Exam Questions GSEC

GIAC Security Essentials Certification

https://www.2passeasy.com/dumps/GSEC/

NEW QUESTION 1
You work as a Linux technician for Tech Perfect Inc. You have lost the password of the root. You want to provide a new password. Which of the following steps will you take to accomplish the task?

A. The password of the root user cannot be change
B. Use the PASSWD root comman
C. Reboot the compute
D. Reboot the computer in run level 0. Use INIT=/bin/sh as a boot optio
E. At the bash# prompt, run the PASSWD root comman
F. Reboot the computer in run level 1. Use INIT=/bin/sh as a boot optio
G. At the bash# prompt, run the PASSWD root comman

Answer: D

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
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 4
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 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
The Windows 'tracert' begins by sending what type of packet to the destination host?

A. A UDP packet with a TTL of 1
B. An ICMP Echo Request
C. An ICMP Router Discovery
D. An ICMP Echo Reply

Answer: A

NEW QUESTION 7
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 8
Which Host-based IDS (HIDS) method of log monitoring utilizes a list of keywords or phrases that define the events of interest for the analyst, then takes a list of keywords to watch for and generates alerts when it sees matches in log file activity?

A. Passive analysis
B. Retroactive analysis
C. Exclusive analysis
D. Inclusive analysis

Answer: D

NEW QUESTION 9
What is the discipline of establishing a known baseline and managing that condition known as?

A. Condition deployment
B. Observation discipline
C. Security establishment
D. Configuration management

Answer: C

NEW QUESTION 10
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 10
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 13
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 18
Which of the following is referred to as Electromagnetic Interference (EMI)?

A. Electrical line noise
B. Spike
C. Transient
D. Brownout

Answer: A

NEW QUESTION 22
Where is the source address located in an IPv4 header?

A. At an offset of 20 bytes
B. At an offset of 8 bytes
C. At an offset of 16 bytes
D. At an offset of 12 bytes

Answer:

D

NEW QUESTION 24
Your organization has broken its network into several sections/segments, which are separated by firewalls, ACLs and VLANs. The purpose is to defend segments of the network from potential attacks that originate in a different segment or that attempt to spread across segments.
This style of defense-in-depth protection is best described as which of the following?

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

Answer: B

NEW QUESTION 25
Which of the following protocols implements VPN using IPSec?

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

Answer: C

NEW QUESTION 28
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 32
Your IT security team is responding to a denial of service attack against your server. They have taken measures to block offending IP addresses. Which type of threat control is this?

A. Detective
B. Preventive
C. Responsive
D. Corrective

Answer: D

NEW QUESTION 36
For most organizations, which of the following should be the highest priority when it comes to physical security concerns?

A. Controlling ingress and egress
B. Controlling access to workstations
C. Ensuring employee safety
D. Controlling access to servers
E. Protecting physical assets

Answer: C

NEW QUESTION 38
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 40
In a /24 subnet, which of the following is a valid broadcast address?

A. 200.11.11.1
B. 221.10.10.10
C. 245.20.30.254
D. 192.10.10.255

Answer: D

NEW QUESTION 44
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 45
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 46
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 51
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
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 57
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 58
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 60
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 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
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 priontized 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 cal
B. Clear relevant system log file
C. Getting permission to run the sca
D. Scheduling the scan to run before OS update

Answer: C

NEW QUESTION 67
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 70
You work as a Network Administrator for NetTech Inc. The company wants to encrypt its e-mails. Which of the following will you use to accomplish this?

A. PPTP
B. IPSec
C. PGP
D. NTFS

Answer: C

NEW QUESTION 73
You work as a Network Administrator for Net World Inc. The company has a Linux-based network. You want to mount an SMBFS share from a Linux workstation. Which of the following commands can you use to accomplish the task?
Each correct answer represents a complete solution. Choose two.

A. smbmount

B. mount smb
C. smbfsmount
D. mount -t smbfs

Answer: AD

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 77
Which of the following files contains the shadowed password entries in Linux?

