

GSEC Dumps

GIAC Security Essentials Certification

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



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

Where could you go in Windows XP/2003 to configure Automatic Updates?

- A. Right click on the Start Menu and choose select Properties in the pop-up Men
- B. Open the MMC and choose the Automatic Updates snap-i
- C. Right click on your desktop and choose the automatic update
- D. Go to the System applet in Control Panel and click on the Automatic Updates ico

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 SIP methods is used to setup a new session and add a caller?

- A. ACK
- B. BYE
- C. REGISTER
- D. INVITE
- E. CANCEL

Answer: D

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 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 9

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 10

What is a security feature available with Windows Vista and Windows 7 that was not present in previous Windows operating systems?

- A. Data Execution Prevention (DEP)
- B. User Account Control (UAC)
- C. Encrypting File System (EFS)
- D. Built-in IPSec Client

Answer: B

NEW QUESTION 10

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 13

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

Your organization is developing a network protection plan. No single aspect of your network seems more important than any other. You decide to avoid separating your network into segments or categorizing the systems on the network. Each device on the network is essentially protected in the same manner as all other devices.

This style of defense-in-depth protection is best described as which of the following?

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

Answer: A

NEW QUESTION 19

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 23

You are responsible for a Microsoft based network. Your servers are all clustered. Which of the following are the likely reasons for the clustering? Each correct answer represents a complete solution. Choose two.

- A. Reduce power consumption
- B. Ease of maintenance
- C. Load balancing
- D. Failover

Answer: CD

NEW QUESTION 25

You work as a Network Administrator for McNeil Inc. You are installing an application. You want to view the log file whenever a new entry is added to the `/var/log/messages` log file. Which of the following commands will you use to accomplish this?

- A. `TAIL -show /var/log/messages`
- B. `TAIL -f /var/log/messages`
- C. `TAIL -50 /var/log/messages`
- D. `TAIL -view /var/log/messages`

Answer: B

NEW QUESTION 27

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 28

You work as a Network Administrator for World Perfect Inc. The company has a Linux-based network. You have configured a Linux Web server on the network. A user complains that the Web server is not responding to requests. The process list on the server shows multiple instances of the HTTPD process. You are required to stop the Web service. Which of the following commands will you use to resolve the issue?

- A. `killall httpd`
- B. `endall httpd`
- C. `kill httpd`
- D. `end httpd`

Answer: A

NEW QUESTION 29

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 33

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 startup shell of Maria from `bash` to `tcsh`. Which of the following commands will John use to accomplish the task? Each correct answer represents a complete solution. Choose all that apply.

- A. `usermod -s`
- B. `chage`
- C. `usermod -u`
- D. `useradd -s`

Answer: AD

NEW QUESTION 34

Your customer wants to make sure that only computers he has authorized can get on his Wi-Fi. What is the most appropriate security measure you can recommend?

- A. A firewall
- B. WPA encryption
- C. WEP encryption
- D. Mac filtering

Answer: D

NEW QUESTION 36

You are responsible for technical support at a company. One of the employees complains that his new laptop cannot connect to the company wireless network. You have verified that he is entering a valid password/passkey. What is the most likely problem?

- A. A firewall is blocking hi
- B. His laptop is incompatibl
- C. MAC filtering is blocking hi
- D. His operating system is incompatibl

Answer: C

NEW QUESTION 39

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 41

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 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 47

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 48

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 53

What would the file permission example "rwsr-x" translate to in absolute mode?

- A. 1755
- B. 6755
- C. 6645
- D. 1644

Answer: B

NEW QUESTION 54

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

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

Answer: B

NEW QUESTION 56

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 60

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 Internet
- 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 firewall
- 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 enforced
- D. A secure network design will seek to separate resources by providing a security boundary between systems that have different network security requirements

Answer: D

NEW QUESTION 65

You work as a Network Administrator for Secure World Inc. The company has a Linux-based network. You want to run a command with the changed root directory. Which of the following commands will you use?

- A. ls <new root> <command>
- B. chroot <new root> <command>
- C. route <new root> <command>
- D. chdir <new root> <command>

Answer: B

NEW QUESTION 68

In preparation to do a vulnerability scan against your company's systems. You've taken the steps below:

You've notified users that there will be a system test.

You've prioritized and selected your targets and subnets.

You've configured the system to do a deep scan.

You have a member of your team on call to answer questions.

Which of the following is a necessary step to take prior to starting the scan?

