COMPTIA BR0-001 EXAM QUESTIONS & ANSWERS

Number: BR0-001
Passing Score: 800
Time Limit: 120 min
File Version: 34.4

http://www.gratisexam.com/

COMPTIA BR0-001 EXAM QUESTIONS & ANSWERS

Exam Name: CompTIA Bridge Exam - Security+

Examsheets

QUESTION 1
Which method is LEAST intrusive to check the environment for known software flaws?

A. Port scanner
B. Vulnerability scanner
C. Penetration test
D. Protocol analyzer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
On a remote machine, which action will you usually take to determine the operating system?

A. MAC flooding
B. System fingerprinting
C. DNS spoofing
D. Privilege escalation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which description is true about the process of securely removing information from media (e.g. hard drive) for future use?

A. Deleting
B. Reformatting
C. Sanitization
D. Destruction

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Why malware that uses virtualization techniques is difficult to detect?

A. The malware may be implementing a proxy server for command and control.
B. A portion of the malware may have been removed by the IDS.
C. The malware may be using a Trojan to infect the system.
D. The malware may be running at a more privileged level than the antivirus software.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
You work as the network administrator at certways .com. The certways .com network uses the RBAC (Role Based Access Control) model. You must plan the security strategy for users to access resources on the certways .com network. The types of resources you must control access to are mailboxes, and files and printers. Certways.com is divided into distinct departments and functions named Finance, Sales, Research and Development, and Production respectively. Each user has its own workstation, and accesses resources based on the department wherein he/she works. You must determine which roles to create to support the RBAC (Role Based Access Control) model. Which of the following roles should you create?

A. Create mailbox, and file and printer roles.
B. Create Finance, Sales, Research and Development, and Production roles.
C. Create user and workstation roles.
D. Create allow access and deny access roles.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
What technology is able to isolate a host OS from some types of security threats?

GRATIS EXAM
Free Practice Exams
http://www.gratisexam.com/

A. Kiting
B. Virtualization
C. Cloning
D. Intrusion detection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which method could identify when unauthorized access has occurred?

A. Implement session termination mechanism.

B. Implement previous logon notification.
C. Implement session lock mechanism.
D. Implement two-factor authentication.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
The Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates. An executive uses PKI to encrypt sensitive emails sent to an assistant. In addition to encrypting the body of the email, the executive wants to encrypt the signature so that the assistant can verify that the email actually came from the executive. Which asymmetric key should be used by the executive to encrypt the signature?

A. Shared
B. Private
C. Hash
D. Public

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Why implement security logging on a DNS server?

A. To monitor unauthorized zone transfers
B. To perform penetration testing on the DNS server
C. To control unauthorized DNS DoS
D. To measure the DNS server performance

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which one of the following items will permit an administrator to find weak passwords on the network?

A. A password generator
B. A network mapper
C. A hash function
D. A rainbow table

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 11
You work as a network administrator for your company. Taking personal safety into consideration, what fire suppression substances types can effectively prevent damage to electronic equipment?

A. Halon
B. CO
C. Water
D. Foam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
A company has implemented a policy stating that users will only receive access to the systems needed to perform their job duties. This is an example of:

A. separation of duties
B. least privilege
C. concurrent session control
D. access control

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which item will MOST likely permit an attacker to make a switch function like a hub?

A. MAC flooding
B. DNS spoofing
C. ARP poisoning
D. DNS poisoning

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
A company's new employees are asked to sign a document that describes the methods of and purposes for accessing the company's IT systems.
Which of the following BEST describes this document?

A. Privacy Act of 1974
B. Authorized Access Policy
C. Due diligence form
D. Acceptable Use Policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which item can reduce the attack surface of an operating system?

A. Installing HIDS
B. Patch management
C. Installing antivirus
D. Disabling unused services

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which encryption method is often used along with L2TP?

A. 3DES
B. S/MIME
C. SSH
D. IPSec

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
After the maximum number attempts have failed, which of the following could set an account to lockout for 30 minutes?

A. Account lockout threshold
B. Account lockout duration
C. Password complexity requirements
D. Key distribution center

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
You work as a network technician. You have been asked to reconstruct the infrastructure of an organization. You should make sure that the virtualization technology is implemented securely. What should be taken into consideration while implementing virtualization technology?

A. The technician should perform penetration testing on all the virtual servers to monitor performance.
B. The technician should verify that the virtual servers and the host have the latest service packs and patches applied.
C. The technician should verify that the virtual servers are dual homed so that traffic is securely separated.
D. The technician should subnet the network so each virtual server is on a different network segment.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which of the following is the BEST place to obtain a hotfix or patch for an application or system?

A. An email from the vendor
B. A newsgroup or forum
C. The manufacturer's website
D. A CD-ROM

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Which algorithms can best encrypt large amounts of data?

