

**Comptia.Actualtests.SY0-301.v2013-11-23.by.BigK.664q**

Number: SY0-301  
Passing Score: 750  
Time Limit: 90 min  
File Version: 14.5



<http://www.gratisexam.com/>

**Exam Code: SY0-301**

**Exam Name: Comptia CompTIA Security+ Certification Exam 2011 version**



## **Exam A**

### **QUESTION 1**

Which of the following is the BEST filtering device capable of stateful packet inspection?

- A. Switch
- B. Protocol analyzer
- C. Firewall
- D. Router

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### **QUESTION 2**

An employee's workstation is connected to the corporate LAN. Due to content filtering restrictions, the employee attaches a 3G Internet dongle to get to websites that are blocked by the corporate gateway. Which of the following BEST describes a security implication of this practice?

- A. A corporate LAN connection and a 3G Internet connection are acceptable if a host firewall is installed.
- B. The security policy should be updated to state that corporate computer equipment should be dual-homed.
- C. Content filtering should be disabled because it may prevent access to legitimate sites.
- D. Network bridging must be avoided, otherwise it may join two networks of different classifications.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### **QUESTION 3**

In order to provide flexible working conditions, a company has decided to allow some employees remote access into corporate headquarters. Which of the following security technologies could be used to provide remote access? (Select TWO).

- A. Subnetting
- B. NAT
- C. Firewall
- D. NAC
- E. VPN

**Correct Answer:** CE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### **QUESTION 4**

If a security issue is resolved, which of the following risk management strategies was used?

- A. Deterrence
- B. Acceptance
- C. Mitigation
- D. Avoidance

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 5

Which of the following is the BEST approach to perform risk mitigation of user access control rights?



<http://www.gratisexam.com/>

- A. Conduct surveys and rank the results.
- B. Perform routine user permission reviews.
- C. Implement periodic vulnerability scanning.
- D. Disable user accounts that have not been used within the last two weeks.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 6

Used in conjunction, which of the following are PII? (Select TWO).

- A. Marital status
- B. Favorite movie
- C. Pet's name
- D. Birthday
- E. Full name

**Correct Answer:** DE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 7

In a disaster recovery situation, operations are to be moved to an alternate site. Computers and network connectivity are already present; however, production backups are several days out-of-date. Which of the following site types is being described?

- A. Cold site
- B. High availability site
- C. Warm site
- D. Hot site

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 8**

Which of the following malware types is an antivirus scanner MOST unlikely to discover? (Select TWO).

- A. Trojan
- B. Pharming
- C. Worms
- D. Virus
- E. Logic bomb

**Correct Answer:** BE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 9**

Which of the following threats corresponds with an attacker targeting specific employees of a company?

- A. Spear phishing
- B. Phishing
- C. Pharming
- D. Man-in-the-middle

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 10**

Which of the following attacks would password masking help mitigate?

- A. Shoulder surfing
- B. Brute force
- C. Tailgating
- D. Impersonation

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 11**

If cookies with non-random sequence numbers are issued upon authentication, which of the following attack types can occur?

- A. Directory traversal
- B. Session hijacking
- C. Cross-site scripting
- D. SQL injection

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 12**

Two systems are being designed. System A has a high availability requirement. System B has a high security requirement with less emphasis on system uptime. Which of the following configurations BEST fits the need for each system?

- A. System A fails open. System B fails closed.
- B. System A and System B both fail closed.
- C. System A and System B both fail open.
- D. System A fails closed. System B fails open.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 13**

An existing application has never been assessed from a security perspective. Which of the following is the BEST assessment technique in order to identify the application's security posture?

- A. Baseline reporting
- B. Protocol analysis
- C. Threat modeling
- D. Functional testing

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 14**

A security firm has been engaged to assess a software application. A production-like test environment, login details, production documentation and source code have been provided. Which of the following types of testing

is being described?

- A. White box
- B. Gray box
- C. Black box
- D. Red teaming

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 15**

A user has forgotten their account password. Which of the following is the BEST recovery strategy?

- A. Upgrade the authentication system to use biometrics instead.
- B. Temporarily disable password complexity requirements.
- C. Set a temporary password that expires upon first use.
- D. Retrieve the user password from the credentials database.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 16**

All of the following are valid cryptographic hash functions EXCEPT:

- A. RIPEMD.
- B. RC4.
- C. SHA-512.
- D. MD4.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 17**

When a certificate issuer is not recognized by a web browser, which of the following is the MOST common reason?

- A. Lack of key escrow
- B. Self-signed certificate
- C. Weak certificate pass-phrase
- D. Weak certificate cipher

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 18**

Which of the following PKI components identifies certificates that can no longer be trusted?

- A. CRL
- B. CA public key
- C. Escrow
- D. Recovery agent

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 19**

Which of the following can prevent an unauthorized person from accessing the network by plugging into an open network jack?

- A. 802.1x
- B. DHCP
- C. 802.1q
- D. NIPS

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 20**

MAC filtering is a form of which of the following?

- A. Virtualization
- B. Network Access Control
- C. Virtual Private Networking
- D. Network Address Translation

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 21**

Which of the following authentication protocols forces centralized wireless authentication?

- A. WPA2-Personal

- B. WPA2-Enterprise
- C. WPA2-CCMP
- D. WPA2-TKIP

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 22**

A company that purchases insurance to reduce risk is an example of which of the following?

- A. Risk deterrence
- B. Risk acceptance
- C. Risk avoidance
- D. Risk transference

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 23**

Which of the following is a method to prevent ad-hoc configuration mistakes?

- A. Implement an auditing strategy
- B. Implement an incident management strategy
- C. Implement a patch management strategy
- D. Implement a change management strategy

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 24**

Which of the following risks may result from improper use of social networking and P2P software?

- A. Shoulder surfing
- B. Denial of service
- C. Information disclosure
- D. Data loss prevention

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 25**

Which of the following malware types is BEST described as protecting itself by hooking system processes and hiding its presence?

- A. Botnet
- B. Rootkit
- C. Logic bomb
- D. Virus

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 26**

A computer is put into a restricted VLAN until the computer's virus definitions are up-to-date. Which of the following BEST describes this system type?

- A. NAT
- B. NIPS
- C. NAC
- D. DMZ

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 27**

Which of the following would be used for secure remote terminal access?

- A. SSH
- B. TFTP
- C. SCP
- D. SFTP

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 28**

Without validating user input, an application becomes vulnerable to all of the following EXCEPT:

- A. buffer overflow.
- B. command injection.
- C. spear phishing.
- D. SQL injection.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 29**

After verifying that the server and database are running, Jane, the administrator, is still unable to make a TCP connection to the database. Which of the following is the MOST likely cause for this?

- A. The server has data execution prevention enabled
- B. The server has TPM based protection enabled
- C. The server has HIDS installed
- D. The server is running a host-based firewall

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 30**

Which of the following is used to detect an unknown security vulnerability?

- A. Application fuzzing
- B. Application configuration baseline
- C. Patch management
- D. ID badge

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 31**

Which of the following is a best practice before deploying a new desktop operating system image?

- A. Install network monitoring software
- B. Perform white box testing
- C. Remove single points of failure
- D. Verify operating system security settings

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 32**

Securing mobile devices involves which of the following checklists?

- A. Key escrow, trust model, CRL
- B. Cross-site scripting, XSRF, fuzzing
- C. Screen lock, encryption, remote wipe
- D. Black box, gray box, white box testing

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### **QUESTION 33**

Which of the following steps should follow the deployment of a patch?

- A. Antivirus and anti-malware deployment
- B. Audit and verification
- C. Fuzzing and exploitation
- D. Error and exception handling

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### **QUESTION 34**

Lack of internal security resources and high availability requirements are factors that may lead a company to consider:

- A. patch management.
- B. encryption.
- C. cloud computing.
- D. anti-malware software.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### **QUESTION 35**

Which of the following would be used when a higher level of security is desired for encryption key storage?

- A. TACACS+
- B. L2TP
- C. LDAP
- D. TPM

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 36**

Which of the following is the default port for SCP and SSH?

- A. 21
- B. 22
- C. 404
- D. 443

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 37**

Which of the following default ports does the hypertext transfer protocol use for non-secure network connections?

- A. 20
- B. 21
- C. 80
- D. 8080

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 38**

Which of the following BEST describes using a smart card and typing in a PIN to gain access to a system?

- A. Biometrics
- B. PKI
- C. Single factor authentication
- D. Multifactor authentication

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 39**

Which of the following result types would Jane, a security administrator, MOST likely look for during a penetration test?

- A. Inability to gain administrative access

- B. Open ports
- C. Ability to bypass security controls
- D. Incorrect configurations

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 40**

A small business owner has asked the security consultant to suggest an inexpensive means to deter physical intrusions at their place of business. Which of the following would BEST meet their request?

- A. Fake cameras
- B. Proximity readers
- C. Infrared cameras
- D. Security guards

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 41**

Employee badges are encoded with a private encryption key and specific personal information. The encoding is then used to provide access to the network. Which of the following describes this access control type?

- A. Smartcard
- B. Token
- C. Discretionary access control
- D. Mandatory access control

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 42**

Which of the following devices would MOST likely have a DMZ interface?

- A. Firewall
- B. Switch
- C. Load balancer
- D. Proxy

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 43**

Which of the following is used to digitally sign an email?

- A. Private key
- B. Public key
- C. Sender's IP
- D. Sender's MAC address

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 44**

Pete, the company Chief Information Officer (CIO), has been receiving numerous emails from the help desk directing Pete to a link to verify credentials. Which of the following attacks is underway?

- A. Replay attack
- B. Pharming
- C. Privilege escalation
- D. Spear phishing

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 45**

Pete, a security administrator, noticed that the network analyzer is displaying packets that have all the bits in the option field turned on. Which of the following attacks is underway?

- A. X-Mas
- B. DDoS
- C. Birthday
- D. Smurf

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 46**

Which of the following tools would Matt, a security administrator, MOST likely use to analyze a malicious payload?

- A. Vulnerability scanner

- B. Fuzzer
- C. Port scanner
- D. Protocol analyzer

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 47**

Which of the following is Jane, a security administrator, MOST likely to install in order to capture and analyze zero day exploits?

- A. Honeypot
- B. Antivirus
- C. IPS
- D. IDS

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 48**

Which of the following can be implemented to detect file system variations?

- A. EXT3
- B. Hashing
- C. Encryption
- D. NIDS

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 49**

Which of the following threats is MOST likely to be mitigated by implementing cross-site scripting prevention tools?

- A. Resource starvation
- B. Insider threat
- C. Spear phishing
- D. Session hijacking

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 50**

An attacker has gained access to the corporate network and is attempting to brute force a password to gain access to the accounting system. Which of the following, if implemented, will protect the server?

- A. Single sign-on
- B. Password history
- C. Limit logon attempts
- D. Directory services

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 51**

Pete, a security administrator, wants to check user password complexity. Which of the following is the BEST tool to use?

- A. Password history
- B. Password logging
- C. Password cracker
- D. Password hashing

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 52**

Which of the following can hide confidential or malicious data in the whitespace of other files (e.g. JPEGs)?

- A. Hashing
- B. Transport encryption
- C. Digital signatures
- D. Steganography

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 53**

Certificates are used for: (Select TWO).

- A. client authentication.
- B. WEP encryption.



- C. access control lists.
- D. code signing.
- E. password hashing.

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 54**

When implementing SSL VPN, which of the following is the FASTEST cipher that Pete, an administrator, can use?

- A. 3DES
- B. AES
- C. DES
- D. RC4

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 55**

Which of the following network devices will prevent port scans?

- A. Firewall
- B. Load balancers
- C. NIDS
- D. Sniffer

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 56**

Which of the following is an operational control?

- A. Concurrent session control
- B. System security categorization
- C. Contingency planning
- D. Session locks

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 57**

Which of the following is a hardware based encryption device?

- A. EFS
- B. TrueCrypt
- C. TPM
- D. SLE

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 58**

Which of the following is the MOST important step for preserving evidence during forensic procedures?

- A. Involve law enforcement
- B. Chain of custody
- C. Record the time of the incident
- D. Report within one hour of discovery

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 59**

Employees of a company have received emails that fraudulently claim to be from the company's security department. The emails ask the employees to sign-on to an Internet website to verify passwords and personal information. This is an example of which type of attack?

- A. Spam
- B. Pharming
- C. Man-in-the-middle
- D. Vishing

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 60**

A company has implemented software to enforce full disk and removable media encryption for all computers. Which of the following threats can still expose sensitive data on these computers?

- A. Spam
- B. Botnet infection

- C. Stolen laptop
- D. Header manipulation

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 61**

Which of the following MOST interferes with network-based detection techniques?

- A. Mime-encoding
- B. SSL
- C. FTP
- D. Anonymous email accounts

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 62**

Which of the following secure coding concepts can prevent the unintentional execution of malicious code entered in place of proper commands?

- A. Patch management
- B. Proper exception handling
- C. Code reviews
- D. Input validation

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 63**

A certificate authority takes which of the following actions in PKI?

- A. Signs and verifies all infrastructure messages
- B. Issues and signs all private keys
- C. Publishes key escrow lists to CRLs
- D. Issues and signs all root certificates

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 64**

To ensure the security of a PKI, security technicians should regularly update which of the following, by checking with the CA for newer versions?

- A. CRLs
- B. Expiration lists
- C. Preshared keys
- D. Public keys

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 65**

Use of a smart card to authenticate remote servers remains MOST susceptible to which of the following attacks?

- A. Malicious code on the local system
- B. Shoulder surfing
- C. Brute force certificate cracking
- D. Distributed dictionary attacks

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 66**

An administrator is provided two accounts: one with administrative access but not network services, and the other account with other network services but no administrative access. Which of the following describes this scenario?

- A. Least privilege
- B. Mandatory access control
- C. Multifactor authentication
- D. Separation of duties

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 67**

Separation of duties is often implemented between developers and administrators in order to separate which of the following?

- A. More experienced employees from less experienced employees
- B. Changes to program code and the ability to deploy to production

- C. Upper level management users from standard development employees
- D. The network access layer from the application access layer

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 68**

Which of the following will require exceptions when considering the use of 802.1x port security?

- A. Switches
- B. Printers
- C. Laptops
- D. Desktops

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 69**

Which of the following may cause Jane, the security administrator, to seek an ACL work around?

- A. Zero day exploit
- B. Dumpster diving
- C. Virus outbreak
- D. Tailgating

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 70**

Which of the following is MOST likely to lead to a breach of security in which Matt, an unauthorized employee, accidentally views sensitive data?

- A. Lack of business continuity plan
- B. Lack of logging and auditing access to files
- C. Lack of chain of custody procedure
- D. Lack of data labeling, handling, and disposal policies

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 71**

A security administrator needs to update the OS on all the switches in the company. Which of the following **MUST** be done before any actual switch configuration is performed?

- A. The request needs to be sent to the incident management team.
- B. The request needs to be approved through the incident management process.
- C. The request needs to be approved through the change management process.
- D. The request needs to be sent to the change management team.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 72**

Jane, an individual, has recently been calling various financial offices pretending to be another person to gain financial information. Which of the following attacks is being described?

- A. Phishing
- B. Tailgating
- C. Pharming
- D. Vishing

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 73**

The security administrator wants each user to individually decrypt a message but allow anybody to encrypt it. Which of the following **MUST** be implemented to allow this type of authorization?

- A. Use of CA certificate
- B. Use of public keys only
- C. Use of private keys only
- D. Use of public and private keys

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 74**

Jane, a user in the company, is in charge of various financial roles but needs to prepare for an upcoming audit. She uses the same account to access each financial system. Which of the following security controls will **MOST** likely be implemented within the company?

- A. Account lockout policy
- B. Account password enforcement

- C. Password complexity enabled
- D. Separation of duties

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 75**

Pete, an employee, is granted access to only areas of a network folder needed to perform his job. Which of the following describes this form of access control?

- A. Separation of duties
- B. Time of day restrictions
- C. Implicit deny
- D. Least privilege

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 76**

A security administrator notices unusual activity from a default account when reviewing system logs and finds the account has been compromised. After investigating the incident, the administrator determines the account can be disabled to prevent any further incidents because the account was not necessary for any job functions. Which of the following could have prevented this incident?

- A. Enhanced password complexity
- B. Disabling unnecessary accounts
- C. Reviewing centralized logs
- D. Disabling unnecessary services

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 77**

A CRL is comprised of:

- A. malicious IP addresses.
- B. trusted CA's.
- C. untrusted private keys.
- D. public keys.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 78**

Which of the following can be implemented to prevent Matt, a user, from connecting a hub or switch to a single switch port to access network resources with multiple devices? (Select TWO).

- A. Subnetting
- B. NAC
- C. VLAN
- D. DMZ
- E. Port security

**Correct Answer:** BE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 79**

Which of the following devices utilizes behavior heuristics to detect or prevent intrusion into network resources?

- A. NIPS
- B. VPN concentrators
- C. NAT router
- D. Flood guard

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 80**

Which of the following may significantly reduce data loss if multiple drives fail at the same time?

- A. Virtualization
- B. RAID
- C. Load balancing
- D. Server clustering

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 81**

Which of the following would MOST likely belong in the DMZ? (Select TWO).

- A. Finance servers



- B. Backup servers
- C. Web servers
- D. SMTP gateways
- E. Laptops

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 82**

Which of the following protocols would MOST likely be implemented if Pete, a user, wants to transfer files reliably from one location to another?

- A. SNMP
- B. SSH
- C. ICMP
- D. SFTP

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 83**

Which of the following is a strong cryptographic system used by Windows based systems for authentication?

- A. SSO
- B. DES
- C. NTLMv2
- D. LANMAN

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 84**

Which of the following algorithms has well documented collisions? (Select TWO).

- A. AES
- B. MD5
- C. SHA
- D. SHA-256
- E. RSA

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 85**

Which of the following describes common concerns when implementing IPS?

- A. Legitimate traffic will be incorrectly blocked
- B. False negatives will disrupt network throughput
- C. Incompatibilities with existing routers will result in a DoS
- D. Security alerts will be minimal until adequate traffic is collected

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 86**

Which of the following describes an issue encountered when reconstructing a security incident through the examination of security logs collected from multiple servers?

- A. Proprietary log formats prevent review of security alerts
- B. Some operating systems do not natively export security logs
- C. Security logs are often encrypted
- D. Inconsistent time settings interfere with sequential event analysis

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 87**

When verifying file integrity on a remote system that is bandwidth limited, which of the following tool combinations provides the STRONGEST confidence?

- A. MD5 and 3DES
- B. MD5 and SHA-1
- C. SHA-256 and RSA
- D. SHA-256 and AES

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 88**

Jane, the security administrator, needs to be able to test malicious code in an environment where it will not harm the rest of the network. Which of the following would allow Jane to perform this kind of testing?

- A. Local isolated environment

- B. Networked development environment
- C. Infrastructure as a Service
- D. Software as a Service

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 89**

A company is sending out a message to all users informing them that all internal messages need to be digitally signed. This is a form of which of the following concepts?

- A. Availability
- B. Non-repudiation
- C. Authorization
- D. Cryptography

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 90**

While performing basic forensic analysis of a hard drive in Sara's, the security administrator, possession, which of the following should be verified during the analysis?

- A. Witness statements
- B. Image hashes
- C. Chain of custody
- D. Order of volatility

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 91**

A server containing critical data will cost the company \$200/hour if it were to be unavailable due to DoS attacks. The security administrator expects the server to become unavailable for a total of two days next year. Which of the following is true about the ALE?

- A. The ALE is \$48.
- B. The ALE is \$400.
- C. The ALE is \$4,800.
- D. The ALE is \$9,600.

**Correct Answer:** D

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 92**

Jane, a user, installs software downloaded from a trusted website. The installed software causes unwanted pop-ups for pharmaceuticals. Which of the following BEST describes the type of threat?

- A. Trojan
- B. Backdoor
- C. Spyware
- D. Adware

**Correct Answer: D**

**Section: (none)**

**Explanation****Explanation/Reference:****QUESTION 93**

Sara, a security administrator, notices a number of ports being scanned on the perimeter firewall. At first the scanning appears random, but after monitoring the logs for 30 minutes, she determines that the whole port range is being scanned and all TCP flags are being turned on. Which of the following BEST describes this type of threat?

- A. Smurf attack
- B. X-Mas attack
- C. Spoofing
- D. Malicious insider threat

**Correct Answer: B**

**Section: (none)**

**Explanation****Explanation/Reference:****QUESTION 94**

The Chief Information Officer (CIO) receives a call from an individual who states they are from the IT department. The caller wants to know the CIO's ID and password to validate their account as part of a yearly account revalidation process. Which of the following BEST describes this scenario?

- A. Spam
- B. Hoax
- C. Spoofing
- D. Vishing

**Correct Answer: D**

**Section: (none)**

**Explanation****Explanation/Reference:**

**QUESTION 95**

To reduce an organization's risk exposure by verifying compliance with company policy, which of the following should be performed periodically?

- A. Qualitative analysis
- B. Quantitative analysis
- C. Routine audits
- D. Incident management

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 96**

Which of the following can be implemented if a security administrator wants only certain devices connecting to the wireless network?

- A. Disable SSID broadcast
- B. Install a RADIUS server
- C. Enable MAC filtering
- D. Lowering power levels on the AP

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 97**

A system administrator decides to use SNMPv3 on the network router in AuthPriv mode. Which of the following algorithm combinations would be valid?

- A. AES-RC4
- B. 3DES-MD5
- C. RSA-DSA
- D. SHA1-HMAC

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 98**

Which of the following are encryption algorithms that can use a 128-bit key size? (Select TWO).

- A. AES
- B. RC4
- C. Twofish
- D. DES

E. SHA2

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 99**

Unsolicited address items and messages are discovered on a Chief Information Officer's (CIO's) smartphone. Additionally, files on an administrator's smartphone are changed or missing. Which of the following BEST describes what may have happened?

- A. The CIO and the Administrator were both bluesnarfed.
- B. The CIO and the Administrator were both bluejacked.
- C. The CIO was bluejacked and the Administrator was bluesnarfed.
- D. The CIO was bluesnarfed and the Administrator was bluejacked.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 100**

Which of the following devices, connected to an IDS, would allow capture of the MOST traffic?

- A. Switch
- B. Router
- C. Firewall
- D. Hub

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 101**

In an enterprise environment, which of the following would be the BEST way to prevent users from accessing inappropriate websites when AUP requirements are constantly changing?

- A. Deploy a network proxy server.
- B. Configure Internet content filters on each workstation.
- C. Deploy a NIDS.
- D. Deploy a HIPS.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 102**

Broadcast traffic is having a negative impact on network performance. Which of the following might help minimize this issue?

- A. Use NAT to hide the IPs of each of the workstations.
- B. Separate the network onto a number of different switches.
- C. Separate the network into a number of different VLANs.
- D. Route all the unicast traffic through the proxy server.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 103**

A new wireless router has been compromised, blocking all of the company computers from using the router. Which of the following is the MOST likely cause for this issue?

- A. There was a backdoor account on the router.
- B. The default password on the router was not changed.
- C. The attacker discovered the WEP key of the router.
- D. The attacker had gone dumpster diving to find the router's credentials.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 104**

A company wants to maintain a backup site, and is more concerned about site maintenance cost rather than high availability following a disaster. Which of the following is the BEST solution?

