



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

You work as a Linux technician for Tech Perfect Inc. You have lost the password of the root. You want to provide a new password. Which of the following steps will you take to accomplish the task?

- A. The password of the root user cannot be change
- B. Use the PASSWD root comman
- C. Reboot the compute
- D. Reboot the computer in run level 0. Use INIT=/bin/sh as a boot optio
- E. At the bash# prompt, run the PASSWD root comman
- F. Reboot the computer in run level 1. Use INIT=/bin/sh as a boot optio
- G. At the bash# prompt, run the PASSWD root comman

Answer: D

NEW QUESTION 2

At what point in the Incident Handling process should an organization determine its approach to notifying law enforcement?

- A. When performing analysis
- B. When preparing policy
- C. When recovering from the incident
- D. When reacting to an incident

Answer: D

NEW QUESTION 3

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 4

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

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

Answer: C

NEW QUESTION 5

What is the maximum passphrase length in Windows 2000/XP/2003?

- A. 255 characters
- B. 127 characters
- C. 95 characters
- D. 63 characters

Answer: B

NEW QUESTION 6

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

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

Answer: D

NEW QUESTION 7

The Windows 'tracert' begins by sending what type of packet to the destination host?

- A. A UDP packet with a TTL of 1
- B. An ICMP Echo Request
- C. An ICMP Router Discovery
- D. An ICMP Echo Reply

Answer: A

NEW QUESTION 8

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 9

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 10

Which of the following are the types of access controls?

Each correct answer represents a complete solution. Choose three.

- A. Physical
- B. Administrative
- C. Automatic
- D. Technical

Answer: ABD

NEW QUESTION 10

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 11

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 port
- B. The server is on a different network
- C. The client-side source ports are different
- D. The clients are on different subnet

Answer: C

NEW QUESTION 14

What is a security feature available with Windows Vista and Windows 7 that was not present in previous Windows operating systems?

- A. Data Execution Prevention (DEP)
- B. User Account Control (UAC)
- C. Encrypting File System (EFS)
- D. Built-in IPSec Client

Answer: B

NEW QUESTION 17

You work as a Network Administrator for Rick International. The company has a TCP/IP-based network. A user named Kevin wants to set an SSH terminal at

home to connect to the company's network. You have to configure your company's router for it. By default, which of the following standard ports does the SSH protocol use for connection?

- A. 443
- B. 22
- C. 21
- D. 80

Answer: B

NEW QUESTION 19

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 21

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 24

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 25

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 26

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 31

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 35

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 39

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 44

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 45

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 46

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 50

Which of the following is referred to as Electromagnetic Interference (EMI)?

- A. Electrical line noise
- B. Spike
- C. Transient
- D. Brownout

Answer: A

NEW QUESTION 54

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 59

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 61

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 66

Which of the following protocols implements VPN using IPSec?

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

Answer: C

NEW QUESTION 70

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 73

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 78

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 79

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 84

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 89

When discussing access controls, which of the following terms describes the process of determining the activities or functions that an Individual is permitted to perform?

- A. Authentication
- B. Identification
- C. Authorization
- D. Validation

Answer: C

NEW QUESTION 90

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 service
- B. If someone were to randomly browse to the rogue port 80 service they could be compromised
- C. This is a technique commonly used to perform a denial of service on the local web server
- D. HTTP traffic is usually allowed outbound to port 80 through the firewall in most environments

Answer: D

NEW QUESTION 92

Which Linux file lists every process that starts at boot time?

- A. inetd
- B. netsrv
- C. initd
- D. inittab

Answer: D

NEW QUESTION 94

Users at the Marketing department are receiving their new Windows XP Professional workstations. They will need to maintain local work files in the first logical volume, and will use a second volume for the information shared between the area group. Which is the best file system design for these workstations?

- A. Both volumes should be converted to NTFS at install time
- B. First volume should be FAT32 and second volume should be NTFS
- C. First volume should be EFS and second volume should be FAT32.
- D. Both volumes should be converted to FAT32 with NTFS DACL

Answer: A

NEW QUESTION 99

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 102

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

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

Answer: A

NEW QUESTION 104

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 107

You are going to upgrade your hard disk's file system from FAT to NTFS. What are the major advantages of the NTFS file system over FAT16 and FAT32 file systems?

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

- A. NTFS gives better file security than FAT16 and FAT32.
- B. Automatic backu
- C. NTFS file system supports for larger hard disk
- D. NTFS give improved disk compression than FAT16 and FAT32.

Answer: ACD

NEW QUESTION 108

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 109

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

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

Answer: D

NEW QUESTION 110

Which of the following statements about buffer overflow is true?

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

Answer: C

NEW QUESTION 115

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

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

You've prioritized and selected your targets and subnets.

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

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

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

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

Answer: C

NEW QUESTION 118

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 121

What type of malware is a self-contained program that has the ability to copy itself without parasitically infecting other host code?