A. Asymmetric key algorithms
B. Symmetric key algorithms
C. ECC algorithms
D. Hashing algorithms

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Which of the following is a suppression method for a Class C fire?

A. Water

B. Soda acid
C. Dry powder
D. Carbon dioxide (CO2)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Look at the following items carefully, which one is a cryptographic representation of non- repudiation?

A. Digital signature
B. Symmetric key
C. Internet key exchange
D. Certificate authority

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Which of the following can be used by an attacker to footprint a system?

A. Man-in-the-middle attack
B. RADIUS
C. Port scanner
D. Password cracker

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
You work as a network administrator for your company. Your company requires you to improve the physical security of a data center located inside the office building. The data center already maintains a physical access log and has a video surveillance system. Which additional control can be performed?

A. ACL
B. Defense-in-depth
C. Logical token
D. Mantrap

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
After analyzing vulnerability and applying a security patch, which non-intrusive action should be taken to verify that the vulnerability was truly removed?

A. Update the antivirus definition file.
B. Apply a security patch from the vendor.
C. Repeat the vulnerability scan.
D. Perform a penetration test.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which item best describes an instance where a biometric system identifies legitimate users as being unauthorized?

A. False acceptance
B. False positive
C. False rejection
D. False negative

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

GRATIS EXAM
Free Practice Exams

http://www.gratisexam.com/

QUESTION 27
Which authentication method does the following sequence: Logon request, encrypts value response, server, challenge, compare encrypts results, authorize or fail referred to?

A. Certificates
B. Security Tokens
C. CHAP
D. Kerberos

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Which of the following can be used by an administrator to proactively collect information on attackers and their attempted methods of gaining access to the internal network?

A. DMZ
B. Honeypot
C. NIDS
D. NIPS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Which of the following statements is TRUE regarding the CHAP authentication system?

A. A certificate being handed from the server to the client once authentication has been established. If you have a pass, you can wander throughout the network. BUT limited access is allowed.
B. If your token does not grant you access to certain information, that information will either not be displayed or your access will be denied. The authentication system creates a token every time a user or a session begins. At the completion of a session, the token is destroyed
C. The authentication process uses a Key Distribution Center (KDC) to orchestrate the entire process. The KDC authenticates the network. Principles can be users, programs, or systems.
The KDC provides a ticket to the network. Once this ticket is issued, it can be used to authenticate against other principles. This occurs automatically when a request or service is performed by another network.
D. The initiator sends a logon request from the client to the server. The server sends a challenge back to the client. The challenge is encrypted and then sent back to the server. The server compares the value from the client and if the information matches, the server grants authorization. If the response fails, the session fails and the request phase starts over

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which description is true about how to accomplish steganography in graphic files?

A. Replacing the most significant bit of each byte
B. Replacing the most significant byte of each bit
C. Replacing the least significant byte of each bit
D. Replacing the least significant bit of each byte

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
In computing, promiscuous mode is a configuration of a network card that makes the card pass all traffic it receives to the central processing unit rather than just packets addressed to it - a feature normally used for packet sniffing. Which of the following is placed in promiscuous mode, according to the data flow, to permit a NIDS to monitor the traffic?

A. Filter
B. Sensor
C. Appliance
D. Console

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Identify the service provided by message authentication code (MAC) hash:

A. data recovery.
B. fault tolerance.
C. key recovery.
D. integrity

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which security policy will be most likely used while attempting to mitigate the risks involved with allowing a user to access company email via their cell phone?

A. The cell phone should require a password after a set period of inactivity.
B. The cell phone should have data connection abilities disabled.
C. The cell phone should only be used for company related emails.
D. The cell phone data should be encrypted according to NIST standards.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Which item will allow for fast, highly secure encryption of a USB flash drive?

A. 3DES
B. SHA-1

C. MD5
D. AES256

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Communication is important to maintaining security because communication keeps:

A. the network bandwidth usage under control
B. the user community informed of threats
C. law enforcement informed of what is being done
D. the IT security budget justified

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Which tool can help the technician to find all open ports on the network?

A. Router ACL
B. Performance monitor
C. Protocol analyzer
D. Network scanner

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Which security action should be finished before access is given to the network?

A. Identification and authorization
B. Identification and authentication
C. Authentication and authorization
D. Authentication and password

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
To aid in preventing the execution of malicious code in email clients, which of the following should be done by the email administrator?

A. Spam and anti-virus filters should be used
B. Regular updates should be performed
C. Preview screens should be disabled
D. Email client features should be disabled

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Which security applications require frequent signature updates? (Select TWO).

A. Antivirus
B. Firewall
C. PKI
D. IDS

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
In computing, virtualization is a broad term that refers to the abstraction of computer resources. Which is a security reason to implement virtualization throughout the network infrastructure?

