GIAC

Exam Questions GSEC

GIAC Security Essentials Certification

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
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 2
Which of the following SIP methods is used to setup a new session and add a caller?

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

Answer: D

NEW QUESTION 3
When trace route fails to get a timely response for a packet after three tries, which action will it take?

A. It will print '* * *' for the attempts and increase the maximum hop count by on
B. It will exit gracefully, and indicate to the user that the destination is unreachabl
C. It will increase the timeout for the hop and resend the packet
D. It will print '* * *' for the attempts, increment the TTL and try again until the maximum hop coun

Answer: D

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 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 6
Which of the following works at the network layer and hides the local area network IP address and topology?

A. Network address translation (NAT)
B. Hub
C. MAC address
D. Network interface card (NIC)

Answer: A

NEW QUESTION 7
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 8
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 9
What database can provide contact information for Internet domains?

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

Answer: C

NEW QUESTION 10
Two clients connecting from the same public IP address (for example - behind the same NAT firewall) can connect simultaneously to the same web server on the Internet, provided what condition is TRUE?

A. The server is not using a well-known por
B. The server is on a different networ
C. The client-side source ports are differen
D. The clients are on different subnet

Answer: C

NEW QUESTION 10
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 12
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 13
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 14
Which of the following choices accurately describes how PGP works when encrypting email?

A. PGP encrypts the message with the recipients public key, then encrypts this key with a random asymmetric ke

B. PGP creates a random asymmetric key that it uses to encrypt the message, then encrypts this key with the recipient's public key
C. PGP creates a random symmetric key that it uses to encrypt the message, then encrypts this key with the recipient's public key
D. PGP encrypts the message with the recipients public key, then encrypts this key with a random symmetric ke

Answer: B

NEW QUESTION 15
Your organization is developing a network protection plan. No single aspect of your network seems more important than any other. You decide to avoid separating your network into segments or categorizing the systems on the network. Each device on the network is essentially protected in the same manner as all other devices.
This style of defense-in-depth protection is best described as which of the following?

A. Uniform protection
B. Threat-oriented
C. Information-centric
D. Protected enclaves

Answer: A

NEW QUESTION 20
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 22
You are responsible for a Microsoft based network. Your servers are all clustered. Which of the following are the likely reasons for the clustering?
Each correct answer represents a complete solution. Choose two.

A. Reduce power consumption
B. Ease of maintenance
C. Load balancing
D. Failover

Answer: CD

NEW QUESTION 26
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 28
You work as a Network Administrator for McNeil Inc. You are installing an application. You want to view the log file whenever a new entry is added to the /var/log/messages log file. Which of the following commands will you use to accomplish this?

A. TAIL -show /var/log/messages
B. TAIL -f /var/log/messages
C. TAIL -50 /var/log/messages
D. TAIL -view /var/log/messages

Answer: B

NEW QUESTION 29
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 31

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 33
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 38
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 42
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 46
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 50
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 54
Which of the following protocols implements VPN using IPSec?

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

Answer: C

NEW QUESTION 57
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 60
Which of the following utilities provides an efficient way to give specific users permission to use specific system commands at the root level of a Linux operating system?

A. Snort
B. Apache
C. SSH
D. SUDO

Answer: D

NEW QUESTION 64
Which of the following best describes the level of risk associated with using proprietary crypto algorithms.?

A. Proprietary cryptographic algorithms are required by law to use shorter key lengths in the United States, so the risk is hig
B. Proprietary algorithms have not been subjected to public scrutiny, so they have been checked less throughly for vulnerabilitie
C. Proprietary algorithms are less likely be vulnerable than algorithms that have been publicly disclosed because of enhanced secrecy of the algorith
D. Proprietary algorithms are not known to generally be any more or less vulnerable than publicly scrutinized algorithm

Answer: B

NEW QUESTION 67
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 69
For most organizations, which of the following should be the highest priority when it comes to physical security concerns?