- A. Cold site
- B. Remote site
- C. Hot site
- D. Warm site

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 105**

Which of the following would be the MOST likely reason to use a cluster of host servers to support load balancing?

- A. Confidentiality by distributing traffic across multiple host servers
- B. Enhance security by obscuring the physical host of the guest server

- C. Availability by distributing connections across multiple servers
- D. Integrity by separating traffic across multiple guest servers

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 106**

Which of the following controls is considered to be the MOST effective type of physical security?

- A. Access lists
- B. Cipher lock
- C. Chain link fence
- D. Mantrap

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 107**

An administrator notices that former temporary employees' accounts are still active on a domain. Which of the following can be implemented to increase security and prevent this from happening?

- A. Implement a password expiration policy.
- B. Implement an account expiration date for permanent employees.
- C. Implement time of day restrictions for all temporary employees.
- D. Run a last logon script to look for inactive accounts.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 108**

Which of the following devices is used to capture and analyze data packets when Jane, an unauthorized user, is trying to gain access to a network?

- A. Sniffer
- B. VPN concentrator
- C. Packet filtering firewall
- D. Router

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 109**

A password history value of three means which of the following?

- A. Three different passwords are used before one can be reused.
- B. A password cannot be reused once changed for three years.
- C. After three hours a password must be re-entered to continue.
- D. The server stores passwords in the database for three days.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 110**

Which of the following devices is BEST suited for servers that need to store private keys?

- A. Hardware security module
- B. Hardened network firewall
- C. Solid state disk drive
- D. Hardened host firewall

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 111**

A targeted email attack sent to Sara, the company's Chief Executive Officer (CEO), is known as which of the following?

- A. Whaling
- B. Bluesnarfing
- C. Vishing
- D. Dumpster diving

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 112**

In regards to secure coding practices, why is input validation important?

- A. It mitigates buffer overflow attacks.
- B. It makes the code more readable.
- C. It provides an application configuration baseline.
- D. It meets gray box testing standards.

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 113**

A security administrator needs to determine which system a particular user is trying to login to at various times of the day. Which of the following log types would the administrator check?

- A. Firewall
- B. Application
- C. IDS
- D. Security

**Correct Answer:** D  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 114**

If Pete, a security administrator, wants to ensure that certain users can only gain access to the system during their respective shifts, which of the following best practices would he implement?

- A. Separation of duties
- B. Time of day restrictions
- C. Implicit deny rule
- D. Least privilege

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 115**

Which of the following MUST be updated immediately when an employee is terminated to prevent unauthorized access?

- A. Registration
- B. CA
- C. CRL
- D. Recovery agent

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 116**

A security administrator is observing congestion on the firewall interfaces and a high number of half open incoming connections from different external IP addresses. Which of the following attack types is underway?

- A. Cross-site scripting
- B. SPIM
- C. Client-side
- D. DDoS

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 117**

Which of the following application security testing techniques is implemented when an automated system generates random input data?

- A. Fuzzing
- B. XSRF
- C. Hardening
- D. Input validation

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 118**

Which of the following can be used by a security administrator to successfully recover a user's forgotten password on a password protected file?

- A. Cognitive password
- B. Password sniffing
- C. Brute force
- D. Social engineering

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 119**

Which of the following BEST describes a protective countermeasure for SQL injection?

- A. Eliminating cross-site scripting vulnerabilities
- B. Installing an IDS to monitor network traffic
- C. Validating user input in web applications
- D. Placing a firewall between the Internet and database servers

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 120**

Which of the following BEST describes a common security concern for cloud computing?

- A. Data may be accessed by third parties who have compromised the cloud platform
- B. Antivirus signatures are not compatible with virtualized environments
- C. Network connections are too slow
- D. CPU and memory resources may be consumed by other servers in the same cloud

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 121**

Sara, a user, downloads a keygen to install pirated software. After running the keygen, system performance is extremely slow and numerous antivirus alerts are displayed. Which of the following BEST describes this type of malware?

- A. Logic bomb
- B. Worm
- C. Trojan
- D. Adware

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 122**

Which of the following should be considered to mitigate data theft when using CAT5 wiring?

- A. CCTV
- B. Environmental monitoring
- C. Multimode fiber
- D. EMI shielding

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 123**

To help prevent unauthorized access to PCs, a security administrator implements screen savers that lock the PC after five minutes of inactivity. Which of the following controls is being described in this situation?

- A. Management
- B. Administrative
- C. Technical
- D. Operational

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 124**

Pete, a network administrator, is capturing packets on the network and notices that a large amount of the traffic on the LAN is SIP and RTP protocols. Which of the following should he do to segment that traffic from the other traffic?

- A. Connect the WAP to a different switch.
- B. Create a voice VLAN.
- C. Create a DMZ.
- D. Set the switch ports to 802.1q mode.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 125**

Which of the following IP addresses would be hosts on the same subnet given the subnet mask 255.255.255.224? (Select TWO).

- A. 10.4.4.125
- B. 10.4.4.158
- C. 10.4.4.165
- D. 10.4.4.189
- E. 10.4.4.199

**Correct Answer: CD**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 126**

Which of the following transportation encryption protocols should be used to ensure maximum security between a web browser and a web server?

- A. SSLv2
- B. SSHv1

- C. RSA
- D. TLS

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 127**

Developers currently have access to update production servers without going through an approval process. Which of the following strategies would BEST mitigate this risk?

- A. Incident management
- B. Clean desk policy
- C. Routine audits
- D. Change management

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 128**

Which of the following is a difference between TFTP and FTP?

- A. TFTP is slower than FTP.
- B. TFTP is more secure than FTP.
- C. TFTP utilizes TCP and FTP uses UDP.
- D. TFTP utilizes UDP and FTP uses TCP.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 129**

Which of the following defines when Pete, an attacker, attempts to monitor wireless traffic in order to perform malicious activities?

- A. XSS
- B. SQL injection
- C. Directory traversal
- D. Packet sniffing

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 130**

Which of the following would MOST likely ensure that swap space on a hard disk is encrypted?

- A. Database encryption
- B. Full disk encryption
- C. Folder and file encryption
- D. Removable media encryption

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 131**

Configuring the mode, encryption methods, and security associations are part of which of the following?

- A. IPSec
- B. Full disk encryption
- C. 802.1x
- D. PKI

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 132**

A security administrator has just finished creating a hot site for the company. This implementation relates to which of the following concepts?

- A. Confidentiality
- B. Availability
- C. Succession planning
- D. Integrity

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 133**

Which of the following should Matt, a security administrator, include when encrypting smartphones? (Select TWO).

- A. Steganography images
- B. Internal memory
- C. Master boot records

- D. Removable memory cards
- E. Public keys

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 134**

Which of the following is the below pseudo-code an example of? IF VARIABLE (CONTAINS NUMBERS = TRUE) THEN EXIT

- A. Buffer overflow prevention
- B. Input validation
- C. CSRF prevention
- D. Cross-site scripting prevention

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 135**

A system administrator is using a packet sniffer to troubleshoot remote authentication. The administrator detects a device trying to communicate to TCP port 49. Which of the following authentication methods is MOST likely being attempted?

- A. RADIUS
- B. TACACS+
- C. Kerberos
- D. LDAP

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 136**

If Organization A trusts Organization B and Organization B trusts Organization C, then Organization A trusts Organization C. Which of the following PKI concepts is this describing?

- A. Transitive trust
- B. Public key trust
- C. Certificate authority trust
- D. Domain level trust

**Correct Answer:** A

**Section:** (none)

**Explanation**



**Explanation/Reference:**

**QUESTION 137**

Which of the following concepts is BEST described as developing a new chain of command in the event of a contingency?

- A. Business continuity planning
- B. Continuity of operations
- C. Business impact analysis
- D. Succession planning

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 138**

Which of the following protocols is used to authenticate the client and server's digital certificate?

- A. PEAP
- B. DNS
- C. TLS
- D. ICMP

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 139**

Which of the following security concepts would Sara, the security administrator, use to mitigate the risk of data loss?

- A. Record time offset
- B. Clean desk policy
- C. Cloud computing
- D. Routine log review

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 140**

Which of the following is an example of multifactor authentication?

- A. Credit card and PIN

- B. Username and password
- C. Password and PIN
- D. Fingerprint and retina scan

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 141**

After Matt, a user, enters his username and password at the login screen of a web enabled portal, the following appears on his screen:

`Please only use letters and numbers on these fields`

Which of the following is this an example of?

- A. Proper error handling
- B. Proper input validation
- C. Improper input validation
- D. Improper error handling

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 142**

Matt, a developer, recently attended a workshop on a new application. The developer installs the new application on a production system to test the functionality. Which of the following is most likely affected?

- A. Application design
- B. Application security
- C. Initial baseline configuration
- D. Management of interfaces

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 143**

Which of the following is an authentication and accounting service that uses TCP for connecting to routers and switches?

- A. DIAMETER
- B. RADIUS
- C. TACACS+
- D. Kerberos

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 144**

Which of the following can BEST help prevent cross-site scripting attacks and buffer overflows on a production system?

- A. Input validation
- B. Network intrusion detection system
- C. Anomaly-based HIDS
- D. Peer review

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 145**

Pete, a security engineer, maintains up-to-date virus scan signatures on all systems. Which of the following should Pete do as well to prevent the exploiting of known vulnerabilities?

- A. Application patching
- B. White box penetration testing
- C. Vulnerability assessment
- D. Port scanning

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 146**

If Pete, the administrator, is blocking port 69, which of the following protocols will this affect?

- A. TFTP
- B. FTP
- C. RDP
- D. DNS

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 147**

Which of the following should be connected to the fire alarm system in order to help prevent the spread of a fire in a server room without data loss to assist in an FM-200 deployment?

- A. Water base sprinkler system
- B. Electrical
- C. HVAC
- D. Video surveillance

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 148**

Pete, a home user, is trying to secure his wireless network from his technical neighbor. Which of the following should Pete implement on his access point to keep his neighbor from accessing his wireless network and viewing Pete's online chats?

- A. WPA
- B. RIPMD
- C. WEP
- D. LEAP

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 149**

Matt, a security consultant, has been tasked with increasing server fault tolerance and has been given no budget to accomplish his task. Which of the following can Matt implement to ensure servers will withstand hardware failure?

- A. Hardware load balancing
- B. RAID
- C. A cold site
- D. A host standby

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 150**

Pete has obtained a highly sensitive document and has placed it on a network drive which has been formatted with NTFS and is shared via CIFS. Which of the following access controls apply to the sensitive file on the server?

- A. Discretionary
- B. Rule based

- C. Role based
- D. Mandatory

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 151**

Matt, the backup operator, is implementing a new backup plan. Which of the following is the MOST important step in a backup plan to ensure the disaster recovery plan is executed without any incidents?

- A. Verify that the data on the backup tapes can be restored on a test server.
- B. Verify that the backup plan is stored in digital format on the backup tapes.
- C. Verify that the data on the backup tapes can be restored on the web server.
- D. Verify that all backup data is encrypted on the tape and store the encryption key offsite.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 152**

Which of the following information should Pete, an employee at a pharmaceutical company, review during the company-wide information security awareness training, before handling customer data?

- A. Acceptable use policy
- B. Account management procedures
- C. Laws and regulations
- D. End user license agreement

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 153**

Matt has installed a new KDC for his corporate environment. Which of the following authentication protocols is Matt planning to implement across the organization?

- A. LDAP
- B. RADIUS
- C. Kerberos
- D. XTACACS

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 154**

Which of the following uses only a private key?

- A. RSA
- B. ECC
- C. AES
- D. SHA

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 155**

Sara, a security manager, received the results of a vulnerability assessment stating that several accounts were enabled, even though the employees had been terminated in months prior. Which of the following needs to be performed to ensure this issue is mitigated for future tests?

- A. Change management reviews
- B. Routine account audits
- C. Incident management audits
- D. User rights and permissions reviews

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 156**

Matt, a security manager, receives the results of a social engineering exercise. An attacker was able to successfully impersonate Sara, a company executive, over the phone when contacting the helpdesk and gained access to her password. After further research, it was determined that someone in the company had thrown out printouts of Sara's calendar for that week, showing when she would be traveling on business. Which of the following should employees be trained on to help mitigate this issue in the future?

- A. Password behaviors
- B. Help desk procedures
- C. Secure disposal policy
- D. Clean desk policies

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 157**

Sara is sniffing traffic on a wireless network configured with WEP. She obtains numerous packets and then

attempts to breach the network. Which of the following is Sara MOST likely attempting?

- A. Bluejacking
- B. IV attack
- C. Evil twin
- D. War driving

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 158**

Matt, a security technician, has been tasked with updating client anti-virus solutions. He makes sure that all of the workstations have been properly updated. Later that day, he receives a call from a user stating that their PC is unresponsive and the screen blanks out every few minutes. Matt goes to the website of the anti-virus vendor and sees that new virus definitions are available. Which of the following is the MOST likely cause of the behavior that the user is reporting?

- A. A zero-day attack
- B. IV attack
- C. XML injection
- D. Cross-site scripting

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 159**

Pete, a network administrator, needs to implement a VPN. Which of the following could he use to accomplish this objective? (Select TWO).

- A. SMTP
- B. SNMP
- C. IPSec
- D. SSL
- E. SCP
- F. SFTP

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 160**

Matt has recently implemented a new network design at his organization and wishes to actively test security controls on the new network. Which of the following should Matt perform?

- A. Vulnerability assessment
- B. Black box testing
- C. White box testing
- D. Penetration testing

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 161**

Jane has implemented an array of four servers to accomplish one specific task. This is BEST known as which of the following?

- A. Clustering
- B. RAID
- C. Load balancing
- D. Virtualization

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 162**

Pete, an employee, was recently indicted for fraud charges. Jane, a new security technician at the company, was tasked with collecting information from Pete's workstation. Jane seized the hard drive from the workstation without collecting any other information from the workstation. Which of the following principles did Jane violate?

- A. Track man hours and expense
- B. Order of volatility
- C. Damage control
- D. Preservation of evidence

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 163**

A database server containing personal information and a file server containing non-critical information must be secured. Which of the following would be a BEST practice to secure the servers? (Select TWO).

- A. Place the file server behind a door requiring biometric authorization.
- B. Place both servers under the system administrator's desk.
- C. Place the database server behind a door with a cipher lock.
- D. Place the file server in an unlocked rack cabinet.
- E. Place the database server behind a door requiring biometric authorization.



**Correct Answer:** AE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 164**

A company is experiencing an extraordinary amount of web traffic that is crippling the server. The web traffic suddenly stops. The mail server experiences the same amount of traffic as before then crashes. Which of the following attacks would this BEST describe?

- A. DoS
- B. Spam
- C. Man-in-the-middle
- D. Replay

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 165**

Which of the following would ensure confidentiality and authorization to the management interface of a router?

- A. Enable an access list and RADIUS
- B. Enable SSH and TACACS
- C. Enable an access list and PKI
- D. Enable LDAP and strong passwords

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 166**

Which of the following BEST describes a demilitarized zone?

- A. A buffer zone between protected and unprotected networks.
- B. A network where all servers exist and are monitored.
- C. A sterile, isolated network segment with access lists.
- D. A private network that is protected by a firewall and a VLAN.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 167**

Which of the following statements BEST describes the basic functionality of a network firewall?

- A. Improves communication between trusted and non-trusted networks
- B. Redirects accepted traffic to the proper VLAN
- C. Provides stateful packet inspection of TCP traffic
- D. Accepts and rejects data based on content

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 168**

Which of the following BEST describes the function of a protocol analyzer?

- A. It allows a security technician to decrypt packets as they traverse the network.
- B. It allows a security technician to encrypt packets as they traverse the network.
- C. It allows a security technician to perform deep state packet inspection.
- D. It allows a security technician to perform hardware device troubleshooting.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 169**

Which of the following network solutions would BEST allow Jane, a security technician, to host an extranet application for her company?

- A. Platform as a Service
- B. Infrastructure as a Service
- C. Storage as a Service
- D. Software as a Service

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 170**

Which of the following network design elements BEST provides a testing environment to perform malware analysis?

- A. Platform as a Service (PaaS)
- B. DMZ
- C. Virtualization
- D. Proxies

**Correct Answer:** C

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 171**

Matt, a security technician, is attempting to explain why some of the company policies should be changed for high risk IT positions. Which of the following concepts BEST explains his support for fraud detection?

- A. Time of day restrictions is more likely to discover fraud than the other fraud detection methods.
- B. Least privilege principles allow internal audit teams to discover fraud while a staff member is out of the office.
- C. Separation of duties is a better fraud detection method than mandatory vacations; therefore, it should be used.
- D. Mandatory vacations support the company discovering fraud while staff members are out of the office.

**Correct Answer: D**

**Section: (none)**

**Explanation****Explanation/Reference:****QUESTION 172**

Jane, a security technician, is working with the network firewall team to implement access controls at the company's demarc as part of the initiation of configuration management processes. One of the network technicians asks Jane to explain the access control type found in a firewall. With which of the following should Jane respond?

- A. Rule based access control
- B. Role based access control
- C. Discretionary access control
- D. Mandatory access control

**Correct Answer: A**

**Section: (none)**

**Explanation****Explanation/Reference:****QUESTION 173**

Sara, a security administrator, has been tasked with explaining smart cards to the company's management team. Which of the following are smart cards? (Select TWO).

- A. DAC
- B. Tokens
- C. CAC
- D. ACL
- E. PIV

**Correct Answer: CE**

**Section: (none)**

**Explanation****Explanation/Reference:**

**QUESTION 174**

Jane, a security architect, is implementing security controls throughout her organization. Which of the following BEST explains the vulnerability in the formula that a Risk = Threat x Vulnerability x Impact?

- A. Vulnerability is related to the risk that an event will take place.
- B. Vulnerability is related to value of potential loss.
- C. Vulnerability is related to the probability that a control will fail.
- D. Vulnerability is related to the probability of the event.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 175**

Jane, a security analyst, has recently implemented a password complexity requirement within the company systems. Which of the following BEST explains this requirement?

- A. Accounts shall be required to adhere to no less than 15 characters for all personnel accounts.
- B. Accounts shall have two uppercase, two lowercase, and one number or special character.
- C. Accounts shall be changed no less than every ninety (90) days for service accounts.
- D. Accounts shall be disabled after a period of thirty (30) days if the account has not logged on within that time period.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 176**

Pete, an email administrator, notices that Sara and Matt are exchanging image files back and forth. Pete opens an image and sees the image is from the company's intranet. Pete checks the MD5 hash of the file on the Internet page versus the file Sara and Matt are sending and the hash values do not match. Which of the following is this MOST likely an example of?

- A. Key escrow
- B. Steganography
- C. Digital signature
- D. Non-repudiation

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 177**

The HR department has been rotating positions in their own department and hiring new employees to fill positions. It is the end of the year and Pete, the CEO, is concerned about performance reviews and salaries

being leaked from the corporate file server. Which of the following should Pete request be done to ensure only the required employees have access to the performance reviews?

- A. Perform an audit for access.
- B. Encrypt the data.
- C. Check the logs for access.
- D. Move the data to a USB drive.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 178**

Jane is building a new web server. Jane only wants to run a web server on a workstation so she disables the default web site, turns off FTP, adds a certificate, and enables port 443 on the web server. Jane is performing which of the following?

- A. Application patch management
- B. Exception handling
- C. Application hardening
- D. Application baselining

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 179**

Pete's boss is concerned with the amount of down time the shipping and receiving server is having. He asks Pete to provide him with numbers on the mean time between failures. Which of the following equations could Pete perform to provide this information to his boss?

- A. Calculate the Annual Loss Expectancy for the year.
- B. Track the man hours and expenses of the system being down for a month.
- C. The operational time of the server divided by the number of times the system went down.
- D. Calculate the Annual Rate of Occurrence for the year.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 180**

The information security department regularly walks the campus and around the buildings looking for unauthorized open wireless networks. This is an example of which of the following?

- A. A site survey
- B. Antenna placement

- C. War dialing
- D. War driving

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 181**

Sara, an attacker, launches a man-in-the-middle attack against Pete. While sniffing Pete's network traffic, Sara is able to acquire the current cookies Pete is using. Which of the following can Sara use these cookies for?

- A. Buffer overflow
- B. Header manipulation
- C. ARP poisoning
- D. Session hijacking

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 182**

Users are reporting having trouble connecting to a certain web server. Pete, the security engineer, discovers the server appears to be running optimally at the OS level. Upon deeper investigation, Pete determines that the server is suspiciously flooding users with RST packets when they attempt to connect. Which of the following tools did Pete MOST likely use to discover this?

- A. Honeynet
- B. Network sniffer
- C. Vulnerability scanner
- D. Port scanner

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 183**

The lobby of the hotel allows users to plug in their laptops to access the Internet. This network is also used for the IP based phones in the hotel lobby. Mike, the security engineer, wants to secure the phones so that guests cannot electronically eavesdrop on other guests. Which of the following would Mike MOST likely implement?

- A. VLAN
- B. Port security
- C. MPLS
- D. Separate voice gateway

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 184**

Jane, the security engineer, is tasked with hardening routers. She would like to ensure that network access to the corporate router is allowed only to the IT group and from authorized machines. Which of the following would MOST likely be implemented to meet this security goal? (Select TWO).

- A. SNMP
- B. HTTPS
- C. ACL
- D. Disable console
- E. SSH
- F. TACACS+

**Correct Answer: CF**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 185**

Jane, the network administrator, would like wireless users to authenticate to the network's RADIUS server via EAP prior to connecting to the WLAN. Which of the following would MOST likely be implemented to facilitate this authentication?

- A. 802.1x
- B. WPA2-PSK
- C. WEP
- D. TACACS+

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 186**

After a new firewall has been installed, devices cannot obtain a new IP address. Which of the following ports should Matt, the security administrator, open on the firewall?

- A. 25
- B. 68
- C. 80
- D. 443

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 187**

Which of the following could Sara, an administrator, use in a workplace to remove sensitive data at rest from the premises?

- A. Network sniffer
- B. Personally owned devices
- C. Vulnerability scanner
- D. Hardware locks

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 188**

Pete, the system administrator, has concerns regarding users losing their company provided smartphones. Pete's focus is on equipment recovery. Which of the following BEST addresses his concerns?

- A. Enforce device passwords.
- B. Use remote sanitation.
- C. Enable GPS tracking.
- D. Encrypt stored data.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 189**

Pete, the system administrator, wishes to monitor and limit users' access to external websites. Which of the following would BEST address this?

- A. Block all traffic on port 80.
- B. Implement NIDS.
- C. Use server load balancers.
- D. Install a proxy server.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 190**

Sara, the security administrator, must configure the corporate firewall to allow all public IP addresses on the internal interface of the firewall to be translated to one public IP address on the external interface of the same firewall. Which of the following should Sara configure?



- A. PAT
- B. NAP
- C. DNAT
- D. NAC

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 191**

An external company has notified Jane at ABC Co. that their web server was attacked by one of ABC's IP addresses. The external company provides the time of the attack and the following log information:

SRC IP: 182.45.88.12  
SRC Port: TCP 1335  
DST IP: 12.42.8.122  
DST Port: TCP 443

Given that ABC uses PAT at their firewall, which of the following is true about this incident?

