



**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

Which of the following protocols is used to send e-mails on the Internet?

- A. SMTP
- B. IMAP4
- C. POP3
- D. HTTP

**Answer:** A

#### NEW QUESTION 2

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

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

**Answer:** C

#### NEW QUESTION 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 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 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 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 7

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 8

Which of the following radio frequencies is used by the IEEE 802.11a wireless network?

- A. 3.7 GHz
- B. 7.0 GHz
- C. 2.4 GHz
- D. 5.0 GHz

**Answer:** D

#### NEW QUESTION 9

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 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 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 15

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 17

On which of the following OSI model layers does IPSec operate? A. Physical layer

- A. Network layer
- B. Data-link layer
- C. Session layer

**Answer:** B

#### NEW QUESTION 22

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 27

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 28

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 31

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 32

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 33

Where is the source address located in an IPv4 header?

- A. At an offset of 20 bytes
- B. At an offset of 8 bytes
- C. At an offset of 16 bytes
- D. At an offset of 12 bytes

**Answer:** D

#### NEW QUESTION 38

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 40

Which of the following protocols implements VPN using IPSec?

- A. SLIP

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

**Answer:** C

#### NEW QUESTION 43

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 45

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 47

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. CONFIG.EXE

**Answer:** C

#### NEW QUESTION 48

Your IT security team is responding to a denial of service attack against your server. They have taken measures to block offending IP addresses. Which type of threat control is this?

- A. Detective
- B. Preventive
- C. Responsive
- D. Corrective

**Answer:** D

#### NEW QUESTION 51

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 54

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 57

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

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

**Answer:** B

#### NEW QUESTION 62

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 65

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 70

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

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

**Answer:** B

#### NEW QUESTION 75

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

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

**Answer:** A

#### NEW QUESTION 78

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 82

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 87

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 91

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 94

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 96

What would the file permission example "rwsr-sr-x" translate to in absolute mode?

- A. 1755
- B. 6755
- C. 6645
- D. 1644

**Answer:** B

#### NEW QUESTION 100

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 105

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 108

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 113

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

- A. Spoofing
- B. SMB signing



- C. Wiretapping
- D. Phishing

**Answer: C**

#### NEW QUESTION 117

You ask your system administrator to verify user compliance with the corporate policies on password strength, namely that all passwords will have at least one numeral, at least one letter, at least one special character and be 15 characters long. He comes to you with a set of compliance tests for use with an offline password cracker. They are designed to examine the following parameters of the password:

- \* they contain only numerals
- \* they contain only letters
- \* they contain only special characters
- \* they contain only letters and numerals
- " they contain only letters and special characters
- \* they contain only numerals and special characters

Of the following, what is the benefit to using this set of tests?

- A. They are focused on cracking passwords that use characters prohibited by the password policy
- B. They find non-compliant passwords without cracking compliant password
- C. They are focused on cracking passwords that meet minimum complexity requirements
- D. They crack compliant and non-compliant passwords to determine whether the current policy is strong enough

**Answer: B**

#### NEW QUESTION 118

Which of the following tools is also capable of static packet filtering?

- A. netstat.exe
- B. ipsecpol.exe
- C. ipconfig.exe
- D. net.exe

**Answer: B**

#### NEW QUESTION 122

An employee is currently logged into the corporate web server, without permission. You log into the web server as 'admin' and look for the employee's username: "dmaul" using the "who" command. This is what you get back:

- A. The contents of the /var/log/messages file has been altered
- B. The contents of the bash history file has been altered
- C. The contents of the utmp file has been altered
- D. The contents of the http logs have been altered

**Answer: B**

#### NEW QUESTION 125

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. PTP
- B. IPSec
- C. PGP
- D. NTFS

**Answer:** C

#### NEW QUESTION 127

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 128

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 132

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 133

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 137

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 138

You are an Intrusion Detection Analyst and the system has alerted you to an Event of Interest (EOI) that appears to be activity generated by a worm. You investigate and find that the network traffic was normal. How would this type of alert be categorized?

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

**Answer:** A

#### NEW QUESTION 139

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 140

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 141

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 XOR Ring with previous cipher text block but input to the block cipher is not randomized
- B. Plaintext patterns are concealed and input to the block cipher is randomized by XOR Ring with previous cipher text block
- 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 XOR Ring with previous cipher text block

**Answer:** C

#### NEW QUESTION 144

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 145

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 147

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 151

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

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

**Answer:** A

#### NEW QUESTION 155

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 160**

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 161**

How are differences in configuration settings handled between Domain and Local Group Policy Objects (GPOs)?

- A. Local and Domain GPOs control different configuration settings, so there will not be conflict
- B. Settings in the domain-wide GPO override conflicting settings in the local GPO on each compute
- C. Settings in the local GPO override conflicting settings when the domain-wide GPO is applied
- D. Precedence depends on which GPO was updated first

**Answer:** B

**NEW QUESTION 165**

The process of enumerating all hosts on a network defines which of the following activities?

- A. Port scanning
- B. Vulnerability scanning
- C. GPS mapping
- D. Network mapping

**Answer:** D

**NEW QUESTION 168**

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 170**

Which of the following is an UDP based protocol?

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

**Answer:** B

**NEW QUESTION 175**

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

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

**Answer:** B

**NEW QUESTION 180**

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 182

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 185

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 188

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 190

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

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

**Answer:** B

#### NEW QUESTION 193

What protocol is a WAN technology?

