

GIAC

Exam Questions GSEC

GIAC Security Essentials Certification



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 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 All Night
- B. disk ACCESS failed
- C. SETI@HOME
- D. SaNS2006

Answer: D

NEW QUESTION 3

Which of the following is an Implementation of PKI?

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

Answer: A

NEW QUESTION 4

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

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

Answer: D

NEW QUESTION 5

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

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

Answer: D

NEW QUESTION 6

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 7

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 8

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

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

Answer: A

NEW QUESTION 9

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

What database can provide contact information for Internet domains?

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

Answer: C

NEW QUESTION 10

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 13

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 16

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 20

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 21

Which of the following choices accurately describes how PGP works when encrypting email?

- A. PGP encrypts the message with the recipients public key, then encrypts this key with a random asymmetric ke
- B. PGP creates a random asymmetric key that it uses to encrypt the message, then encrypts this key with the recipient's public key
- C. PGP creates a random symmetric key that it uses to encrypt the message, then encrypts this key with the recipient's public key
- D. PGP encrypts the message with the recipients public key, then encrypts this key with a random symmetric ke

Answer: B

NEW QUESTION 24

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 25

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 30

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 32

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 36

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

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

Answer: B

NEW QUESTION 38

When designing wireless networks, one strategy to consider is implementing security mechanisms at all layers of the OSI model. Which of the following protection mechanisms would protect layer 1?

- A. Hardening applications
- B. Limit RF coverage
- C. Employing firewalls
- D. Enabling strong encryption

Answer: B

NEW QUESTION 40

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 integrity
- B. It uses Authentication Header (AH) for data integrity
- C. It uses Password Authentication Protocol (PAP) for user authentication
- D. It uses Encapsulating Security Payload (ESP) for data confidentiality

Answer: BD

NEW QUESTION 41

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 43

Which of the following statements about Microsoft's VPN client software is FALSE?

- A. The VPN interface can be figured into the route table
- B. The VPN interface has the same IP address as the interface to the network it's been specified to protect
- C. The VPN client software is built into the Windows operating system
- D. The VPN tunnel appears as simply another adapter

Answer: B

NEW QUESTION 48

Which of the following statements would describe the term "incident" when used in the branch of security known as Incident Handling?

- A. Any observable network event
- B. Harm to systems
- C. Significant threat of harm to systems
- D. A and C
- E. A, B, and C
- F. B and C
- G. A and B

Answer: D

NEW QUESTION 50

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 52

Which type of risk assessment results are typically categorized as low, medium, or high-risk events?

- A. Technical
- B. Qualitative
- C. Management
- D. Quantitative

Answer: B

NEW QUESTION 57

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 60

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 possible
- B. Make sure to allow all TCP 3389 traffic through the external firewall
- 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 vulnerabilities

Answer: B

NEW QUESTION 61

Which of the following statements about Secure Sockets Layer (SSL) are true? Each correct answer represents a complete solution. Choose two.

- A. It provides communication privacy, authentication, and message integrity
- B. It provides mail transfer service
- C. It uses a combination of public key and symmetric encryption for security of data
- D. It provides connectivity between Web browser and Web server

Answer: AC

NEW QUESTION 63

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 65

Which of the following applications would be BEST implemented with UDP instead of TCP?

- A. A multicast streaming application
- B. A web browser
- C. A DNS zone transfer
- D. A file transfer application

Answer: A

NEW QUESTION 67

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

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

Answer: D

NEW QUESTION 68

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

- A. Prevention controls
- B. Detection controls
- C. Monitoring controls
- D. Subversive controls

Answer: A

NEW QUESTION 69

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 72

Which of the following statements about the authentication concept of information security management is true?

- A. It ensures the reliable and timely access to resource
- B. It ensures that modifications are not made to data by unauthorized personnel or processes
- C. It determines the actions and behaviors of a single individual within a system, and identifies that particular individual
- D. It establishes the users' identity and ensures that the users are who they say they are

Answer: D

NEW QUESTION 77

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 81

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

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

Answer: D

NEW QUESTION 82

Which of the following statements about buffer overflow is true?

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

Answer: C

NEW QUESTION 83

Which of the following is generally practiced by the police or any other recognized governmental authority?

- A. Spoofing
- B. SMB signing
- C. Wiretapping
- D. Phishing

Answer: C

NEW QUESTION 84

Which of the following elements is the most important requirement to ensuring the success of a business continuity plan?