- A. Jane cannot identify the ABC's internal IP address that launched the attack because it happened over HTTPS.
- B. The external company must provide the packet payload in order for Jane to identify the ABC's IP that launched the attack.
- C. The external company did not provide enough information for Jane to be able to identify the ABC's internal IP that launched the attack.
- D. Jane can identify the ABC's internal IP address that launched the attack by reviewing the Firewall logs.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 192**

Which of the following settings can Jane, the network administrator, implement in the computer lab to ensure that user credentials cannot be captured by the next computer user?

- A. Implement full drive encryption on all lab computers.
- B. Reverse the computer to its original state upon reboot.
- C. Do not display last username in logon screen.
- D. Deploy privacy screens on all lab computers.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 193**

Jane, a security administrator, is reviewing the company's official documentation to mitigate the risk of data loss

due to personally owned devices being connected to perform company related work. Which of the following documentation should Jane MOST likely review and update?

- A. Acceptable risk
- B. Data retention policy
- C. Acceptable use policy
- D. End user license agreement

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 194**

After a production outage, which of the following documents contains detailed information on the order in which the system should be restored to service?

- A. Succession planning
- B. Disaster recovery plan
- C. Information security plan
- D. Business impact analysis

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 195**

Pete, a security administrator, has implemented SSH across all network infrastructure devices in the enterprise. Which of the following protocols will be used to exchange keying material within SSH?

- A. Transport layer protocol
- B. IPSec
- C. Diffie-Hellman
- D. Secure socket layer

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 196**

A user has just returned from security awareness training, where users were encouraged to strengthen their passwords and voicemail codes. Which of the following would be the MOST secure password for the user's workstation?

- A. H0me0nTh3Range
- B. Letme1nNow
- C. \$3cur1#y

D. Passw0rd99

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 197**

Matt must come up with a design solution which will enable remote users to securely access network resources. Which of the following design elements will enable Matt to meet this objective?

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 198**

Sara, a security technician, has been asked to design a solution which will enable external users to have access to a Web server, while keeping the internal network unaffected by this access. Which of the following would BEST meet this objective?

- A. Place the Web server on a VLAN
- B. Place the Web server inside of the internal firewall
- C. Place the Web server in a DMZ
- D. Place the Web server on a VPN

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 199**

Pete needs to open ports on the firewall to allow for secure transmission of files. Which of the following ports should be opened on the firewall?

- A. TCP 23
- B. UDP 69
- C. TCP 22
- D. TCP 21

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 200**

A company that provides streaming media has recently experienced latency during certain times of the day. Which of the following would mitigate the latency issue?

- A. Web security gateway
- B. Firewall
- C. Load balancing
- D. VPN concentrator

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 201**

Matt, a security technician, notices a high number of ARP spoofing attacks on his network. Which of the following design elements would mitigate ARP spoofing attacks?

- A. Flood guards
- B. Implicit deny
- C. VLANs
- D. Loop protection

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 202**

Matt works for an organization that requires data to be recovered in the shortest amount of time possible. Which of the following backup types would BEST meet the organization's needs?

- A. Full backups daily
- B. Differential backups monthly
- C. Full backups weekly
- D. Incremental backups monthly

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 203**

How would a technician secure a router configuration if placed in an unsecured closet?

- A. Mount the router into an immovable rack.
- B. Enable SSH for maintenance of the router.

- C. Disable the console port on the router.
- D. Label the router with contact information.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 204**

Which of the following firewall rules would only block tftp traffic and record it?

- A. deny udp any server log
- B. deny udp any server eq 69
- C. deny tcp any server log
- D. deny udp any server eq 69 log

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 205**

Which of the following services should be disabled to stop attackers from using a web server as a mail relay?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 206**

Mapping one IP address to another IP address is an example of:

- A. MAC.
- B. DMZ.
- C. NAC.
- D. NAT.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 207**

A security administrator has a requirement to encrypt several directories that are non-hierarchical. Which of the following encryption models would BEST meet this requirement?

- A. AES512
- B. Database encryption
- C. File encryption
- D. Full disk encryption

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 208**

Pete, a security analyst, has been tasked with explaining the different types of malware to his colleagues. The two malware types that the group seems to be most interested in are backdoors and logic bombs. Which of the following differentiates these two types of malware?

- A. A backdoor is a coding issue that can be discovered by proper configuration management processes.
- B. A logic bomb is typically hidden within the boot sector of the hard drive and is used to cause DDoS.
- C. A backdoor is a third generation attack which is typically low risk because only highly trained staff can achieve it.
- D. A logic bomb is undetectable by current antivirus signatures because a patch has not been issued.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 209**

Pete, a security analyst, has been tasked with explaining the different types of malware to his colleagues. The two malware types that the group seems to be most interested in are botnets and viruses. Which of the following explains the difference between these two types of malware?

- A. Viruses are a subset of botnets which are used as part of SYN attacks.
- B. Botnets are a subset of malware which are used as part of DDoS attacks.
- C. Viruses are a class of malware which create hidden openings within an OS.
- D. Botnets are used within DR to ensure network uptime and viruses are not.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 210**

Which of the following BEST explains the use of an HSM within the company servers?

- A. Thumb drives present a significant threat which is mitigated by HSM.
- B. Software encryption can perform multiple functions required by HSM.

- C. Data loss by removable media can be prevented with DLP.
- D. Hardware encryption is faster than software encryption.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 211**

Which of the following technologies can store multi-tenant data with different security requirements?

- A. Data loss prevention
- B. Trusted platform module
- C. Hard drive encryption
- D. Cloud computing

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 212**

Which of the following technologies prevents USB drives from being recognized by company systems?

- A. Registry keys
- B. Full disk encryption
- C. USB encryption
- D. Data loss prevention

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 213**

Matt, a security analyst, needs to implement encryption for company data and also prevent theft of company data. Where and how should Matt meet this requirement?

- A. Matt should implement access control lists and turn on EFS.
- B. Matt should implement DLP and encrypt the company database.
- C. Matt should install Truecrypt and encrypt the company server.
- D. Matt should install TPMs and encrypt the company database.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 214**

Which of the following types of encryption will help in protecting files on a PED?

- A. Mobile device encryption
- B. Transport layer encryption
- C. Encrypted hidden container
- D. Database encryption

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 215**

Which of the following is MOST closely associated with BitLocker?

- A. ACL
- B. DOS
- C. DLP
- D. TPM

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 216**

Pete, a security analyst, has been informed that the development team has plans to develop an application which does not meet the company's password policy. Which of the following should Pete do NEXT?

- A. Contact the Chief Information Officer and ask them to change the company password policy so that the application is made compliant.
- B. Tell the application development manager to code the application to adhere to the company's password policy.
- C. Ask the application development manager to submit a risk acceptance memo so that the issue can be documented.
- D. Inform the Chief Information Officer of non-adherence to the security policy so that the developers can be reprimanded.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 217**

Sara, a security manager, has decided to force expiration of all company passwords by the close of business day. Which of the following BEST supports this reasoning?

- A. A recent security breach in which passwords were cracked.



- B. Implementation of configuration management processes.
- C. Enforcement of password complexity requirements.
- D. Implementation of account lockout procedures.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 218**

Which of the following presents the STRONGEST access control?

- A. MAC
- B. TACACS
- C. DAC
- D. RBAC

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 219**

Which of the following encompasses application patch management?

- A. Configuration management
- B. Policy management
- C. Cross-site request forgery
- D. Fuzzing

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 220**

Sara, an application developer, implemented error and exception handling alongside input validation. Which of the following does this help prevent?

- A. Buffer overflow
- B. Pop-up blockers
- C. Cross-site scripting
- D. Fuzzing

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 221**

Which of the following is the LEAST volatile when performing incident response procedures?

- A. Registers
- B. RAID cache
- C. RAM
- D. Hard drive

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 222**

Which of the following can allow Sara, a security analyst, to encrypt individual files on a system?

- A. EFS
- B. Single sign-on
- C. TLS
- D. Journaled file system

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 223**

An encryption method where the plain text and cipher text are always the same size is an example of which of the following types of encryption?

- A. RC4
- B. MD5
- C. Stream Cipher
- D. Block Cipher

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 224**

The information security team does a presentation on social media and advises the participants not to provide too much personal information on social media web sites. This advice would BEST protect people from which of the following?

- A. Rainbow tables attacks
- B. Brute force attacks

- C. Birthday attacks
- D. Cognitive passwords attacks

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 225**

The compliance team comes out with a new policy that all data stored on tapes over 3 years must be degaussed. This BEST describes which of the following types of policies?

- A. Data handling
- B. Data classification
- C. Data labeling
- D. Data disposal

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 226**

Pete's corporation has outsourced help desk services to a large provider. Management has published a procedure that requires all users, when receiving support, to call a special number. Users then need to enter the code provided to them by the help desk technician prior to allowing the technician to work on their PC. Which of the following does this procedure prevent?

- A. Collusion
- B. Impersonation
- C. Pharming
- D. Transitive Access

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 227**

Pete, the security engineer, would like to prevent wireless attacks on his network. Pete has implemented a security control to limit the connecting MAC addresses to a single port. Which of the following wireless attacks would this address?

- A. Interference
- B. Man-in-the-middle
- C. ARP poisoning
- D. Rogue access point

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 228**

Jane, the security administrator, is having issues with unauthorized users connecting to the wireless network. For administrative reasons, she cannot implement any wireless encryption methods. Which of the following can she implement to prevent unauthorized users from connecting to the network?

- A. NIPS
- B. Disable unused ports
- C. MAC filtering
- D. WEP

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 229**

Matt, the security administrator, wants to secure the wireless network. Which of the following encryption methods offers the MOST security?

- A. WPA2 ENT AES
- B. WPA2 PSK AES
- C. WPA2 ENT TKIP
- D. WPA2 PSK TKIP

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 230**

Sara, the IT administrator, wants to control which devices can connect to the wireless network. Which of the following can she implement to accomplish this task?

- A. WPA2 Enterprise with AES encryption
- B. Decrease the WAP's power levels
- C. Static IP addressing
- D. MAC address filtering

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 231**

When a new network drop was installed, the cable was run across several fluorescent lights. The users of the new network drop experience intermittent connectivity. Which of the following environmental controls was MOST likely overlooked during installation?

- A. Humidity sensors
- B. EMI shielding
- C. Channel interference
- D. Cable kinking

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 232**

Pete, the Chief Security Officer, wishes to institute annual security policy training for all users. The training's purpose is to educate users about access to sensitive data. Which of the following should be included in the training?

- A. Revalidation of user account privileges.
- B. Review of guidelines for network stored data permissions.
- C. Implementation of new password procedures.
- D. Installation of disk-based encryption to protect data.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 233**

Pete, the system administrator, has blocked users from accessing social media web sites. In addition to protecting company information from being accidentally leaked, which additional security benefit does this provide?

- A. No competition with the company's official social presence
- B. Protection against malware introduced by banner ads
- C. Increased user productivity based upon fewer distractions
- D. Elimination of risks caused by unauthorized P2P file sharing

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 234**

Pete, the system administrator, is concerned about unauthorized access at all entrances into the building. PIN pad readers have been installed, but users have developed the habit of holding the door for others behind them. Which of the following would BEST prevent this?

- A. Install mantraps at every unmanned entrance.

- B. Replace the PIN pad readers with card readers.
- C. Implement video and audio surveillance equipment.
- D. Require users to sign conduct policies forbidding these actions.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 235**

Which of the following is a MAIN objective of implementing a clean desk user policy?

- A. Coax users into accepting cloud computing as a viable option.
- B. Enforce notions that other users cannot be trusted.
- C. Verify that user accounts are strong and complex.
- D. Ensure that no sensitive data is left unsupervised.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 236**

Jane, a network administrator, has configured a 48-port switch to isolate four different departments. Which of the following has Jane MOST likely configured on the switch?

- A. NAC
- B. 802.1x
- C. VLAN
- D. DMZ

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 237**

A network stream needs to be encrypted. Sara, the network administrator, has selected a cipher which will encrypt 8 bits at a time before sending the data across the network. Which of the following has Sara selected?

- A. Block cipher
- B. Stream cipher
- C. CRC
- D. Hashing algorithm

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 238**

Pete, a security auditor, has detected clear text passwords between the RADIUS server and the authenticator. Which of the following is configured in the RADIUS server and what technologies should the authentication protocol be changed to?

- A. PAP, MSCHAPv2
- B. CHAP, PAP
- C. MSCHAPv2, NTLMv2
- D. NTLM, NTLMv2

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 239**

Which of the following BEST describes a SQL Injection attack?

- A. The attacker attempts to have the receiving server pass information to a back-end database from which it can compromise the stored information.
- B. The attacker attempts to have the receiving server run a payload using programming commonly found on web servers.
- C. The attacker overwhelms a system or application, causing it to crash and bring the server down to cause an outage.
- D. The attacker overwhelms a system or application, causing it to crash, and then redirects the memory address to read from a location holding the payload.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 240**

Which of the following is a hardware-based security technology included in a computer?

- A. Symmetric key
- B. Asymmetric key
- C. Whole disk encryption
- D. Trusted platform module

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 241**

Jane, the administrator of a small company, wishes to track people who access the secured server room, which

is secured only by a simple hardware key lock. Jane does not have much of a budget or the approval to make significant construction changes. Given the limitations, which of the following can she do in the meantime?

- A. Implement an access log and a security guard
- B. Install a 24/7 closed-circuit camera system
- C. Install a separate hardware lock with limited keys
- D. Implement a cipher key lock

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 242**

An administrator with a small company has begun to implement a backup strategy of the company's critical financial data. Which of the following is the MOST secure place to store the back-ups?

- A. Near the data servers, for ease of restoration
- B. Next to where the physical records (e.g. paper) are stored
- C. At a remote off-site location
- D. With the financial department

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 243**

Which of the following describes how Sara, an attacker, can send unwanted advertisements to a mobile device?

- A. Man-in-the-middle
- B. Bluejacking
- C. Bluesnarfing
- D. Packet sniffing

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 244**

Matt, a security administrator, is receiving reports about several SQL injections and buffer overflows through his company's website. Which of the following would reduce the amount of these attack types?

- A. Antivirus
- B. Anti-spam
- C. Input validation
- D. Host based firewalls



**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 245**

A new server image is being created and Sara, the security administrator, would like a baseline created for the servers. Which of the following needs to be taken into account for the baseline?

- A. Disabling all unnecessary services
- B. Enabling all default accounts
- C. Disabling all accounts
- D. Enabling all default services

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 246**

Pete, a person who appears to be from a delivery company, is holding a stack of boxes. He requests that the door be held open as he enters the office. Which of following attacks has MOST likely taken place? (Select TWO).

- A. Impersonation
- B. Vishing
- C. Shoulder surfing
- D. Tailgating
- E. Whaling

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 247**

The Chief Information Officer (CIO) is concerned that passwords may be written down and posted in plain sight. Which of the following would BEST mitigate this risk?

- A. Password expiration policy
- B. Clean desk policy
- C. Enforce greater password complexity
- D. Acceptable use policy

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 248**

Pete, an employee, is terminated from the company and the legal department needs documents from his encrypted hard drive. Which of the following should be used to accomplish this task? (Select TWO).

- A. Private hash
- B. Recovery agent
- C. Public key
- D. Key escrow
- E. CRL

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 249**

A company is concerned about proprietary information leaving the network via email. Which of the following is the BEST solution to remediate the risk?

- A. Block port 25 on the network
- B. Deploy a firewall on the e-mail server
- C. Filter incoming traffic
- D. Filter outgoing traffic

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 250**

Several departments within a company have a business need to send high volumes of confidential information to customers via email. Which of the following is the BEST solution to mitigate unintentional exposure of confidential information?

- A. Employ encryption on all outbound emails containing confidential information.
- B. Employ exact data matching and prevent inbound emails with Data Loss Prevention.
- C. Employ hashing on all outbound emails containing confidential information.
- D. Employ exact data matching and encrypt inbound e-mails with Data Loss Prevention.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 251**

A company had decided to assign employees laptops instead of desktops to mitigate the risk of company closures due to disasters. Which of the following is the company trying to ensure?

- A. Succession planning
- B. Fault tolerance
- C. Continuity of operations
- D. Removing single points of failure

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 252**

Sara, a security administrator, has implemented outbound email filtering. Which of the following would this MOST likely protect Sara's company from?

- A. Data loss
- B. Phishing
- C. SPAM solicitation
- D. Distributed denial of service attacks

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 253**

Pete, the security administrator, wants to ensure that traffic to the corporate intranet is secure using HTTPS. He configures the firewall to deny traffic to port 80. Now users cannot connect to the intranet even through HTTPS. Which of the following is MOST likely causing the issue?

- A. The web server is configured on the firewall's DMZ interface.
- B. The VLAN is improperly configured.
- C. The firewall's MAC address has not been entered into the filtering list.
- D. The firewall executes an implicit deny.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 254**

Sara, the network security administrator, wants to separate Finance department traffic from the rest of the company. The company uses the following IP addresses:

Servers and switches: 192.168.1.1 - 192.168.1.40

Users: 192.168.1.70 - 192.168.1.110

Finance Users: 192.168.1.200 - 192.168.1.250

Which of the following would BEST meet Sara's goal?

- A. Separate Gateways and Subnet mask of 255.255.255.254

- B. VLAN and Subnet mask of 255.255.255.252
- C. QoS and Subnet mask of 255.255.255.254
- D. SwitchPort Security and a Subnet mask of 255.255.255.252

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 255**

Which of the following ports are used for secure SNMP and FTPS by default? (Select TWO).

- A. 21
- B. 22
- C. 123
- D. 161
- E. 443
- F. 8080

**Correct Answer:** DE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 256**

Which of the following wireless security algorithms is vulnerable to dictionary attacks when weak passwords are used?

- A. LEAP
- B. EAP-TLS
- C. PEAP
- D. EAP-FAST

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 257**

Power and data cables from the network center travel through the building's boiler room. Which of the following should be used to prevent data emanation?

- A. Video monitoring
- B. EMI shielding
- C. Plenum CAT6 UTP
- D. Fire suppression

**Correct Answer:** B

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 258**

Mike, a user, receives an email from his grandmother stating that she is in another country and needs money. The email address belongs to his grandmother. Which of the following attacks is this?

- A. Man-in-the-middle
- B. Spoofing
- C. Relaying
- D. Pharming

**Correct Answer: B**

**Section: (none)**

**Explanation****Explanation/Reference:****QUESTION 259**

Sara, a user, receives several unwanted instant messages. Which of the following types of attacks is this?

- A. Phishing
- B. Vishing
- C. Spam
- D. Spim

**Correct Answer: D**

**Section: (none)**

**Explanation****Explanation/Reference:****QUESTION 260**

Sara, a security administrator, has changed access point signal strength and antenna placement to help prevent which of the following wireless attacks?

- A. Evil twin
- B. War driving
- C. Bluesnarfing
- D. IV attack

**Correct Answer: B**

**Section: (none)**

**Explanation****Explanation/Reference:****QUESTION 261**

Which of the following ports is MOST likely using a secure protocol, by default?

- A. 21

- B. 80
- C. 110
- D. 443

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 262**

Which of the following network ports is MOST likely associated with HTTPS, by default?

- A. 53
- B. 80
- C. 123
- D. 443

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 263**

Which of the following allows Mike, a security technician, to view network traffic for analysis?

- A. Spam filter
- B. Sniffer
- C. Router
- D. Switch

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 264**

Which of the following should Matt, a security technician, apply to the network for loop protection?

- A. Spanning tree
- B. Log analysis
- C. Implicit deny
- D. Load balancers

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 265**

Which of the following network administration principles is MOST closely associated with firewall ACLs?

- A. Log analysis
- B. Port address translation
- C. Implicit deny
- D. Stateful inspection

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 266**

Which of the following protocols can be used to secure traffic for telecommuters?

- A. WPA
- B. IPSec
- C. ICMP
- D. SMTP

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 267**

Which of the following should Sara, a security technician, use to reduce the possibility of an attacker discovering the company's wireless network?

- A. Disable SSID broadcast
- B. Implement TKIP
- C. Apply MAC filtering
- D. Upgrade WEP to WPA

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 268**

Which of the following is a management control?

- A. Logon banners
- B. Written security policy
- C. SYN attack prevention
- D. Access Control List (ACL)

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 269**

Which of the following risk concepts BEST supports the identification of fraud?

- A. Risk transference
- B. Management controls
- C. Mandatory vacations
- D. Risk calculation

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 270**

Which of the following incident response aspects allows Pete, the security technician, to identify who caused a Distributed Denial of Service (DDoS) attack?

- A. Network logs
- B. Live system image
- C. Record time offset
- D. Screenshots

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 271**

Which of the following security strategies allows a company to limit damage to internal systems and provides loss control?

- A. Restoration and recovery strategies
- B. Deterrent strategies
- C. Containment strategies
- D. Detection strategies

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 272**

Which of the following must Mike, a user, implement if he wants to send a secret message to Jane, a co-



worker, by embedding it within an image?

- A. Transport encryption
- B. Steganography
- C. Hashing
- D. Digital signature

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 273**

In order for Sara, a client, to logon to her desktop computer, she must provide her username, password, and a four digit PIN. Which of the following authentication methods is Sara using?

- A. Three factor
- B. Single factor
- C. Two factor
- D. Four factor

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 274**

Which of the following must Jane, a security administrator, implement to ensure all wired ports are authenticated before a user is allowed onto the network?

- A. Intrusion prevention system
- B. Web security gateway
- C. Network access control
- D. IP access control lists

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 275**

Mike, a server engineer, has received four new servers and must place them in a rack in the datacenter. Which of the following is considered best practice?

- A. All servers' air exhaust toward the cold aisle.
- B. All servers' air intake toward the cold aisle.
- C. Alternate servers' air intake toward the cold and hot aisle.
- D. Servers' air intake must be parallel to the cold/hot aisles.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 276**

Mike, a security analyst, has captured a packet with the following payload:

GET ../../../../system32/cmd.exe

Which of the following is this an example of?

- A. SQL injection
- B. Directory traversal
- C. XML injection
- D. Buffer overflow

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 277**

Sara, the security administrator, needs to open ports on the firewall to allow for secure data transfer. Which of the following TCP ports would allow for secure transfer of files by default?

- A. 21
- B. 22
- C. 23
- D. 25

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 278**

Which of the following technologies would allow for a secure tunneled connection from one site to another? (Select TWO).

- A. SFTP
- B. IPSec
- C. SSH
- D. HTTPS
- E. ICMP

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 279**

Which of the following sets numerous flag fields in a TCP packet?

- A. XMAS
- B. DNS poisoning
- C. SYN flood
- D. ARP poisoning

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 280**

Which of the following devices is MOST commonly used to create a VLAN?

- A. Hub
- B. Router
- C. Firewall
- D. Switch

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 281**

Which of the following network design elements provides for a one-to-one relationship between an internal network address and an external network address?

- A. NAT
- B. NAC
- C. VLAN
- D. PAT

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 282**

Using proximity card readers instead of the traditional key punch doors would help to mitigate:

- A. impersonation.
- B. tailgating.
- C. dumpster diving.

D. shoulder surfing.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 283**

In planning for a firewall implementation, Pete, a security administrator, needs a tool to help him understand what traffic patterns are normal on his network. Which of the following tools would help Pete determine traffic patterns?