A. Controlling ingress and egress
B. Controlling access to workstations
C. Ensuring employee safety
D. Controlling access to servers
E. Protecting physical assets

Answer: C

NEW QUESTION 71
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 possibl
B. Make sure to allow all TCP 3389 traffic through the external firewal
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 vulnerabilitie

Answer: B

NEW QUESTION 74
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 78
Which of the following are the types of intrusion detection systems?
Each correct answer represents a complete solution. Choose all that apply.

A. Host-based intrusion detection system (HIDS)
B. Client-based intrusion detection system (CIDS)
C. Server-based intrusion detection system (SIDS)
D. Network intrusion detection system (NIDS)

Answer: AD

NEW QUESTION 83
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 88
What does an attacker need to consider when attempting an IP spoofing attack that relies on guessing Initial Sequence Numbers (ISNs)?

A. These attacks work against relatively idle server
B. These attacks rely on a modified TCP/IP stack to functio
C. These attacks can be easily traced back to the sourc
D. These attacks only work against Linux/Unix host

Answer: A

NEW QUESTION 92
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 97
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 102
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 106
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 108
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 111
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 116
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 117
Which of the following Unix syslog message priorities is the MOST severe?

A. err
B. emerg
C. crit
D. alert

Answer: B

NEW QUESTION 122
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 123
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 124
Which of the following monitors program activities and modifies malicious activities on a system?

A. Back door
B. HIDS
C. NIDS
D. RADIUS

Answer: B

NEW QUESTION 126
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 priontized 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 cal
B. Clear relevant system log file
C. Getting permission to run the sca
D. Scheduling the scan to run before OS update

Answer: C

NEW QUESTION 128
Which of the following elements is the most important requirement to ensuring the success of a business continuity plan?

A. Disaster Recover Plans
B. Anticipating all relevant threats
C. Executive buy-in
D. Clearly defining roles and responsibilities
E. Training

Answer: C

NEW QUESTION 130
What is the term for a game in which for every win there must be an equivalent loss?

A. Asymmetric
B. Untenable
C. Zero-sum
D. Gain-oriented

Answer: C

NEW QUESTION 134
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 137
While building multiple virtual machines on a single host operating system, you have determined that each virtual machine needs to work on the network as a separate entity with its own unique IP address on the same logical subnet. You also need to limit each guest operating system to how much system resources it has access to. Which of the following correctly identifies steps that must be taken towards setting up these virtual environments?

A. The virtual machine software must define a separate virtual network Interface to each virtual machine and then define which unique logical hard drive partition should be available to the guest operating syste
B. The virtual machine software must define a separate virtual network interface since each system needs to have an IP address on the same logical subnet requiring they use the same physical interface on the host operating syste
C. The virtual machine software must define a separate virtual network interface to each virtual machine as well as how much RAM should be available to each virtual machin
D. The virtual machine software establishes the existence of the guest operating systems and the physical system resources to be used by that system will be configured from within the guest operating syste
E. The virtual machine software must define a separate physical network interface to each virtual machine so that the guest operating systems can have unique IP addresses and then define how much of the systems RAM is available to the guest operating syste

Answer: E

NEW QUESTION 142
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 143
Which of the following files contains the shadowed password entries in Linux?

A. /etc/passwd
B. /etc/shadow
C. /etc/profile
D. /etc/shdpwd

Answer: B

NEW QUESTION 147
You have been hired to design a TCP/IP-based network that will contain both Unix and Windows computers. You are planning a name resolution strategy. Which of the following services will best suit the requirements of the network?

A. APIPA
B. LMHOSTS
C. DNS
D. DHCP
E. WINS

Answer: C

NEW QUESTION 151
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 154
What is the key difference between Electronic Codebook mode and other block cipher modes like Cipher Block Chaining, Cipher-Feedback and Output-Feedback?