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

Answer: C

NEW QUESTION 87

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

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

Answer: A

NEW QUESTION 91

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 92

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 95

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 97

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 system
- 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 system
- 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 machine
- 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 system
- 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 system's RAM is available to the guest operating system

Answer: E

NEW QUESTION 101

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 102

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 106

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

- A. APIPA
- B. LMHOSTS
- C. DNS

D. DHCP
E. WINS

Answer: C

NEW QUESTION 109

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 server
- B. The client always authenticates the server
- C. The server always authenticates the client
- D. The server can optionally authenticate the client

Answer: BD

NEW QUESTION 112

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 113

SSL session keys are available in which of the following lengths?

- A. 40-bit and 128-bit
- B. 64-bit and 128-bit
- C. 128-bit and 1,024-bit
- D. 40-bit and 64-bit

Answer: A

NEW QUESTION 116

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 119

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 122

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 124

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 126

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 127

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 128

CORRECT TEXT

Fill in the blank with the correct answer to complete the statement below.

The permission is the minimum required permission that is necessary for a user to enter a directory and list its contents.

A.

Answer: Read

NEW QUESTION 129

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 130

When a host on a remote network performs a DNS lookup of www.google.com, which of the following is likely to provide an Authoritative reply?

- A. The local DNS server
- B. The top-level DNS server for .com
- C. The DNS server for google.com
- D. The root DNS server

Answer: A

NEW QUESTION 131

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 136

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 141

Which of the following protocols provides maintenance and error reporting function?

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

Answer: B

NEW QUESTION 143

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 144

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 149

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 151

Which of the following types of computers is used for attracting potential intruders?

- A. Files pot
- B. Honey pot
- C. Data pot
- D. Bastion host

Answer: B

NEW QUESTION 152

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 156

What protocol is a WAN technology?

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

Answer: D

NEW QUESTION 157

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 158

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 offsite
- B. Take a full backup daily and use six-tape rotation
- C. Take a full backup on Monday and an incremental backup on each of the following weekdays
- D. Keep Monday's backup offsite
- 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 weekdays
- G. Keep Monday's backup offsite
- H. Take a full backup daily with one tape taken offsite weekly

Answer: A

NEW QUESTION 160

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 164

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 167

Which of the following statements would be seen in a Disaster Recovery Plan?

- A. "Instructions for notification of the media can be found in Appendix A"
- B. "The Emergency Response Plan should be executed in the case of any physical disaster listed on page 3."
- C. "The target for restoration of business operations is 72 hours from the declaration of disaster."
- D. "After arriving at the alternate site, utilize the server build checklist to rebuild all servers on the server rebuild list."

Answer: D

NEW QUESTION 170

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 command
- B. Make the user accounts of all the sales managers the members of the root group
- C. Provide password of root user to all the sales manager
- D. Ask each sales manager to run the application as the root user
- E. As the application is owned by the root, no changes are required

