

# 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 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 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 of the following SIP methods is used to setup a new session and add a caller?

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

**Answer:** D

#### NEW QUESTION 7

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 8

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

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

**Answer:** A

#### NEW QUESTION 9

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 10

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 15

What database can provide contact information for Internet domains?

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

**Answer:** C

#### NEW QUESTION 17

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 19

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 24

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 26

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

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

**Answer:** D

#### NEW QUESTION 28

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 33

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 38

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 42

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 46

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 50

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 51

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 54

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 55

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 59

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 61

Which of the following protocols implements VPN using IPSec?

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

**Answer:** C

**NEW QUESTION 62**

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 67**

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

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

**Answer:** D

**NEW QUESTION 72**

Which choice best describes the line below?

```
alert tcp any any -> 192.168.1.0/24 80 (content: /cgi-bin/test.cgi"; msg: "Attempted CGI-BIN Access!!");
```

- A. Tcpdump filter
- B. IP tables rule
- C. Wire shark filter
- D. Snort rule

**Answer:** D

**NEW QUESTION 75**

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 79**

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 time
- B. First volume should be FAT32 and second volume should be NTFS
- 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 83**

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 85**

Which aspect of UNIX systems was process accounting originally developed for?

- A. Data warehouse
- B. Time sharing
- C. Process tracking
- D. Real time

**Answer:** C

#### NEW QUESTION 88

Which of the following is a term that refers to unsolicited e-mails sent to a large number of e-mail users?

- A. Hotfix
- B. Spam
- C. Biometrics
- D. Buffer overflow

**Answer: B**

#### NEW QUESTION 90

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 92

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 95

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 99

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 passwords
- 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 103

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

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

**Answer: B**

#### NEW QUESTION 107

An employee is currently logged into the corporate web server, without permission. You log into the web server as 'admin' and look for the employee's username: 'dmaul' using the 'who' command. This is what you get back:



```
[user@localhost ~]$ who
admin :0 2010-09-11 06:49
dvader pts/3 2010-09-11 08:07 (localhost.localdomain)
hsolo pts/4 2010-09-11 08:14 (192.168.54.3)
cdooku pts/4 2010-09-11 08:14 (192.168.54.5)
```

- A. The contents of the /var/log/messages file has been altered
- B. The contents of the bash history file has been altered
- C. The contents of the utmp file has been altered
- D. The contents of the http logs have been altered

**Answer: B**

#### NEW QUESTION 108

What type of malware is a self-contained program that has the ability to copy itself without parasitically infecting other host code?

- A. Trojans
- B. Boot infectors
- C. Viruses
- D. Worms

**Answer: D**

#### NEW QUESTION 111

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 112

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 115

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. PTP
- B. IPSec
- C. PGP
- D. NTFS

**Answer: C**

#### NEW QUESTION 117

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 118

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 122

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 127

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 130

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 135

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 140

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 145

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 146

What is the key difference between Electronic Codebook mode and other block cipher modes like Cipher Block Chaining, Cipher-Feedback and Output-Feedback?

- A. Plaintext patterns are concealed by XOR Ring with previous cipher text block but input to the block cipher is not randomized
- B. Plaintext patterns are concealed and input to the block cipher is randomized by XOR Ring with previous cipher text block

- C. Plaintext patterns encrypted with the same key will always generate the same Cipher text pattern
- D. Plaintext patterns are not concealed but input to the block cipher is randomized by XO Ring with previous cipher text bloc

**Answer:** C

#### NEW QUESTION 149

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 152

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 156

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 160

Which of the following describes software technologies that improve portability, manageability, and compatibility of applications by encapsulating them from the underlying operating system on which they are executed?

- A. System registry
- B. Group Policy
- C. Application virtualization
- D. System control

**Answer:** C

#### NEW QUESTION 164

What is the maximum number of connections a normal Bluetooth device can handle at one time?

- A. 2
- B. 4
- C. 1
- D. 8
- E. 7

**Answer:** E

#### NEW QUESTION 169

Which of the following is an UDP based protocol?

- A. telnet
- B. SNMP
- C. IMAP
- D. LDAP

**Answer:** B

#### NEW QUESTION 173

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 177**

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 179**

What protocol is a WAN technology?

