Exam Questions GSEC

GIAC Security Essentials Certification

https://www.2passeasy.com/dumps/GSEC/

NEW QUESTION 1
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 2
When Net Stumbler is initially launched, it sends wireless frames to which of the following addresses?

A. Broadcast address
B. Default gateway address
C. Subnet address
D. Network address

Answer: A

NEW QUESTION 3
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 4
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 5
If you do NOT have an original file to compare to, what is a good way to identify steganography in potential carrier files?

A. Determine normal properties through methods like statistics and look for changes
B. Determine normal network traffic patterns and look for changes
C. Find files with the extension .stg
D. Visually verify the files you suspect to be steganography messages

Answer: A

NEW QUESTION 6
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 7
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 8
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 9
A US case involving malicious code is brought to trial. An employee had opened a helpdesk ticket to report specific instances of strange behavior on her system. The IT helpdesk representative collected information by interviewing the user and escalated the ticket to the system administrators. As the user had regulated and sensitive data on her computer, the system administrators had the hard drive sent to the company's forensic consultant for analysis and configured a new hard drive for the user. Based on the recommendations from the forensic consultant and the company's legal department, the CEO decided to prosecute the author of the malicious code. During the court case, which of the following would be able to provide direct evidence?

A. The IT helpdesk representative
B. The company CEO
C. The user of the infected system
D. The system administrator who removed the hard drive

Answer: C

NEW QUESTION 10
Which of the following statements about Microsoft's VPN client software is FALSE?

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

Answer: B

NEW QUESTION 10
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 15
What is the command-line tool for Windows XP and later that allows administrators the ability to get or set configuration data for a very wide variety of computer and user account settings?

A. IPCONFIG.EXE
B. NETSTAT.EXE
C. WMIC.EXE
D. C0NF1G.EXE

Answer: C

NEW QUESTION 18
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 21
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 23
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 27
Why would someone use port 80 for deployment of unauthorized services?

A. Google will detect the service listing on port 80 and post a link, so that people all over the world will surf to the rogue servic
B. If someone were to randomly browse to the rogue port 80 service they could be compromise
C. This is a technique commonly used to perform a denial of service on the local web serve
D. HTTP traffic is usually allowed outbound to port 80 through the firewall in most environment

Answer: D

NEW QUESTION 29
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 tim
B. First volume should be FAT32 and second volume should be NTF
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 34
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 domai

Answer: E

NEW QUESTION 36
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. SCHTASKS.EXE
B. SCHEDULETSKS.EXE
C. SCHEDULR.EXE
D. SCHRUN.EXE

Answer: A

NEW QUESTION 38
Which of the following statements about buffer overflow is true?

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

Answer: C

NEW QUESTION 41
Which of the following is generally practiced by the police or any other recognized governmental authority?

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

Answer: C

NEW QUESTION 43

You are doing some analysis of malware on a Unix computer in a closed test network. The IP address of the computer is 192.168.1.120. From a packet capture, you see the malware is attempting to do a DNS query for a server called iamabadserver.com so that it can connect to it. There is no DNS server on the test network to do name resolution. You have another computer, whose IP is 192.168.1.115, available on the test network that you would like for the malware connect to it instead. How do you get the malware to connect to that computer on the test network?

A. You modify the HOSTS file on the computer you want the malware to connect to and add an entry that reads: 192.168.1.120 iamabadserver iamabadserver.com
B. You modify the HOSTS file on the Unix computer your malware is running on and add an entry that reads: 192.168.1.115 iamabadserveriamabadserver.com
C. You modify the HOSTS file on the Unix computer your malware is running on and add an entry that reads: 192.168.1.120 iamabadserver iamabadserver.com
D. You modify the HOSTS file on the computer you want the malware to connect to and add an entry that reads: 192.168.1.115 iamabadserver iamabadserver.com

Answer: B

NEW QUESTION 46

Which of the following is a backup strategy?

A. Differential
B. Integrational
C. Recursive
D. Supplemental

Answer: A

NEW QUESTION 51

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 55

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 59

What is the name of the command-line tool for Windows that can be used to manage audit policies on remote systems?