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

Answer: C

NEW QUESTION 157
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 160
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 163
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 167

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 169
Which of the following tools is used to query the DNS servers to get detailed information about IP addresses, MX records, and NS servers?

A. NBTSTAT
B. NSLOOKUP
C. PING
D. NETSTAT

Answer: B

NEW QUESTION 174
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 manuall
B. Rerun the system patching routine
C. Contact the incident response tea
D. Ignore the findings as false positive

Answer: A

NEW QUESTION 179
Which of the following describes software technologies that improve portability, manageability, and compatibility of applications by encapsulating them from the underlying operating system on which they are executed?

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

Answer: C

NEW QUESTION 183
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 188
Which of the following is an UDP based protocol?

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

Answer: B

NEW QUESTION 192
It is possible to sniff traffic from other hosts on a switched Ethernet network by impersonating which type of network device?

A. Switch
B. Bridge
C. Hub
D. Router

Answer: D

NEW QUESTION 195
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 200
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 202
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 203
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 205
Mark works as a Network Administrator for NetTech Inc. The company has a Windows 2003 domain- based network. The network contains ten Windows 2003 member servers, 150 Windows XP Professional client computers. According to the company's security policy, Mark needs to check whether all the computers in the network have all available security updates and shared folders. He also needs to check the file system type on each computer's hard disk. Mark installs and runs MBSACLI.EXE with the appropriate switches on a server. Which of the following tasks will he accomplish?

A. None of the tasks will be accomplishe
B. He will be able to check the file system type on each computer's hard dis
C. He will be able to accomplish all the task
D. He will be able to check all available security updates and shared folder

Answer: C

NEW QUESTION 208
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 213
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 215
What is the first thing that should be done during the containment step of incident handling?

A. Change all the passwords
B. Secure the area
C. Prepare the Jump bag
D. Notify management
E. Prepare a report

Answer: B

NEW QUESTION 220
Which of the following statements would be seen in a Disaster Recovery Plan?

A. "Instructions for notification of the media can be found in Appendix A"
B. "The Emergency Response Plan should be executed in the case of any physical disaster listed on page 3."
C. "The target for restoration of business operations is 72 hours from the declaration of disaster."
D. "After arriving at the alternate site, utilize the server build checklist to rebuild all servers on the server rebuild list."

Answer: D

NEW QUESTION 225
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 230
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 231
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 235
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 236
You work as a Network Administrator for NetTech Inc. When you enter http://66.111.64.227 in the browser's address bar, you are able to access the site. But, you are unable to access the site when you enter http://www.uCertify.com. What is the most likely cause?

A. DNS entry is not available for the host nam
B. The site's Web server is offlin
C. The site's Web server has heavy traffi
D. WINS server has no NetBIOS name entry for the serve

Answer: A

NEW QUESTION 241

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

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

Answer: B

NEW QUESTION 242
Analyze the screenshot below. What is the purpose of this message?

A. To gather non-specific vulnerability information
B. To get the user to download malicious software
C. To test the browser plugins for compatibility
D. To alert the user to infected software on the compute

Answer: D

NEW QUESTION 247
What type of attack can be performed against a wireless network using the tool Kismet?

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

Answer: B

NEW QUESTION 249
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 251
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 253
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 255
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 256
Which of the following is a characteristic of hash operations?

A. Asymmetric
B. Non-reversible
C. Symmetric
D. Variable length output

Answer: D

NEW QUESTION 259
Validating which vulnerabilities in a network environment are able to be exploited by an attacker is called what?

A. Anomaly detection
B. Vulnerability scanning
C. Perimeter assessment
D. Penetration testing

Answer: B

NEW QUESTION 261
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 265
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 266
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 270
Which of the following quantifies the effects of a potential disaster over a period of time?

A. Risk Assessment
B. Business Impact Analysis
C. Disaster Recovery Planning
D. Lessons Learned

Answer: B

NEW QUESTION 272
Which of the following processes is known as sanitization?

