Exam Questions GSEC

GIAC Security Essentials Certification

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

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

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

Answer: A

NEW QUESTION 2
Which of the following is a 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 3
Which of the following should be implemented to protect an organization from spam?

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

Answer: C

NEW QUESTION 4
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 5
If you do NOT have an original file to compare to, what is a good way to identify steganography in potential carrier files?

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

Answer: A

NEW QUESTION 6
What database can provide contact information for Internet domains?

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

Answer: C

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
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 9
Which of the following is a name, symbol, or slogan with which a product is identified?

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

Answer: B

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

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

Answer: A

NEW QUESTION 11
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 14
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 19
Which of the following protocols is used by a host that knows its own MAC (Media Access Control) address to query a server for its own IP address?

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

Answer: A

NEW QUESTION 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
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 26
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 27
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 29
A US case involving malicious code is brought to trial. An employee had opened a helpdesk ticket to report specific instances of strange behavior on her system. The IT helpdesk representative collected information by interviewing the user and escalated the ticket to the system administrators. As the user had regulated and sensitive data on her computer, the system administrators had the hard drive sent to the company's forensic consultant for analysis and configured a new hard drive for the user. Based on the recommendations from the forensic consultant and the company's legal department, the CEO decided to prosecute the author of the malicious code. During the court case, which of the following would be able to provide direct evidence?

A. The IT helpdesk representative
B. The company CEO
C. The user of the infected system
D. The system administrator who removed the hard drive

Answer: C

NEW QUESTION 33
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 37
Which of the following protocols implements VPN using IPSec?

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

Answer: C

NEW QUESTION 41
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 46
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 50
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 53
Why would someone use port 80 for deployment of unauthorized services?

A. Google will detect the service listing on port 80 and post a link, so that people all over the world will surf to the rogue servic
B. If someone were to randomly browse to the rogue port 80 service they could be compromise
C. This is a technique commonly used to perform a denial of service on the local web serve
D. HTTP traffic is usually allowed outbound to port 80 through the firewall in most environment

Answer: D

NEW QUESTION 56
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 57
Which Linux file lists every process that starts at boot time?

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

Answer: D

NEW QUESTION 58
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 62
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 67
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 71
Which of the following would be a valid reason to use a Windows workgroup?

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

Answer: D

NEW QUESTION 76
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 80
Which of the following groups represents the most likely source of an asset loss through the inappropriate use of computers?

A. Visitors
B. Customers
C. Employees
D. Hackers

Answer: C

NEW QUESTION 81
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 84
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 88
You ask your system administrator to verify user compliance with the corporate policies on password strength, namely that all passwords will have at least one numeral, at least one letter, at least one special character and be 15 characters long. He comes to you with a set of compliance tests for use with an offline password cracker. They are designed to examine the following parameters of the password:
* they contain only numerals
* they contain only letters
* they contain only special characters
* they contain only letters and numerals
" they contain only letters and special characters
* they contain only numerals and special characters
Of the following, what is the benefit to using this set of tests?

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

Answer: B

NEW QUESTION 93
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 96
What is the term for a game in which for every win there must be an equivalent loss?

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

Answer: C

NEW QUESTION 99
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 103
Which of the following classes of fire comes under Class C fire?

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

Answer: D

NEW QUESTION 104
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 105
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 107
Which of the following statements regarding the Secure Sockets Layer (SSL) security model are true?
Each correct answer represents a complete solution. Choose two.

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

Answer: BD

NEW QUESTION 109
A folder D:\Files\Marketing has the following NTFS permissions:
. Administrators: Full Control
. Marketing: Change and Authenticated
. Users: Read
It has been shared on the server as "MARKETING", with the following share permissions:
. Full Control share permissions for the Marketing group
Which of the following effective permissions apply if a user from the Sales group accesses the \\FILESERVER\MARKETING shared folder?

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

Answer: C

NEW QUESTION 110
Which of the following is a backup strategy?

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

Answer: A

NEW QUESTION 114
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 115
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 119
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 123

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 127
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 128
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 130
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 135
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 138
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 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 140
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 145
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 146
What protocol is a WAN technology?

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

Answer: D

NEW QUESTION 150
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 151
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 156
Which of the following Linux commands can change both the username and group name a file belongs to?

A. chown
B. chgrp
C. chmod
D. newgrp

Answer: B

NEW QUESTION 158
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 159
Which of the following areas of a network contains DNS servers and Web servers for Internet users?

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

Answer: D

NEW QUESTION 163
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 168
What file instructs programs like Web spiders NOT to search certain areas of a site?

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

Answer: A

NEW QUESTION 169
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 170
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 174
Which of the following languages enable programmers to store cookies on client computers? Each correct answer represents a complete solution. Choose two.

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

Answer: BD

NEW QUESTION 176
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 179
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 182
When an IIS filename extension is mapped, what does this mean?

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

Answer: B

NEW QUESTION 184
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 189
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 194
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 196
The Return on Investment (ROI) measurement used in Information Technology and Information Security fields is typically calculated with which formula?

A. ROI = (gain - expenditure)/(expenditure) X 100%
B. ROI = (gain + expenditure)/(expenditure) X 100%
C. ROI = (loss + expenditure)/(expenditure) X 100%
D. ROI = (loss - expenditure)/(expenditure) X 100%

Answer: A

NEW QUESTION 201
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 202
Which of the following services resolves host name to IP Address?

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

Answer: C

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

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

Answer: B

NEW QUESTION 209
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 214
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 216
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 219
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 220
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 224
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 226
What is the name of the registry key that is used to manage remote registry share permissions for the whole registry?

A. regkey
B. regmng
C. winreg
D. rrsreg

Answer: C

NEW QUESTION 227
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 230
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 235
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 239
During which of the following steps is the public/private key-pair generated for Public Key Infrastructure (PKI)?

A. Key Recovery
B. Initialization
C. Registration
D. Certification

Answer: B

NEW QUESTION 243
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 247
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 251
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 255
How many bytes does it take to represent the hexadecimal value OxFEDCBA?

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

Answer: C

NEW QUESTION 256
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 258
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 263
You are examining a packet capture session in Wire shark and see the packet shown in the accompanying image. Based on what you see, what is the appropriate protection against this type of attempted attack?

A. Block DNS traffic across the router

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

Answer: C

NEW QUESTION 268
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 272
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 275
Which of the following books deals with confidentiality?

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

Answer: B

NEW QUESTION 276
What would the following IP tables command do?
IP tables -I INPUT -s 99.23.45.1/32 -j DROP

A. Drop all packets from the source address
B. Input all packers to the source address
C. Log all packets to or from the specified address
D. Drop all packets to the specified address

Answer: A

NEW QUESTION 281
Which of the following statements about policy is FALSE?

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

Answer: D

NEW QUESTION 282
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 284
Which of the following networking topologies uses a hub to connect computers?

A. Bus
B. Ring
C. Star

D. Cycle

Answer: C

NEW QUESTION 286
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 290
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 295
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 296
Which of the following statements about the integrity concept of information security management are true?
Each correct answer represents a complete solution. Choose three.

A. It ensures that unauthorized modifications are not made to data by authorized personnel or processe
B. It determines the actions and behaviors of a single individual within a system
C. It ensures that internal information is consistent among all subentities and also consistent with the real-world, external situatio
D. It ensures that modifications are not made to data by unauthorized personnel or processe

Answer: ACD

NEW QUESTION 301
.....

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