

GIAC

Exam Questions GSEC

GIAC Security Essentials Certification



NEW QUESTION 1

Which of the following is a Layer 3 device that will typically drop directed broadcast traffic?

- A. Hubs
- B. Bridges
- C. Routers
- D. Switches

Answer: C

NEW QUESTION 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

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 4

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 5

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 6

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 7

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 8

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 9

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 10

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 10

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 12

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 14

Your software developer comes to you with an application that controls a user device. The application monitors its own behavior and that of the device and creates log files. The log files are expected to grow steadily and rapidly. Your developer currently has the log files stored in the /bin folder with the application binary. Where would you suggest that the developer store the log files?

- A. /var/log
- B. /etc/log
- C. /usr/log
- D. /tmp/log
- E. /dev/log

Answer: A

NEW QUESTION 17

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 19

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 24

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 29

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 integrit
- B. It provides mail transfer servic
- C. It uses a combination of public key and symmetric encryption for security of dat
- D. It provides connectivity between Web browser and Web serve

Answer: AC

NEW QUESTION 31

In a /24 subnet, which of the following is a valid broadcast address?

- A. 200.11.11.1
- B. 221.10.10.10
- C. 245.20.30.254
- D. 192.10.10.255

Answer: D

NEW QUESTION 36

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

- A. A multicast streaming applicatio
- B. A web browse
- C. A DNS zone transfe
- D. A file transfer applicatio

Answer: A

NEW QUESTION 40

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 43

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 47

What is the name of the Windows XP/2003 tool that you can use to schedule commands to be executed on remote systems during off-peak hours?

- A. SHTASKS.EXE
- B. SCHEDULETSKS.EXE
- C. SCHEDULR.EXE
- D. SCHRUN.EXE

Answer: A

NEW QUESTION 49

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 52

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 processe
- C. It determines the actions and behaviors of a single individual within a system, and identifies that particular individua
- D. It establishes the users' identity and ensures that the users are who they say they ar

Answer: D

NEW QUESTION 53

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

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

Answer: D

NEW QUESTION 58

An organization monitors the hard disks of its employees' computers from time to time. Which policy does this pertain to?

- A. Privacy policy
- B. Backup policy
- C. User password policy
- D. Network security policy

Answer: A

NEW QUESTION 61

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 64

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 69

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 73

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 78

Your CIO has found out that it is possible for an attacker to clone your company's RFID (Radio Frequency ID) based key cards. The CIO has tasked you with finding a way to ensure that anyone entering the building is an employee. Which of the following authentication types would be the appropriate solution to this problem?

- A. Mandatory Access Controls
- B. Bell-LaPadula
- C. Two-Factor
- D. TACACS

Answer: C

NEW QUESTION 83

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 85

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 87

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 91

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 95

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 99

Which of the following is an advantage of a Host Intrusion Detection System (HIDS) versus a Network Intrusion Detection System (NIDS)?

- A. Ability to detect malicious traffic after it has been decrypted by the host
- B. Ability to decrypt network traffic
- C. Ability to listen to network traffic at the perimeter
- D. Ability to detect malicious traffic before it has been decrypted

Answer: A

NEW QUESTION 103

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

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

Answer: C

NEW QUESTION 107

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 111

What is the motivation behind SYN/FIN scanning?

- A. The SYN/FIN combination is useful for signaling to certain Trojan
- B. SYN/FIN packets are commonly used to launch denial of service attacks against BSD host
- C. The crafted SYN/FIN packet sometimes gets past firewalls and filtering router
- D. A SYN/FIN packet is used in session hijacking to take over a sessio

Answer: B

NEW QUESTION 114

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 authenticate
- B. Both tasks will be accomplishe
- C. None of the tasks will be accomplishe
- D. The wireless network communication will be secure

Answer: D

NEW QUESTION 119

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 120

You have set up a local area network for your company. Your firewall separates your network into several sections: a DMZ with semi-public servers (web, dns, email) and an intranet with private servers. A penetration tester gains access to both sections and installs sniffers in each. He is able to capture network traffic for all the devices in the private section but only for one device (the device with the sniffer) in the DMZ. What can be inferred about the design of the system?

- A. You installed a router in the private section and a switch in the DMZ
- B. You installed a hub in the private section and a switch in the DMZ
- C. You installed a switch in the private section and a hub in the DMZ
- D. You installed a switch in the private section and a router in the DMZ

Answer: B

NEW QUESTION 124

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 127

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 128

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

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

Answer: C

NEW QUESTION 129

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

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

Answer: B

NEW QUESTION 131

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

- A. It is a mature technolog
- B. It is the best network securit
- C. It never needs patchin
- D. It is a firewall replacemen

Answer: A

NEW QUESTION 133

Which of the following heights of fence deters only casual trespassers?

- A. 8 feet
- B. 2 to 2.5 feet
- C. 6 to 7 feet
- D. 3 to 4 feet

Answer: D

NEW QUESTION 138

The Linux command to make the /etc/shadow file, already owned by root, readable only by root is which of the following?

- A. chmod 444/etc/shadow
- B. chown root: root/etc/shadow
- C. chmod 400/etc/shadow
- D. chown 400 /etc/shadow

Answer: C

NEW QUESTION 140

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 145

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 146

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 150

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 154

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 155

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 159

You work as a Network Administrator for Net Perfect Inc. The company has a Linux-based network. You have created a folder named Report. You have made David the owner of the folder. The members of a group named JAdmin can access the folder and have Read, Write, and Execute permissions. No other user can access the folder. You want to ensure that the members of the JAdmin group do not have Write permission on the folder. Also, you want other users to have Read permission on the Report folder. Which of the following commands will you use to accomplish the task?

- A. `chmod 777 report`
- B. `chown david.jadmin report`
- C. `chmod 555 report`
- D. `chmod 754 report`

Answer: D

NEW QUESTION 160

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 165

You work as a Network Administrator for NetTech Inc. To ensure the security of files, you encrypt data files using Encrypting File System (EFS). You want to make a backup copy of the files and maintain security settings. You can backup the files either to a network share or a floppy disk. What will you do to accomplish this?

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

Answer: A

NEW QUESTION 170

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 173

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 174

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 178

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 182

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 187

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 191

The previous system administrator at your company used to rely heavily on email lists, such as vendor lists and Bug Traq to get information about updates and patches. While a useful means of acquiring data, this requires time and effort to read through. In an effort to speed things up, you decide to switch to completely automated updates and patching. You set up your systems to automatically patch your production servers using a cron job and a scripted apt-get upgrade command. Of the following reasons, which explains why you may want to avoid this plan?

- A. The apt-get upgrade command doesn't work with the cron command because of incompatibility
- B. Relying on vendor and 3rd party email lists enables updates via email, for even faster patching
- C. Automated patching of production servers without prior testing may result in unexpected behavior or failures
- D. The command apt-get upgrade is incorrect, you need to run the apt-get update command

Answer: D

NEW QUESTION 192

.....

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](#)