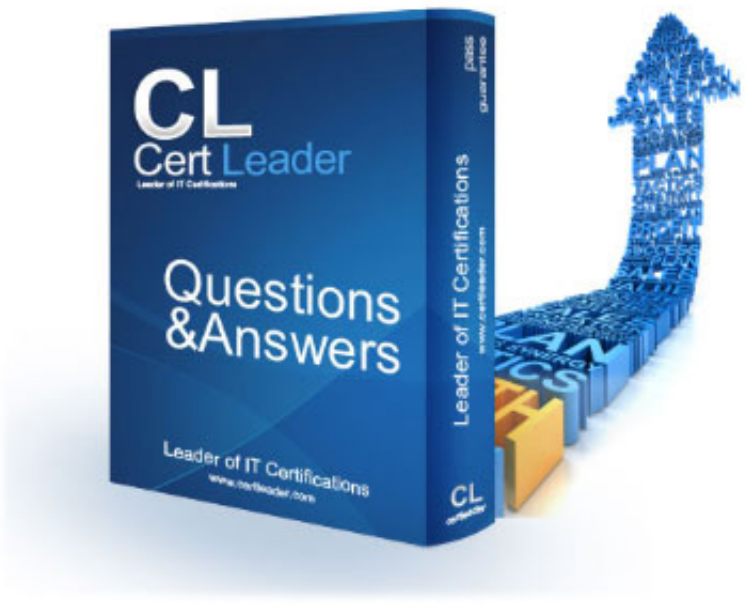
GSEC Dumps

GIAC Security Essentials Certification

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



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 protocols is used to send e-mails on the Internet?

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

Answer: A

NEW QUESTION 3
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 4
Which of the following is a valid password for a system with the default "Password must meet complexity requirements" setting enabled as part of the GPO Password policy requirements?

A. The Cat Chased its Tail AII Night
B. disk ACCESS failed
C. SETI@HOME
D. SaNS2006

Answer: D

NEW QUESTION 5
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 6
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 7
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 8
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 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
Which of the following are the types of access controls?
Each correct answer represents a complete solution. Choose three.

A. Physical
B. Administrative
C. Automatic
D. Technical

Answer: ABD

NEW QUESTION 10
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 12
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 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 16
Which of the following is a name, symbol, or slogan with which a product is identified?

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

Answer: B

NEW QUESTION 20
On which of the following OSI model layers does IPSec operate? A. Physical layer

A. Network layer
B. Data-link layer
C. Session layer

Answer: B

NEW QUESTION 22
Which of the below choices should an organization start with when implementing an effective risk management process?

A. Implement an incident response plan
B. Define security policy requirements
C. Conduct periodic reviews
D. Design controls and develop standards for each technology you plan to deploy

Answer: B

NEW QUESTION 26
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 29
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 33
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 38
John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. John is working as a root user on the Linux operating system. He is currently working on his C based new traceroute program. Since, many processes are running together on the system, he wants to give the highest priority to the cc command process so that he can test his program, remove bugs, and submit it to the office in time. Which of the following commands will John use to give the highest priority to the cc command process?

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

Answer: C

NEW QUESTION 43
Which of the following statements about IPSec are true?
Each correct answer represents a complete solution. Choose two.

A. It uses Internet Protocol (IP) for data integrit
B. It uses Authentication Header (AH) for data integrit
C. It uses Password Authentication Protocol (PAP) for user authenticatio
D. It uses Encapsulating Security Payload (ESP) for data confidentialit

Answer: BD

NEW QUESTION 46
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 51
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 56
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 58
Which of the following is NOT a recommended best practice for securing Terminal Services and Remote Desktop?

A. Require TLS authentication and data encryption whenever possibl
B. Make sure to allow all TCP 3389 traffic through the external firewal
C. Group Policy should be used to lock down the virtual desktops of thin-client user
D. Consider using IPSec or a VPN in addition to the RDP encryption if you are concerned about future RDP vulnerabilitie

Answer: B

NEW QUESTION 63
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 68
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 69

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

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

Answer: D

NEW QUESTION 70
Users at the Marketing department are receiving their new Windows XP Professional workstations. They will need to maintain local work files in the first logical volume, and will use a second volume for the information shared between the area group. Which is the best file system design for these workstations?

A. Both volumes should be converted to NTFS at install tim
B. First volume should be FAT32 and second volume should be NTF
C. First volume should be EFS and second volume should be FAT32.
D. Both volumes should be converted to FAT32 with NTFS DACL

Answer: A

NEW QUESTION 73
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 78
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 83
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 87
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 90
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 93
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 98
Which of the following elements is the most important requirement to ensuring the success of a business continuity plan?

A. Disaster Recover Plans
B. Anticipating all relevant threats
C. Executive buy-in
D. Clearly defining roles and responsibilities
E. Training

Answer: C

NEW QUESTION 101
Which of the following is a benefit to utilizing Cygwin for Windows?

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

Answer: A

NEW QUESTION 103
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 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
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 114

What type of formal document would include the following statement?
Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal application of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies, and if there is any uncertainty, employees should consult their supervisor or manager.

A. Company privacy statement
B. Remote access policy
C. Acceptable use policy
D. Non-disclosure agreement

Answer: C

NEW QUESTION 119
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 122
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 126
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 131
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 134
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 138
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 139
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
The process of enumerating all hosts on a network defines which of the following activities?

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

Answer: D

NEW QUESTION 145
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 149
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 150
Which of the following protocols provides maintenance and error reporting function?

A. UDP
B. ICMP
C. PPP
D. IGMP

Answer: B

NEW QUESTION 154
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 157
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 158
Which of the following ports is the default port for Layer 2 Tunneling Protocol (L2TP)?