A. SECEDTT.EXE
B. POLCLI.EXE
C. REMOTEAUDIT.EXE
D. AUDITPOL.EXE

Answer: D

NEW QUESTION 61

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 66

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 71
Which of the following is an UDP based protocol?

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

Answer: B

NEW QUESTION 76
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
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 82
A sensor that uses a light beam and a detecting plate to alarm if the light beam is obstructed is most commonly used to identify which of the following threats?

A. Power
B. Smoke
C. Natural Gas
D. Water
E. Toxins

Answer: B

NEW QUESTION 84
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 89
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 comman
B. Make the user accounts of all the sales managers the members of the root grou
C. Provide password of root user to all the sales manager
D. Ask each sales manager to run the application as the root use
E. As the application is owned by the root, no changes are require

Answer: A

NEW QUESTION 91

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 95
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 97
You work as a Network Administrator for Tech2tech Inc. You have configured a network-based IDS for your company. You have physically installed sensors at all key positions throughout the network such that they all report to the command console.
What will be the key functions of the sensors in such a physical layout?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: BC

NEW QUESTION 101
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 102
Which of the following is a signature-based intrusion detection system (IDS) ?

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

Answer: B

NEW QUESTION 107
Which of the following items are examples of preventive physical controls? Each correct answer represents a complete solution. Choose three.

A. Biometric access controls
B. Closed-circuit television monitors
C. Fire extinguishers
D. Locks and keys

Answer: ACD

NEW QUESTION 110
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 115

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 computatio
B. John the Ripper is much slower for auditing passwords encrypted with MD5 and Blowfis
C. John's MD5 cracking routine uses a simplified central computing loop that decreases the cost of each hash computatio
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 119
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 Interne
C. The packets may be deliberately spoofed by an attacke
D. The packets are a sign of excess fragmentatio
E. A and B
F. B and C
G. B and D
H. A and D

Answer: B

NEW QUESTION 124
Regarding the UDP header below, what is the length in bytes of the UDP datagrarn?
04 1a 00 a1 00 55 db 51

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

Answer: D

NEW QUESTION 127
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 129
The TTL can be found in which protocol header?

A. It is found in byte 8 of the ICMP heade
B. It is found in byte 8 of the IP heade
C. It is found in byte 8 of the TCP heade
D. It is found in byte 8 of the DNS heade

Answer: B

NEW QUESTION 131
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 por
B. It is a protocol used in the Universal Resource Locater (URL) address line to connect to a secure sit
C. It is a protocol used to provide security for a database server in an internal networ
D. It uses TCP port 80 as the default por

Answer: AB

NEW QUESTION 134
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 139

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 141
You are examining a packet capture session in Wire shark and see the packet shown in the accompanying image. Based on what you see, what is the appropriate protection against this type of attempted attack?

No..	Time	Source	Destination	Dest. Port	Info
35	20.657938	192.168.23.132	192.168.23.255		Echo (p1

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 145
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 147
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 148
When are Group Policy Objects (GPOs) NOT applied automatically to workstations?

A. At 90-minute intervals
B. At logon
C. Every time Windows Explorer is launched
D. At boot-up

Answer: C

NEW QUESTION 150
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 structur
C. Audit logs, physical access, mission statements and network protocols use
D. Backup requirements, employee monitoring, physical access and acceptable us

Answer: D

NEW QUESTION 151
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 overflo
B. They allow an attacker to set a Trojan in the operating system and thus open a backdoor for anytime acces
C. They allow an attacker to replace utility programs that can be used to detect the attacker's activit
D. They allow an attacker to run packet sniffers secretly to capture password

Answer: BCD

NEW QUESTION 152
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 155
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 processe
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 situatio
D. It ensures that modifications are not made to data by unauthorized personnel or processe

Answer: ACD

NEW QUESTION 160
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual GSEC Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the GSEC Product From:

https://www.2passeasy.com/dumps/GSEC/

Money Back Guarantee

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