- A. Placing the incident response team on call
- B. Clear relevant system log file
- C. Getting permission to run the scan
- D. Scheduling the scan to run before OS update

Answer: C

NEW QUESTION 71

Who is responsible for deciding the appropriate classification level for data within an organization?

- A. Data custodian
- B. Security auditor
- C. End user
- D. Data owner

Answer: B

NEW QUESTION 74

When no anomaly is present in an Intrusion Detection, but an alarm is generated, the response is known as.

- A. False negative
- B. False positive
- C. True positive
- D. True negative

Answer: B

NEW QUESTION 78

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 80

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 84

Which of the following commands is used to change file access permissions in Linux?

- A. chgrp
- B. chperm
- C. chmod
- D. chown

Answer: C

NEW QUESTION 85

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 88

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 manually
- B. Rerun the system patching routine
- C. Contact the incident response team
- D. Ignore the findings as false positive

Answer: A

NEW QUESTION 93

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 computer
- C. Settings in the local GPO override conflicting settings when the domain-wide GPO is applied

D. Precedence depends on which GPO was updated first

Answer: B

NEW QUESTION 94

You work as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. You are required to search for the error messages in the /var/log/messages log file. Which of the following commands will you use to accomplish this?

- A. ps /var/log/messages
- B. cat /var/log/messages | look error
- C. cat /var/log/messages | grep error
- D. cat /var/log/messages

Answer: C

NEW QUESTION 99

You are implementing wireless access at a defense contractor. Specifications say, you must implement the AES Encryption algorithm. Which encryption standard should you choose?

- A. WPA
- B. TKIP
- C. WEP
- D. WPA 2

Answer: D

NEW QUESTION 103

You have implemented a firewall on the company's network for blocking unauthorized network connections. Which of the following types of security control is implemented in this case?

- A. Detective
- B. Preventive
- C. Directive
- D. Corrective

Answer: B

NEW QUESTION 104

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 109

To be considered a strong algorithm, an encryption algorithm must be which of the following?

- A. Secret
- B. Well-known
- C. Confidential
- D. Proprietary

Answer: B

NEW QUESTION 114

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

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

Answer: B

NEW QUESTION 119

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 122

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 126

You have set up a local area network for your company. Your firewall separates your network into several sections: a DMZ with semi-public servers (web, dns, email) and an intranet with private servers. A penetration tester gains access to both sections and installs sniffers in each. He is able to capture network traffic for all the devices in the private section but only for one device (the device with the sniffer) in the DMZ. What can be inferred about the design of the system?

- A. You installed a router in the private section and a switch in the DMZ
- B. You installed a hub in the private section and a switch in the DMZ
- C. You installed a switch in the private section and a hub in the DMZ
- D. You installed a switch in the private section and a router in the DMZ

Answer: B

NEW QUESTION 127

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 131

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 136

The Return on Investment (ROI) measurement used in Information Technology and Information Security fields is typically calculated with which formula?

- A. $ROI = (\text{gain} - \text{expenditure}) / (\text{expenditure}) \times 100\%$
- B. $ROI = (\text{gain} + \text{expenditure}) / (\text{expenditure}) \times 100\%$
- C. $ROI = (\text{loss} + \text{expenditure}) / (\text{expenditure}) \times 100\%$
- D. $ROI = (\text{loss} - \text{expenditure}) / (\text{expenditure}) \times 100\%$

Answer: A

NEW QUESTION 140

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 141

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 145

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 150

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 155

Validating which vulnerabilities in a network environment are able to be exploited by an attacker is called what?

- A. Anomaly detection
- B. Vulnerability scanning
- C. Perimeter assessment
- D. Penetration testing

Answer: B

NEW QUESTION 156

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 160

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 165

Which of the following processes is known as sanitization?

- A. Assessing the risk involved in discarding particular informatio
- B. Verifying the identity of a person, network host, or system proces
- C. Physically destroying the media and the information stored on i
- D. Removing the content from the media so that it is difficult to restor

Answer: D

NEW QUESTION 166

What is the main problem with relying solely on firewalls to protect your company's sensitive data?

- A. Their value is limited unless a full-featured Intrusion Detection System is use
- B. Their value is limited because they cannot be changed once they are configure
- C. Their value is limited because operating systems are now automatically patche
- D. Their value is limited because they can be bypassed by technical and non-technical mean

Answer: D

NEW QUESTION 168

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 173

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 176

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-1
- D. Cast

Answer: C

NEW QUESTION 178

Your system has been infected by malware. Upon investigation, you discover that the malware propagated primarily via email. The malware attacked known vulnerabilities for which patches are available, but due to problems with your configuration management system you have no way to know which systems have been patched and which haven't, slowing your progress in patching your network. Of the following, which solution would you use to protect against this propagation vector?