- A. Syslog
- B. Protocol analyzer
- C. Proxy server
- D. Firewall

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 284**

Jane, a security administrator, has asked her technicians to determine if a certificate is valid. Which of the following should be checked to determine whether or not a certificate has been invalidated?

- A. CA
- B. CRL
- C. PKI
- D. CRC

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 285**

TKIP uses which of the following encryption ciphers?

- A. RC5
- B. AES
- C. RC4
- D. 3DES

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 286**

The process of exchanging public keys is BEST explained as which cryptography concept?

- A. Symmetric encryption
- B. Asymmetric encryption
- C. Key escrow
- D. Transport encryption

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 287**

Which of the following network segments would be BEST suited for installing a honeypot?

- A. Management network
- B. Internal network
- C. External network
- D. DMZ network

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 288**

Jane, a security architect, has noticed significant performance loss with the increase in user-base of her PKI infrastructure. Which of the following could she deploy in order to increase response times?

- A. Smart card
- B. CAC
- C. HSM
- D. VPN

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 289**

Jane, an administrator, needs to transfer DNS zone files from outside of the corporate network. Which of the following protocols must be used?

- A. TCP
- B. ICMP
- C. UDP
- D. IP

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 290**

Common access cards use which of the following authentication models?

- A. PKI
- B. XTACACS
- C. RADIUS
- D. TACACS

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 291**

Which of the following does a second authentication requirement mitigate when accessing privileged areas of a website, such as password changes or user profile changes?

- A. Cross-site scripting
- B. Cookie stealing
- C. Packet sniffing
- D. Transitive access

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 292**

Which of the following should Sara, a security technician, educate users about when accessing the company wireless network?

- A. IV attacks
- B. Vishing
- C. Rogue access points
- D. Hoaxes

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 293**

Pete, a security technician, has implemented data loss prevention on a company laptop. Which of the following does this protect against?

- A. Connecting the company laptop to external data networks
- B. Use of USB drives for legitimate operational purposes
- C. Use of unencrypted USB drives for gray box testing
- D. Removal of company information without authorization

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 294**

Sara, an IT security technician, needs to be able to identify who is in possession of a stolen laptop. Which of the following BEST addresses her need?

- A. Remote sanitization
- B. Remote wipe
- C. GPS tracking
- D. Traceroute

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 295**

Which of the following will allow Sara, an IT security technician, to effectively identify a zero-day attack on her systems?

- A. Anti-malware
- B. Antivirus signatures
- C. Host software baseline
- D. Virtualization

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 296**

Mike, an IT security technician, needs to recommend an authentication mechanism which has a high probability of correctly identifying a user. Which of the following BEST meets this need?

- A. Separation of duties
- B. Biometrics
- C. Passwords
- D. Access control list

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 297**

Jane receives a spreadsheet via email and double clicks the attachment executing another program inside the spreadsheet. Which of the following types of malware was executed?

- A. Spyware
- B. Rootkit
- C. Trojan
- D. Botnet

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 298**

Which of the following ports does DNS operate on, by default?

- A. 23
- B. 53
- C. 137
- D. 443

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 299**

Which of the following is a secure alternate to Telnet?

- A. TFTP
- B. HTTPS
- C. SSH
- D. SCP

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 300**

Temporary employees are not allowed to work overtime. The information security department must implement



a control to enforce this measure. Which of the following measures would BEST enforce this policy?

- A. Separation of duties
- B. Personal identification card
- C. Single sign-on
- D. Time of day restrictions

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 301**

Sara from IT Governance wants to provide a mathematical probability of an earthquake using facts and figures. Which of the following concepts would achieve this?

- A. Qualitative Analysis
- B. Impact Analysis
- C. Quantitative Analysis
- D. SLE divided by the ARO

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 302**

A buffer overflow can result in which of the following attack types?

- A. DNS poisoning
- B. Zero-day
- C. Privilege escalation
- D. ARP poisoning

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 303**

Which of the following is an authentication service that uses UDP as a transport medium?

- A. TACACS+
- B. LDAP
- C. Kerberos
- D. RADIUS

**Correct Answer:** D

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 304**

Which of the following is true concerning WEP security?

- A. WEP keys are transmitted in plain text.
- B. The WEP key initialization process is flawed.
- C. The pre-shared WEP keys can be cracked with rainbow tables.
- D. WEP uses the weak RC4 cipher.

**Correct Answer: B**

**Section: (none)**

**Explanation****Explanation/Reference:****QUESTION 305**

Matt, a security administrator, wants to secure VoIP traffic on the internal network from eavesdropping. Which of the following would MOST likely be used?

- A. SSL
- B. SSH
- C. QoS
- D. IPSec

**Correct Answer: D**

**Section: (none)**

**Explanation****Explanation/Reference:****QUESTION 306**

Pete works for a subsidiary company that processes secure transactions for the parent company. Which of the following can be employed to ensure the parent company has access to the subsidiary's encrypted data in an emergency?

- A. Trust model
- B. Public key infrastructure
- C. Symmetrical key encryption
- D. Key escrow

**Correct Answer: D**

**Section: (none)**

**Explanation****Explanation/Reference:****QUESTION 307**

Which of the following can be used on a smartphone to BEST protect against sensitive data loss if the device is stolen? (Select TWO).

- A. Tethering
- B. Screen lock PIN
- C. Remote wipe
- D. Email password
- E. GPS tracking
- F. Device encryption

**Correct Answer:** CF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 308**

Which of the following social engineering attacks is meant for a high-ranking corporate employee?

- A. Pharming
- B. Whaling
- C. Hoax
- D. Vishing

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 309**

Which of the following is an advantage of using group policy to redirect users' local folders to networked drives in regards to data loss prevention?

- A. Sensitive data is not stored on a local computer.
- B. Users can track their data for unauthorized revisions.
- C. Incremental back-ups are stored locally for easy access.
- D. The users are more aware of where their data is stored.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 310**

In the case of laptop theft, which of the following is the BEST action to take to prevent data theft?

- A. Use a third-party hard drive encryption product.
- B. Install the operating system on a non-default partition letter.
- C. Set a BIOS password that must be entered upon system boot.
- D. Enforce a strict complex operating system password.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 311**

Pete, a security administrator, has implemented a policy to prevent data loss. Which of the following is the BEST method of enforcement?

- A. Internet networks can be accessed via personally-owned computers.
- B. Data can only be stored on local workstations.
- C. Wi-Fi networks should use WEP encryption by default.
- D. Only USB devices supporting encryption are to be used.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 312**

Sara, a security administrator, needs to implement the equivalent of a DMZ at the datacenter entrance. Which of the following must she implement?

- A. Video surveillance
- B. Mantrap
- C. Access list
- D. Alarm

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 313**

Jane, a security analyst, is reviewing logs from hosts across the Internet which her company uses to gather data on new malware. Which of the following is being implemented by Jane's company?

- A. Vulnerability scanner
- B. Honeynet
- C. Protocol analyzer
- D. Port scanner

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 314**

Sara, a senior programmer for an application at a software development company, has also assumed an auditing role within the same company. She will be assessing the security of the application. Which of the following will she be performing?

- A. Blue box testing
- B. Gray box testing
- C. Black box testing
- D. White box testing

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 315**

Which of the following procedures would be used to mitigate the risk of an internal developer embedding malicious code into a production system?

- A. Audit management
- B. Mobile device management
- C. Incident management
- D. Change management

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 316**

Mike, a security analyst, is looking to reduce the number of phishing emails received by employees. Which of the following solutions helps prevent this from occurring?

- A. HIDS
- B. NIDS
- C. Antivirus
- D. Spam filter

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 317**

Which of the following BEST describes a directory traversal attack?

- A. A malicious user can insert a known pattern of symbols in a URL to access a file in another section of the directory.
- B. A malicious user can change permissions or lock out user access from a webroot directory or subdirectories.

- C. A malicious user can delete a file or directory in the webroot directory or subdirectories.
- D. A malicious user can redirect a user to another website across the Internet.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 318**

In her morning review of new vendor patches, Jane has identified an exploit that is marked as critical. Which of the following is the BEST course of action?

- A. Jane should wait seven days before testing the patch to ensure that the vendor does not issue an updated version, which would require reapplying the patch.
- B. Jane should download the patch and install it to her workstation to test whether it will be able to be applied to all workstations in the environment.
- C. Jane should alert the risk management department to document the patch and add it to the next monthly patch deployment cycle.
- D. Jane should download the patch to the test network, apply it to affected systems, and evaluate the results on the test systems.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 319**

Matt, a security administrator, has noticed that the website and external systems have been subject to many attack attempts. To verify integrity of the website and critical files, Matt should:

- A. require all visitors to the public web home page to create a username and password to view the pages in the website.
- B. configure the web application firewall to send a reset packet to the incoming IP from where an attack or scan signature has been detected.
- C. create file hashes for website and critical system files, and compare the current file hashes to the baseline at regular time intervals.
- D. reboot the web server and database server nightly after the backup has been completed.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 320**

Jane, a security technician, needs to open ports on a firewall to allow for domain name resolution. Which of the following ports should Jane open? (Select TWO).

- A. TCP 21
- B. TCP 23
- C. TCP 53

- D. UDP 23
- E. UDP 53

**Correct Answer:** CE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 321**

Pete, a security administrator, is working with Jane, a network administrator, to securely design a network at a new location. The new location will have three departments which should be isolated from each other to maintain confidentiality. Which of the following design elements should Pete implement to meet this goal?

- A. VLANs
- B. Port security
- C. VPNs
- D. Flood guards

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 322**

Sara, a security administrator, is configuring a new firewall. She has entered statements into the firewall configuration as follows:

Allow all Web traffic  
Deny all Telnet traffic  
Allow all SSH traffic

Mike, a user on the network, tries unsuccessfully to use RDP to connect to his work computer at home. Which of the following principles BEST explains why Mike's attempt to connect is not successful?

- A. Explicit deny
- B. Loop protection
- C. Implicit deny
- D. Implicit permit

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 323**

Jane, a security administrator, notices that a program has crashed. Which of the following logs should Jane check?

- A. Access log
- B. Firewall log

- C. Audit log
- D. Application log

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 324**

A process in which the functionality of an application is tested with some knowledge of the internal mechanisms of the application is known as:

- A. white hat testing.
- B. black box testing.
- C. black hat testing.
- D. gray box testing.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 325**

Which of the following passwords is the LEAST complex?

- A. MyTrain!45
- B. Mytr@in!!
- C. MyTr@in12
- D. MyTr@in#8

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 326**

Which of the following security benefits would be gained by disabling a terminated user account rather than deleting it?

- A. Retention of user keys
- B. Increased logging on access attempts
- C. Retention of user directories and files
- D. Access to quarantined files

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 327**

Which RAID level is LEAST suitable for disaster recovery plans?

- A. 0
- B. 1
- C. 5
- D. 6

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 328**

Which of the following security architecture elements also has sniffer functionality? (Select TWO).

- A. HSM
- B. IPS
- C. SSL accelerator
- D. WAP
- E. IDS

**Correct Answer:** BE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 329**

During an anonymous penetration test, Jane, a system administrator, was able to identify a shared print spool directory, and was able to download a document from the spool. Which statement BEST describes her privileges?

- A. All users have write access to the directory.
- B. Jane has read access to the file.
- C. All users have read access to the file.
- D. Jane has read access to the directory.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 330**

Sara, an IT security technician, is actively involved in identifying coding issues for her company. Which of the following is an application security technique that she can use to identify unknown weaknesses within the code?

- A. Vulnerability scanning

- B. Denial of service
- C. Fuzzing
- D. Port scanning

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 331**

Sara, an IT security technician, has identified security weaknesses within her company's code. Which of the following is a common security coding issue?

- A. Input validation
- B. Application fuzzing
- C. Black box testing
- D. Vulnerability scanning

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 332**

Which of the following is an application security coding problem?

- A. Error and exception handling
- B. Patch management
- C. Application hardening
- D. Application fuzzing

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 333**

Pete, an IT security technician, needs to establish host based security for company workstations. Which of the following will BEST meet this requirement?

- A. Implement IIS hardening by restricting service accounts.
- B. Implement database hardening by applying vendor guidelines.
- C. Implement perimeter firewall rules to restrict access.
- D. Implement OS hardening by applying GPOs.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 334**

Which of the following data security techniques will allow Matt, an IT security technician, to encrypt a system with speed as its primary consideration?

- A. Hard drive encryption
- B. Infrastructure as a service
- C. Software based encryption
- D. Data loss prevention

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 335**

Jane, an IT security technician, receives a call from the vulnerability assessment team informing her that port 1337 is open on a user's workstation. Which of the following BEST describes this type of malware?

- A. Logic bomb
- B. Spyware
- C. Backdoor
- D. Adware

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 336**

Which of the following is based on asymmetric keys?

- A. CRLs
- B. Recovery agent
- C. PKI
- D. Registration

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 337**

Which of the following is BEST described as a notification control, which is supported by other identification controls?

- A. Fencing

- B. Access list
- C. Guards
- D. Alarm

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 338**

Pete, an employee, needs a certificate to encrypt data. Which of the following would issue Pete a certificate?

- A. Certification authority
- B. Key escrow
- C. Certificate revocation list
- D. Registration authority

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 339**

Which of the following BEST describes the weakness in WEP encryption?

- A. The initialization vector of WEP uses a crack-able RC4 encryption algorithm. Once enough packets are captured an XOR operation can be performed and the asymmetric keys can be derived.
- B. The WEP key is stored in plain text and split in portions across 224 packets of random data. Once enough packets are sniffed the IV portion of the packets can be removed leaving the plain text key.
- C. The WEP key has a weak MD4 hashing algorithm used. A simple rainbow table can be used to generate key possibilities due to MD4 collisions.
- D. The WEP key is stored with a very small pool of random numbers to make the cipher text. As the random numbers are often reused it becomes easy to derive the remaining WEP key.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 340**

Which of the following is used to ensure message integrity during a TLS transmission?

- A. RIPEMD
- B. RSA
- C. AES
- D. HMAC

**Correct Answer:** D

**Section:** (none)

## **Explanation**

### **Explanation/Reference:**

#### **QUESTION 341**

Sara, the Chief Security Officer (CSO), has had four security breaches during the past two years. Each breach has cost the company \$3,000. A third party vendor has offered to repair the security hole in the system for \$25,000. The breached system is scheduled to be replaced in five years. Which of the following should Sara do to address the risk?

- A. Accept the risk saving \$10,000.
- B. Ignore the risk saving \$5,000.
- C. Mitigate the risk saving \$10,000.
- D. Transfer the risk saving \$5,000.

**Correct Answer: D**

**Section: (none)**

## **Explanation**

### **Explanation/Reference:**

#### **QUESTION 342**

A company has asked Pete, a penetration tester, to test their corporate network. Pete was provided with all of the server names, configurations, and corporate IP addresses. Pete was then instructed to stay off of the Accounting subnet as well as the company web server in the DMZ. Pete was told that social engineering was not in the test scope as well. Which of the following BEST describes this penetration test?

- A. Gray box
- B. Black box
- C. White box
- D. Blue box

**Correct Answer: C**

**Section: (none)**

## **Explanation**

### **Explanation/Reference:**

#### **QUESTION 343**

Matt, an administrator, notices a flood fragmented packet and retransmits from an email server. After disabling the TCP offload setting on the NIC, Matt sees normal traffic with packets flowing in sequence again. Which of the following utilities was the MOST likely using to view this issue?

- A. Spam filter
- B. Protocol analyzer
- C. Web application firewall
- D. Load balancer

**Correct Answer: B**

**Section: (none)**

## **Explanation**

### **Explanation/Reference:**

**QUESTION 344**

Which of the following devices can be used to terminate remote user's established SSL or IPSec tunnels? (Select TWO).

- A. NIDS
- B. HIPS
- C. VPN concentrator
- D. Hub
- E. Firewall

**Correct Answer:** CE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 345**

Jane, a user, brings in a laptop from home and gets certificate warnings when connecting to corporate intranet sites. These warnings do not occur when using any of the companies' workstations. Which of the following is MOST likely the issue?

- A. The laptop needs to VPN to bypass the NAC.
- B. The corporate intranet servers do not trust the laptop.
- C. The laptop's CRL enrollment has expired.
- D. The user's certificate store does not trust the CA.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 346**

Which of the following mitigates the loss of a private key in PKI? (Select TWO).

- A. Certificate reissue
- B. Key rotation
- C. Key escrow
- D. Auto enrollment
- E. Recovery agent

**Correct Answer:** CE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 347**

Which of the following specifications would Sara, an administrator, implement as a network access control?

- A. 802.1q
- B. 802.3
- C. 802.11n
- D. 802.1x

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 348**

Which of the following malware types propagates automatically, does not typically hide, requires user interaction, and displays marketing ads?

- A. Logic bombs
- B. Rootkits
- C. Spyware
- D. Worms

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 349**

Which of the following malware types typically disguises itself within another piece of software, requires user interaction, and does not execute on a specific date?

- A. Logic Bomb
- B. Trojan
- C. Worm
- D. Botnet

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 350**

Which of the following is MOST commonly identified as an ARP spoofing attack where no email is sent, and flags within the TCP packet are irrelevant?

- A. Xmas attack
- B. Spam attack
- C. Man-in-the-middle attack
- D. DDoS attack

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 351**

Which of the following is characterized by an attacker attempting to map out an organization's staff hierarchy in order to send targeted emails?

- A. Whaling
- B. Impersonation
- C. Privilege escalation
- D. Spear phishing

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 352**

Which of the following is an attack where Pete spreads USB thumb drives throughout a bank's parking lot in order to have malware installed on the banking systems?

- A. Tailgating
- B. Replay attack
- C. Virus
- D. Social engineering

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 353**

Which of the following attacks significantly relies on staff members wanting to be helpful and supportive of each other?

- A. Spoofing
- B. Tailgating
- C. Dumpster diving
- D. Xmas attack

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 354**

Which of the following is an attacker attempting to discover open wireless access points?



- A. War driving
- B. Packet sniffing
- C. War chalking
- D. Initialization vector

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 355**

Which of the following protocols provides Pete, an administrator, with the HIGHEST level of security for device traps?

- A. ICMP
- B. SNMPv3
- C. SSH
- D. IPSec

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 356**

Which of the following is designed to serve as a risk mitigation strategy?

- A. Personally owned devices
- B. Disaster recovery plan
- C. Calculate proper ROI
- D. Zero day exploits

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 357**

Who should be contacted FIRST in the event of a security breach?

- A. Forensics analysis team
- B. Internal auditors
- C. Incident response team
- D. Software vendors

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 358**

Which process will determine maximum tolerable downtime?

- A. Business Continuity Planning
- B. Contingency Planning
- C. Business Impact Analysis
- D. Disaster Recovery Plan

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 359**

Which of the following provides the MOST protection against zero day attacks via email attachments?

- A. Anti-spam
- B. Anti-virus
- C. Host-based firewalls
- D. Patch management

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 360**

Which of the following access controls enforces permissions based on data labeling at specific levels?

- A. Mandatory access control
- B. Separation of duties access control
- C. Discretionary access control
- D. Role based access control

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 361**

A username provides which of the following?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 362**

Use of group accounts should be minimized to ensure which of the following?

- A. Password security
- B. Regular auditing
- C. Baseline management
- D. Individual accountability

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 363**

Privilege creep among long-term employees can be mitigated by which of the following procedures?

- A. User permission reviews
- B. Mandatory vacations
- C. Separation of duties
- D. Job function rotation

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 364**

In which of the following scenarios is PKI LEAST hardened?

- A. The CRL is posted to a publicly accessible location.
- B. The recorded time offsets are developed with symmetric keys.
- C. A malicious CA certificate is loaded on all the clients.
- D. All public keys are accessed by an unauthorized user.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 365**

A database server has been compromised via an unpatched vulnerability. An investigation reveals that an application crashed at the time of the compromise. Unauthorized code appeared to be running, although there

were no traces of the code found on the file system. Which of the following attack types has MOST likely occurred?

- A. Zero day exploit
- B. SQL injection
- C. LDAP injection
- D. Buffer overflow

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 366**

Which of the following would Sara, a security administrator, utilize to actively test security controls within an organization?

- A. Penetration test
- B. Baselining
- C. Code review
- D. Vulnerability scan

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 367**

Which of the following assessments would Pete, the security administrator, use to actively test that an application's security controls are in place?

- A. Code review
- B. Penetration test
- C. Protocol analyzer
- D. Vulnerability scan

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 368**

Which of the following would Jane, a security administrator, take advantage of to bypass security controls and gain unauthorized remote access into an organization?

- A. Vulnerability scan
- B. Dumpster diving
- C. Virtualization
- D. Penetration test

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 369**

Which of the following would be used to identify the security posture of a network without actually exploiting any weaknesses?

- A. Penetration test
- B. Code review
- C. Vulnerability scan
- D. Brute Force scan

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 370**

The finance department is growing and needs additional computers to support growth. The department also needs to ensure that their traffic is separated from the rest of the network. Matt, the security administrator, needs to add a new switch to accommodate this growth. Which of the following **MUST** Matt configure on the switch to ensure proper network separation?

- A. Implicit deny
- B. VLAN management
- C. Access control lists
- D. Flood guards

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 371**

Pete, the security administrator, wants to ensure that only secure protocols are being used to transfer and copy files. Which of the following protocols should he implement?

- A. SMTP
- B. SCP



<http://www.gratisexam.com/>

- C. FTP
- D. HTTPS

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 372**

Sara, a security administrator, has recently implemented a policy to ban certain attachments from being sent through the corporate email server. This is an example of trying to mitigate which of the following?

- A. SQL injection
- B. LDAP injection
- C. Cross-site scripting
- D. Malicious add-ons

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 373**

Jane, the security administrator, sets up a new AP but realizes too many outsiders are able to connect to that AP and gain unauthorized access. Which of the following would be the BEST way to mitigate this issue and still provide coverage where needed? (Select TWO).

- A. Disable the wired ports
- B. Use channels 1, 4 and 7 only
- C. Enable MAC filtering
- D. Disable SSID broadcast
- E. Switch from 802.11a to 802.11b

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 374**

In the initial stages of an incident response, Matt, the security administrator, was provided the hard drives in question from the incident manager. Which of the following incident response procedures would he need to perform in order to begin the analysis? (Select TWO).

- A. Take hashes
- B. Begin the chain of custody paperwork
- C. Take screen shots
- D. Capture the system image
- E. Decompile suspicious files

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 375**

Which of the following is used to certify intermediate authorities in a large PKI deployment?

- A. Root CA
- B. Recovery agent
- C. Root user
- D. Key escrow

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 376**

Which of the following components **MUST** be trusted by all parties in PKI?

- A. Key escrow
- B. CA
- C. Private key
- D. Recovery key

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 377**

Remote employees login to the network using a device displaying a digital number which changes every five minutes. This is an example of which of the following?

- A. Block cipher
- B. One-time pad
- C. Stream cipher
- D. Digital signature

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 378**

When checking his webmail, Matt, a user, changes the URL's string of characters and is able to get into another user's inbox. This is an example of which of the following?

- A. Header manipulation
- B. SQL injection
- C. XML injection
- D. Session hijacking

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 379**

Sara, an employee, unintentionally downloads malware that exploits a known vulnerability. Which of the following needs to be enforced to keep this incident from recurring in the future?