A. /etc/passwd
B. /etc/shadow
C. /etc/profile
D. /etc/shdpwd

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 83
Which of the following is a backup strategy?

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

Answer: A

NEW QUESTION 85
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 90
Which of the following is a standard Unix command that would most likely be used to copy raw file system data for later forensic analysis?

A. dd
B. backup
C. cp
D. gzip

Answer: A

NEW QUESTION 92

How often is session information sent to the web server from the browser once the session information has been established?

A. With any change in session data
B. With every subsequent request
C. With any hidden form element data
D. With the initial request to register the session

Answer: A

NEW QUESTION 96
When you log into your Windows desktop what information does your Security Access Token (SAT) contain?

A. The Security ID numbers (SIDs) of all the groups to which you belong
B. A list of cached authentications
C. A list of your domain privileges
D. The Security ID numbers (SIDs) of all authenticated local users

Answer: C

NEW QUESTION 101
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 106
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 110
An attacker gained physical access to an internal computer to access company proprietary
data. The facility is protected by a fingerprint biometric system that records both failed and successful entry attempts. No failures were logged during the time periods of the recent breach. The account used when the attacker entered the facility shortly before each incident belongs to an employee who was out of the area. With respect to the biometric entry system, which of the following actions will help mitigate unauthorized physical access to the facility?

A. Try raising the Crossover Error Rate (CER)
B. Try to lower the False Accept Rate (FAR)
C. Try setting the Equal Error Rate (EER) to zero
D. Try to set a lower False Reject Rate (FRR)

Answer: B

NEW QUESTION 115
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 117
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 121

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 124
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 129
You work as a Network Administrator for Net Soft Inc. You are designing a data backup plan for your company's network. The backup policy of the company requires high security and easy recovery of data. Which of the following options will you choose to accomplish this?

A. Take a full backup daily with the previous night's tape taken offsit
B. Take a full backup daily and use six-tape rotatio
C. Take a full backup on Monday and an incremental backup on each of the following weekday
D. Keep Monday's backup offsit
E. Take a full backup on alternate days and keep rotating the tape
F. Take a full backup on Monday and a differential backup on each of the following weekday
G. Keep Monday's backup offsit
H. Take a full backup daily with one tape taken offsite weekl

Answer: A

NEW QUESTION 131
Which of the following is the FIRST step in performing an Operational Security (OP5EC) Vulnerabilities Assessment?

A. Assess the threat
B. Assess vulnerabilities of critical information to the threat
C. Conduct risk versus benefit analysis
D. Implement appropriate countermeasures
E. Identification of critical information

Answer: E

NEW QUESTION 136
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 141
There is not universal agreement on the names of the layers in the TCP/IP networking model. Which of the following is one of the functions of the bottom layer which is sometimes called the Network Access or Link Layer?

A. Provides end-to-end data delivery service for user applications
B. Handles the routing of the data packets over the network
C. Manages IP addressing and encryption for data packets
D. Defines the procedures for interfacing with Ethernet devices

Answer: D

NEW QUESTION 142
What is the motivation behind SYN/FIN scanning?

A. The SYN/FIN combination is useful for signaling to certain Trojan
B. SYN/FIN packets are commonly used to launch denial of service attacks against BSD host
C. The crafted SYN/FIN packet sometimes gets past firewalls and filtering router
D. A SYN/FIN packet is used in session hijacking to take over a sessio

Answer: B

NEW QUESTION 145
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 149
Which of the following is TRUE regarding the ability of attackers to eavesdrop on wireless communications?

A. Eavesdropping attacks cannot be performed through concrete wall
B. Eavesdropping attacks can take place from miles awa
C. Eavesdropping attacks are easily detected on wireless network
D. Eavesdropping attacks require expensive device

Answer: B

NEW QUESTION 151
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 154
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 159
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 162
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 165
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 168
Why are false positives such a problem with IPS technology?