A. To implement additional network services at a lower cost
B. To analyze the various network traffic with protocol analyzers
C. To isolate the various network services and roles
D. To centralize the patch management of network servers

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which of the following access control models uses roles to determine access permissions?

A. MAC
B. DAC
C. RBAC
D. None of the above.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
A user receives an email asking the user to reset the online banking username and password. The email contains a link and when the user accesses the link, the URL that appears in the browser does not match the link. This would be an example of:

A. spoofing
B. phishing
C. hijacking
D. redirecting

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
In computer networking, network address translation (NAT) is the process of modifying network address information in datagram packet headers while in transit across a traffic routing device for the purpose of remapping a given address space into another. Which description is true about a static NAT?

A. A static NAT uses a many to many mapping.
B. A static NAT uses a one to many mapping.
C. A static NAT uses a many to one mapping.
D. A static NAT uses a one to one mapping.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Which of the following protects the confidentiality of data by making the data unreadable to those who don't have the correct key?

A. Hashing
B. Digital signatures
C. Encryption
D. Non-repudiation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
The term tunneling protocol is used to describe when one network protocol called the payload protocol is encapsulated within a different delivery protocol. Which of the following can be used to institute a tunneling protocol for security?

A. FTP
B. IPX/SPX
C. IPSec
D. EAP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
John works as a network administrator for his company. He uses a tool to check SMTP, DNS, POP3, and ICMP packets on the network. This is an example of which of the following?

A. A vulnerability scan
B. A protocol analyzer
C. A penetration test
D. A port scanner

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which system is setup to distract potential attackers?

A. DMZ
B. VLAN
C. Honeypot
D. Firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Most current encryption schemes are based on:

A. digital rights management
B. time stamps
C. randomizing

D. algorithms

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Look at the following scenarios, which one would a penetration test BEST be used for?

A. When providing a proof of concept demonstration for a vulnerability
B. When conducting performance monitoring
C. While in the reconnaissance phase
D. When performing network mapping

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
For the following items, which is a security limitation of virtualization technology?

A. A compromise of one instance will immediately compromise all instances.
B. It increases false positives on the NIDS.
C. Patch management becomes more time consuming.
D. If an attack occurs, it could potentially disrupt multiple servers.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
The IPSec Security Association is managed by

A. ESP
B. ISAKMP
C. IEEE
D. AH

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Why implement virtualization technology? (Select TWO).

A. To reduce recovery time in the event of application failure
B. To eliminate virtual redundancy
C. To decrease access to security resources
D. To provide a secure virtual environment for testing

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Which description is correct about a virtual server implementation attack?

A. system registry will affect all virtual instances.
B. OS kernel will affect all virtual instances.
C. disk partition will affect all virtual instances.
D. RAM will affect all virtual instances.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
For the following items, which is a protocol analyzer?

A. Cain Abel
B. WireShark
C. Nessus
D. John the Ripper

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Message authentication codes are used to provide which service?

A. Integrity
B. Fault recover
C. Key recovery
D. Acknowledgement

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
What are the best practices while installing and securing a new system for a home user? (Select THREE).

A. Use a strong firewall.
B. Install remote control software.
C. Apply all system patches.
D. Apply all service packs.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
How is access control permissions established in the RBAC access control model?

A. The system administrator.
B. The owner of the resource.
C. The role or responsibilities users have in the organization.
D. None of the above.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which of the following can help an administrator to implement a procedure to control inbound and outbound traffic on a network segment?

A. NIDS
B. HIDS
C. ACL
D. Proxy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Which access control model uses Access Control Lists to identify the users who have permissions to a resource?

A. MAC
B. RBAC

C. DAC
D. None of the above.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
A company wants to monitor all network traffic as it traverses their network. Which item will be used by the technician?

A. Honeypot
B. Protocol analyzer
C. HIDS
D. Content filter

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
What is steganography primarily used for?

A. Data integrity
B. Message digest
C. Hide information
D. Encrypt information

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
A user has a sensitive message that needs to be sent in via email. The message needs to be protected from interception. Which of the following should be used when sending the email?

A. Digital signatures
B. Social engineering
C. Encryption
D. Non-repudiation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which intrusion detection system will use well defined models of how an attack occurs?

A. Anomaly
B. Protocol
C. Signature
D. Behavior

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Which of the following refers to the ability to be reasonably certain that data is not disclosed to unintended persons?

A. Non-repudiation
B. Integrity
C. Authentication
D. Confidentiality

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
While surfing the Internet a user encounters a pop-up window that prompts the user to download a browser plug-in. The pop-up window is a certificate which validates the identity of the plug-in developer. Which of the following BEST describes this type of certificate?

A. Software publisher certificate
B. Web certificate
C. Certificate Authority (CA) certificate
D. Server certificate

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Which one of the following options is a vulnerability assessment tool?