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

**Answer:** D

**NEW QUESTION 181**

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 182**

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 weekday
- 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 weekday
- G. Keep Monday's backup offsite
- H. Take a full backup daily with one tape taken offsite weekly

**Answer:** A

**NEW QUESTION 184**

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 186**

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 190**

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 195

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 196

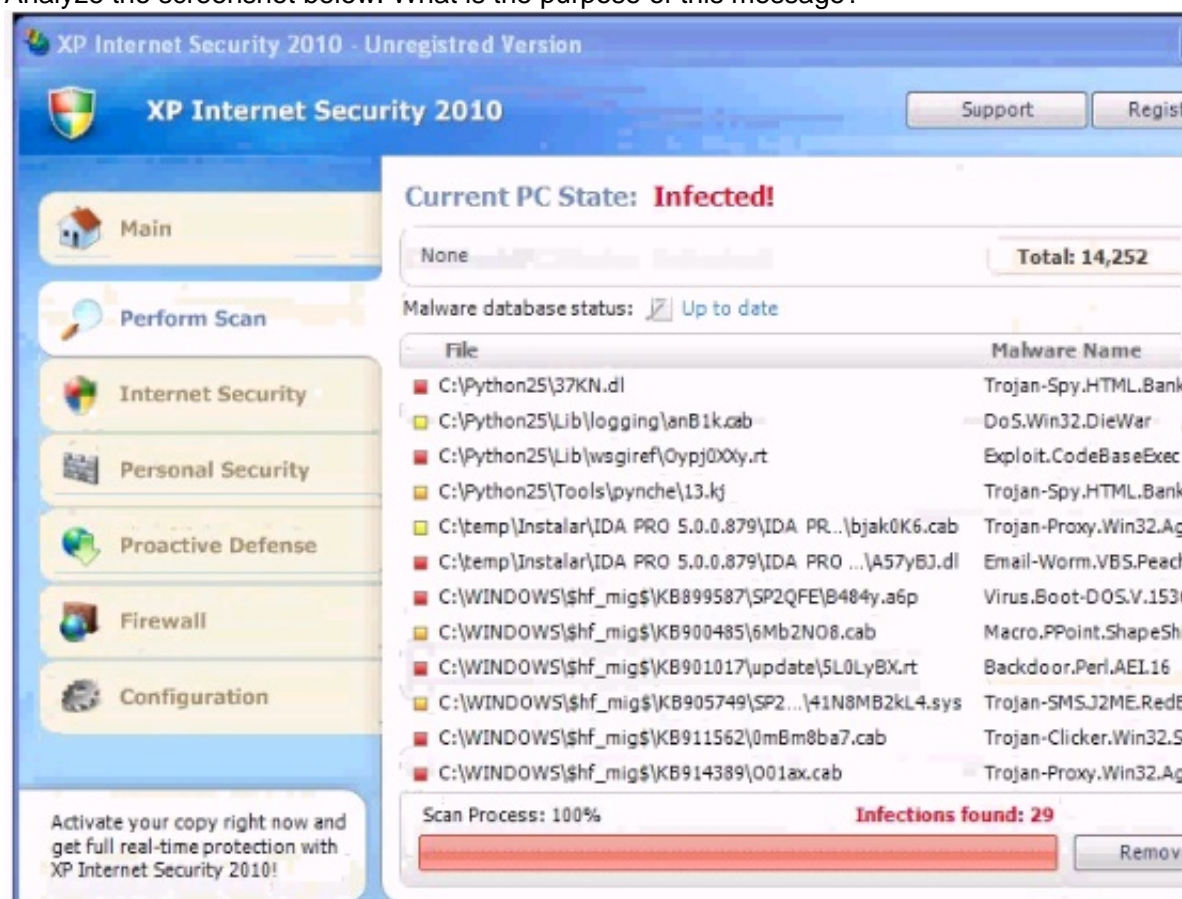
Which of the following is TRUE regarding the ability of attackers to eavesdrop on wireless communications?

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

**Answer: B**

#### NEW QUESTION 197

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 199

What type of attack can be performed against a wireless network using the tool Kismet?

- A. IP spoofing
- B. Eavesdropping
- C. Masquerading
- D. Denial of Service

**Answer: B**

#### NEW QUESTION 204

Why are false positives such a problem with IPS technology?

- A. File integrity is not guarantee
- B. Malicious code can get into the network
- C. Legitimate services are not delivered
- D. Rules are often misinterpreted

**Answer:** D

#### NEW QUESTION 208

Which of the following is a required component for successful 802.1x network authentication?

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

**Answer:** A

#### NEW QUESTION 213

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 215

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

- A. DDOS attacks are perpetrated by many distributed hosts
- B. DDOS affects many distributed targets
- C. Regular DOS focuses on a single route
- D. DDOS affects the entire Internet

**Answer:** A

#### NEW QUESTION 218

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 219

You work as a Network Administrator for McRobert Inc. You want to know the NetBIOS name of your computer. Which of the following commands will you use?

