GIAC

Exam Questions GSEC

GIAC Security Essentials Certification

NEW QUESTION 1
Which of the following is an Implementation of PKI?

A. SSL
B. 3DES
C. Kerberos
D. SHA-1

Answer: A

NEW QUESTION 2
At what point in the Incident Handling process should an organization determine its approach to notifying law enforcement?

A. When performing analysis
B. When preparing policy
C. When recovering from the incident
D. When reacting to an incident

Answer: D

NEW QUESTION 3
When Net Stumbler is initially launched, it sends wireless frames to which of the following addresses?

A. Broadcast address
B. Default gateway address
C. Subnet address
D. Network address

Answer: A

NEW QUESTION 4
Which of the following hardware devices prevents broadcasts from crossing over subnets?

A. Bridge
B. Hub
C. Router
D. Modem

Answer: C

NEW QUESTION 5
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 6
When trace route fails to get a timely response for a packet after three tries, which action will it take?

A. It will print '* * *' for the attempts and increase the maximum hop count by on
B. It will exit gracefully, and indicate to the user that the destination is unreachabl
C. It will increase the timeout for the hop and resend the packet
D. It will print '* * *' for the attempts, increment the TTL and try again until the maximum hop coun

Answer: D

NEW QUESTION 7
Which Defense-in-Depth model involves identifying various means by which threats can become manifest and providing security mechanisms to shut them down?

A. Vector-oriented
B. Uniform protection
C. Information centric defense
D. Protected enclaves

Answer: A

NEW QUESTION 8
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 9
Which of the following works at the network layer and hides the local area network IP address and topology?

A. Network address translation (NAT)
B. Hub
C. MAC address
D. Network interface card (NIC)

Answer: A

NEW QUESTION 10
If you do NOT have an original file to compare to, what is a good way to identify steganography in potential carrier files?

A. Determine normal properties through methods like statistics and look for changes
B. Determine normal network traffic patterns and look for changes
C. Find files with the extension .stg
D. Visually verify the files you suspect to be steganography messages

Answer: A

NEW QUESTION 10
What database can provide contact information for Internet domains?

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

Answer: C

NEW QUESTION 11
Two clients connecting from the same public IP address (for example - behind the same NAT firewall) can connect simultaneously to the same web server on the Internet, provided what condition is TRUE?

A. The server is not using a well-known por
B. The server is on a different networ
C. The client-side source ports are differen
D. The clients are on different subnet

Answer: C

NEW QUESTION 14
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 18
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 19
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 22
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 26
Which of the following protocols is used by a host that knows its own MAC (Media Access Control) address to query a server for its own IP address?

A. RARP
B. ARP
C. DNS
D. RDNS

Answer: A

NEW QUESTION 31
Which of the following authentication methods are used by Wired Equivalent Privacy (WEP)? Each correct answer represents a complete solution. Choose two.

A. Anonymous authentication
B. Mutual authentication
C. Open system authentication
D. Shared key authentication

Answer: CD

NEW QUESTION 36
Your software developer comes to you with an application that controls a user device. The application monitors its own behavior and that of the device and creates log files. The log files are expected to grow steadily and rapidly. Your developer currently has the log files stored in the /bin folder with the application binary. Where would you suggest that the developer store the log files?

A. /var/log
B. /etc/log
C. /usr/log
D. /tmp/log
E. /dev/log

Answer: A

NEW QUESTION 40
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 42
Which of the following protocols implements VPN using IPSec?

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

Answer: C

NEW QUESTION 47
Which of the following utilities provides an efficient way to give specific users permission to use specific system commands at the root level of a Linux operating system?

A. Snort

B. Apache
C. SSH
D. SUDO

Answer: D

NEW QUESTION 49
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 50
Which of the following are the types of intrusion detection systems?
Each correct answer represents a complete solution. Choose all that apply.

A. Host-based intrusion detection system (HIDS)
B. Client-based intrusion detection system (CIDS)
C. Server-based intrusion detection system (SIDS)
D. Network intrusion detection system (NIDS)

Answer: AD

NEW QUESTION 55
What is the process of simultaneously installing an operating system and a Service Pack called?

A. Synchronous Update
B. Slipstreaming
C. Simultaneous Update
D. Synchronizing

Answer: B

NEW QUESTION 58
Which Linux file lists every process that starts at boot time?

