

GIAC

Exam Questions GSEC

GIAC Security Essentials Certification



NEW QUESTION 1

What database can provide contact information for Internet domains?

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

Answer: C

NEW QUESTION 2

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 3

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 4

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 5

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 6

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 7

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 8

Which of the following protocols implements VPN using IPSec?

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

Answer: C

NEW QUESTION 9

Which of the following are used to suppress gasoline and oil fires? Each correct answer represents a complete solution. Choose three.

- A. Halon
- B. CO2
- C. Soda acid
- D. Water

Answer: ABC

NEW QUESTION 10

Which of the following is NOT a recommended best practice for securing Terminal Services and Remote Desktop?

- A. Require TLS authentication and data encryption whenever possible
- B. Make sure to allow all TCP 3389 traffic through the external firewall
- C. Group Policy should be used to lock down the virtual desktops of thin-client user
- D. Consider using IPSec or a VPN in addition to the RDP encryption if you are concerned about future RDP vulnerabilities

Answer: B

NEW QUESTION 10

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 12

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 17

What is the process of simultaneously installing an operating system and a Service Pack called?

- A. Synchronous Update
- B. Slipstreaming
- C. Simultaneous Update
- D. Synchronizing

Answer: B

NEW QUESTION 18

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

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

Answer: A

NEW QUESTION 23

In PKI, when someone wants to verify that the certificate is valid, what do they use to decrypt the signature?

- A. Receiver's digital signature
- B. X.509 certificate CA's private key
- C. Secret passphrase
- D. CA's public key

Answer: D

NEW QUESTION 24

What is TRUE about Workgroups and Domain Controllers?

- A. By default all computers running Windows 2008 can only form Domain Controllers not Workgroups
- B. Workgroups are characterized by higher costs while Domain Controllers by lower costs
- C. You cannot have stand-alone computers in the midst of other machines that are members of a domain
- D. Workgroup computers cannot share resources, only computers running on the same domain can
- E. You can have stand-alone computers in the midst of other machines that are members of a domain

Answer: E

NEW QUESTION 26

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 28

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 32

Which Defense-in-Depth principle starts with an awareness of the value of each section of information within an organization?

- A. Information centric defense
- B. Uniform information protection
- C. General information protection
- D. Perimeter layering

Answer: A

NEW QUESTION 34

You work as a Network Administrator for McNeil Inc. The company has a Linux-based network. David, a Sales Manager, wants to know the name of the shell that he is currently using. Which of the following commands will he use to accomplish the task?

- A. mv \$shell
- B. echo \$shell
- C. rm \$shell
- D. ls \$shell

Answer: B

NEW QUESTION 36

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 39

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 41

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

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

Answer: BD

NEW QUESTION 42

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 47

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 51

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 54

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 59

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 61

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 65

When you log into your Windows desktop what information does your Security Access Token (SAT) contain?

- A. The Security ID numbers (SIDs) of all the groups to which you belong
- B. A list of cached authentications
- C. A list of your domain privileges
- D. The Security ID numbers (SIDs) of all authenticated local users

Answer: C

NEW QUESTION 66

You have an automated system for patching the operating systems of all your computers. All patches are supposedly current. Yet your automated vulnerability scanner has just reported vulnerabilities that you believe have been patched. Which of the actions below should you take next?

- A. Check some systems manually
- B. Rerun the system patching routine
- C. Contact the incident response team
- D. Ignore the findings as false positive

Answer: A

NEW QUESTION 71

An attacker gained physical access to an internal computer to access company proprietary data. The facility is protected by a fingerprint biometric system that records both failed and successful entry attempts. No failures were logged during the time periods of the recent breach. The account used when the attacker entered the facility shortly before each incident belongs to an employee who was out of the area. With respect to the biometric entry system, which of the following actions will help mitigate unauthorized physical access to the facility?

- A. Try raising the Crossover Error Rate (CER)
- B. Try to lower the False Accept Rate (FAR)
- C. Try setting the Equal Error Rate (EER) to zero
- D. Try to set a lower False Reject Rate (FRR)

Answer: B

NEW QUESTION 75

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 76

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

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

Answer: B

NEW QUESTION 78

You are implementing wireless access at a defense contractor. Specifications say, you must implement the AES Encryption algorithm. Which encryption standard should you choose?

- A. WPA
- B. TKIP
- C. WEP
- D. WPA 2

Answer: D

NEW QUESTION 82

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 86

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 91

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 96

Which of the following TCP dump output lines indicates the first step in the TCP 3-way handshake?