- A. NETSTAT -s
- B. NBTSTAT -s
- C. NBTSTAT -n
- D. NETSTAT -n

**Answer:** C

#### NEW QUESTION 222

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 224

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 Serve
- D. It is good practice to not allow users to send raw SQL commands to the SQL Serve

**Answer:** D

**NEW QUESTION 226**

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 230**

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 232**

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 237**

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 242**

What is the main reason that DES is faster than RSA?

- A. DES is less secur
- B. DES is implemented in hardware and RSA is implemented in softwar
- C. Asymmetric cryptography is generally much faster than symmetri
- D. Symmetric cryptography is generally much faster than asymmetri

**Answer:** D

**NEW QUESTION 243**

In addition to securing the operating system of production honey pot hosts, what is recommended to prevent the honey pots from assuming the identities of production systems that could result in the denial of service for legitimate users?

- A. Deploy the honey pot hosts as physically close as possible to production system
- B. Deploy the honey pot hosts in an unused part of your address spac
- C. Deploy the honey pot hosts to only respond to attack
- D. Deploy the honey pot hosts on used address spac

**Answer:** B

**NEW QUESTION 244**

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 248**

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. Router
- D. Firewall
- E. Repeater
- F. Hub

**Answer:** BCEF

**NEW QUESTION 250**

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 251**

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

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

**Answer:** B

**NEW QUESTION 255**

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

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

**Answer:** D

**NEW QUESTION 257**

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 258**

Which of the following is a benefit of using John the Ripper for auditing passwords?

- A. John's Blowfish cracking routine uses a complex central computing loop that increases the cost of each hash computation
- B. John the Ripper is much slower for auditing passwords encrypted with MD5 and Blowfish
- C. John's MD5 cracking routine uses a simplified central computing loop that decreases the cost of each hash computation
- D. John cannot use the DES bit-slicing technique, so it is much slower than other tools, especially when used against DES-encrypted passwords

**Answer:** C

**NEW QUESTION 261**

Where are user accounts and passwords stored in a decentralized privilege management environment?

- A. On a central authentication server
- B. On more than one server
- C. On each server
- D. On a server configured for decentralized privilege management

**Answer:** C



#### NEW QUESTION 265

Regarding the UDP header below, what is the length in bytes of the UDP datagram?

04 1a 00 a1 00 55 db 51

- A. 161
- B. 81
- C. 219
- D. 85

**Answer:** D

#### NEW QUESTION 266

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 267

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 269

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 272

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 277

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

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

**Answer:** AB

#### NEW QUESTION 280

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 cost

**Answer:** C

#### NEW QUESTION 283

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

- A. Before a system is patched
- B. After a system has been compromised
- C. Before a system has been compromised
- D. During an attack

**Answer:** C

#### NEW QUESTION 284

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 password
- B. The user account is shared by more than one user
- C. The user account is disabled
- D. The user account does not exist

**Answer:** A

#### NEW QUESTION 285

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 286

How many bytes does it take to represent the hexadecimal value 0xFEDCBA?

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

**Answer:** C

#### NEW QUESTION 289

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 290

Which of the following statements about Network Address Translation (NAT) are true? Each correct answer represents a complete solution. Choose two.

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

**Answer:** AC

#### NEW QUESTION 294

You are examining a packet capture session in Wireshark 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 (ping) to 192.168.23.255

- 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 297**

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 302**

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 303**

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 304**

While using Wireshark to investigate complaints of users being unable to login to a web application, you come across an HTTP POST submitted through your web application. The contents of the POST are listed below. Based on what you see below, which of the following would you recommend to prevent future damage to your database?

```
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 308**

Which of the following books deals with confidentiality?

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

**Answer:** B

**NEW QUESTION 311**

Which of the following are examples of Issue-Specific policies all organizations should address?

- A. Perimeter filtering guides, break times for employees, desktop neatness and backup procedure
- B. Rogue wireless access points, auditing, break time for employees and organizational structure

- C. Audit logs, physical access, mission statements and network protocols use
- D. Backup requirements, employee monitoring, physical access and acceptable use

**Answer:** D

#### NEW QUESTION 315

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 packets 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 316

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 319

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

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

**Answer:** C

#### NEW QUESTION 320

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 324

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 326

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 processes
- 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 situation
- D. It ensures that modifications are not made to data by unauthorized personnel or processes

**Answer:** ACD

#### NEW QUESTION 327

.....

## 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](#)**