

# 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 an Implementation of PKI?

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

**Answer:** A

#### NEW QUESTION 3

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 4

Which of the following hardware devices prevents broadcasts from crossing over subnets?

- A. Bridge
- B. Hub
- C. Router
- D. Modem

**Answer:** C

#### NEW QUESTION 5

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 6

Which class of IDS events occur when the IDS fails to alert on malicious data?

- A. True Negative
- B. True Positive
- C. False Positive
- D. False Negative

**Answer:** D

#### NEW QUESTION 7

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 8

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 9

During a scheduled evacuation training session the following events took place in this order:

- \* 1. Evacuation process began by triggering the building fire alarm.
- \* 2a. The meeting point leader arrived first at the designated meeting point and immediately began making note of who was and was not accounted for.
- \* 2b. Stairwell and door monitors made it to their designated position to leave behind a box of flashlights and prop the stairway doors open with a garbage can so employees can find exits and dispose of food and beverages.
- 2c. Special needs assistants performed their assigned responsibility to help employees out that require special assistance.
- \* 3. The safety warden communicated with the meeting point leader via walkie talkie to collect a list of missing personnel and communicated this information back to the searchers.
- \* 4. Searchers began checking each room and placing stick-it notes on the bottom of searched doors to designate which areas were cleared.
- \* 5. All special need assistants and their designated wards exited the building.
- \* 6. Searchers complete their assigned search pattern and exit with the Stairwell/door monitors.

Given this sequence of events, which role is in violation of its expected evacuation tasks?

- A. Safety warden
- B. Stairwell and door monitors
- C. Meeting point leader
- D. Searchers
- E. Special needs assistants

**Answer: B**

#### NEW QUESTION 10

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 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 12

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

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 17

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 21

Which of the following authentication methods are used by Wired Equivalent Privacy (WEP)? Each correct answer represents a complete solution. Choose two.

- A. Anonymous authentication
- B. Mutual authentication
- C. Open system authentication
- D. Shared key authentication

**Answer:** CD

#### NEW QUESTION 25

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 27

Which of the following protocols implements VPN using IPSec?

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

**Answer:** C

#### NEW QUESTION 32

Your customer wants to make sure that only computers he has authorized can get on his Wi-Fi. What is the most appropriate security measure you can recommend?

- A. A firewall
- B. WPA encryption
- C. WEP encryption
- D. Mac filtering

**Answer:** D

#### NEW QUESTION 34

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 37

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 41

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

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

**Answer:** C

#### NEW QUESTION 42

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 45

In preparation to do a vulnerability scan against your company's systems. You've taken the steps below:

You've notified users that there will be a system test.

You've prioritized and selected your targets and subnets.

You've configured the system to do a deep scan.

You have a member of your team on call to answer questions.

Which of the following is a necessary step to take prior to starting the scan?

- A. Placing the incident response team on call
- B. Clear relevant system log file
- C. Getting permission to run the scan
- D. Scheduling the scan to run before OS update

**Answer:** C

#### NEW QUESTION 48

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 49

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 54

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 56

Which of the following is required to be backed up on a domain controller to recover Active Directory?

- A. System state data
- B. Operating System files
- C. User's personal data
- D. Installed third party application's folders

**Answer:** A

**NEW QUESTION 58**

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 63**

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 68**

Which access control mechanism requires a high amount of maintenance since all data must be classified, and all users granted appropriate clearance?

- A. Mandatory
- B. Discretionary
- C. Rule set-based
- D. Role-Based

**Answer:** A

**NEW QUESTION 72**

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 74**

Which of the following is NOT typically used to mitigate the war dialing threat?

- A. Setting up monitored modems on special phone numbers
- B. Setting modems to auto-answer mode
- C. Proactively scanning your own phone numbers
- D. Monitoring call logs at the switch

**Answer:** B

**NEW QUESTION 78**

What protocol is a WAN technology?

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

**Answer:** D

**NEW QUESTION 80**

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 81

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 86

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 91

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 96

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 98

You work as a Network Administrator for McNeil Inc. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest domain-based network. The company's management has decided to provide laptops to its sales team members. These laptops are equipped with smart card readers. The laptops will be configured as wireless network clients. You are required to accomplish the following tasks: The wireless network communication should be secured.

The laptop users should be able to use smart cards for getting authenticated. In order to accomplish the tasks, you take the following steps:

Configure 802.1x and WEP for the wireless connections. Configure the PEAP-MS-CHAP v2 protocol for authentication. What will happen after you have taken these steps?

- A. The laptop users will be able to use smart cards for getting authenticated
- B. Both tasks will be accomplished
- C. None of the tasks will be accomplished
- D. The wireless network communication will be secure

**Answer:** D

#### NEW QUESTION 100

What technical control provides the most critical layer of defense if an intruder is able to bypass all physical security controls and obtain tapes containing critical data?

- A. Camera Recordings
- B. Security guards
- C. Encryption
- D. Shredding
- E. Corrective Controls

**Answer:** C

#### NEW QUESTION 102

What is the unnoticed theft of sensitive data from a laptop owned by an organization's CEO an example of in information warfare?



- A. Non-zero sum game
- B. Win-win situation
- C. Zero-sum game
- D. Symmetric warfare

**Answer:** D

**NEW QUESTION 107**

Which of the following are advantages of Network Intrusion Detection Systems (NIDS)?

- A. Analysis of encrypted traffic
- B. Provide insight into network traffic
- C. Detection of network operations problems
- D. Provide logs of network traffic that can be used as part of other security measure
- E. Inexpensive to manage
- F. B, C, and D
- G. A, C, and E
- H. B, D, and E
- I. A, B, and C

**Answer:** C

**NEW QUESTION 109**

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 111**

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 115**

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 117**

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 119**

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 121

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 password

**Answer: C**

#### NEW QUESTION 126

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 130

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 destination
- D. These fields are incremented each time a packet is transmitted to indicate the number of routers that an IP packet has traversed

**Answer: A**

#### NEW QUESTION 132

Which of the following is TRUE regarding Ethernet?

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

**Answer: C**

#### NEW QUESTION 134

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 138

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

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

**Answer: D**

#### NEW QUESTION 141

If Linux server software is a requirement in your production environment which of the following should you NOT utilize?

- A. Debian
- B. Mandrake
- C. Cygwin
- D. Red Hat

**Answer: C**

#### NEW QUESTION 145

Which layer of the TCP/IP Protocol Stack is responsible for port numbers?

- A. Network

- B. Transport
- C. Internet
- D. Application

**Answer: B**

#### NEW QUESTION 146

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 147

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 148

.....

## 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](#)**