Answer: A

NEW QUESTION 175

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 179

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 182

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 183

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 185

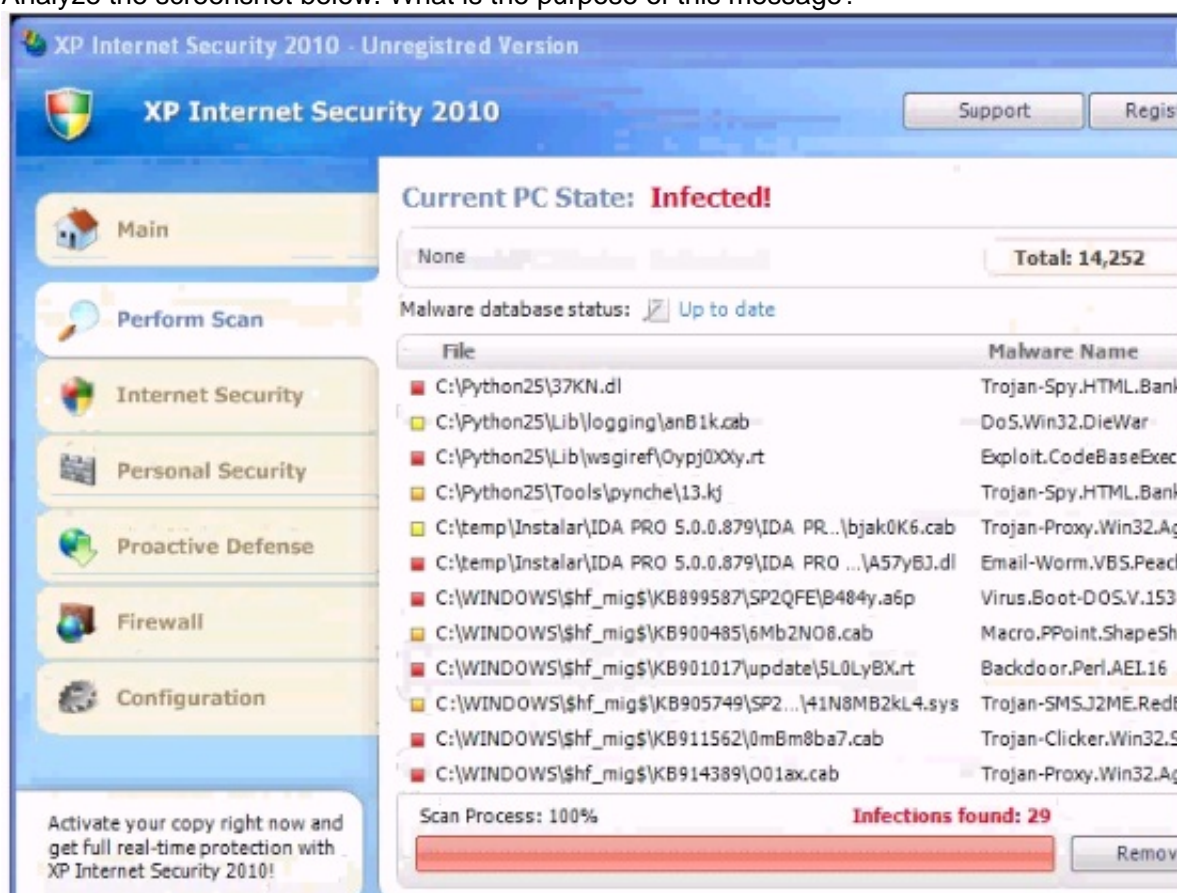
To be considered a strong algorithm, an encryption algorithm must be which of the following?

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

Answer: B

NEW QUESTION 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 190

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 194

You work as a Network Administrator for Tech2tech Inc. You have configured a network-based IDS for your company. You have physically installed sensors at all key positions throughout the network such that they all report to the command console.

What will be the key functions of the sensors in such a physical layout?

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

- A. To collect data from operating system logs
- B. To notify the console with an alert if any intrusion is detected
- C. To analyze for known signatures
- D. To collect data from Web servers

Answer: BC

NEW QUESTION 196

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 200

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 203

There are three key factors in selecting a biometric mechanism. What are they?

- A. Reliability, encryption strength, and cost
- B. Encryption strength, authorization method, and cost
- C. Reliability, user acceptance, and cost
- D. User acceptance, encryption strength, and cost

Answer: C

NEW QUESTION 207

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

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

Answer: A

NEW QUESTION 210

Against policy, employees have installed Peer-to-Peer applications on their workstations and they are using them over TCP port 80 to download files via the

company network from other Peer-to-Peer users on the Internet. Which of the following describes this threat?

- A. Firewall subversion
- B. Backdoor installation
- C. Malicious software infection
- D. Phishing attempt

Answer: A

NEW QUESTION 215

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

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

Answer: C

NEW QUESTION 217

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

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

Answer: B

NEW QUESTION 222

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 patches
- B. SQL Server should be installed on the same box as your IIS web server when they communicate as part of the web application
- C. It is good practice to never use integrated Windows authentication for SQL Server
- D. It is good practice to not allow users to send raw SQL commands to the SQL Server

Answer: D

NEW QUESTION 224

Which of the following is an advantage of an Intrusion Detection System?

- A. It is a mature technology
- B. It is the best network security
- C. It never needs patching
- D. It is a firewall replacement

Answer: A

NEW QUESTION 228

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 230

Which of the following features of Windows 7 allows an administrator to both passively review installed software and configure policies to prevent out-of-date or insecure software from running?

- A. Direct Access
- B. Software Restriction Policies
- C. App Locker
- D. User Account Control

Answer: C

NEW QUESTION 232

Which of the following processes is known as sanitization?

- A. Assessing the risk involved in discarding particular information
- B. Verifying the identity of a person, network host, or system process

- C. Physically destroying the media and the information stored on it
- D. Removing the content from the media so that it is difficult to restore

Answer: D

NEW QUESTION 235

A new data center is being built where customer credit information will be processed and stored. Which of the following actions will help maintain the confidentiality of the data?