- A. 07:09:43.368615 download.net 39904 > ftp.com.21: S 733381829:733381829(0) win 8760 <mss 1460> (DF)
- B. 07:09:43.370302 ftp.com.21 > download.net.39904: S 1192930639:1192930639(0) ack 733381830 win 1024 <mss 1460> (DF)
- C. 09:09:22.346383 ftp.com.21 > download.net.39904: , rst 1 win 2440(DF)
- D. 07:09:43.370355 download.net.39904 > ftp.com.21: , ack 1 win 8760 (DF)

Answer: A

NEW QUESTION 99

What protocol is a WAN technology?

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

Answer: D

NEW QUESTION 102

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 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 108

Which of the following Linux commands can change both the username and group name a file belongs to?

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

Answer: B

NEW QUESTION 109

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 112

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 117

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 119

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 away
- C. Eavesdropping attacks are easily detected on wireless network
- D. Eavesdropping attacks require expensive device

Answer: B

NEW QUESTION 121

When an IIS filename extension is mapped, what does this mean?

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

Answer: B

NEW QUESTION 123

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 128

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 130

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

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

Answer: C

NEW QUESTION 131

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 135

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 138

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

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

Answer: B

NEW QUESTION 143

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 space
- C. Deploy the honey pot hosts to only respond to attack
- D. Deploy the honey pot hosts on used address space

Answer: B

NEW QUESTION 148

When using Pretty Good Privacy (PGP) to digitally sign a message, the signature is created in a two-step process. First, the message to be signed is submitted to PGP's cryptographic hash algorithm. What is one of the hash algorithms used by PGP for this process?

- A. Blowfish
- B. DES
- C. SHA-1
- D. Cast

Answer: C

NEW QUESTION 153

Which of the following protocols are used to provide secure communication between a client and a server over the Internet?
Each correct answer represents a part of the solution. Choose two.

- A. SSL
- B. HTTP
- C. TLS
- D. SNMP

Answer: AC

NEW QUESTION 154

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 156

A Host-based Intrusion Prevention System (HIPS) software vendor records how the Firefox Web browser interacts with the operating system and other applications, and identifies all areas of Firefox functionality. After collecting all the data about how Firefox should work, a database is created with this information, and it is fed into the HIPS software. The HIPS then monitors Firefox whenever it's in use. What feature of HIPS is being described in this scenario?

- A. Signature Matching
- B. Application Behavior Monitoring
- C. Host Based Sniffing
- D. Application Action Modeling

Answer: B

NEW QUESTION 157

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

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

Answer: B

NEW QUESTION 159

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 163

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. John is working as a root user on the Linux operating system. He wants to change the modified date and time of the file private.txt to 11 Nov 2009 02:59:58 am. Which of the following commands will John use to accomplish his task?

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

- A. rm private.txt #11 Nov 2009 02:59:58 am
- B. touch -d "11 Nov 2009 02:59:58 am" private.txt
- C. touch private.txt #11 Nov 2009 02:59:58 am
- D. touch -t 200911110259.58 private.txt

Answer: BD

NEW QUESTION 165

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 166

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 cos

Answer: C

NEW QUESTION 168

What does the "x" character in the second field of the user account record of the /etc/passwd file indicate?

- A. The user account is using a shadow passwor
- B. The user account is shared by more than one use
- C. The user account is disable
- D. The user account does not exis

Answer: A

NEW QUESTION 172

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 176

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 addresse
- B. It allows external network clients access to internal service
- C. It allows the computers in a private network to share a global, ISP assigned address to connect to the Interne
- D. It provides added security by using Internet access to deny or permit certain traffic from the Bastion Hos

Answer: AC

NEW QUESTION 181

Which of the following terms is used for the process of securing a system or a device on a network infrastructure?

- A. Hardening
- B. Authentication
- C. Cryptography
- D. Sanitization

Answer: A

NEW QUESTION 184

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 189

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 192

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 197

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

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

Answer: C

NEW QUESTION 201

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 204

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 207

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 209

What are the two actions the receiver of a PGP email message can perform that allows establishment of trust between sender and receiver?

- A. Decode the message by decrypting the asymmetric key with his private key, then using the asymmetric key to decrypt the message
- B. Decode the message by decrypting the symmetric key with his private key, then using the symmetric key to decrypt the message
- C. Decode the message by decrypting the symmetric key with his public key, then using the symmetric key to decrypt the message
- D. Decrypt the message by encrypting the digital signature with his private key, then using the digital signature to decrypt the message

Answer: A

NEW QUESTION 210

.....

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](#)