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

Answer: D

NEW QUESTION 62
In PKI, when someone wants to verify that the certificate is valid, what do they use to decrypt the signature?

A. Receiver's digital signature
B. X.509 certificate CA's private key
C. Secret passphrase
D. CA's public key

Answer: D

NEW QUESTION 65
What is TRUE about Workgroups and Domain Controllers?

A. By default all computers running Windows 2008 can only form Domain Controllers not Workgroups
B. Workgroups are characterized by higher costs while Domain Controllers by lower costs
C. You cannot have stand-alone computers in the midst of other machines that are members of a domain
D. Workgroup computers cannot share resources, only computers running on the same domain can
E. You can have stand-alone computers in the midst of other machines that are members of a domai

Answer: E

NEW QUESTION 68
Which of the following is a type of countermeasure that can be deployed to ensure that a threat vector does not meet a vulnerability?

A. Prevention controls
B. Detection controls

C. Monitoring controls
D. Subversive controls

Answer: A

NEW QUESTION 73
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 77
You are going to upgrade your hard disk's file system from FAT to NTFS. What are the major advantages of the NTFS file system over FAT16 and FAT32 file systems?
Each correct answer represents a complete solution. Choose all that apply.

A. NTFS gives better file security than FAT16 and FAT32.
B. Automatic backu
C. NTFS file system supports for larger hard disk
D. NTFS give improved disk compression than FAT16 and FAT32.

Answer: ACD

NEW QUESTION 79
Which of the following would be a valid reason to use a Windows workgroup?

A. Lower initial cost
B. Simplicity of single sign-on
C. Centralized control
D. Consistent permissions and rights

Answer: D

NEW QUESTION 81
You have reason to believe someone with a domain user account has been accessing and modifying sensitive spreadsheets on one of your application servers. You decide to enable auditing for the files to see who is accessing and changing them. You enable the Audit Object Access policy on the files via Group Policy. Two weeks later, when you check on
the audit logs, you see they are empty. What is the most likely reason this has happened?

A. You cannot enable auditing on files, just folders
B. You did not enable auditing on the files
C. The person modifying the files turned off auditing
D. You did not save the change to the policy

Answer: B

NEW QUESTION 85
Which of the following Unix syslog message priorities is the MOST severe?

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

Answer: B

NEW QUESTION 90
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 93
With regard to defense-in-depth, which of the following statements about network design principles is correct?

A. A secure network design requires that systems that have access to the Internet should not be accessible from the Internet and that systems accessible from the

Internet should not have access to the Interne
B. A secure network design requires that networks utilize VLAN (Virtual LAN) implementations to insure that private and semi-public systems are unable to reach each other without going through a firewal
C. A secure network design will seek to provide an effective administrative structure by providing a single choke-point for the network from which all security controls and restrictions will be enforce
D. A secure network design will seek to separate resources by providing a security boundary between systems that have different network security requirement

Answer: D

NEW QUESTION 96
Which of the following statements about buffer overflow is true?

A. It manages security credentials and public keys for message encryptio
B. It is a collection of files used by Microsoft for software updates released between major service pack release
C. It is a condition in which an application receives more data than it is configured to accep
D. It is a false warning about a viru

Answer: C

NEW QUESTION 101
What type of malware is a self-contained program that has the ability to copy itself without parasitically infecting other host code?

A. Trojans
B. Boot infectors
C. Viruses
D. Worms

Answer: D

NEW QUESTION 105
Which of the following proxy servers provides administrative controls over the content?

A. Content filtering web proxy server
B. Caching proxy server
C. Forced proxy server
D. Web proxy server

Answer: A

NEW QUESTION 110
You have been hired to design a TCP/IP-based network that will contain both Unix and Windows computers. You are planning a name resolution strategy. Which of the following services will best suit the requirements of the network?

A. APIPA
B. LMHOSTS
C. DNS
D. DHCP
E. WINS

Answer: C

NEW QUESTION 115
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 119
A folder D:\Files\Marketing has the following NTFS permissions:
. Administrators: Full Control
. Marketing: Change and Authenticated
. Users: Read
It has been shared on the server as "MARKETING", with the following share permissions:
. Full Control share permissions for the Marketing group
Which of the following effective permissions apply if a user from the Sales group accesses the \\FILESERVER\MARKETING shared folder?