A. AirSnort
B. John the Ripper

C. Cain Abel
D. Nessus

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Which key can be used by a user to log into their network with a smart card?

A. Public key
B. Cipher key
C. Shared key
D. Private key

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
Which of the following describes a type of algorithm that cannot be reversed in order to decode the data?

A. Symmetric
B. One Way Function
C. Asymmetric
D. Pseudorandom Number Generator (PRNG)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Which description is correct about authentication headers (AH)?

A. The authentication information is a keyed hash based on all of the bytes in the packet.
B. The authentication information may be the same on different packets if the integrity remains in place.
C. The authentication information hash will increase by one if the bytes remain the same on transfer.
D. The authentication information hash will remain the same if the bytes change on transfer.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
The MOST common Certificate Server port required for secure web page access is port:

A. 25
B. 80
C. 443
D. 446

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Many unauthorized staff have been entering the data center by piggybacking authorized staff. The CIO has mandated to stop this behavior. Which technology should be installed at the data center to prevent piggybacking?

A. Mantrap
B. Token access
C. Security badges
D. Hardware locks

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Secret Key encryption is also known as:

A. symmetrical
B. replay
C. one way function.
D. asymmetrical

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
A digital signature or digital signature scheme is a type of asymmetric cryptography. For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. While using a digital signature, the message digest is encrypted with which key?

A. Senders public key
B. Receivers private key

C. Receivers public key
D. Senders private key

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Which access control system allows the owner of a resource to establish access permissions to that resource?

A. MAC
B. DAC
C. RBAC
D. None of the above.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Which of the following is considered the weakest encryption?

A. SHA
B. DES
C. RSA
D. AES

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
For the following items, which one is a collection of server's setup to attract hackers?

A. Honeypot
B. VLAN
C. Honeynet
D. DMZ

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Which of the following statements regarding the MAC access control models is TRUE?

A. The Mandatory Access Control (MAC) model is a dynamic model.
B. In the Mandatory Access Control (MAC) the owner of a resource establishes access privileges to that resource.
C. In the Mandatory Access Control (MAC) users cannot share resources dynamically.
D. The Mandatory Access Control (MAC) model is not restrictive.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Why does a technician use a password cracker?

A. To look for weak passwords on the network
B. To enforce password complexity requirements
C. To change users passwords if they have forgotten them
D. To change a users passwords when they leave the company

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
In computing, a Uniform Resource Locator (URL) is a type of Uniform Resource Identifier (URI) that specifies where an identified resource is available and the mechanism for retrieving it. When a user attempts to go to a website, he notices the URL has changed, which attack will MOST likely cause the problem?

A. ARP poisoning
B. DLL injection
C. DNS poisoning
D. DDoS attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
Which of the following are types of certificate-based authentication? (Select TWO)

A. Many-to-one mapping
B. One-to-one mapping
C. One-to-many mapping

D. Many-to-many mapping

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
What should be taken into consideration while executing proper logging procedures? (Select TWO).

A. The information that is needed to reconstruct events
B. The password requirements for user accounts
C. The virtual memory allocated on the log server
D. The amount of disk space required

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Network traffic is data in a network. Which tool can be used to review network traffic for clear text passwords?

A. Firewall
B. Protocol analyzer
C. Password cracker
D. Port scanner

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
The ability to logon to multiple systems with the same credentials is typically known as:

A. decentralized management
B. single sign-on
C. Role Based Access Control (RBAC)
D. centralized management

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
The first step in risk identification would be to identify:

A. assets
B. costs
C. threats
D. vulnerabilities

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Which of the following would be MOST important to have to ensure that a company will be able to recover in case of severe environmental trouble or destruction?

A. Disaster recovery plan
B. Alternate sites
C. Offsite storage
D. Fault tolerant systems

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
During a live response to an unauthorized access, a forensics specialist executes a command on the computer being investigated. Which of the following commands would be used to display the current network connections on the local computer?

A. NETSTAT
B. IPCONFIG / IFCONFIG
C. nmap
D. netcat

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Patch management must be combined with full-featured systems management to be effective. Determining which patches are needed, applying the patches and which of the following are three generally accepted activities of patch management?

A. Backing up the patch file executables to a network share
B. Updating the firewall configuration to include the patches
C. Auditing for the successful application of the patches
D. Running a NIDS report to list the remaining vulnerabilities

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Documentation describing a group expected minimum behavior is known as:Documentation describing a group? expected minimum behavior is known as:

A. the need to know
B. acceptable usage
C. the separation of duties
D. a code of ethics

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Which of the following is not an organizational policy that reduces the impact of fraud?

A. job rotation.
B. password complexity rules.
C. escorting procedures.
D. separation of duties.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
An important component of a good data retention policy is:

A. backup software licensing
B. offsite storage
C. magnetic media sorting
D. server drive redundancy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

http://www.gratisexam.com/