A. Assessing the risk involved in discarding particular informatio
B. Verifying the identity of a person, network host, or system proces
C. Physically destroying the media and the information stored on i
D. Removing the content from the media so that it is difficult to restor

Answer: D

NEW QUESTION 276

Which of the following defines the communication link between a Web server and Web applications?

A. CGI
B. PGP
C. Firewall
D. IETF

Answer: A

NEW QUESTION 279
What is SSL primarily used to protect you against?

A. Session modification
B. SQL injection
C. Third-patty sniffing
D. Cross site scripting

Answer: C

NEW QUESTION 281
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 286
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. Brouter
D. Firewall
E. Repeater
F. Hub

Answer: BCEF

NEW QUESTION 287
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 288
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 291
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 296

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

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

Answer: B

NEW QUESTION 298
You are examining an IP packet with a header of 40 bytes in length and the value at byte 0 of the packet header is 6. Which of the following describes this packet?

A. This is an IPv4 packet; the protocol encapsulated in the payload is unspecifie
B. This is an IPv4 packet with a TCP payloa
C. This is an IPv6 packet; the protocol encapsulated in the payload is unspecifie
D. This is an IPv6 packet with a TCP payloa

Answer: C

NEW QUESTION 299
Which of the following protocols allows an e-mail client to access and manipulate a remote e-mail file without downloading it to the local computer?

A. IMAP
B. SNMP
C. POP3
D. SMTP

Answer: A

NEW QUESTION 302
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 303
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 307
Where are user accounts and passwords stored in a decentralized privilege management environment?

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

Answer: C

NEW QUESTION 310
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 313

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 316
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 320
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 321
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 domai
C. Ethernet is shared medi
D. Stations are not required to listen before they transmi

Answer: C

NEW QUESTION 324
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 327
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 329
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 334
How many bytes does it take to represent the hexadecimal value OxFEDCBA?

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

Answer: C

NEW QUESTION 336
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 341
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 networ
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 344
You work as a Network Administrator for Tech Perfect Inc. The company has a Linux-based network. You want to kill a process running on a Linux server. Which of the following commands will you use to know the process identification number (PID) of the process?

A. killall
B. ps
C. getpid
D. kill

Answer: B

NEW QUESTION 345
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 347
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 351
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?

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 356
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 360
Which of the following is used to allow or deny access to network resources?

A. Spoofing
B. ACL
C. System hardening
D. NFS

Answer: B

NEW QUESTION 364
Which command would allow an administrator to determine if a RPM package was already installed?

A. rpm -s
B. rpm -q
C. rpm -a
D. rpm -t

Answer: B

NEW QUESTION 366
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 ba
B. Conduct a forensic analysis of all evidence collected BEFORE starting the chain of custod
C. Take photographs of all persons who have had access to the compute
D. Check the backup integrity using a checksum utility like MD5, and sign and seal each piece of collected evidence in a plastic ba

Answer: D

NEW QUESTION 370
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?

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 375
Which of the following books deals with confidentiality?

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

Answer: B

NEW QUESTION 379
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 380
Which of the following networking topologies uses a hub to connect computers?

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

Answer: C

NEW QUESTION 385
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 387
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 389
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 messag
B. Decode the message by decrypting the symmetric key with his private key, then using the symmetric key to decrypt the messag
C. Decode the message by decrypting the symmetric key with his public key, then using the symmetric key to decrypt the messag
D. Decrypt the message by encrypting the digital signature with his private key, then using the digital signature to decrypt the messag

Answer: A

NEW QUESTION 394
In trace route results, what is the significance of an * result?

A. A listening port was identifie
B. A reply was returned in less than a secon

C. The target host was successfully reache
D. No reply was received for a particular ho

Answer: D

NEW QUESTION 397
......

Relate Links

100% Pass Your GSEC Exam with Exambible Prep Materials

https://www.exambible.com/GSEC-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/