A. No access
B. Full Control
C. Read
D. Change

Answer: C

NEW QUESTION 123
Which of the following is a backup strategy?

A. Differential
B. Integrational
C. Recursive
D. Supplemental

Answer: A

NEW QUESTION 125
You are reviewing a packet capture file from your network intrusion detection system. In the packet stream, you come across a long series of "no operation" (NOP) commands. In addition to the NOP commands, there appears to be a malicious payload. Of the following, which is the most appropriate preventative measure for this type of attack?

A. Limits on the number of failed logins
B. Boundary checks on program inputs
C. Controls against time of check/time of use attacks
D. Restrictions on file permissions

Answer: C

NEW QUESTION 129
Which of the following tools is used to query the DNS servers to get detailed information about IP addresses, MX records, and NS servers?

A. NBTSTAT
B. NSLOOKUP
C. PING
D. NETSTAT

Answer: B

NEW QUESTION 132
You have an automated system for patching the operating systems of all your computers. All patches are supposedly current. Yet your automated vulnerability scanner has just reported vulnerabilities that you believe have been patched. Which of the actions below should you take next?

A. Check some systems manuall
B. Rerun the system patching routine
C. Contact the incident response tea
D. Ignore the findings as false positive

Answer: A

NEW QUESTION 137
How are differences in configuration settings handled between Domain and Local Group Policy Objects (GPOs)?

A. Local and Domain GPOs control different configuration settings, so there will not be conflict
B. Settings in the domain-wide GPO override conflicting settings in the local GPO on each compute
C. Settings in the local GPO override conflicting settings when the domain-wide GPO is applie
D. Precedence depends on which GPO was updated firs

Answer: B

NEW QUESTION 138
Which access control mechanism requires a high amount of maintenance since all data must be classified, and all users granted appropriate clearance?

A. Mandatory
B. Discretionary
C. Rule set-based
D. Role-Based

Answer: A

NEW QUESTION 142
What is the maximum number of connections a normal Bluetooth device can handle at one time?

A. 2
B. 4
C. 1
D. 8
E. 7

Answer: E

NEW QUESTION 146
Which of the following applications cannot proactively detect anomalies related to a computer?

A. Firewall installed on the computer
B. NIDS
C. HIDS
D. Anti-virus scanner

Answer: B

NEW QUESTION 151
It is possible to sniff traffic from other hosts on a switched Ethernet network by impersonating which type of network device?

A. Switch
B. Bridge
C. Hub
D. Router

Answer: D

NEW QUESTION 155
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 158
Which of the following TCP dump output lines indicates the first step in the TCP 3-way handshake?

A. 07:09:43.368615 download.net 39904 > ftp.com.21: S 733381829:733381829(0) win 8760 <mss 1460> (DF)
B. 07:09:43.370302 ftp.com.21 > download.net.39904: S 1192930639:1192930639(0} ack 733381830 win 1024 <mss 1460> (DF)
C. 09:09:22.346383 ftp.com.21 > download.net.39904: , rst 1 win 2440(DF)
D. 07:09:43.370355 download.net.39904 > ftp.com.21: , ack 1 win 8760 (DF)

Answer: A

NEW QUESTION 160
Mark works as a Network Administrator for NetTech Inc. The company has a Windows 2003 domain- based network. The network contains ten Windows 2003 member servers, 150 Windows XP Professional client computers. According to the company's security policy, Mark needs to check whether all the computers in the network have all available security updates and shared folders. He also needs to check the file system type on each computer's hard disk. Mark installs and runs MBSACLI.EXE with the appropriate switches on a server. Which of the following tasks will he accomplish?

A. None of the tasks will be accomplishe
B. He will be able to check the file system type on each computer's hard dis
C. He will be able to accomplish all the task
D. He will be able to check all available security updates and shared folder

Answer: C

NEW QUESTION 163
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 166
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 170
What file instructs programs like Web spiders NOT to search certain areas of a site?

A. Robots.txt
B. Restricted.txt
C. Spider.txt
D. Search.txt

Answer: A

NEW QUESTION 175
Which of the following languages enable programmers to store cookies on client computers? Each correct answer represents a complete solution. Choose two.

