, encryption strength, and cost

Answer: C

NEW QUESTION 138
Which of the following is a signature-based intrusion detection system (IDS) ?

A. RealSecure
B. Snort
C. StealthWatch
D. Tripwire

Answer: B

NEW QUESTION 142
Which of the following is a characteristic of hash operations?

A. Asymmetric
B. Non-reversible
C. Symmetric
D. Variable length output

Answer: D

NEW QUESTION 143
Many IIS servers connect to Microsoft SQL databases. Which of the following statements about SQL server security is TRUE?

A. SQL Server patches are part of the operating system patche
B. SQL Server should be installed on the same box as your IIS web server when they communicate as part of the web applicatio
C. It is good practice to never use integrated Windows authentication for SQL Serve
D. It is good practice to not allow users to send raw SQL commands to the SQL Serve

Answer: D

NEW QUESTION 148
Which of the following heights of fence deters only casual trespassers?

A. 8 feet
B. 2 to 2.5 feet
C. 6 to 7 feet
D. 3 to 4 feet

Answer: D

NEW QUESTION 152
The Linux command to make the /etc/shadow file, already owned by root, readable only by root is which of the following?

A. chmod 444/etc/shadow
B. chown root: root/etc/shadow
C. chmod 400/etc/shadow
D. chown 400 /etc/shadow

Answer: C

NEW QUESTION 153
Which of the following features of Windows 7 allows an administrator to both passively review installed software and configure policies to prevent out-of-date or insecure software from running?

A. Direct Access
B. Software Restriction Policies
C. App Locker
D. User Account Control

Answer: C

NEW QUESTION 154
Which of the following items are examples of preventive physical controls? Each correct answer represents a complete solution. Choose three.

A. Biometric access controls
B. Closed-circuit television monitors
C. Fire extinguishers
D. Locks and keys

Answer: ACD

NEW QUESTION 159
A new data center is being built where customer credit information will be processed and stored. Which of the following actions will help maintain the confidentiality of the data?

A. Environmental sensors in the server room
B. Access control system for physical building
C. Automated fire detection and control systems
D. Frequent off-site backup of critical databases

Answer: B

NEW QUESTION 162
Which of the following defines the communication link between a Web server and Web
applications?

A. CGI
B. PGP
C. Firewall
D. IETF

Answer: A

NEW QUESTION 163
When using Pretty Good Privacy (PGP) to digitally sign a message, the signature is created in a two-step process. First, the message to be signed is submitted to PGP's cryptographic hash algorithm. What is one of the hash algorithms used by PGP for this process?

A. Blowfish
B. DES
C. SHA-l
D. Cast

Answer: C

NEW QUESTION 168
Which of the following protocols are used to provide secure communication between a client and a server over the Internet?
Each correct answer represents a part of the solution. Choose two.

A. SSL
B. HTTP
C. TLS
D. SNMP

Answer: AC

NEW QUESTION 171
What is the most secure way to address an unused Windows service so it cannot be exploited by malware?

A. Firewall it
B. Set to manual startup
C. Disable it
D. Uninstall it

Answer: D

NEW QUESTION 175
A Host-based Intrusion Prevention System (HIPS) software vendor records how the Firefox Web browser interacts with the operating system and other applications, and identifies all areas of Firefox functionality. After collecting all the data about how Firefox should work, a database is created with this information, and it is fed into the HIPS software. The HIPS then monitors Firefox whenever it's in use. What feature of HIPS is being described in this scenario?

A. Signature Matching
B. Application Behavior Monitoring
C. Host Based Sniffing
D. Application Action Modeling

Answer: B

NEW QUESTION 178
Which of the following is a benefit of using John the Ripper for auditing passwords?

A. John's Blowfish cracking routine uses a complex central computing loop that increases the cost of each hash computatio
B. John the Ripper is much slower for auditing passwords encrypted with MD5 and Blowfis
C. John's MD5 cracking routine uses a simplified central computing loop that decreases the cost of each hash computatio
D. John cannot use the DES bit-slicing technique, so it is much slower than other tools, especially when used against DES-encrypted password

Answer: C

NEW QUESTION 181
When considering ingress filtering, why should all inbound packets be dropped if they contain a source address from within the protected network address space?