- A. Input validation
- B. Active pop-up blocker
- C. Application hardening and error validation
- D. Patch management

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 380**

Which of the following is being used when a message is buried within the pixels of an image?

- A. Steganography
- B. Block cipher
- C. Encryption
- D. Hashing

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 381**

Elliptic curve cryptography: (Select TWO)

- A. is used in both symmetric and asymmetric encryption.
- B. is used mostly in symmetric encryption.
- C. is mostly used in embedded devices.
- D. produces higher strength encryption with shorter keys.
- E. is mostly used in hashing algorithms.

**Correct Answer:** CD

**Section:** (none)



### **Explanation**

### **Explanation/Reference:**

#### **QUESTION 382**

Which of the following would an antivirus company use to efficiently capture and analyze new and unknown malicious attacks?

- A. Fuzzer
- B. IDS
- C. Proxy
- D. Honeynet

**Correct Answer: D**

**Section: (none)**

### **Explanation**

### **Explanation/Reference:**

#### **QUESTION 383**

Which of the following is used to translate a public IP to a private IP?

- A. NAT
- B. CCMP
- C. NAC
- D. VLAN

**Correct Answer: A**

**Section: (none)**

### **Explanation**

### **Explanation/Reference:**

#### **QUESTION 384**

Why is it important for a penetration tester to have established an agreement with management as to which systems and processes are allowed to be tested?

- A. Penetration test results are posted publicly, and some systems tested may contain corporate secrets.
- B. Penetration testers always need to have a comprehensive list of servers, operating systems, IP subnets, and department personnel prior to ensure a complete test.
- C. Having an agreement allows the penetration tester to look for other systems out of scope and test them for threats against the in-scope systems.
- D. Some exploits when tested can crash or corrupt a system causing downtime or data loss.

**Correct Answer: D**

**Section: (none)**

### **Explanation**

### **Explanation/Reference:**

#### **QUESTION 385**

An administrator wants to minimize the amount of time needed to perform backups during the week. It is also

acceptable to the administrator for restoration to take an extended time frame. Which of the following strategies would the administrator MOST likely implement?

- A. Full backups on the weekend and incremental during the week
- B. Full backups on the weekend and full backups every day
- C. Incremental backups on the weekend and differential backups every day
- D. Differential backups on the weekend and full backups every day

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 386**

Which of the following can be used in code signing?

- A. AES
- B. RC4
- C. GPG
- D. CHAP

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 387**

Sara, an administrator, disables the beacon function of an access point. Which of the following is accomplished by this?

- A. The AP stops broadcasting radio frequencies.
- B. The SSID is not broadcasted by the AP.
- C. The AP presence is undetectable by wireless sniffers.
- D. Wireless clients are now required to use 2.4 GHz.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 388**

Which of the following can use RC4 for encryption? (Select TWO).

- A. CHAP
- B. SSL
- C. WEP
- D. AES
- E. 3DES

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 389**

Which of the following defines a business goal for system restoration and acceptable data loss?

- A. MTTR
- B. MTBF
- C. RPO
- D. Warm site

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 390**

Which of the following defines an organization goal for acceptable downtime during a disaster or other contingency?

- A. MTBF
- B. MTTR
- C. RTO
- D. RPO

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 391**

Which of the following is an attack vector that can cause extensive physical damage to a datacenter without physical access?

- A. CCTV system access
- B. Dial-up access
- C. Changing environmental controls
- D. Ping of death

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 392**

An ACL placed on which of the following ports would block IMAP traffic?

- A. 110
- B. 143
- C. 389
- D. 465

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 393**

Which of the following provides the HIGHEST level of confidentiality on a wireless network?

- A. Disabling SSID broadcast
- B. MAC filtering
- C. WPA2
- D. Packet switching

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 394**

A new AP has been installed and there are problems with packets being dropped. Which of the following BEST explains the packet loss?

- A. EMI
- B. XML injection
- C. DDoS
- D. Botnet

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 395**

Which of the following intrusion detection methods may generate an alert when Matt, an employee, accesses a server during non-business hours?

- A. Signature
- B. Time of Day restrictions
- C. Heuristic
- D. Behavioral

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 396**

Which of the following controls should be used to verify a person in charge of payment processing is not colluding with anyone to pay fraudulent invoices?

- A. Least privilege
- B. Security policy
- C. Mandatory vacations
- D. Separation of duties

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 397**

Which of the following techniques describes the use of application isolation during execution to prevent system compromise if the application is compromised?

- A. Least privilege
- B. Sandboxing
- C. Black box
- D. Application hardening

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 398**

Which of the following allows a company to maintain access to encrypted resources when employee turnover is high?

- A. Recovery agent
- B. Certificate authority
- C. Trust model
- D. Key escrow

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 399**

Which of the following security methods should be used to ensure mobile devices are not removed by unauthorized users when the owner is away from their desk?

- A. Screen lock
- B. Biometrics
- C. Strong passwords
- D. Cable lock

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 400**

Which of the following should be implemented to stop an attacker from mapping out addresses and/or devices on a network?

- A. Single sign on
- B. IPv6
- C. Secure zone transfers
- D. VoIP

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 401**

Jane, a network technician, notices that users' Internet homepages have been changed to sites that include malware. Which of the following will change the default homepage for the Internet browser to be the same for all users?

- A. Flush the DNS cache
- B. Remove workstations from the domain
- C. Upgrade the Internet browser
- D. Implement group policies

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 402**

A security administrator wants to scan an infected workstation to understand how the infection occurred. Which of the following should the security administrator do FIRST before scanning the workstation?

- A. Make a complete hard drive image
- B. Remove the memory
- C. Defragment the hard drive
- D. Delete all temporary Internet files

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 403**

Matt, an IT administrator, wants to protect a newly built server from zero day attacks. Which of the following would provide the BEST level of protection?

- A. HIPS
- B. Antivirus
- C. NIDS
- D. ACL

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 404**

The lead security engineer has been brought in on a new software development project. The software development team will be deploying a base software version and will make multiple software revisions during the project life cycle. The security engineer on the project is concerned with the ability to roll back software changes that cause bugs and/or security concerns. Which of the following should the security engineer suggest to BEST address this issue?

- A. Develop a change management policy incorporating network change control.
- B. Develop a change management policy incorporating hardware change control.
- C. Develop a change management policy incorporating software change control.
- D. Develop a change management policy incorporating oversight of the project lifecycle.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 405**

A new wireless network was installed in an office building where there are other wireless networks. Which of the following can the administrator disable to help limit the discovery of the new network?

- A. DHCP
- B. Default user account
- C. MAC filtering
- D. SSID broadcast

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 406**

Which of the following anti-malware solutions can be implemented to mitigate the risk of phishing?

- A. Host based firewalls
- B. Anti-spyware
- C. Anti-spam
- D. Anti-virus

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 407**

Which of the following can be used to mitigate risk if a mobile device is lost?

- A. Cable lock
- B. Transport encryption
- C. Voice encryption
- D. Strong passwords

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 408**

Implementation of server clustering is an example of which of the following security concepts?

- A. Traceability
- B. Availability
- C. Integrity
- D. Confidentiality

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 409**

The annual loss expectancy can be calculated by:

- A. dividing the annualized rate of return by single loss expectancy.
- B. multiplying the annualized rate of return and the single loss expectancy.
- C. subtracting the single loss expectancy from the annualized rate of return.
- D. adding the single loss expectancy and the annualized rate of return.



**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 410**

Which of the following datacenter environmental controls must be properly configured to prevent equipment failure from water?

- A. Lighting
- B. Temperature
- C. Humidity
- D. Halon fire suppression

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 411**

Which of the following should the security administrator do when taking a forensic image of a hard drive?

- A. Image the original hard drive, hash the image, and analyze the original hard drive.
- B. Copy all the files from the original into a separate hard drive, and hash all the files.
- C. Hash the original hard drive, image the original hard drive, and hash the image.
- D. Image the original hard drive, hash the original hard drive, and analyze the hash.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 412**

In order to prevent and detect fraud, which of the following should be implemented?

- A. Job rotation
- B. Risk analysis
- C. Incident management
- D. Employee evaluations

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 413**

A vulnerability scan detects an unpatched application that does not exist on the server. Which of the following is the BEST explanation?

- A. File corruption
- B. False positive
- C. Wrong system was scanned
- D. Signature needs to be updated on the tool

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 414**

Mike, a network administrator, has been asked to passively monitor network traffic to the company's sales websites. Which of the following would be BEST suited for this task?

- A. HIDS
- B. Firewall
- C. NIPS
- D. Spam filter

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 415**

An administrator notices an unusual spike in network traffic from many sources. The administrator suspects that:

- A. it is being caused by the presence of a rogue access point.
- B. it is the beginning of a DDoS attack.
- C. the IDS has been compromised.
- D. the internal DNS tables have been poisoned.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 416**

Mike, a security professional, is tasked with actively verifying the strength of the security controls on a company's live modem pool. Which of the following activities is MOST appropriate?

- A. War dialing
- B. War chalking
- C. War driving
- D. Bluesnarfing

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 417**

Mike, a system administrator, anticipating corporate downsizing this coming November writes a malicious program to execute three weeks later if his account is removed. Which of the following attacks is this?

- A. Rootkit
- B. Virus
- C. Logic Bomb
- D. Worm

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 418**

The Compliance Department implements a policy stating the Security Analyst must only review security changes and the Security Administrator will implement the changes. This is example of which of the following?

- A. Job rotation
- B. Discretionary access control
- C. Trust models
- D. Separation of duties

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 419**

An encrypted message is sent using PKI from Sara, a client, to a customer. Sara claims she never sent the message. Which of the following aspects of PKI BEST ensures the identity of the sender?

- A. CRL
- B. Non-repudiation
- C. Trust models
- D. Recovery agents

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 420**

Which of the following protocols would be used to verify connectivity between two remote devices at the

LOWEST level of the OSI model?

- A. DNS
- B. SCP
- C. SSH
- D. ICMP

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 421**

Sara, a user, needs to copy a file from a Linux workstation to a Linux server using the MOST secure file transfer method available. Which of the following protocols would she use?

- A. SCP
- B. FTP
- C. SNMP
- D. TFTP

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 422**

Users require access to a certain server depending on their job function. Which of the following would be the MOST appropriate strategy for securing the server?

- A. Common access card
- B. Role based access control
- C. Discretionary access control
- D. Mandatory access control

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 423**

Jane, a security administrator, has observed repeated attempts to break into a server. Which of the following is designed to stop an intrusion on a specific server?

- A. HIPS
- B. NIDS
- C. HIDS
- D. NIPS

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 424**

Matt, the security administrator, notices a large number of alerts on the NIDS. Upon further inspection, it is determined that no attack has really taken place. This is an example of a:

- A. false negative.
- B. true negative.
- C. false positive.
- D. true positive.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 425**

Sara, a visitor, plugs her Ethernet cable into an open jack in a wall outlet and is unable to connect to the network. This is MOST likely an example of:

- A. port security.
- B. implicit deny.
- C. flood guards.
- D. loop protection.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 426**

Matt, the IT Manager, wants to create a new network available to virtual servers on the same hypervisor, and does not want this network to be routable to the firewall. How could this BEST be accomplished?

- A. Create a VLAN without a default gateway.
- B. Remove the network from the routing table.
- C. Create a virtual switch.
- D. Commission a stand-alone switch.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 427**

The security principle that is targeted when implementing ACLs is:

- A. integrity.
- B. availability.
- C. confidentiality.
- D. responsibility.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 428**

Which of the following is true about two security administrators who are using asymmetric encryption to send encrypted messages to each other?

- A. When one encrypts the message with the private key, the other can decrypt it with the private key.
- B. When one encrypts the message with the private key, the other can decrypt it with the public key.
- C. When one encrypts the message with the public key, the other can use either the public or the private to decrypt it.
- D. When one encrypts the message with the public key, the other can decrypt it with the public key.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 429**

A security administrator has configured FTP in passive mode. Which of the following ports should the security administrator allow on the firewall by default?

- A. 20
- B. 21
- C. 22
- D. 23

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 430**

Which of the following top to bottom sequential firewall rules will allow SSH communication?

- A. DENY ANY ANY  
PERMIT ANY ANY TCP 22  
PERMIT ANY ANY UDP 22
- B. PERMIT ANY ANY UDP 22  
PERMIT ANY ANY TCP 21  
DENY ANY ANY

- C. PERMIT ANY ANY TCP 23  
PERMIT ANY ANY TCP 22  
DENY ANY ANY
- D. PERMIT ANY ANY TCP 23  
DENY ANY ANY  
PERMIT ANY ANY TCP 22

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 431**

A company that purchased an HVAC system for the datacenter is MOST concerned with which of the following?

- A. Availability
- B. Integrity
- C. Confidentiality
- D. Fire suppression

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 432**

Which of the following Data Loss Prevention strategies is used to ensure that unauthorized users cannot access information stored in specified fields?

- A. Whole disk encryption
- B. Trust models
- C. Database encryption
- D. Individual file encryption

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 433**

Which of the following devices can Sara, an administrator, implement to detect and stop known attacks?

- A. Signature-based NIDS
- B. Anomaly-based NIDS
- C. Signature-based NIPS
- D. Anomaly-based NIPS

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 434**

Which of the following protocols would be implemented to secure file transfers using SSL?

- A. TFTP
- B. SCP
- C. SFTP
- D. FTPS

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 435**

Which of the following security concepts are used for data classification and labeling to protect data? (Select TWO).

- A. Need to know
- B. Role based access control
- C. Authentication
- D. Identification
- E. Authorization

**Correct Answer: AE**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 436**

Which of the following cryptography concepts describes securing a file during download?

- A. Trust model
- B. Non-repudiation
- C. Transport encryption
- D. Key escrow

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 437**

Which of the following secure file transfer methods uses port 22 by default?



- A. FTPS
- B. SFTP
- C. SSL
- D. S/MIME

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 438**

A drawback of utilizing unmonitored proximity badge readers is that they perform:

- A. authentication without authorization.
- B. authorization with authentication.
- C. authorization without authentication.
- D. authentication with authorization.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 439**

While setting up a secure wireless corporate network, which of the following should Pete, an administrator, avoid implementing?

- A. EAP-TLS
- B. PEAP
- C. WEP
- D. WPA

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 440**

Pete, a security administrator, instructs the networking team to push out security updates for a suite of programs on client workstations. This is an example of which of the following?

- A. Cross-site scripting prevention
- B. Application configuration baseline
- C. Application hardening
- D. Application patch management

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 441**

Which of the following are used to implement VPNs? (Select TWO).

- A. SFTP
- B. IPSec
- C. HTTPS
- D. SNMP
- E. SSL

**Correct Answer:** BE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 442**

A company is concerned about physical laptop theft. Which of the following is the LEAST expensive way to prevent this threat?

- A. Bollards
- B. Full disk encryption
- C. Cable locks
- D. Safes

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 443**

A security administrator wants to check user password complexity. Which of the following is the BEST tool to use?

- A. Password history
- B. Password logging
- C. Password cracker
- D. Password hashing

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 444**

A user in the company is in charge of various financial roles but needs to prepare for an upcoming audit. They use the same account to access each financial system. Which of the following security controls will MOST likely be implemented within the company?

- A. Account lockout policy
- B. Account password enforcement
- C. Password complexity enabled
- D. Separation of duties

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 445**

A CRL is comprised of:

- A. Malicious IP addresses.
- B. Trusted CA's.
- C. Untrusted private keys.
- D. Public keys.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 446**

Which of the following is BEST used as a secure replacement for TELNET?

- A. HTTPS
- B. HMAC
- C. GPG
- D. SSH

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 447**

An email client says a digital signature is invalid and the sender cannot be verified. The recipient is concerned with which of the following concepts?

- A. Integrity
- B. Availability
- C. Confidentiality
- D. Remediation

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 448**

Which of the following is an effective way to ensure the BEST temperature for all equipment within a datacenter?

- A. Fire suppression
- B. Raised floor implementation
- C. EMI shielding
- D. Hot or cool aisle containment

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 449**

Which of the following would a security administrator implement in order to discover comprehensive security threats on a network?

- A. Design reviews
- B. Baseline reporting
- C. Vulnerability scan
- D. Code review

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 450**

Which of the following is an example of a false positive?

- A. Anti-virus identifies a benign application as malware.
- B. A biometric iris scanner rejects an authorized user wearing a new contact lens.
- C. A user account is locked out after the user mistypes the password too many times.
- D. The IDS does not identify a buffer overflow.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 451**

Data execution prevention is a feature in most operating systems intended to protect against which type of attack?

- A. Cross-site scripting

- B. Buffer overflow
- C. Header manipulation
- D. SQL injection

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 452**

Please be aware that if you do not accept these terms you will not be allowed to take this CompTIA exam and you will forfeit the fee paid.

- A. RETURN TO EXAM
- B. EXIT EXAM

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 453**

Which of the following is the MOST secure protocol to transfer files?

- A. FTP
- B. FTPS
- C. SSH
- D. TELNET

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 454**

Suspicious traffic without a specific signature was detected. Under further investigation, it was determined that these were false indicators. Which of the following security devices needs to be configured to disable future false alarms?

- A. Signature based IPS
- B. Signature based IDS
- C. Application based IPS
- D. Anomaly based IDS

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 455**

A company storing data on a secure server wants to ensure it is legally able to dismiss and prosecute staff who intentionally access the server via Telnet and illegally tamper with customer data. Which of the following administrative controls should be implemented to BEST achieve this?

- A. Command shell restrictions
- B. Restricted interface
- C. Warning banners
- D. Session output pipe to /dev/null

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 456**

Which of the following protocols is used to authenticate the client and server's digital certificate?

- A. PEAP
- B. DNS
- C. TLS
- D. ICMP

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 457**

After Matt, a user, enters his username and password at the login screen of a web enabled portal, the following appears on his screen:

`Please only use letters and numbers on these fields'

Which of the following is this an example of?

- A. Proper error handling
- B. Proper input validation
- C. Improper input validation
- D. Improper error handling

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 458**

Which of the following should the security administrator implement to limit web traffic based on country of

origin? (Select THREE).

- A. Spam filter
- B. Load balancer
- C. Antivirus
- D. Proxies
- E. Firewall
- F. NIDS
- G. URL filtering

**Correct Answer:** DEG

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 459**

Several bins are located throughout a building for secure disposal of sensitive information. Which of the following does this prevent?

- A. Dumpster diving
- B. War driving
- C. Tailgating
- D. War chalking

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 460**

Sara, a company's security officer, often receives reports of unauthorized personnel having access codes to the cipher locks of secure areas in the building. Sara should immediately implement which of the following?

- A. Acceptable Use Policy
- B. Physical security controls
- C. Technical controls
- D. Security awareness training

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 461**

Users at a company report that a popular news website keeps taking them to a web page with derogatory content. This is an example of which of the following?

- A. Evil twin
- B. DNS poisoning

- C. Vishing
- D. Session hijacking

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 462**

A security administrator implements access controls based on the security classification of the data and need-to-know information. Which of the following BEST describes this level of access control?

- A. Implicit deny
- B. Role-based Access Control
- C. Mandatory Access Controls
- D. Least privilege

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 463**

Which of the following could cause a browser to display the message below?

"The security certificate presented by this website was issued for a different website's address."

- A. The website certificate was issued by a different CA than what the browser recognizes in its trusted CAs.
- B. The website is using a wildcard certificate issued for the company's domain.
- C. HTTPS://127.0.0.1 was used instead of HTTPS://localhost.
- D. The website is using an expired self signed certificate.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 464**

Which of the following pseudocodes can be used to handle program exceptions?

- A. If program detects another instance of itself, then kill program instance.
- B. If user enters invalid input, then restart program.
- C. If program module crashes, then restart program module.
- D. If user's input exceeds buffer length, then truncate the input.

**Correct Answer:** C

**Section:** (none)

**Explanation**



**Explanation/Reference:**

**QUESTION 465**

Which of the following technologies uses multiple devices to share work?

- A. Switching
- B. Load balancing
- C. RAID
- D. VPN concentrator

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 466**

Which of the following protocols uses an asymmetric key to open a session and then establishes a symmetric key for the remainder of the session?

- A. SFTP
- B. HTTPS
- C. TFTP
- D. TLS

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 467**

Which of the following mitigation strategies is established to reduce risk when performing updates to business critical systems?

- A. Incident management
- B. Server clustering
- C. Change management
- D. Forensic analysis

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 468**

Which of the following can Pete, a security administrator, use to distribute the processing effort when generating hashes for a password cracking program?

- A. RAID

- B. Clustering
- C. Redundancy
- D. Virtualization

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 469**

Which of the following should Jane, a security administrator, perform before a hard drive is analyzed with forensics tools?

- A. Identify user habits
- B. Disconnect system from network
- C. Capture system image
- D. Interview witnesses

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 470**

Jane, an administrator, needs to make sure the wireless network is not accessible from the parking area of their office. Which of the following would BEST help Jane when deploying a new access point?

- A. Placement of antenna
- B. Disabling the SSID
- C. Implementing WPA2
- D. Enabling the MAC filtering

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 471**

Which of the following allows Pete, a security technician, to provide the MOST secure wireless implementation?

- A. Implement WPA
- B. Disable SSID
- C. Adjust antenna placement
- D. Implement WEP

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 472**

Which of the following application attacks is used to gain access to SEH?

- A. Cookie stealing
- B. Buffer overflow
- C. Directory traversal
- D. XML injection

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 473**

Which of the following should Pete, a security manager, implement to reduce the risk of employees working in collusion to embezzle funds from their company?

- A. Privacy Policy
- B. Least Privilege
- C. Acceptable Use
- D. Mandatory Vacations

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 474**

Which of the following will allow Pete, a security analyst, to trigger a security alert because of a tracking cookie?

- A. Network based firewall
- B. Anti-spam software
- C. Host based firewall
- D. Anti-spyware software

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 475**

Which of the following protocols allows for secure transfer of files? (Select TWO).

- A. ICMP
- B. SNMP
- C. SFTP

- D. SCP
- E. TFTP

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 476**

During a penetration test from the Internet, Jane, the system administrator, was able to establish a connection to an internal router, but not successfully log in to it. Which ports and protocols are MOST likely to be open on the firewall? (Select FOUR).

- A. 21
- B. 22
- C. 23
- D. 69
- E. 3389
- F. SSH
- G. Terminal services
- H. Rlogin
- I. Rsync
- J. Telnet

**Correct Answer:** BCFJ

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 477**

An IT security technician needs to establish host based security for company workstations. Which of the following will BEST meet this requirement?

- A. Implement IIS hardening by restricting service accounts.
- B. Implement database hardening by applying vendor guidelines.
- C. Implement perimeter firewall rules to restrict access.
- D. Implement OS hardening by applying GPOs.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 478**

Which of the following is the MOST specific plan for various problems that can arise within a system?

- A. Business Continuity Plan
- B. Continuity of Operation Plan

- C. Disaster Recovery Plan
- D. IT Contingency Plan

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 479**

Pete, an IT Administrator, needs to secure his server room. Which of the following mitigation methods would provide the MOST physical protection?

- A. Sign in and sign out logs
- B. Mantrap
- C. Video surveillance
- D. HVAC

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 480**

Which of the following fire suppression systems is MOST likely used in a datacenter?