- A. Environmental sensors in the server room
- B. Access control system for physical building
- C. Automated fire detection and control systems
- D. Frequent off-site backup of critical databases

Answer: B

NEW QUESTION 240

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 241

Which of the following are network connectivity devices?

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

- A. Network analyzer
- B. Bridge
- C. Brouter
- D. Firewall
- E. Repeater
- F. Hub

Answer: BCEF

NEW QUESTION 245

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 250

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 253

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 256

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 261

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 unspecified
- B. This is an IPv4 packet with a TCP payload
- C. This is an IPv6 packet; the protocol encapsulated in the payload is unspecified
- D. This is an IPv6 packet with a TCP payload

Answer: C

NEW QUESTION 265

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 267

When considering ingress filtering, why should all inbound packets be dropped if they contain a source address from within the protected network address space?

- A. The packets are probably corrupt
- B. The packets may have been accidentally routed onto the Internet
- C. The packets may be deliberately spoofed by an attacker
- D. The packets are a sign of excess fragmentation
- E. A and B
- F. B and C
- G. B and D
- H. A and D

Answer: B

NEW QUESTION 270

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 272

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 274

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 volume
- B. Copy the files to a network share on a FAT32 volume
- C. Place the files in an encrypted folder
- D. Then, copy the folder to a floppy disk
- E. Copy the files to a floppy disk that has been formatted using Windows 2000 Professional

Answer: A

NEW QUESTION 276

What is the function of the TTL (Time to Live) field in IPv4 and the Hop Limit field in IPv6 In an IP Packet header?

- A. These fields are decremented each time a packet is retransmitted to minimize the possibility of routing loop
- B. These fields are initialized to an initial value to prevent packet fragmentation and fragmentation attack
- C. These fields are recalculated based on the required time for a packet to arrive at its destinatio
- D. These fields are incremented each time a packet is transmitted to indicate the number of routers that an IP packet has traverse

Answer: A

NEW QUESTION 277

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 282

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 286

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 288

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

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

Answer: D

NEW QUESTION 289

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 network
- 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 293

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 295

If a DNS client wants to look up the IP address for good.news.com and does not receive an authoritative reply from its local DNS server, which name server is most likely to provide an authoritative reply?

- A. The news.com domain name server
- B. The .com (top-level) domain name server
- C. The .(root-level) domain name server
- D. The .gov (top-level) domain name server

Answer: A

NEW QUESTION 299

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 304

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?

No. .	Time	Source	Destination	Dest. Port	Info
35	20.657938	192.168.23.132	192.168.23.255		Echo (pi

- 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 309

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 311

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 316

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 320

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

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

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

STEP 3 - Deliver collected evidence to law enforcement officials.

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

Answer: D

NEW QUESTION 325

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?

```
POST /samplelogin.cfm HTTP/1.1
Host: www.example.com
User-Agent: Mozilla/5.0 (X11; U; en-US;) Gecko/200910 Ubuntu/8.4
Firefox/2.6
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.example.com/
Cookie: SID=026DCB9CBBF2339C2CBFAEBA8F1DD656;
Content-Type: application/x-www-form-urlencoded
Content-Length: 64
username='a'&password=DROP+TABLE+members;+--
```

- 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 326

Which of the following statements about policy is FALSE?

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

Answer: D

NEW QUESTION 328

Which of the following terms refers to the process in which headers and trailers are added around user data?

- A. Encapsulation
- B. Authentication
- C. Authorization
- D. Encryption

Answer: A

NEW QUESTION 331

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 overflow
- B. They allow an attacker to set a Trojan in the operating system and thus open a backdoor for anytime access
- C. They allow an attacker to replace utility programs that can be used to detect the attacker's activities
- D. They allow an attacker to run packet sniffers secretly to capture passwords

Answer: BCD

NEW QUESTION 332

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

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

Answer: C

NEW QUESTION 334

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 335

One of your Linux systems was compromised last night. According to change management history and a recent vulnerability scan, the system's patches were up-to-date at the time of the attack. Which of the following statements is the Most Likely explanation?

- A. It was a zero-day exploi
- B. It was a Trojan Horse exploi
- C. It was a worm exploi
- D. It was a man-in-middle exploi

Answer: A

NEW QUESTION 340

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 341

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The GSEC Practice Test Here](#)