A. The packets are probably corrupte
B. The packets may have been accidentally routed onto the Interne
C. The packets may be deliberately spoofed by an attacke
D. The packets are a sign of excess fragmentatio
E. A and B
F. B and C
G. B and D
H. A and D

Answer: B

NEW QUESTION 184
Regarding the UDP header below, what is the length in bytes of the UDP datagrarn?
04 1a 00 a1 00 55 db 51

A. 161
B. 81
C. 219
D. 85

Answer: D

NEW QUESTION 185
John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. John is working as a root user on the Linux operating system. He wants to change the modified date and time of the file private.txt to 11 Nov 2009 02:59:58 am. Which of the following commands will John use to accomplish his task?
Each correct answer represents a complete solution. Choose all that apply.

A. rm private.txt #11 Nov 2009 02:59:58 am
B. touch -d "11 Nov 2009 02:59:58 am" private.txt
C. touch private.txt #11 Nov 2009 02:59:58 am
D. touch -t 200911110259.58 private.txt

Answer: BD

NEW QUESTION 187
The TTL can be found in which protocol header?

A. It is found in byte 8 of the ICMP heade
B. It is found in byte 8 of the IP heade
C. It is found in byte 8 of the TCP heade
D. It is found in byte 8 of the DNS heade

Answer: B

NEW QUESTION 189
How many bytes does it take to represent the hexadecimal value OxFEDCBA?

A. 12
B. 2
C. 3
D. 6

Answer: C

NEW QUESTION 193
Which of the following tools is used to configure, control, and query the TCP/IP network interface parameters?

A. NSLOOKUP
B. IPCONFIG
C. ARP
D. IFCONFIG

Answer: D

NEW QUESTION 195
If a DNS client wants to look up the IP address for good.news.com and does not receive an authoritative reply from its local DNS server, which name server is most likely to provide an authoritative reply?

A. The news.com domain name server
B. The .com (top-level) domain name server
C. The .(root-level) domain name server
D. The .gov (top-level) domain name server

Answer: A

NEW QUESTION 196
If Linux server software is a requirement in your production environment which of the following should you NOT utilize?

A. Debian
B. Mandrake
C. Cygwin
D. Red Hat

Answer: C

NEW QUESTION 197
While using Wire shark to investigate complaints of users being unable to login to a web application, you come across an HTTP POST submitted through your web application. The contents of the POST are listed below. Based on what you see below, which of the following would you recommend to prevent future damage to your database?

A. Use ssh to prevent a denial of service attack
B. Sanitize user inputs to prevent injection attacks
C. Authenticate users to prevent hackers from using your database
D. Use https to prevent hackers from inserting malware

Answer: D

NEW QUESTION 201
John works as a professional Ethical Hacker. He is assigned a project to test the security of www.we- are-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 conduct a buffer overflo
B. They allow an attacker to set a Trojan in the operating system and thus open a backdoor for anytime acces
C. They allow an attacker to replace utility programs that can be used to detect the attacker's activit
D. They allow an attacker to run packet sniffers secretly to capture password

Answer: BCD

NEW QUESTION 203
One of your Linux systems was compromised last night. According to change management history and a recent vulnerability scan, the system's patches were up-to-date at the time of the attack. Which of the following statements is the Most Likely explanation?

A. It was a zero-day exploi
B. It was a Trojan Horse exploi
C. It was a worm exploi
D. It was a man-in-middle exploi

Answer: A

NEW QUESTION 205
An IT security manager is trying to quickly assess the risks associated with not implementing a corporate firewall system. What sort of risk assessment is most appropriate?

A. Annualized Risk Assessment
B. Qualitative risk assessment
C. Quantitative risk assessment
D. Technical Risk Assessment
E. Iterative Risk Assessment

Answer: B

NEW QUESTION 208
In trace route results, what is the significance of an * result?

A. A listening port was identifie
B. A reply was returned in less than a secon
C. The target host was successfully reache
D. No reply was received for a particular ho

Answer: D

NEW QUESTION 209
......