- A. FM-200
- B. Dry-pipe
- C. Wet-pipe
- D. Vacuum

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 481**

A security administrator has installed a new KDC for the corporate environment. Which of the following authentication protocols is the security administrator planning to implement across the organization?

- A. LDAP
- B. RADIUS
- C. Kerberos
- D. XTACACS

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 482**

While opening an email attachment, Pete, a customer, receives an error that the application has encountered an unexpected issue and must be shut down. This could be an example of which of the following attacks?

- A. Cross-site scripting
- B. Buffer overflow
- C. Header manipulation
- D. Directory traversal

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 483**

Jane has recently implemented a new network design at her organization and wishes to passively identify security issues with the new network. Which of the following should Jane perform?

- A. Vulnerability assessment
- B. Black box testing
- C. White box testing
- D. Penetration testing

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 484**

A security technician is working with the network firewall team to implement access controls at the company's demarc as part of the initiation of configuration management processes. One of the network technicians asks the security technician to explain the access control type found in a firewall. With which of the following should the security technician respond?

- A. Rule based access control
- B. Role based access control
- C. Discretionary access control
- D. Mandatory access control

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 485**

Jane, a security administrator, has been tasked with explaining authentication services to the company's management team. The company runs an active directory infrastructure. Which of the following solutions BEST relates to the host authentication protocol within the company's environment?

- A. Kerberos
- B. Least privilege
- C. TACACS+
- D. LDAP

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 486**

Pete, the compliance manager, wants to meet regulations. Pete would like certain ports blocked only on all computers that do credit card transactions. Which of the following should Pete implement to BEST achieve this goal?

- A. A host-based intrusion prevention system
- B. A host-based firewall
- C. Antivirus update system
- D. A network-based intrusion detection system

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 487**

Pete, the system administrator, wants to restrict access to advertisements, games, and gambling web sites. Which of the following devices would BEST achieve this goal?

- A. Firewall
- B. Switch
- C. URL content filter
- D. Spam filter

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 488**

Matt, a security analyst, needs to select an asymmetric encryption method that allows for the same level of encryption strength with a lower key length than is typically necessary. Which of the following encryption methods offers this capability?

- A. Twofish
- B. Diffie-Hellman
- C. ECC
- D. RSA

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 489**

Sara, a security analyst, is trying to prove to management what costs they could incur if their customer database was breached. This database contains 250 records with PII. Studies show that the cost per record for a breach is \$300. The likelihood that their database would be breached in the next year is only 5%. Which of the following is the ALE that Sara should report to management for a security breach?

- A. \$1,500
- B. \$3,750
- C. \$15,000
- D. \$75,000

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 490**

Methods to test the responses of software and web applications to unusual or unexpected inputs is known as:

- A. Brute force.
- B. HTML encoding.
- C. Web crawling.
- D. Fuzzing.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 491**

Sara, a security architect, has developed a framework in which several authentication servers work together to increase processing power for an application. Which of the following does this represent?

- A. Warm site
- B. Load balancing
- C. Clustering
- D. RAID

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 492**

Which statement is TRUE about the operation of a packet sniffer?

- A. It can only have one interface on a management network.
- B. They are required for firewall operation and stateful inspection.
- C. The Ethernet card must be placed in promiscuous mode.
- D. It must be placed on a single virtual LAN interface.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 493**

Which of the following firewall rules only denies DNS zone transfers?

- A. deny udp any any port 53
- B. deny ip any any
- C. deny tcp any any port 53
- D. deny all dns packets

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 494**

Which of the following does full disk encryption prevent?

- A. Client side attacks
- B. Clear text access
- C. Database theft
- D. Network-based attacks

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 495**

Pete, a developer, writes an application. Jane, the security analyst, knows some things about the overall application but does not have all the details. Jane needs to review the software before it is released to production. Which of the following reviews should Jane conduct?

- A. Gray Box Testing
- B. Black Box Testing
- C. Business Impact Analysis
- D. White Box Testing

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 496**

Which of the following can be implemented with multiple bit strength?

- A. AES
- B. DES
- C. SHA-1
- D. MD5
- E. MD4

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 497**

Pete, the system administrator, is reviewing his disaster recovery plans. He wishes to limit the downtime in the event of a disaster, but does not have the budget approval to implement or maintain an offsite location that ensures 99.99% availability. Which of the following would be Pete's BEST option?

- A. Use hardware already at an offsite location and configure it to be quickly utilized.
- B. Move the servers and data to another part of the company's main campus from the server room.
- C. Retain data back-ups on the main campus and establish redundant servers in a virtual environment.
- D. Move the data back-ups to the offsite location, but retain the hardware on the main campus for redundancy.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 498**

Which of the following is an advantage of implementing individual file encryption on a hard drive which already deploys full disk encryption?

- A. Reduces processing overhead required to access the encrypted files
- B. Double encryption causes the individually encrypted files to partially lose their properties
- C. Individually encrypted files will remain encrypted when copied to external media
- D. File level access control only apply to individually encrypted files in a fully encrypted drive

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 499**

An IT director is looking to reduce the footprint of their company's server environment. They have decided to move several internally developed software applications to an alternate environment, supported by an external company. Which of the following BEST describes this arrangement?

- A. Infrastructure as a Service
- B. Storage as a Service
- C. Platform as a Service
- D. Software as a Service

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 500**

A forensic analyst is reviewing electronic evidence after a robbery. Security cameras installed at the site were facing the wrong direction to capture the incident. The analyst ensures the cameras are turned to face the proper direction. Which of the following types of controls is being used?

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 501**

A security administrator wishes to change their wireless network so that IPSec is built into the protocol and NAT is no longer required for address range extension. Which of the following protocols should be used in this scenario?

- A. WPA2
- B. WPA
- C. IPv6
- D. IPv4

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 502**

The network administrator is responsible for promoting code to applications on a DMZ web server. Which of the following processes is being followed to ensure application integrity?

- A. Application hardening
- B. Application firewall review
- C. Application change management
- D. Application patch management

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 503**

An IT auditor tests an application as an authenticated user. This is an example of which of the following types of testing?

- A. Penetration
- B. White box
- C. Black box
- D. Gray box

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 504**

The manager has a need to secure physical documents every night, since the company began enforcing the clean desk policy. The BEST solution would include: (Select TWO).

- A. Fire- or water-proof safe.
- B. Department door locks.
- C. Proximity card.
- D. 24-hour security guard.
- E. Locking cabinets and drawers.

**Correct Answer:** AE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 505**

Which of the following is an important implementation consideration when deploying a wireless network that uses a shared password?

- A. Authentication server
- B. Server certificate
- C. Key length
- D. EAP method

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 506**

Which of the following would satisfy wireless network implementation requirements to use mutual authentication and usernames and passwords?

- A. EAP-MD5
- B. WEP
- C. PEAP-MSCHAPv2
- D. EAP-TLS

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 507**

Some customers have reported receiving an untrusted certificate warning when visiting the company's website. The administrator ensures that the certificate is not expired and that customers have trusted the original issuer of the certificate. Which of the following could be causing the problem?

- A. The intermediate CA certificates were not installed on the server.
- B. The certificate is not the correct type for a virtual server.
- C. The encryption key used in the certificate is too short.
- D. The client's browser is trying to negotiate SSL instead of TLS.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 508**

A security analyst needs to ensure all external traffic is able to access the company's front-end servers but protect all access to internal resources. Which of the following network design elements would MOST likely be recommended?

- A. DMZ
- B. Cloud computing
- C. VLAN
- D. Virtualization

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 509**

A company's business model was changed to provide more web presence and now its ERM software is no longer able to support the security needs of the company. The current data center will continue to provide network and security services. Which of the following network elements would be used to support the new business model?

- A. Software as a Service
- B. DMZ
- C. Remote access support
- D. Infrastructure as a Service

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 510**

Which of the following network devices is used to analyze traffic between various network interfaces?

- A. Proxies
- B. Firewalls
- C. Content inspection
- D. Sniffers

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 511**

Layer 7 devices used to prevent specific types of html tags are called:

- A. Firewalls.
- B. Content filters.
- C. Routers.
- D. NIDS.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 512**

A network administrator needs to provide daily network usage reports on all layer 3 devices without compromising any data while gathering the information. Which of the following would be configured to provide these reports?

- A. SNMP
- B. SNMPv3

- C. ICMP
- D. SSH

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 513**

A security administrator has been tasked to ensure access to all network equipment is controlled by a central server such as TACACS+. This type of implementation supports which of the following risk mitigation strategies?

- A. User rights and permissions review
- B. Change management
- C. Data loss prevention
- D. Implement procedures to prevent data theft

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 514**

Company A sends a PGP encrypted file to company B. If company A used company B's public key to encrypt the file, which of the following should be used to decrypt data at company B?

- A. Registration
- B. Public key
- C. CRLs
- D. Private key

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 515**

Which of the following types of authentication solutions use tickets to provide access to various resources from a central location?

- A. Biometrics
- B. PKI
- C. ACLs
- D. Kerberos

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 516**

A corporation is looking to expand their data center but has run out of physical space in which to store hardware. Which of the following would offer the ability to expand while keeping their current data center operated by internal staff?

- A. Virtualization
- B. Subnetting
- C. IaaS
- D. SaaS

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 517**

After viewing wireless traffic, an attacker notices the following networks are being broadcasted by local access points:

Corpnet

Coffeeshop

FreePublicWifi

Using this information the attacker spoofs a response to make nearby laptops connect back to a malicious device. Which of the following has the attacker created?

- A. Infrastructure as a Service
- B. Load balancer
- C. Evil twin
- D. Virtualized network

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 518**

Which of the following concepts is enforced by certifying that email communications have been sent by who the message says it has been sent by?

- A. Key escrow
- B. Non-repudiation
- C. Multifactor authentication
- D. Hashing



**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 519**

After a recent breach, the security administrator performs a wireless survey of the corporate network. The security administrator notices a problem with the following output:

MACSSIDENCRYPTIONPOWERBEACONS

00:10:A1:36:12:CCMYCORPWPA2 CCMP601202

00:10:A1:49:FC:37MYCORPWPA2 CCMP709102

FB:90:11:42:FA:99MYCORPWPA2 CCMP403031

00:10:A1:AA:BB:CCMYCORPWPA2 CCMP552021

00:10:A1:FA:B1:07MYCORPWPA2 CCMP306044

Given that the corporate wireless network has been standardized, which of the following attacks is underway?

- A. Evil twin
- B. IV attack
- C. Rogue AP
- D. DDoS

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 520**

Input validation is an important security defense because it:

- A. rejects bad or malformed data.
- B. enables verbose error reporting.
- C. protects mis-configured web servers.
- D. prevents denial of service attacks.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 521**

In order to maintain oversight of a third party service provider, the company is going to implement a Governance, Risk, and Compliance (GRC) system. This system is promising to provide overall security posture

coverage. Which of the following is the MOST important activity that should be considered?

- A. Continuous security monitoring
- B. Baseline configuration and host hardening
- C. Service Level Agreement (SLA) monitoring
- D. Security alerting and trending

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 522**

A recent audit of a company's identity management system shows that 30% of active accounts belong to people no longer with the firm. Which of the following should be performed to help avoid this scenario? (Select TWO).

- A. Automatically disable accounts that have not been utilized for at least 10 days.
- B. Utilize automated provisioning and de-provisioning processes where possible.
- C. Request that employees provide a list of systems that they have access to prior to leaving the firm.
- D. Perform regular user account review / revalidation process.
- E. Implement a process where new account creations require management approval.

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 523**

The Chief Information Officer (CIO) has mandated web based Customer Relationship Management (CRM) business functions be moved offshore to reduce cost, reduce IT overheads, and improve availability. The Chief Risk Officer (CRO) has agreed with the CIO's direction but has mandated that key authentication systems be run within the organization's network. Which of the following would BEST meet the CIO and CRO's requirements?

- A. Software as a Service
- B. Infrastructure as a Service
- C. Platform as a Service
- D. Hosted virtualization service

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 524**

Which of the following provides the BEST application availability and is easily expanded as demand grows?

- A. Server virtualization

- B. Load balancing
- C. Active-Passive Cluster
- D. RAID 6

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 525**

An administrator connects VoIP phones to the same switch as the network PCs and printers. Which of the following would provide the BEST logical separation of these three device types while still allowing traffic between them via ACL?

- A. Create three VLANs on the switch connected to a router
- B. Define three subnets, configure each device to use their own dedicated IP address range, and then connect the network to a router
- C. Install a firewall and connect it to the switch
- D. Install a firewall and connect it to a dedicated switch for each device type

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 526**

Which of the following wireless security measures can an attacker defeat by spoofing certain properties of their network interface card?

- A. WEP
- B. MAC filtering
- C. Disabled SSID broadcast
- D. TKIP

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 527**

Which of the following provides additional encryption strength by repeating the encryption process with additional keys?

- A. AES
- B. 3DES
- C. TwoFish
- D. Blowfish

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 528**

Which of the following BEST describes part of the PKI process?

- A. User1 decrypts data with User2's private key
- B. User1 hashes data with User2's public key
- C. User1 hashes data with User2's private key
- D. User1 encrypts data with User2's public key

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 529**

Two members of the finance department have access to sensitive information. The company is concerned they may work together to steal information. Which of the following controls could be implemented to discover if they are working together?

- A. Least privilege access
- B. Separation of duties
- C. Mandatory access control
- D. Mandatory vacations

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 530**

A system administrator attempts to ping a hostname and the response is 2001:4860:0:2001::68. Which of the following replies has the administrator received?

- A. The loopback address
- B. The local MAC address
- C. IPv4 address
- D. IPv6 address

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 531**

Which of the following allows a network administrator to implement an access control policy based on individual

user characteristics and NOT on job function?

- A. Attributes based
- B. Implicit deny
- C. Role based
- D. Rule based

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 532**

Which of the following is a best practice when a mistake is made during a forensics examination?

- A. The examiner should verify the tools before, during, and after an examination.
- B. The examiner should attempt to hide the mistake during cross-examination.
- C. The examiner should document the mistake and workaround the problem.
- D. The examiner should disclose the mistake and assess another area of the disc.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 533**

Which of the following allows lower level domains to access resources in a separate Public Key Infrastructure?

- A. Trust Model
- B. Recovery Agent
- C. Public Key
- D. Private Key

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 534**

Which of the following offers the LEAST secure encryption capabilities?

- A. TwoFish
- B. PAP
- C. NTLM
- D. CHAP

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 535**

Which of the following network architecture concepts is used to securely isolate at the boundary between networks?

- A. VLAN
- B. Subnetting
- C. DMZ
- D. NAT

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 536**

Datacenter access is controlled with proximity badges that record all entries and exits from the datacenter. The access records are used to identify which staff members accessed the data center in the event of equipment theft. Which of the following **MUST** be prevented in order for this policy to be effective?

- A. Password reuse
- B. Phishing
- C. Social engineering
- D. Tailgating

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 537**

Elastic cloud computing environments often reuse the same physical hardware for multiple customers over time as virtual machines are instantiated and deleted. This has important implications for which of the following data security concerns?

- A. Hardware integrity
- B. Data confidentiality
- C. Availability of servers
- D. Integrity of data

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 538**

When implementing fire suppression controls in a datacenter it is important to:

- A. Select a fire suppression system which protects equipment but may harm technicians.
- B. Ensure proper placement of sprinkler lines to avoid accidental leakage onto servers.
- C. Integrate maintenance procedures to include regularly discharging the system.
- D. Use a system with audible alarms to ensure technicians have 20 minutes to evacuate.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 539**

Vendors typically ship software applications with security settings disabled by default to ensure a wide range of interoperability with other applications and devices. A security administrator should perform which of the following before deploying new software?

- A. Application white listing
- B. Network penetration testing
- C. Application hardening
- D. Input fuzzing testing

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 540**

A technician is deploying virtual machines for multiple customers on a single physical host to reduce power consumption in a data center. Which of the following should be recommended to isolate the VMs from one another?

- A. Implement a virtual firewall
- B. Install HIPS on each VM
- C. Virtual switches with VLANs
- D. Develop a patch management guide

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 541**

Mandatory vacations are a security control which can be used to uncover which of the following?

- A. Fraud committed by a system administrator
- B. Poor password security among users
- C. The need for additional security staff
- D. Software vulnerabilities in vendor code

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 542**

Each server on a subnet is configured to only allow SSH access from the administrator's workstation. Which of the following BEST describes this implementation?

- A. Host-based firewalls
- B. Network firewalls
- C. Network proxy
- D. Host intrusion prevention

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 543**

During a security assessment, an administrator wishes to see which services are running on a remote server. Which of the following should the administrator use?

- A. Port scanner
- B. Network sniffer
- C. Protocol analyzer
- D. Process list

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 544**

In which of the following categories would creating a corporate privacy policy, drafting acceptable use policies, and group based access control be classified?

- A. Security control frameworks
- B. Best practice
- C. Access control methodologies
- D. Compliance activity

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 545**



Disabling unnecessary services, restricting administrative access, and enabling auditing controls on a server are forms of which of the following?

- A. Application patch management
- B. Cross-site scripting prevention
- C. Creating a security baseline
- D. System hardening

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 546**

A system administrator has noticed vulnerability on a high impact production server. A recent update was made available by the vendor that addresses the vulnerability but requires a reboot of the system afterwards. Which of the following steps should the system administrator implement to address the vulnerability?

- A. Test the update in a lab environment, schedule downtime to install the patch, install the patch and reboot the server and monitor for any changes
- B. Test the update in a lab environment, backup the server, schedule downtime to install the patch, install the patch, and monitor for any changes
- C. Test the update in a lab environment, backup the server, schedule downtime to install the patch, install the update, reboot the server, and monitor for any changes
- D. Backup the server, schedule downtime to install the patch, installs the patch and monitor for any changes

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 547**

Which of the following services are used to support authentication services for several local devices from a central location without the use of tokens?

- A. TACACS+
- B. Smartcards
- C. Biometrics
- D. Kerberos

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 548**

A network administrator has recently updated their network devices to ensure redundancy is in place so that:

- A. switches can redistribute routes across the network.
- B. environmental monitoring can be performed.

- C. single points of failure are removed.
- D. hot and cold aisles are functioning.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 549**

A network administrator recently updated various network devices to ensure redundancy throughout the network. If an interface on any of the Layer 3 devices were to go down, traffic will still pass through another interface and the production environment would be unaffected. This type of configuration represents which of the following concepts?

- A. High availability
- B. Load balancing
- C. Backout contingency plan
- D. Clustering

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 550**

A system administrator needs to ensure that certain departments have more restrictive controls to their shared folders than other departments. Which of the following security controls would be implemented to restrict those departments?

- A. User assigned privileges
- B. Password disablement
- C. Multiple account creation
- D. Group based privileges

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 551**

A network analyst received a number of reports that impersonation was taking place on the network. Session tokens were deployed to mitigate this issue and defend against which of the following attacks?

- A. Replay
- B. DDoS
- C. Smurf
- D. Ping of Death

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 552**

Which of the following controls would prevent an employee from emailing unencrypted information to their personal email account over the corporate network?

- A. DLP
- B. CRL
- C. TPM
- D. HSM

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 553**

Which of the following is a measure of biometrics performance which rates the ability of a system to correctly authenticate an authorized user?

- A. Failure to capture
- B. Type II
- C. Mean time to register
- D. Template capacity

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 554**

A company with a US-based sales force has requested that the VPN system be configured to authenticate the sales team based on their username, password and a client side certificate. Additionally, the security administrator has restricted the VPN to only allow authentication from the US territory. How many authentication factors are in use by the VPN system?

- A. 1
- B. 2
- C. 3
- D. 4

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 555**

A software development company wants to implement a digital rights management solution to protect its intellectual property. Which of the following should the company implement to enforce software digital rights?

- A. Transport encryption
- B. IPsec
- C. Non-repudiation
- D. Public key infrastructure

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 556**

Users are unable to connect to the web server at IP 192.168.0.20. Which of the following can be inferred of a firewall that is configured ONLY with the following ACL?

PERMIT TCP ANY HOST 192.168.0.10 EQ 80

PERMIT TCP ANY HOST 192.168.0.10 EQ 443

- A. It implements stateful packet filtering.
- B. It implements bottom-up processing.
- C. It failed closed.
- D. It implements an implicit deny.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 557**

Which of the following security awareness training is BEST suited for data owners who are concerned with protecting the confidentiality of their data?

- A. Social networking use training
- B. Personally owned device policy training
- C. Tailgating awareness policy training
- D. Information classification training

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 558**

A security administrator is concerned about the strength of user's passwords. The company does not want to implement a password complexity policy. Which of the following can the security administrator implement to mitigate the risk of an online password attack against users with weak passwords?

- A. Increase the password length requirements
- B. Increase the password history
- C. Shorten the password expiration period
- D. Decrease the account lockout time

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 559**

A company has purchased an application that integrates into their enterprise user directory for account authentication. Users are still prompted to type in their usernames and passwords. Which of the following types of authentication is being utilized here?

- A. Separation of duties
- B. Least privilege
- C. Same sign-on
- D. Single sign-on

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 560**

Which of the following are Data Loss Prevention (DLP) strategies that address data in transit issues? (Select TWO).

- A. Scanning printing of documents.
- B. Scanning of outbound IM (Instance Messaging).
- C. Scanning copying of documents to USB.
- D. Scanning of SharePoint document library.
- E. Scanning of shared drives.
- F. Scanning of HTTP user traffic.

**Correct Answer:** BF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 561**

A user casually browsing the Internet is redirected to a warez site where a number of pop-ups appear. After clicking on a pop-up to complete a survey, a drive-by download occurs. Which of the following is MOST likely to be contained in the download?

- A. Backdoor
- B. Spyware

- C. Logic bomb
- D. DDoS
- E. Smurf

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 562**

A security administrator plans on replacing a critical business application in five years. Recently, there was a security flaw discovered in the application that will cause the IT department to manually re-enable user accounts each month at a cost of \$2,000. Patching the application today would cost \$140,000 and take two months to implement. Which of the following should the security administrator do in regards to the application?

- A. Avoid the risk to the user base allowing them to re-enable their own accounts
- B. Mitigate the risk by patching the application to increase security and saving money
- C. Transfer the risk replacing the application now instead of in five years
- D. Accept the risk and continue to enable the accounts each month saving money

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 563**

The IT department has setup a share point site to be used on the intranet. Security has established the groups and permissions on the site. No one may modify the permissions and all requests for access are centrally managed by the security team. This is an example of which of the following control types?

- A. Rule based access control
- B. Mandatory access control
- C. User assigned privilege
- D. Discretionary access control

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 564**

Purchasing receives a phone call from a vendor asking for a payment over the phone. The phone number displayed on the caller ID matches the vendor's number. When the purchasing agent asks to call the vendor back, they are given a different phone number with a different area code. Which of the following attack types is this?

- A. Hoax
- B. Impersonation
- C. Spear phishing

D. Whaling

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 565**

Purchasing receives an automated phone call from a bank asking to input and verify credit card information. The phone number displayed on the caller ID matches the bank. Which of the following attack types is this?

- A. Hoax
- B. Phishing
- C. Vishing
- D. Whaling

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 566**

The IT department has setup a website with a series of questions to allow end users to reset their own accounts. Which of the following account management practices does this help?