A. TCP port 443
B. UDP port 161
C. TCP port 110
D. UDP port 1701

Answer: D

NEW QUESTION 162
A sensor that uses a light beam and a detecting plate to alarm if the light beam is obstructed is most commonly used to identify which of the following threats?

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

Answer: B

NEW QUESTION 167
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 168
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 169
What protocol is a WAN technology?

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

Answer: D

NEW QUESTION 172
Which common firewall feature can be utilized to generate a forensic trail of evidence and to identify attack trends against your network?

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

Answer: C

NEW QUESTION 175
Which port category does the port 110 fall into?

A. Well known port
B. Dynamic port
C. Private port
D. Application port

Answer: A

NEW QUESTION 180
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 185
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 190
You work as a Network Administrator for Net Perfect Inc. The company has a Linux-based network. You are configuring an application server. An application named Report, which is owned by the root user, is placed on the server. This application requires superuser permission to write to other files. All sales managers of the company will be using the application. Which of the following steps will you take in order to enable the sales managers to run and use the Report application?

A. Change the Report application to a SUID comman
B. Make the user accounts of all the sales managers the members of the root grou
C. Provide password of root user to all the sales manager
D. Ask each sales manager to run the application as the root use
E. As the application is owned by the root, no changes are require

Answer: A

NEW QUESTION 195
Which of the following is the reason of using Faraday cage?

A. To prevent Denial-of-Service (DoS) attack
B. To prevent shoulder surfing
C. To prevent mail bombing
D. To prevent data emanation

Answer: D

NEW QUESTION 196
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 200
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 202
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 207

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 208
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 210
Which of the following is a required component for successful 802.lx network authentication?

A. Supplicant
B. 3rd-party Certificate Authority
C. Ticket Granting Server (TGS)
D. IPSec

Answer: A

NEW QUESTION 211
How is a Distributed Denial of Service (DDOS) attack distinguished from a regular DOS attack?

A. DDOS attacks are perpetrated by many distributed host
B. DDOS affects many distributed target
C. Regular DOS focuses on a single route
D. DDOS affects the entire Interne

Answer: A

NEW QUESTION 212
Which of the following services resolves host name to IP Address?

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

Answer: C

NEW QUESTION 213
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 214
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 218
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 222
Which of the following quantifies the effects of a potential disaster over a period of time?

A. Risk Assessment
B. Business Impact Analysis
C. Disaster Recovery Planning
D. Lessons Learned

Answer: B

NEW QUESTION 227
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 232
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 236
Which of the following protocols are used to provide secure communication between a client and a server over the Internet?
Each correct answer represents a part of the solution. Choose two.

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

Answer: AC

NEW QUESTION 239
When a packet leaving the network undergoes Network Address Translation (NAT), which of the following is changed?

A. TCP Sequence Number
B. Source address
C. Destination port
D. Destination address

Answer: B

NEW QUESTION 240
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 241
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 245
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 248
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 250
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 253
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 257
IPS devices that are classified as "In-line NIDS" devices use a combination of anomaly analysis, signature-based rules, and what else to identify malicious events on the network?

A. Firewall compatibility rules
B. Application analysis
C. ICMP and UDP active scanning
D. MAC address filtering

Answer: B

NEW QUESTION 262
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 por
B. It is a protocol used in the Universal Resource Locater (URL) address line to connect to a secure sit
C. It is a protocol used to provide security for a database server in an internal networ
D. It uses TCP port 80 as the default por

Answer: AB

NEW QUESTION 263
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 266
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 270
Which of the following tools is used to configure, control, and query the TCP/IP network interface parameters?

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

Answer: D

NEW QUESTION 274
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 279
You work as a Network Administrator for Net World Inc. The company has a Linux-based network. For testing purposes, you have configured a default IP-table with several filtering rules. You want to reconfigure the table. For this, you decide to remove the rules from all the chains in the table. Which of the following commands will you use?

A. IPTABLES -D
B. IPTABLES -A
C. IPTABLES -h
D. IPTABLES -F

Answer: D

NEW QUESTION 282
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 285
What is the following sequence of packets demonstrating?

A. telnet.com.telnet > client.com.38060: F 4289:4289(0) ack 92 win 1024
B. client.com.38060 > telnet.com.telnet: .ack 4290 win 8760 (DF)
C. client.com.38060 > telnet.com.telnet: F 92:92(0) ack 4290 win 8760 (DF)
D. telnet.com.telnet > client.com.38060: .ack 93 win 1024

Answer: C

NEW QUESTION 290
You work as an Administrator for McRoberts Inc. The company has a Linux-based network. You are logged in as a non-root user on your client computer. You want to delete all files from the /garbage directory. You want that the command you will use should prompt for the root user password. Which of the following commands will you use to accomplish the task?

A. rm -rf /garbage*
B. del /garbage/*.*
C. rm -rf /garbage* /SU
D. su -c "RM -rf /garbage*"

Answer: D

NEW QUESTION 291
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 296
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 301
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 302
Which of the following books deals with confidentiality?

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

Answer: B

NEW QUESTION 304
John works as a professional Ethical Hacker. He is assigned a project to test the security of www.we- are-secure.com. He installs a rootkit on the Linux server of the We-are-secure network. Which of the following statements are true about rootkits?

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

A. They allow an attacker to conduct a buffer overflo
B. They allow an attacker to set a Trojan in the operating system and thus open a backdoor for anytime acces
C. They allow an attacker to replace utility programs that can be used to detect the attacker's activit
D. They allow an attacker to run packet sniffers secretly to capture password

Answer: BCD

NEW QUESTION 309
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 312
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 313
.....

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