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

**Answer:** D

#### NEW QUESTION 196

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 201

Which port category does the port 110 fall into?

- A. Well known port
- B. Dynamic port
- C. Private port
- D. Application port

**Answer:** A

#### NEW QUESTION 205

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 weekdays
- 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 weekdays
- G. Keep Monday's backup offsite
- H. Take a full backup daily with one tape taken offsite weekly

**Answer:** A

#### NEW QUESTION 210

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 211

Which of the following areas of a network contains DNS servers and Web servers for Internet users?

- A. VPN
- B. MMZ
- C. VLAN
- D. DMZ

**Answer:** D

#### NEW QUESTION 216

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 217

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 220

To be considered a strong algorithm, an encryption algorithm must be which of the following?

- A. Secret
- B. Well-known
- C. Confidential
- D. Proprietary

**Answer:** B

#### NEW QUESTION 222

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 227

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 232

The Return on Investment (ROI) measurement used in Information Technology and Information Security fields is typically calculated with which formula?

- A.  $ROI = (\text{gain} - \text{expenditure}) / (\text{expenditure}) \times 100\%$
- B.  $ROI = (\text{gain} + \text{expenditure}) / (\text{expenditure}) \times 100\%$
- C.  $ROI = (\text{loss} + \text{expenditure}) / (\text{expenditure}) \times 100\%$
- D.  $ROI = (\text{loss} - \text{expenditure}) / (\text{expenditure}) \times 100\%$

**Answer:** A

#### NEW QUESTION 237

What is the unnoticed theft of sensitive data from a laptop owned by an organization's CEO an example of in information warfare?

- A. Non-zero sum game
- B. Win-win situation
- C. Zero-sum game
- D. Symmetric warfare

**Answer:** D

#### NEW QUESTION 242

Why are false positives such a problem with IPS technology?

- A. File integrity is not guarantee
- B. Malicious code can get into the network
- C. Legitimate services are not delivered
- D. Rules are often misinterpreted

**Answer:** D

#### NEW QUESTION 247

There are three key factors in selecting a biometric mechanism. What are they?

- A. Reliability, encryption strength, and cost
- B. Encryption strength, authorization method, and cost
- C. Reliability, user acceptance, and cost
- D. User acceptance, encryption strength, and cost

**Answer:** C

#### NEW QUESTION 250

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 253

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 254

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 255

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

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

**Answer:** D

#### NEW QUESTION 258

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 259

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 260

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

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

**Answer:** C

#### NEW QUESTION 265

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 266

Which of the following systems acts as a NAT device when utilizing VMware in NAT mode?

- A. Guest system
- B. Local gateway
- C. Host system
- D. Virtual system

**Answer:** D

#### NEW QUESTION 268

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 272

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 274

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 275

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 279

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 281

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 283

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 287

The TTL can be found in which protocol header?

- A. It is found in byte 8 of the ICMP header
- B. It is found in byte 8 of the IP header
- C. It is found in byte 8 of the TCP header

D. It is found in byte 8 of the DNS header

**Answer:** B

#### NEW QUESTION 288

You are the security director for an off-shore banking site. From a business perspective, what is a major factor to consider before running your new vulnerability scanner against the company's business systems?

- A. It may harm otherwise healthy system
- B. It may produce false negative result
- C. It may generate false positive result
- D. It may not return enough benefit for the cost

**Answer:** C

#### NEW QUESTION 293

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 297

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 298

In order to capture traffic for analysis, Network Intrusion Detection Systems (NIDS) operate with network cards in what mode?

- A. Discrete
- B. Reporting
- C. Promiscuous
- D. Alert

**Answer:** C

#### NEW QUESTION 303

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 307

The following three steps belong to the chain of custody for federal rules of evidence. What additional step is recommended between steps 2 and 3?

STEP 1 - Take notes: who, what, where, when and record serial numbers of machine(s) in question.

STEP 2 - Do a binary backup if data is being collected.

STEP 3 - Deliver collected evidence to law enforcement officials.

- A. Rebuild the original hard drive from scratch, and sign and seal the good backup in a plastic bag
- B. Conduct a forensic analysis of all evidence collected BEFORE starting the chain of custody
- C. Take photographs of all persons who have had access to the computer
- D. Check the backup integrity using a checksum utility like MD5, and sign and seal each piece of collected evidence in a plastic bag

**Answer:** D

#### NEW QUESTION 310

While using Wireshark 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 311

Which of the following are examples of Issue-Specific policies all organizations should address?

- A. Perimeter filtering guides, break times for employees, desktop neatness and backup procedure
- B. Rogue wireless access points, auditing, break time for employees and organizational structur
- C. Audit logs, physical access, mission statements and network protocols use
- D. Backup requirements, employee monitoring, physical access and acceptable us

**Answer:** D

#### NEW QUESTION 312

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.we-are-secure.com. He installs a rootkit on the Linux server of the We-are-secure network. Which of the following statements are true about rootkits?

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

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

**Answer:** BCD

#### NEW QUESTION 313

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

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

**Answer:** C

#### NEW QUESTION 316

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 320

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 325

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 330

Included below is the output from a resource kit utility run against local host.

Which command could have produced this output?

- A. Schtasks
- B. Task kill
- C. SC
- D. Task list

**Answer:** D

#### NEW QUESTION 335

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 338

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 339

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

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

**Answer:** A

#### NEW QUESTION 342

.....

## 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/>