- A. Encrypt the emails on the server
- B. Scan and block suspect email attachments at the email server
- C. Install a firewall between the email server and the Internet
- D. Separate the email server from the trusted portions of the network

Answer: B

NEW QUESTION 181

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 184

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 189

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 190

An employee attempting to use your wireless portal reports receiving the error shown below. Which scenario is occurring?

- A. A denial-of-service attack is preventing a response from the porta
- B. Another access point is deauthenticating legitimate client
- C. The encrypted data is being intercepted and decrypte
- D. Another access point is attempting to intercept the dat

Answer: D

NEW QUESTION 194

Which of the following BEST describes the two job functions of Microsoft Baseline Security Analyzer (MBSA)?

- A. Vulnerability scanner and auditing tool
- B. Auditing tool and alerting system
- C. Configuration management and alerting system
- D. Security patching and vulnerability scanner

Answer: D

NEW QUESTION 197

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 200

Which of the following statements about Hypertext Transfer Protocol Secure (HTTPS) are true? Each correct answer represents a complete solution. Choose two.

- A. It uses TCP port 443 as the default port
- B. It is a protocol used in the Universal Resource Locator (URL) address line to connect to a secure site
- C. It is a protocol used to provide security for a database server in an internal network
- D. It uses TCP port 80 as the default port

Answer: AB

NEW QUESTION 203

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 208

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 209

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 addresses
- B. It allows external network clients access to internal services
- C. It allows the computers in a private network to share a global, ISP assigned address to connect to the Internet
- D. It provides added security by using Internet access to deny or permit certain traffic from the Bastion Host

Answer: AC

NEW QUESTION 212

Which of the following terms is used for the process of securing a system or a device on a network infrastructure?

- A. Hardening
- B. Authentication
- C. Cryptography
- D. Sanitization

Answer: A

NEW QUESTION 214

In order to capture traffic for analysis, Network Intrusion Detection Systems (NIDS) operate with network cards in what mode?

- A. Discrete
- B. Reporting
- C. Promiscuous
- D. Alert

Answer: C

NEW QUESTION 218

Which of the following is used to allow or deny access to network resources?

- A. Spoofing
- B. ACL
- C. System hardening
- D. NFS

Answer: B

NEW QUESTION 219

The following three steps belong to the chain of custody for federal rules of evidence. What additional step is recommended between steps 2 and 3?

STEP 1 - Take notes: who, what, where, when and record serial numbers of machine(s) in question.

STEP 2 - Do a binary backup if data is being collected.

STEP 3 - Deliver collected evidence to law enforcement officials.

- A. Rebuild the original hard drive from scratch, and sign and seal the good backup in a plastic bag
- B. Conduct a forensic analysis of all evidence collected BEFORE starting the chain of custody
- C. Take photographs of all persons who have had access to the computer
- D. Check the backup integrity using a checksum utility like MD5, and sign and seal each piece of collected evidence in a plastic bag

Answer: D

NEW QUESTION 220

While using Wireshark 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 221

Which of the following statements about policy is FALSE?

- A. A well-written policy contains definitions relating to "what" to do
- B. A well-written policy states the specifics of "how" to do something
- 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 thing

Answer: D

NEW QUESTION 223

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

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

Answer: C

NEW QUESTION 224

Which of the following is a new Windows Server 2008 feature for the Remote Desktop Protocol (RDP)?

- A. The ability to allow the administrator to choose a port other than the default RDP port (TCP 3389)
- B. The ability to support connections from mobile devices like smart phones
- C. The ability to allow clients to authenticate over TLS
- D. The ability to allow clients to execute individual applications rather than using a terminal desktop

Answer: D

NEW QUESTION 229

The previous system administrator at your company used to rely heavily on email lists, such as vendor lists and Bug Traq to get information about updates and patches. While a useful means of acquiring data, this requires time and effort to read through. In an effort to speed things up, you decide to switch to completely automated updates and patching. You set up your systems to automatically patch your production servers using a cron job and a scripted apt-get upgrade command. Of the following reasons, which explains why you may want to avoid this plan?

- A. The apt-get upgrade command doesn't work with the cron command because of incompatibility
- B. Relying on vendor and 3rd party email lists enables updates via email, for even faster patching
- C. Automated patching of production servers without prior testing may result in unexpected behavior or failures
- D. The command apt-get upgrade is incorrect, you need to run the apt-get update command

Answer: D

NEW QUESTION 232

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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