- A. Account Disablements
- B. Password Expiration
- C. Password Complexity
- D. Password Recovery

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 567**

An information bank has been established to store contacts, phone numbers and other records. A UNIX application needs to connect to the index server using port 389. Which of the following authentication services should be used on this port by default?

- A. RADIUS
- B. Kerberos
- C. TACACS+
- D. LDAP

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 568**

An internal auditor is concerned with privilege creep that is associated with transfers inside the company. Which mitigation measure would detect and correct this?

- A. User rights reviews
- B. Least privilege and job rotation
- C. Change management
- D. Change Control

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 569**

Which of the following is the default port for TFTP?

- A. 20
- B. 69
- C. 21
- D. 68

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 570**

Which of the following concepts are included on the three sides of the "security triangle"? (Select THREE).

- A. Confidentiality
- B. Availability
- C. Integrity
- D. Authorization
- E. Authentication
- F. Continuity

**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 571**

Which of the following concepts allows an organization to group large numbers of servers together in order to deliver a common service?

- A. Clustering



- B. RAID
- C. Backup Redundancy
- D. Cold site

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 572**

Which of the following security concepts identifies input variables which are then used to perform boundary testing?

- A. Application baseline
- B. Application hardening
- C. Secure coding
- D. Fuzzing

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 573**

Users need to exchange a shared secret to begin communicating securely. Which of the following is another name for this symmetric key?

- A. Session Key
- B. Public Key
- C. Private Key
- D. Digital Signature

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 574**

Which of the following cryptographic related browser settings allows an organization to communicate securely?

- A. SSL 3.0/TLS 1.0
- B. 3DES
- C. Trusted Sites
- D. HMAC

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 575**

Which of the following is the BEST reason to provide user awareness and training programs for organizational staff?

- A. To ensure proper use of social media
- B. To reduce organizational IT risk
- C. To detail business impact analyses
- D. To train staff on zero-days

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 576**

A firewall technician has been instructed to disable all non-secure ports on a corporate firewall. The technician has blocked traffic on port 21, 69, 80, and 137-139. The technician has allowed traffic on ports 22 and 443. Which of the following correctly lists the protocols blocked and allowed?

- A. Blocked: TFTP, HTTP, NetBIOS; Allowed: HTTPS, FTP
- B. Blocked: FTP, TFTP, HTTP, NetBIOS; Allowed: SFTP, SSH, SCP, HTTPS
- C. Blocked: SFTP, TFTP, HTTP, NetBIOS; Allowed: SSH, SCP, HTTPS
- D. Blocked: FTP, HTTP, HTTPS; Allowed: SFTP, SSH, SCP, NetBIOS

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 577**

A security administrator is responsible for performing periodic reviews of user permission settings due to high turnover and internal transfers at a corporation. Which of the following BEST describes the procedure and security rationale for performing such reviews?

- A. Review all user permissions and group memberships to ensure only the minimum set of permissions required to perform a job is assigned.
- B. Review the permissions of all transferred users to ensure new permissions are granted so the employee can work effectively.
- C. Ensure all users have adequate permissions and appropriate group memberships, so the volume of help desk calls is reduced.
- D. Ensure former employee accounts have no permissions so that they cannot access any network file stores and resources.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 578**

A system administrator is responding to a legal order to turn over all logs from all company servers. The system administrator records the system time of all servers to ensure that:

- A. HDD hashes are accurate.
- B. the NTP server works properly.
- C. chain of custody is preserved.
- D. time offset can be calculated.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 579**

While rarely enforced, mandatory vacation policies are effective at uncovering:

- A. Help desk technicians with oversight by multiple supervisors and detailed quality control systems.
- B. Collusion between two employees who perform the same business function.
- C. Acts of incompetence by a systems engineer designing complex architectures as a member of a team.
- D. Acts of gross negligence on the part of system administrators with unfettered access to system and no oversight.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 580**

A company hires outside security experts to evaluate the security status of the corporate network. All of the company's IT resources are outdated and prone to crashing. The company requests that all testing be performed in a way which minimizes the risk of system failures. Which of the following types of testing does the company want performed?

- A. Penetration testing
- B. WAF testing
- C. Vulnerability scanning
- D. White box testing

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 581**

A security administrator notices that a specific network administrator is making unauthorized changes to the firewall every Saturday morning. Which of the following would be used to mitigate this issue so that only security administrators can make changes to the firewall?

- A. Mandatory vacations
- B. Job rotation
- C. Least privilege
- D. Time of day restrictions

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 582**

A security administrator notices large amounts of traffic within the network heading out to an external website. The website seems to be a fake bank site with a phone number that when called, asks for sensitive information. After further investigation, the security administrator notices that a fake link was sent to several users. This is an example of which of the following attacks?

- A. Vishing
- B. Phishing
- C. Whaling
- D. SPAM
- E. SPIM

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 583**

After a user performed a war driving attack, the network administrator noticed several similar markings where WiFi was available throughout the enterprise. Which of the following is the term used to describe these markings?

- A. IV attack
- B. War dialing
- C. Rogue access points
- D. War chalking

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 584**

The system administrator notices that their application is no longer able to keep up with the large amounts of traffic their server is receiving daily. Several packets are dropped and sometimes the server is taken offline. Which of the following would be a possible solution to look into to ensure their application remains secure and available?

- A. Cloud computing

- B. Full disk encryption
- C. Data Loss Prevention
- D. HSM

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 585**

After a recent internal audit, the security administrator was tasked to ensure that all credentials must be changed within 90 days, cannot be repeated, and cannot contain any dictionary words or patterns. All credentials will remain enabled regardless of the number of attempts made. Which of the following types of user account options were enforced? (Select TWO).

- A. Recovery
- B. User assigned privileges
- C. Lockout
- D. Disablement
- E. Group based privileges
- F. Password expiration
- G. Password complexity

**Correct Answer:** FG

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 586**

A security analyst has been notified that trade secrets are being leaked from one of the executives in the corporation. When reviewing this executive's laptop they notice several pictures of the employee's pets are on the hard drive and on a cloud storage network. When the analyst hashes the images on the hard drive against the hashes on the cloud network they do not match. Which of the following describes how the employee is leaking these secrets?

- A. Social engineering
- B. Steganography
- C. Hashing
- D. Digital signatures

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 587**

During a routine audit a web server is flagged for allowing the use of weak ciphers. Which of the following should be disabled to mitigate this risk? (Select TWO).

- A. SSL 1.0
- B. RC4
- C. SSL 3.0
- D. AES
- E. DES
- F. TLS 1.0

**Correct Answer:** AE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 588

Review the following diagram depicting communication between PC1 and PC2 on each side of a router. Analyze the network traffic logs which show communication between the two computers as captured by the computer with IP 10.2.2.10.

DIAGRAM

PC1 PC2

[192.168.1.30]-----[INSIDE 192.168.1.1 router OUTSIDE 10.2.2.1]-----[10.2.2.10]

LOGS

10:30:22, SRC 10.2.2.1:3030, DST 10.2.2.10:80, SYN

10:30:23, SRC 10.2.2.10:80, DST 10.2.2.1:3030, SYN/ACK

10:30:24, SRC 10.2.2.1:3030, DST 10.2.2.10:80, ACK

Given the above information, which of the following can be inferred about the above environment?

- A. 192.168.1.30 is a web server.
- B. The web server listens on a non-standard port.
- C. The router filters port 80 traffic.
- D. The router implements NAT.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 589

The Chief Information Officer (CIO) wants to implement a redundant server location to which the production server images can be moved within 48 hours and services can be quickly restored, in case of a catastrophic failure of the primary datacenter's HVAC. Which of the following can be implemented?

- A. Cold site
- B. Load balancing
- C. Warm site
- D. Hot site

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 590**

The security administrator is observing unusual network behavior from a workstation. The workstation is communicating with a known malicious destination over an encrypted tunnel. A full antivirus scan, with an updated antivirus definition file, does not show any signs of infection. Which of the following has happened on the workstation?

- A. Zero-day attack
- B. Known malware infection
- C. Session hijacking
- D. Cookie stealing

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 591**

Which of the following controls can be used to prevent the disclosure of sensitive information stored on a mobile device's removable media in the event that the device is lost or stolen?

- A. Hashing
- B. Screen locks
- C. Device password
- D. Encryption

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 592**

Which of the following should be performed to increase the availability of IP telephony by prioritizing traffic?

- A. Subnetting
- B. NAT
- C. Quality of service
- D. NAC

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 593**

A malicious program modified entries in the LMHOSTS file of an infected system. Which of the following protocols would have been affected by this?

- A. ICMP
- B. BGP
- C. NetBIOS
- D. DNS

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 594**

A victim is logged onto a popular home router forum site in order to troubleshoot some router configuration issues. The router is a fairly standard configuration and has an IP address of 192.168.1.1. The victim is logged into their router administrative interface in one tab and clicks a forum link in another tab. Due to clicking the forum link, the home router reboots. Which of the following attacks MOST likely occurred?

- A. Brute force password attack
- B. Cross-site request forgery
- C. Cross-site scripting
- D. Fuzzing

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 595**

Which of the following assets is MOST likely considered for DLP?

- A. Application server content
- B. USB mass storage devices
- C. Reverse proxy
- D. Print server

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 596**

In order to securely communicate using PGP, the sender of an email must do which of the following when sending an email to a recipient for the first time?

- A. Import the recipient's public key
- B. Import the recipient's private key



- C. Export the sender's private key
- D. Export the sender's public key

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 597**

A hacker has discovered a simple way to disrupt business for the day in a small company which relies on staff working remotely. In a matter of minutes the hacker was able to deny remotely working staff access to company systems with a script. Which of the following security controls is the hacker exploiting?

- A. DoS
- B. Account lockout
- C. Password recovery
- D. Password complexity

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 598**

A security specialist has been asked to evaluate a corporate network by performing a vulnerability assessment. Which of the following will MOST likely be performed?

- A. Identify vulnerabilities, check applicability of vulnerabilities by passively testing security controls.
- B. Verify vulnerabilities exist, bypass security controls and exploit the vulnerabilities.
- C. Exploit security controls to determine vulnerabilities and mis-configurations.
- D. Bypass security controls and identify applicability of vulnerabilities by passively testing security controls.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 599**

A security technician is attempting to access a wireless network protected with WEP. The technician does not know any information about the network. Which of the following should the technician do to gather information about the configuration of the wireless network?

- A. Spoof the MAC address of an observed wireless network client
- B. Ping the access point to discover the SSID of the network
- C. Perform a dictionary attack on the access point to enumerate the WEP key
- D. Capture client to access point disassociation packets to replay on the local PC's loopback

**Correct Answer:** A

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 600**

After an assessment, auditors recommended that an application hosting company should contract with additional data providers for redundant high speed Internet connections. Which of the following is MOST likely the reason for this recommendation? (Select TWO).

- A. To allow load balancing for cloud support
- B. To allow for business continuity if one provider goes out of business
- C. To eliminate a single point of failure
- D. To allow for a hot site in case of disaster
- E. To improve intranet communication speeds

**Correct Answer:** BC

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 601**

A router has a single Ethernet connection to a switch. In the router configuration, the Ethernet interface has three sub-interfaces, each configured with ACLs applied to them and 802.1q trunks. Which of the following is MOST likely the reason for the sub-interfaces?

- A. The network uses the subnet of 255.255.255.128.
- B. The switch has several VLANs configured on it.
- C. The sub-interfaces are configured for VoIP traffic.
- D. The sub-interfaces each implement quality of service.

**Correct Answer:** B

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 602**

Which of the following should be enabled in a laptop's BIOS prior to full disk encryption?

- A. USB
- B. HSM
- C. RAID
- D. TPM

**Correct Answer:** D

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 603**

Company employees are required to have workstation client certificates to access a bank website. These certificates were backed up as a precautionary step before the new computer upgrade. After the upgrade and restoration, users state they can access the bank's website, but not login. Which of the following is MOST likely the issue?

- A. The IP addresses of the clients have change
- B. The client certificate passwords have expired on the server
- C. The certificates have not been installed on the workstations
- D. The certificates have been installed on the CA

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 604**

Digital Signatures provide which of the following?

- A. Confidentiality
- B. Authorization
- C. Integrity
- D. Authentication
- E. Availability

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 605**

A user ID and password together provide which of the following?

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 606**

RADIUS provides which of the following?

- A. Authentication, Authorization, Availability
- B. Authentication, Authorization, Auditing
- C. Authentication, Accounting, Auditing
- D. Authentication, Authorization, Accounting

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 607**

A recent intrusion has resulted in the need to perform incident response procedures. The incident response team has identified audit logs throughout the network and organizational systems which hold details of the security breach. Prior to this incident, a security consultant informed the company that they needed to implement an NTP server on the network. Which of the following is a problem that the incident response team will likely encounter during their assessment?

- A. Chain of custody
- B. Tracking man hours
- C. Record time offset
- D. Capture video traffic

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 608**

A recent computer breach has resulted in the incident response team needing to perform a forensics examination. Upon examination, the forensics examiner determines that they cannot tell which captured hard drive was from the device in question. Which of the following would have prevented the confusion experienced during this examination?

- A. Perform routine audit
- B. Chain of custody
- C. Evidence labeling
- D. Hashing the evidence

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 609**

An IT staff member was entering the datacenter when another person tried to piggyback into the datacenter as the door was opened. While the IT staff member attempted to question the other individual by politely asking to see their badge, the individual refused and ran off into the datacenter. Which of the following should the IT staff member do NEXT?

- A. Call the police while tracking the individual on the closed circuit television system
- B. Contact the forensics team for further analysis
- C. Chase the individual to determine where they are going and what they are doing
- D. Contact the onsite physical security team with a description of the individual

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 610**

During a recent user awareness and training session, a new staff member asks the Chief Information Security Officer (CISO) why the company does not allow personally owned devices into the company facilities. Which of the following represents how the CISO should respond?

- A. Company A views personally owned devices as creating an unacceptable risk to the organizational IT systems.
- B. Company A has begun to see zero-day attacks against personally owned devices disconnected from the network.
- C. Company A believes that staff members should be focused on their work while in the company's facilities.
- D. Company A has seen social engineering attacks against personally owned devices and does not allow their use.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 611**

A user has received an email from an external source which asks for details on the company's new product line set for release in one month. The user has a detailed spec sheet but it is marked "Internal Proprietary Information". Which of the following should the user do NEXT?

- A. Contact their manager and request guidance on how to best move forward
- B. Contact the help desk and/or incident response team to determine next steps
- C. Provide the requestor with the email information since it will be released soon anyway
- D. Reply back to the requestor to gain their contact information and call them

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 612**

Which of the following techniques enables a highly secured organization to assess security weaknesses in real time?

- A. Access control lists
- B. Continuous monitoring
- C. Video surveillance
- D. Baseline reporting

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 613**

Which of the following techniques can be used to prevent the disclosure of system information resulting from arbitrary inputs when implemented properly?

- A. Fuzzing
- B. Patch management
- C. Error handling
- D. Strong passwords

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 614**

Encryption of data at rest is important for sensitive information because of which of the following?

- A. Facilitates tier 2 support, by preventing users from changing the OS
- B. Renders the recovery of data harder in the event of user password loss
- C. Allows the remote removal of data following eDiscovery requests
- D. Prevents data from being accessed following theft of physical equipment

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 615**

Which of the following is synonymous with a server's certificate?

- A. Public key
- B. CRL
- C. Private key
- D. Recovery agent

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 616**

A network administrator noticed various chain messages have been received by the company. Which of the following security controls would need to be implemented to mitigate this issue?

- A. Anti-spam

- B. Antivirus
- C. Host-based firewalls
- D. Anti-spyware

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 617**

Which of the following types of application attacks would be used to specifically gain unauthorized information from databases that did not have any input validation implemented?

- A. SQL injection
- B. Session hijacking and XML injection
- C. Cookies and attachments
- D. Buffer overflow and XSS

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 618**

Which of the following should be deployed to prevent the transmission of malicious traffic between virtual machines hosted on a singular physical device on a network?

- A. HIPS on each virtual machine
- B. NIPS on the network
- C. NIDS on the network
- D. HIDS on each virtual machine

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 619**

A security administrator wants to get a real time look at what attackers are doing in the wild, hoping to lower the risk of zero-day attacks. Which of the following should be used to accomplish this goal?

- A. Penetration testing
- B. Honeynets
- C. Vulnerability scanning
- D. Baseline reporting

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 620**

Which of the following protocols is the security administrator observing in this packet capture?

12:33:43, SRC 192.168.4.3:3389, DST 10.67.33.20:8080, SYN/ACK

- A. HTTPS
- B. RDP
- C. HTTP
- D. SFTP

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 621**

Which of the following is true about asymmetric encryption?

- A. A message encrypted with the private key can be decrypted by the same key
- B. A message encrypted with the public key can be decrypted with a shared key.
- C. A message encrypted with a shared key, can be decrypted by the same key.
- D. A message encrypted with the public key can be decrypted with the private key.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 622**

Which of the following is true about an email that was signed by User A and sent to User B?

- A. User A signed with User B's private key and User B verified with their own public key.
- B. User A signed with their own private key and User B verified with User A's public key.
- C. User A signed with User B's public key and User B verified with their own private key.
- D. User A signed with their own public key and User B verified with User A's private key.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 623**

The Chief Information Officer (CIO) is concerned with moving an application to a SaaS cloud provider. Which of the following can be implemented to provide for data confidentiality assurance during and after the migration to the cloud?



- A. HPM technology
- B. Full disk encryption
- C. DLP policy
- D. TPM technology

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 624**

Which of the following protocols encapsulates an IP packet with an additional IP header?

- A. SFTP
- B. IPSec
- C. HTTPS
- D. SSL

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 625**

A program has been discovered that infects a critical Windows system executable and stays dormant in memory. When a Windows mobile phone is connected to the host, the program infects the phone's boot loader and continues to target additional Windows PCs or phones. Which of the following malware categories BEST describes this program?

- A. Zero-day
- B. Trojan
- C. Virus
- D. Rootkit

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 626**

A user has unknowingly gone to a fraudulent site. The security analyst notices the following system change on the user's host:

Old `hosts` file:

127.0.0.1 localhost

New `hosts` file:

127.0.0.1 localhost

5.5.5.5 www.comptia.com

Which of the following attacks has taken place?

- A. Spear phishing
- B. Pharming
- C. Phishing
- D. Vishing

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 627**

An investigator recently discovered that an attacker placed a remotely accessible CCTV camera in a public area overlooking several Automatic Teller Machines (ATMs). It is also believed that user accounts belonging to ATM operators may have been compromised. Which of the following attacks has MOST likely taken place?

- A. Shoulder surfing
- B. Dumpster diving
- C. Whaling attack
- D. Vishing attack

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 628**

A user commuting to work via public transport received an offensive image on their smart phone from another commuter. Which of the following attacks MOST likely took place?

- A. War chalking
- B. Bluejacking
- C. War driving
- D. Bluesnarfing

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 629**

An attacker attempted to compromise a web form by inserting the following input into the username field:

admin)(|(password=\*))

Which of the following types of attacks was attempted?

- A. SQL injection
- B. Cross-site scripting
- C. Command injection
- D. LDAP injection

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 630**

Which of the following is BEST carried out immediately after a security breach is discovered?

- A. Risk transference
- B. Access control revalidation
- C. Change management
- D. Incident management

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 631**

Pete, an employee, attempts to visit a popular social networking site but is blocked. Instead, a page is displayed notifying him that this site cannot be visited. Which of the following is MOST likely blocking Pete's access to this site?

- A. Internet content filter
- B. Firewall
- C. Proxy server
- D. Protocol analyzer

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 632**

How often, at a MINIMUM, should Sara, an administrator, review the accesses and right of the users on her system?

- A. Annually
- B. Immediately after an employee is terminated
- C. Every five years
- D. Every time they patch the server

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 633**

An administrator is concerned that a company's web server has not been patched. Which of the following would be the BEST assessment for the administrator to perform?

- A. Vulnerability scan
- B. Risk assessment
- C. Virus scan
- D. Network sniffer

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 634**

A trojan was recently discovered on a server. There are now concerns that there has been a security breach that allows unauthorized people to access data. The administrator should be looking for the presence of a/an:

- A. Logic bomb.
- B. Backdoor.
- C. Adware application.
- D. Rootkit.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 635**

Which of the following protocols uses TCP instead of UDP and is incompatible with all previous versions?

- A. TACACS
- B. XTACACS
- C. RADIUS
- D. TACACS+

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 636**

Which of the following symmetric key algorithms are examples of block ciphers? (Select THREE).

- A. RC4
- B. 3DES
- C. AES
- D. MD5
- E. PGP
- F. Blowfish

**Correct Answer:** BCF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 637**

Which of the following devices will help prevent a laptop from being removed from a certain location?

- A. Device encryption
- B. Cable locks
- C. GPS tracking
- D. Remote data wipes

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 638**

Which of the following devices is typically used to provide protection at the edge of the network attack surface?

- A. Firewall
- B. Router
- C. Switch
- D. VPN concentrator

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 639**

An employee is granted access to only areas of a network folder needed to perform their job. Which of the following describes this form of access control?

- A. Separation of duties
- B. Time of day restrictions
- C. Implicit deny
- D. Least privilege

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 640**

Matt, an IT security technician, needs to create a way to recover lost or stolen company devices. Which of the following BEST meets this need?

- A. Locking cabinets
- B. GPS tracking
- C. Safe
- D. Firewalls

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 641**

Matt, an account manager, arrives at work early in the morning and cannot log into his workstation. He calls the help desk an hour later to open a trouble ticket, but they tell him there is nothing wrong with his account. Matt tries his login once more and is granted access. Which of the following control types BEST explains this anomaly?

- A. Discretionary access control
- B. Time of day restrictions
- C. Separation of duties
- D. Single sign-on

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 642**

A security technician is attempting to explain why some of the company policies should be changed for high risk IT positions. Which of the following concepts BEST explains the support for fraud detection?

- A. Time of day restrictions is more likely to discover fraud than the other fraud detection methods.
- B. Least privilege principles allow internal audit teams to discover fraud while a staff member is out of the office.
- C. Separation of duties is a better fraud detection method than mandatory vacations; therefore, it should be used.
- D. Mandatory vacations support the company discovering fraud while staff members are out of the office.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 643**

Which of the following can be used to discover if a security attack is occurring on a web server?

- A. Creating a new baseline
- B. Disable unused accounts
- C. Implementing full disk encryption
- D. Monitoring access logs

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 644**

Jane, the CEO, receives an email wanting her to click on a link to change her username and password. Which of the following attacks has she just received?

- A. Hoaxes
- B. Whaling
- C. Bluejacking
- D. Vishing

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 645**

Pete, the system administrator, has instituted a policy banning personal digital music and video players from the company premises. Which of the following would be the BEST reason for such a policy?

- A. The company would be legally liable for any personal device that is lost on its premises.
- B. It is difficult to verify ownership of offline device's digital rights management and ownership.
- C. The media players may act as distractions during work hours and adversely affect user productivity.
- D. If connected to a computer, unknown malware may be introduced into the environment.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 646**

A marketing employee requests read and write permissions to the finance department's folders. The security administrator partially denies this request and only gives the marketing employee read-only permissions. This is an example of which of the following?