- A. Trojans
- B. Boot infectors
- C. Viruses
- D. Worms

Answer: D

NEW QUESTION 124

You work as a Network Administrator for NetTech Inc. The company wants to encrypt its e-mails. Which of the following will you use to accomplish this?

- A. PPTP
- B. IPSec
- C. PGP
- D. NTFS

Answer: C

NEW QUESTION 128

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 130

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 system
- 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 system
- 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 machine
- 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 system
- 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 system's RAM is available to the guest operating system

Answer: E

NEW QUESTION 133

What type of formal document would include the following statement?

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal application of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies, and if there is any uncertainty, employees should consult their supervisor or manager.

- A. Company privacy statement
- B. Remote access policy
- C. Acceptable use policy
- D. Non-disclosure agreement

Answer: C

NEW QUESTION 136

Which of the following classes of fire comes under Class C fire?

- A. Paper or wood fire
- B. Oil fire
- C. Combustible metals fire
- D. Electronic or computer fire

Answer: D

NEW QUESTION 138

When no anomaly is present in an Intrusion Detection, but an alarm is generated, the response is known as.

- A. False negative
- B. False positive
- C. True positive
- D. True negative

Answer: B

NEW QUESTION 142

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 145

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 150

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 154

SSL session keys are available in which of the following lengths?

- A. 40-bit and 128-bit
- B. 64-bit and 128-bit
- C. 128-bit and 1,024-bit
- D. 40-bit and 64-bit

Answer: A

NEW QUESTION 155

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 160

Which of the following is a backup strategy?

- A. Differential

- B. Integrational
- C. Recursive
- D. Supplemental

Answer: A

NEW QUESTION 161

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 166

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 170

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 172

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 174

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 178

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 180

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

- A. Mandatory Access Controls
- B. Bell-LaPadula

- C. Two-Factor
- D. TACACS

Answer: C

NEW QUESTION 183

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 184

You work as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. You are required to search for the error messages in the `/var/log/messages` log file. Which of the following commands will you use to accomplish this?

- A. `ps /var/log/messages`
- B. `cat /var/log/messages | look error`
- C. `cat /var/log/messages | grep error`
- D. `cat /var/log/messages`

Answer: C

NEW QUESTION 186

Which of the following applications cannot proactively detect anomalies related to a computer?

- A. Firewall installed on the computer
- B. NIDS
- C. HIDS
- D. Anti-virus scanner

Answer: B

NEW QUESTION 191

Which of the following protocols describes the operation of security In H.323? A. H.239

- A. H.245
- B. H.235
- C. H.225

Answer: C

NEW QUESTION 196

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 199

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 201

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 types of computers is used for attracting potential intruders?

- A. Files pot
- B. Honey pot
- C. Data pot
- D. Bastion host

Answer: B

NEW QUESTION 204

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 208

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 accomplished
- B. He will be able to check the file system type on each computer's hard disk
- 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 212

What protocol is a WAN technology?

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

Answer: D

NEW QUESTION 214

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 215

You work as a Network Administrator for Net Soft Inc. You are designing a data backup plan for your company's network. The backup policy of the company requires high security and easy recovery of data. Which of the following options will you choose to accomplish this?

- A. Take a full backup daily with the previous night's tape taken offsite
- B. Take a full backup daily and use six-tape rotation
- C. Take a full backup on Monday and an incremental backup on each of the following weekday
- D. Keep Monday's backup offsite
- E. Take a full backup on alternate days and keep rotating the tape
- F. Take a full backup on Monday and a differential backup on each of the following weekday
- G. Keep Monday's backup offsite
- H. Take a full backup daily with one tape taken offsite weekly

Answer: A

NEW QUESTION 217

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 222

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 224

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 229

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 232

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 234

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 237

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

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

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

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

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

Answer: D

NEW QUESTION 243

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

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

Answer: C

NEW QUESTION 246

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 249

You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network. You have configured a firewall on the network. A filter has been applied to block all the ports. You want to enable sending and receiving of emails on the network. Which of the following ports will you open?

Each correct answer represents a complete solution. Choose two.

- A. 80
- B. 25
- C. 20
- D. 110

Answer: BD

NEW QUESTION 254

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

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

H. B, D, and E
I. A, B, and C

Answer: C

NEW QUESTION 257

Which of the following is a required component for successful 802.lx network authentication?

- A. Supplicant
- B. 3rd-party Certificate Authority
- C. Ticket Granting Server (TGS)
- D. IPSec

Answer: A

NEW QUESTION 261

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 263

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 268

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 270

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 275

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 280

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 284

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 288

Which of the following TCP packet flags indicates that host should IMMEDIATELY terminate the connection containing the packet?

- A. FIN
- B. URG
- C. SYN
- D. RST

Answer: D

NEW QUESTION 291

Which of the following are network connectivity devices?