A. DHTML
B. Perl
C. HTML
D. JavaScript

Answer: BD

NEW QUESTION 180
You work as a Network Administrator for NetTech Inc. When you enter http://66.111.64.227 in the browser's address bar, you are able to access the site. But, you are unable to access the site when you enter http://www.uCertify.com. What is the most likely cause?

A. DNS entry is not available for the host nam
B. The site's Web server is offlin
C. The site's Web server has heavy traffi
D. WINS server has no NetBIOS name entry for the serve

Answer: A

NEW QUESTION 183
You work as a Network Administrator for McNeil Inc. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest domain-based network. The company's management has decided to provide laptops to its sales team members. These laptops are equipped with smart card readers. The laptops will be configured as wireless network clients. You are required to accomplish the following tasks:
The wireless network communication should be secured.
The laptop users should be able to use smart cards for getting authenticated. In order to accomplish the tasks, you take the following steps:
Configure 802.1x and WEP for the wireless connections. Configure the PEAP-MS-CHAP v2 protocol for authentication. What will happen after you have taken these steps?

A. The laptop users will be able to use smart cards for getting authenticate
B. Both tasks will be accomplishe
C. None of the tasks will be accomplishe
D. The wireless network communication will be secure

Answer: D

NEW QUESTION 184
When an IIS filename extension is mapped, what does this mean?

A. Files with the mapped extensions cannot be interpreted by the web serve
B. The file and all the data from the browser's request are handed off to the mapped interprete
C. The files with the mapped extensions are interpreted by CMD.EX
D. The files with the mapped extensions are interpreted by the web browse

Answer: B

NEW QUESTION 186
What technical control provides the most critical layer of defense if an intruder is able to bypass all physical security controls and obtain tapes containing critical data?

A. Camera Recordings
B. Security guards
C. Encryption
D. Shredding
E. Corrective Controls

Answer: C

NEW QUESTION 190
Analyze the screenshot below. What is the purpose of this message?

A. To gather non-specific vulnerability information
B. To get the user to download malicious software
C. To test the browser plugins for compatibility
D. To alert the user to infected software on the compute

Answer: D

NEW QUESTION 191
What type of attack can be performed against a wireless network using the tool Kismet?

A. IP spoofing
B. Eavesdropping
C. Masquerading
D. Denial of Service

Answer: B

NEW QUESTION 195
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 196
What is the unnoticed theft of sensitive data from a laptop owned by an organization's CEO an example of in information warfare?

A. Non-zero sum game
B. Win-win situation
C. Zero-sum game
D. Symmetric warfare

Answer: D

NEW QUESTION 199
Which of the following are advantages of Network Intrusion Detection Systems (NIDS)?

A. Analysis of encrypted traffic
B. Provide insight into network traffic
C. Detection of network operations problems
D. Provide logs of network traffic that can be used as part of other security measure
E. Inexpensive to manage
F. B, C, and D
G. A, C, and E
H. B, D, and E
I. A, B, and C

Answer: C

NEW QUESTION 200
If the NET_ID of the source and destination address in an IP (Internet Protocol) packet match, which answer BEST describes the routing method the sending host will use?

A. Local (or direct) routing
B. Circuit switch routing
C. Dynamic (or changeable) routing
D. Remote (or indirect) routing

Answer: A

NEW QUESTION 205
Which of the following services resolves host name to IP Address?

A. Computer Browser
B. DHCP
C. DNS
D. WINS

Answer: C

NEW QUESTION 207
Which of the following is a signature-based intrusion detection system (IDS) ?

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

Answer: B

NEW QUESTION 208
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 212
Which of the following is an advantage of an Intrusion Detection System?

A. It is a mature technolog
B. It is the best network securit
C. It never needs patchin
D. It is a firewall replacemen

Answer: A

NEW QUESTION 217
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 218
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 220
What is SSL primarily used to protect you against?

A. Session modification
B. SQL injection
C. Third-patty sniffing
D. Cross site scripting

Answer: C

NEW QUESTION 224
Which of the following TCP packet flags indicates that host should IMMEDIATELY terminate the connection containing the packet?

A. FIN
B. URG
C. SYN
D. RST

Answer: D

NEW QUESTION 228
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 230
What defensive measure could have been taken that would have protected the confidentiality of files that were divulged by systems that were compromised by malware?