A. File integrity is not guarantee
B. Malicious code can get into the networ
C. Legitimate services are not delivere
D. Rules are often misinterprete

Answer: D

NEW QUESTION 169
Which of the following is a signature-based intrusion detection system (IDS) ?

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

Answer: B

NEW QUESTION 174
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 177
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 181
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 185
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 190
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 192
Which of the following is an advantage of private circuits versus VPNs?

A. Flexibility
B. Performance guarantees
C. Cost
D. Time required to implement

Answer: B

NEW QUESTION 196
Which Windows event log would you look in if you wanted information about whether or not a specific diver was running at start up?

A. Application
B. System
C. Startup
D. Security

Answer: B

NEW QUESTION 198
Which of the following systems acts as a NAT device when utilizing VMware in NAT mode?

A. Guest system
B. Local gateway
C. Host system
D. Virtual system

Answer: D

NEW QUESTION 199
You are examining an IP packet with a header of 40 bytes in length and the value at byte 0 of the packet header is 6. Which of the following describes this packet?

A. This is an IPv4 packet; the protocol encapsulated in the payload is unspecifie
B. This is an IPv4 packet with a TCP payloa
C. This is an IPv6 packet; the protocol encapsulated in the payload is unspecifie
D. This is an IPv6 packet with a TCP payloa

Answer: C

NEW QUESTION 202
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 205
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 210
Which of the following is a private, RFC 1918 compliant IP address that would be assigned to a DHCP scope on a private LAN?

A. 127.0.0.100
B. 169.254.1.50
C. 10.254.1.50
D. 172.35.1.100

Answer: C

NEW QUESTION 215
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 217
You work as a Network Administrator for NetTech Inc. To ensure the security of files, you encrypt data files using Encrypting File System (EFS).
You want to make a backup copy of the files and maintain security settings. You can backup the files either to a network share or a floppy disk. What will you do to accomplish this?

A. Copy the files to a network share on an NTFS volum
B. Copy the files to a network share on a FAT32 volum
C. Place the files in an encrypted folde
D. Then, copy the folder to a floppy dis
E. Copy the files to a floppy disk that has been formatted using Windows 2000 Professiona

Answer: A

NEW QUESTION 221
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 222
Which of the following is TRUE regarding Ethernet?

A. Stations are not required to monitor their transmission to check for collision
B. Several stations are allowed to be transmitting at any given time within a single collision domai
C. Ethernet is shared medi
D. Stations are not required to listen before they transmi

Answer: C

NEW QUESTION 227
You are the security director for an off-shore banking site. From a business perspective, what is a major factor to consider before running your new vulnerability scanner against the company's business systems?

A. It may harm otherwise healthy system
B. It may produce false negative result
C. It may generate false positive result
D. It may not return enough benefit for the cos

Answer: C

NEW QUESTION 231
When should you create the initial database for a Linux file integrity checker?

A. Before a system is patched
B. After a system has been compromised
C. Before a system has been compromised

D. During an attack

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 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 243
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 246
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 247
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 251
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 252
When are Group Policy Objects (GPOs) NOT applied automatically to workstations?

A. At 90-minute intervals
B. At logon
C. Every time Windows Explorer is launched
D. At boot-up

Answer: C

NEW QUESTION 255
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 257
Which of the following books deals with confidentiality?

A. Purple Book
B. Orange Book
C. Red Book
D. Brown Book

Answer: B

NEW QUESTION 262
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 264
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 268
Which of the following SIP INVITE lines indicates to the remote registrar the VoIP phone that initiated the call?

A. Via
B. To
C. From-Agent
D. User-Agent

Answer: D

NEW QUESTION 270
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 273
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual GSEC Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the GSEC Product From:

https://www.2passeasy.com/dumps/GSEC/

Money Back Guarantee

GSEC Practice Exam Features:

* GSEC Questions and Answers Updated Frequently

* GSEC Practice Questions Verified by Expert Senior Certified Staff

* GSEC Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* GSEC Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year