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

- A. Network analyzer
- B. Bridge
- C. Router
- D. Firewall
- E. Repeater
- F. Hub

Answer: BCEF

NEW QUESTION 294

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 299

Your system has been infected by malware. Upon investigation, you discover that the malware propagated primarily via email. The malware attacked known vulnerabilities for which patches are available, but due to problems with your configuration management system you have no way to know which systems have been patched and which haven't, slowing your progress in patching your network. Of the following, which solution would you use to protect against this propagation vector?

- A. Encrypt the emails on the server
- B. Scan and block suspect email attachments at the email server
- C. Install a firewall between the email server and the Internet
- D. Separate the email server from the trusted portions of the network

Answer: B

NEW QUESTION 303

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 308

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 310

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 315

What defensive measure could have been taken that would have protected the confidentiality of files that were divulged by systems that were compromised by malware?

- A. Ingress filtering at the host level
- B. Monitoring for abnormal traffic flow
- C. Installing file integrity monitoring software
- D. Encrypting the files locally when not in use

Answer: D

NEW QUESTION 317

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 unspecified
- B. This is an IPv4 packet with a TCP payload
- C. This is an IPv6 packet; the protocol encapsulated in the payload is unspecified
- D. This is an IPv6 packet with a TCP payload

Answer: C

NEW QUESTION 322

Which of the following is a benefit of using John the Ripper for auditing passwords?

- A. John's Blowfish cracking routine uses a complex central computing loop that increases the cost of each hash computation
- B. John the Ripper is much slower for auditing passwords encrypted with MD5 and Blowfish
- C. John's MD5 cracking routine uses a simplified central computing loop that decreases the cost of each hash computation
- D. John cannot use the DES bit-slicing technique, so it is much slower than other tools, especially when used against DES-encrypted password

Answer: C

NEW QUESTION 326

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 330

What is the name of the registry key that is used to manage remote registry share permissions for the whole registry?

- A. regkey
- B. regmng
- C. winreg
- D. rrsreg

Answer: C

NEW QUESTION 332

Regarding the UDP header below, what is the length in bytes of the UDP datagram?

04 1a 00 a1 00 55 db 51

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

Answer: D

NEW QUESTION 335

An employee attempting to use your wireless portal reports receiving the error shown below. Which scenario is occurring?

- A. A denial-of-service attack is preventing a response from the porta
- B. Another access point is deauthenticating legitimate client
- C. The encrypted data is being intercepted and decrypte
- D. Another access point is attempting to intercept the dat

Answer: D

NEW QUESTION 339

Which of the following is a private, RFC 1918 compliant IP address that would be assigned to a DHCP scope on a private LAN?

- A. 127.0.0.100
- B. 169.254.1.50
- C. 10.254.1.50
- D. 172.35.1.100

Answer: C

NEW QUESTION 341

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 346

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 349

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 350

Which of the following BEST describes the two job functions of Microsoft Baseline Security Analyzer (MBSA)?

- A. Vulnerability scanner and auditing tool
- B. Auditing tool and alerting system
- C. Configuration management and alerting system
- D. Security patching and vulnerability scanner

Answer: D

NEW QUESTION 353

Which of the following is TRUE regarding Ethernet?

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

Answer: C

NEW QUESTION 355

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 359

Which of the following statements best describes where a border router is normally placed?

- A. Between your firewall and your internal network
- B. Between your firewall and DNS server
- C. Between your ISP and DNS server
- D. Between your ISP and your external firewall

Answer: D

NEW QUESTION 364

You are examining a packet capture session in Wireshark 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 368

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 369

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 371

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

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

Answer: B

NEW QUESTION 376

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 378

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 380

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 384

What would the following IP tables command do?
IP tables -I INPUT -s 99.23.45.1/32 -j DROP

- A. Drop all packets from the source address
- B. Input all packers to the source address
- C. Log all packets to or from the specified address
- D. Drop all packets to the specified address

Answer: A

NEW QUESTION 386

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 391

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

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

Answer: C

NEW QUESTION 395

Which of the following is a new Windows Server 2008 feature for the Remote Desktop Protocol (RDP)?

- A. The ability to allow the administrator to choose a port other than the default RDP port (TCP 3389)
- B. The ability to support connections from mobile devices like smart phones
- C. The ability to allow clients to authenticate over TLS
- D. The ability to allow clients to execute individual applications rather than using a terminal desktop

Answer: D

NEW QUESTION 399

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 400

Which of the following SIP INVITE lines indicates to the remote registrar the VoIP phone that initiated the call?

- A. Via
- B. To
- C. From-Agent
- D. User-Agent

Answer: D

NEW QUESTION 401

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 404

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

- A. A listening port was identified
- B. A reply was returned in less than a second
- C. The target host was successfully reached
- D. No reply was received for a particular host

Answer: D

NEW QUESTION 405

.....

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/>