A. Ingress filtering at the host level
B. Monitoring for abnormal traffic flow
C. Installing file integrity monitoring software
D. Encrypting the files locally when not in use

Answer: D

NEW QUESTION 233
Which of the following protocols allows an e-mail client to access and manipulate a remote e-mail file without downloading it to the local computer?

A. IMAP
B. SNMP
C. POP3
D. SMTP

Answer: A

NEW QUESTION 235
Where are user accounts and passwords stored in a decentralized privilege management environment?

A. On a central authentication serve
B. On more than one serve
C. On each serve
D. On a server configured for decentralized privilege managemen

Answer: C

NEW QUESTION 236
What does the "x" character in the second field of the user account record of the /etc/passwd file indicate?

A. The user account is using a shadow passwor
B. The user account is shared by more than one use
C. The user account is disable
D. The user account does not exis

Answer: A

NEW QUESTION 238
Which of the following statements best describes where a border router is normally placed?

A. Between your firewall and your internal network
B. Between your firewall and DNS server
C. Between your ISP and DNS server
D. Between your ISP and your external firewall

Answer: D

NEW QUESTION 243
How many bytes does it take to represent the hexadecimal value OxFEDCBA?

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

Answer: C

NEW QUESTION 247
Which of the following statements about DMZ are true?
Each correct answer represents a complete solution. Choose two.

A. It is the boundary between the Internet and a private networ
B. It is an anti-virus software that scans the incoming traffic on an internal networ
C. It contains company resources that are available on the Internet, such as Web servers and FTP server

D. It contains an access control list (ACL).

Answer: AC

NEW QUESTION 252
You work as a Network Administrator for Tech Perfect Inc. The company has a Linux-based network. You want to kill a process running on a Linux server. Which of the following commands will you use to know the process identification number (PID) of the process?

A. killall
B. ps
C. getpid
D. kill

Answer: B

NEW QUESTION 256
Which of the following statements about Network Address Translation (NAT) are true? Each correct answer represents a complete solution. Choose two.

A. It reduces the need for globally unique IP addresse
B. It allows external network clients access to internal service
C. It allows the computers in a private network to share a global, ISP assigned address to connect to the Interne
D. It provides added security by using Internet access to deny or permit certain traffic from the Bastion Hos

Answer: AC

NEW QUESTION 261
You are examining a packet capture session in Wire shark and see the packet shown in the accompanying image. Based on what you see, what is the appropriate protection against this type of attempted attack?

A. Block DNS traffic across the router
B. Disable forwarding of unsolicited TCP requests
C. Disable IP-directed broadcast requests
D. Block UDP packets at the firewall

Answer: C

NEW QUESTION 262
Which command would allow an administrator to determine if a RPM package was already installed?

A. rpm -s
B. rpm -q
C. rpm -a
D. rpm -t

Answer: B

NEW QUESTION 265
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 268
Which of the following are examples of Issue-Specific policies all organizations should address?

A. Perimeter filtering guides, break times for employees, desktop neatness and backup procedure
B. Rogue wireless access points, auditing, break time for employees and organizational structur
C. Audit logs, physical access, mission statements and network protocols use
D. Backup requirements, employee monitoring, physical access and acceptable us

Answer: D

NEW QUESTION 273
Which of the following statements about policy is FALSE?

A. A well-written policy contains definitions relating to "what" to d
B. A well-written policy states the specifics of "how" to do somethin
C. Security policy establishes what must be done to protect information stored on computer
D. Policy protects people who are trying to do the right thin

Answer: D

NEW QUESTION 274
Which of the following networking topologies uses a hub to connect computers?

A. Bus
B. Ring
C. Star
D. Cycle

Answer: C

NEW QUESTION 277
Included below is the output from a resource kit utility run against local host.
Which command could have produced this output?

A. Schtasks
B. Task kill
C. SC
D. Task list

Answer: D

NEW QUESTION 279
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 283
What are the two actions the receiver of a PGP email message can perform that allows establishment of trust between sender and receiver?

A. Decode the message by decrypting the asymmetric key with his private key, then using the asymmetric key to decrypt the messag
B. Decode the message by decrypting the symmetric key with his private key, then using the symmetric key to decrypt the messag
C. Decode the message by decrypting the symmetric key with his public key, then using the symmetric key to decrypt the messag

D. Decrypt the message by encrypting the digital signature with his private key, then using the digital signature to decrypt the messag

Answer: A

NEW QUESTION 284
......