- A. Job rotation
- B. Separation of duties

- C. Least privilege
- D. Change management

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 647**

Which of the following would Pete, a security administrator, MOST likely implement in order to allow employees to have secure remote access to certain internal network services such as file servers?

- A. Packet filtering firewall
- B. VPN gateway
- C. Switch
- D. Router

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 648**

Jane, an administrator, hears reports of circles being drawn in the parking lot. Because the symbols fall within range of the company's wireless AP, the MOST likely concern is:

- A. that someone has used war chalking to help others access the company's network.
- B. that the symbols indicate the presence of an evil twin of a legitimate AP.
- C. that someone is planning to install an AP where the symbols are, to cause interference.
- D. that a rogue access point has been installed within range of the symbols.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 649**

Enforcing data encryption of removable media ensures that the:

- A. lost media cannot easily be compromised.
- B. media can be identified.
- C. location of the media is known at all times.
- D. identification of the user is non-repudiated.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



**QUESTION 650**

When employees that use certificates leave the company they should be added to which of the following?

- A. PKI
- B. CA
- C. CRL
- D. TKIP

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 651**

Which of the following incident response procedures BEST allows Sara, the security technician, to identify who had possession of a hard drive prior to forensics analysis?

- A. Chain of custody
- B. Tracking man hours
- C. Witnesses
- D. Capturing system images

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 652**

Mike, a security analyst, has captured a packet with the following payload.

GET ../../../../system32/cmd.exe

Which of the following is this an example of?

- A. SQL injection
- B. Directory traversal
- C. XML injection
- D. Buffer overflow

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 653**

A security administrator needs to open ports on the firewall to allow for secure data transfer. Which of the following TCP ports would allow for secure transfer of files by default?

- A. 21
- B. 22
- C. 23
- D. 25

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**



<http://www.gratisexam.com/>

#### **QUESTION 654**

Jane, a security technician, has been tasked with preventing contractor staff from logging into the company network after business hours. Which of the following BEST allows her to accomplish this?

- A. Time of day restrictions
- B. Access control list
- C. Personal identity verification
- D. Mandatory vacations

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 655**

Which of the following can be implemented on a lost mobile device to help recover it?

- A. Remote sanitization
- B. GPS tracking
- C. Voice encryption
- D. Patch management

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 656**

Jane, a security analyst, wants to ensure that data is being stored encrypted, in the event that a corporate laptop is stolen. Which of the following encryption types will accomplish her goal?

- A. IPSec

- B. Secure socket layer
- C. Whole disk
- D. Transport layer security

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 657**

Sara, the Chief Executive Officer (CEO) of a corporation, wishes to receive her corporate email and file attachments on her corporate mobile computing device. If the device is lost or stolen, the BEST security measure to ensure that sensitive information is not comprised would be:

- A. to immediately file a police report and insurance report.
- B. the ability to remotely wipe the device to remove the data.
- C. to immediately issue a replacement device and restore data from the last backup.
- D. to turn on remote GPS tracking to find the device and track its movements.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 658**

In her morning review of new vendor patches, a security administrator has identified an exploit that is marked as critical. Which of the following is the BEST course of action?

- A. The security administrator should wait seven days before testing the patch to ensure that the vendor does not issue an updated version, which would require reapplying the patch.
- B. The security administrator should download the patch and install it to her workstation to test whether it will be able to be applied to all workstations in the environment.
- C. The security administrator should alert the risk management department to document the patch and add it to the next monthly patch deployment cycle.
- D. The security administrator should download the patch to the test network, apply it to affected systems, and evaluate the results on the test systems.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 659**

Users at a corporation are unable to login using the directory access server at certain times of the day. Which of the following concepts BEST describes this lack of access?

- A. Mandatory access control
- B. Least privilege
- C. Time of day restrictions

D. Discretionary access control

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 660**

An administrator might choose to implement a honeypot in order to:

- A. provide load balancing for network switches.
- B. distract potential intruders away from critical systems.
- C. establish a redundant server in case of a disaster.
- D. monitor any incoming connections from the Internet.

**Correct Answer:** B

**Section:** (none)

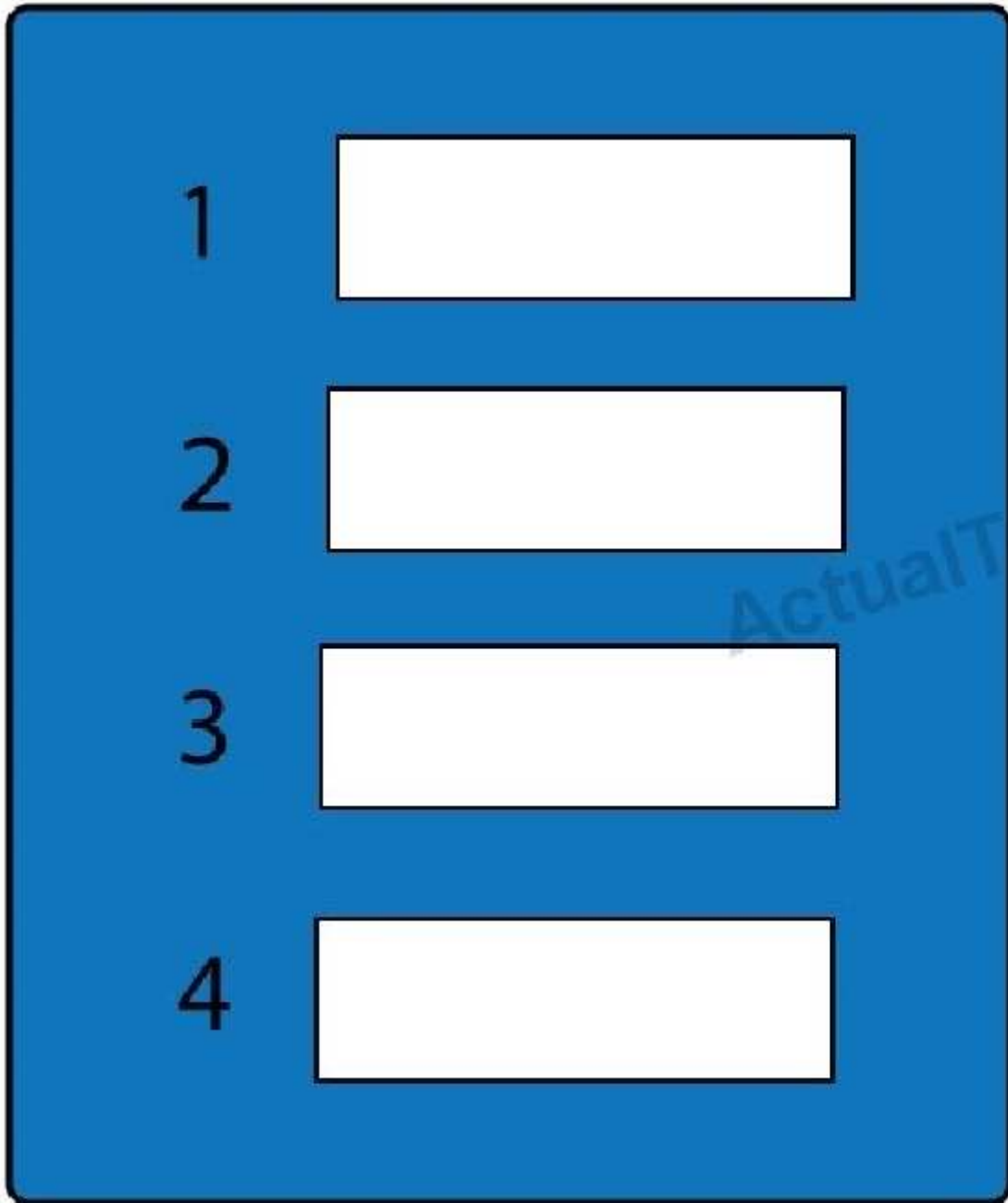
**Explanation**

**Explanation/Reference:**

## Exam B Simulations

### QUESTION 1 DRAG DROP

A forensic analyst is asked to respond to an ongoing network attack on a server. Place the items in the list below in the correct order in which the forensic analyst should preserve them.



1

2

3

4

ActualTests

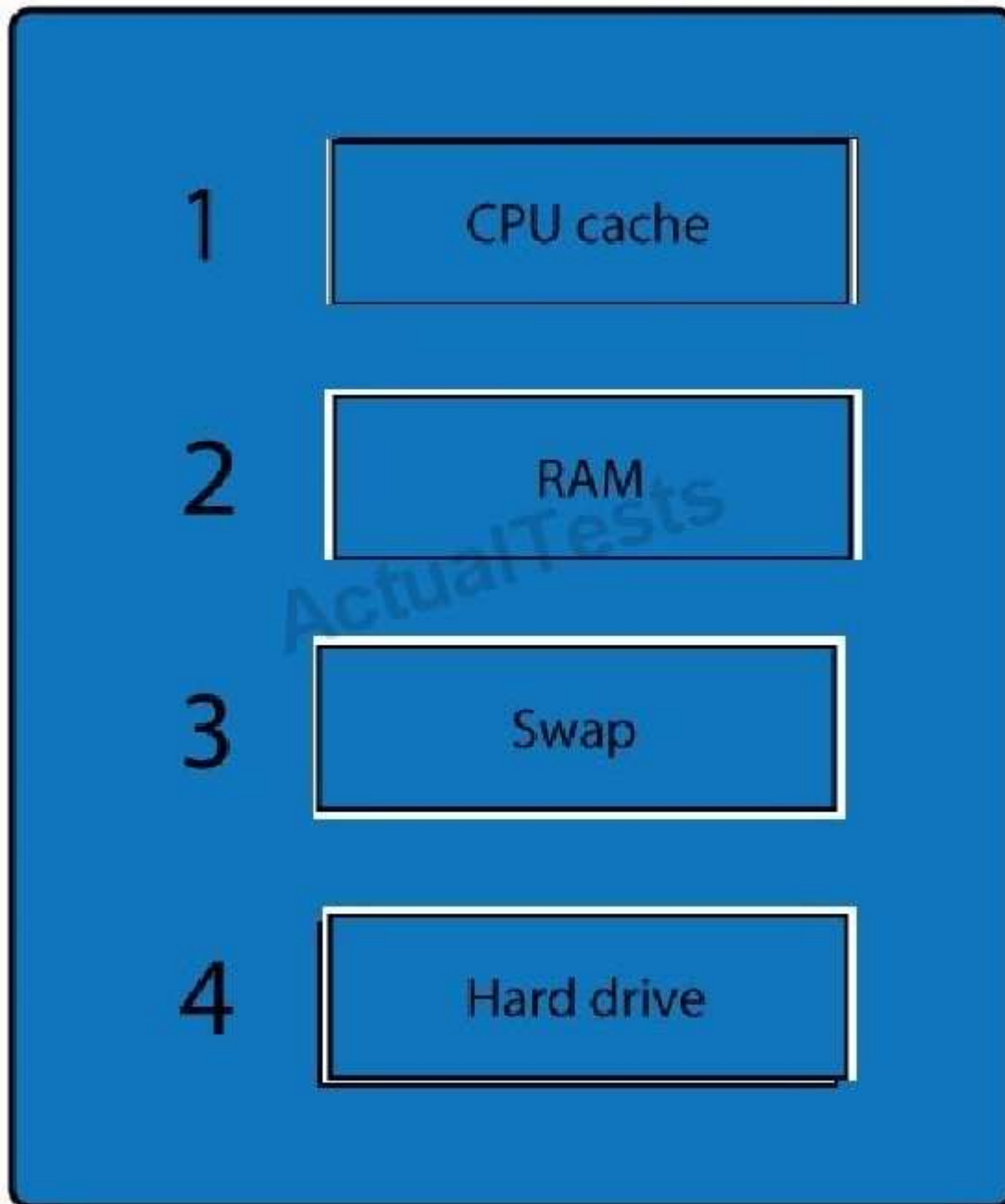
- A.
- B.
- C.
- D.

Correct Answer:

Section: (none)

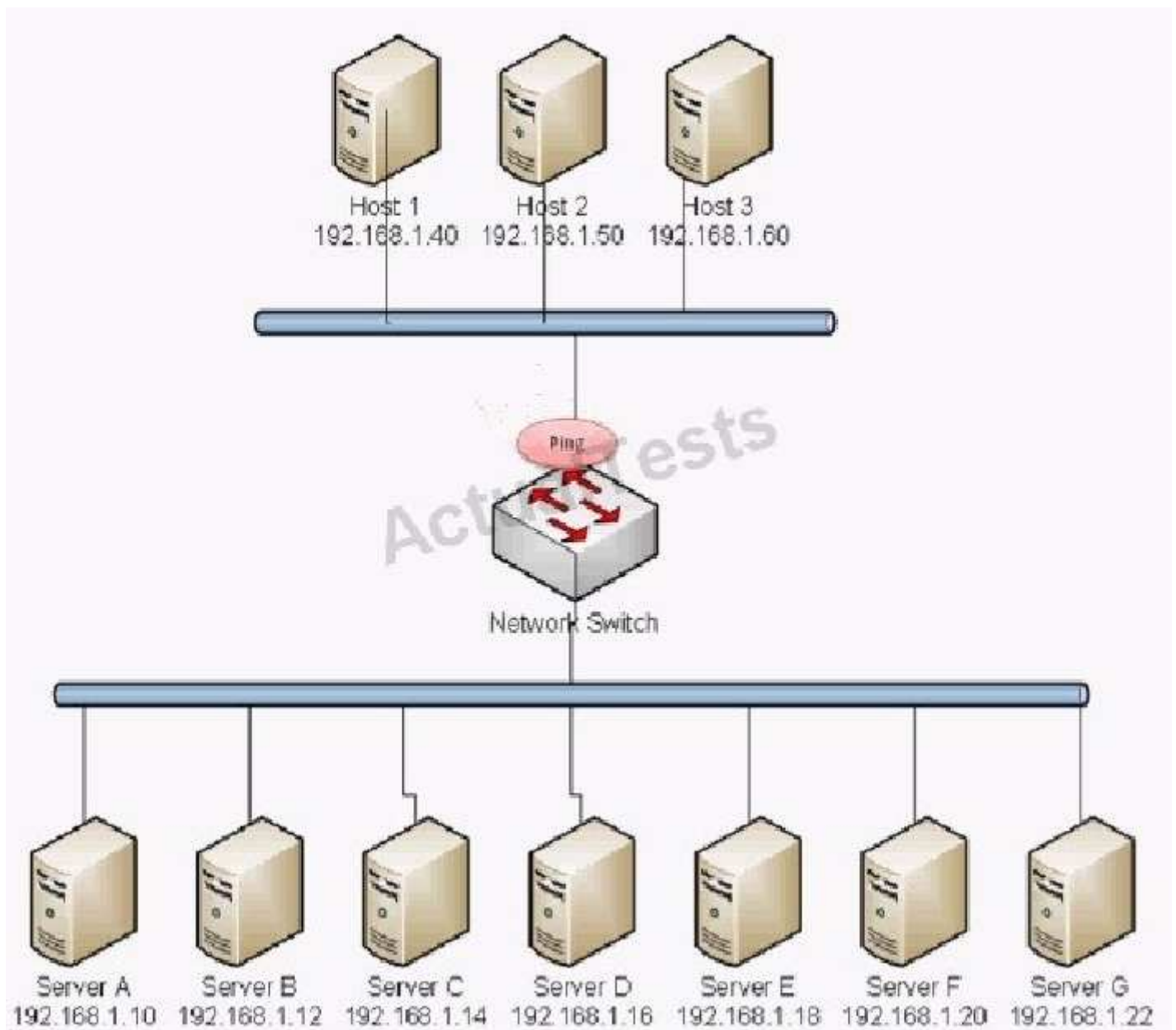
Explanation

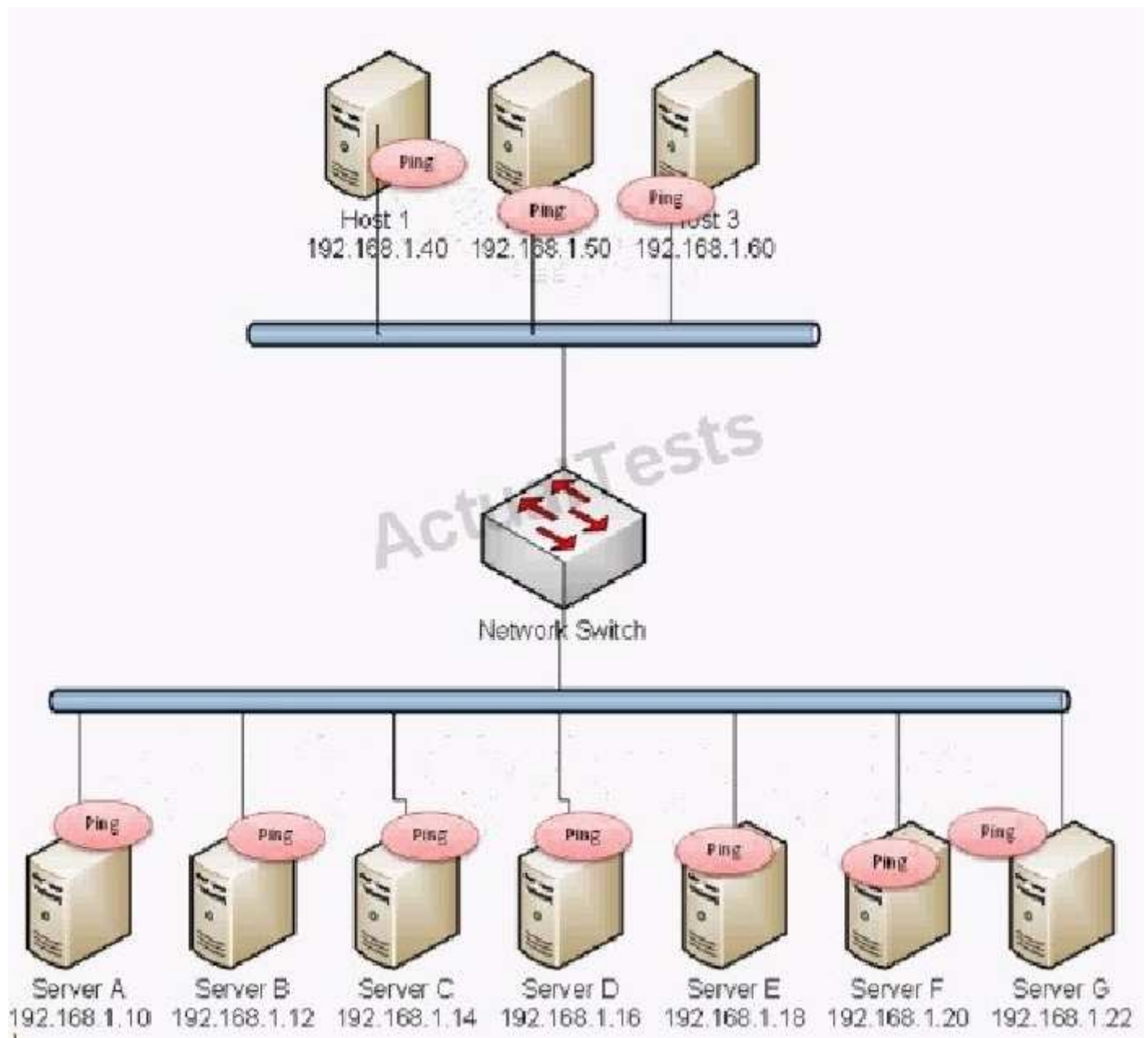
Explanation/Reference:



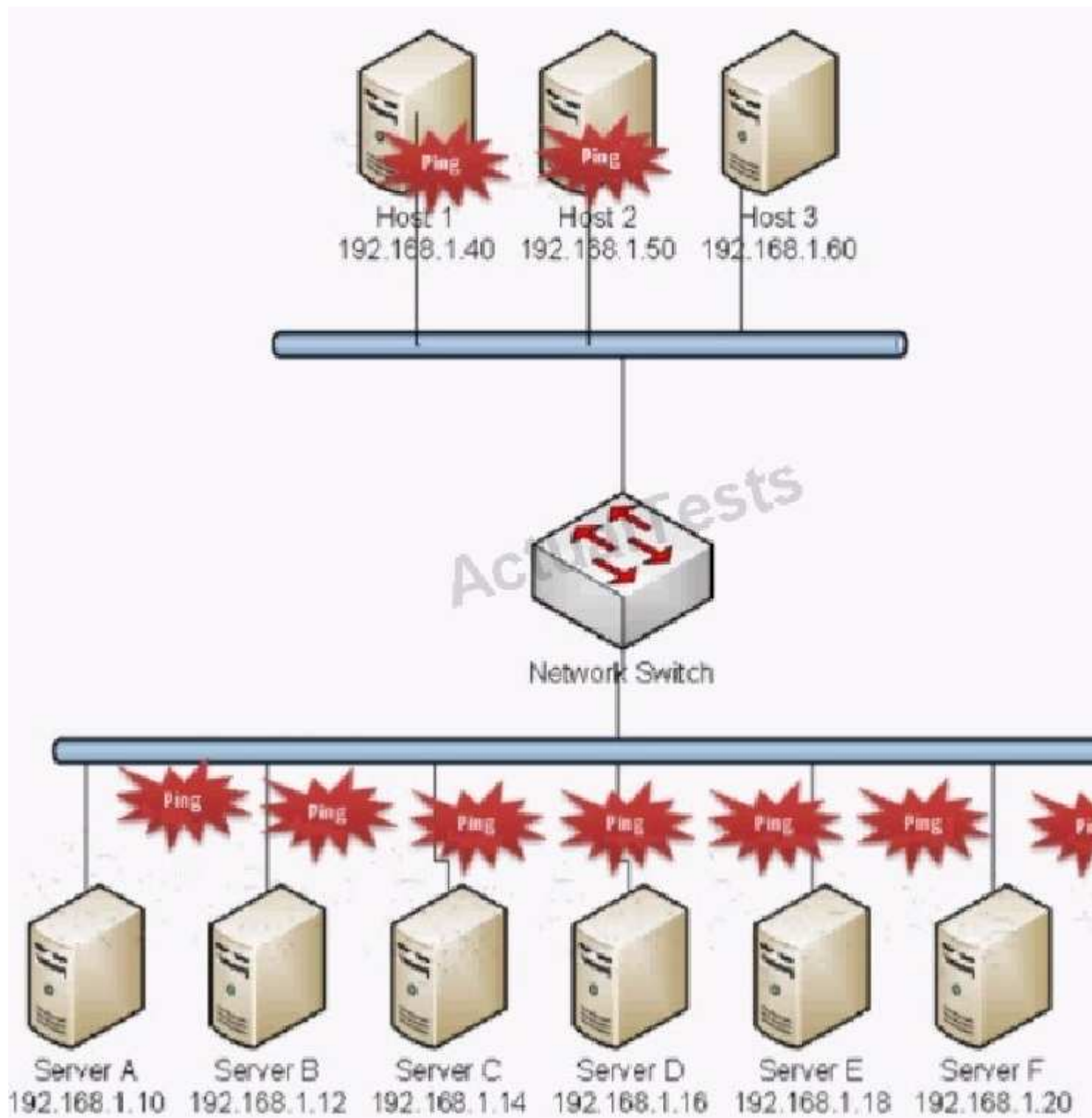
QUESTION 2

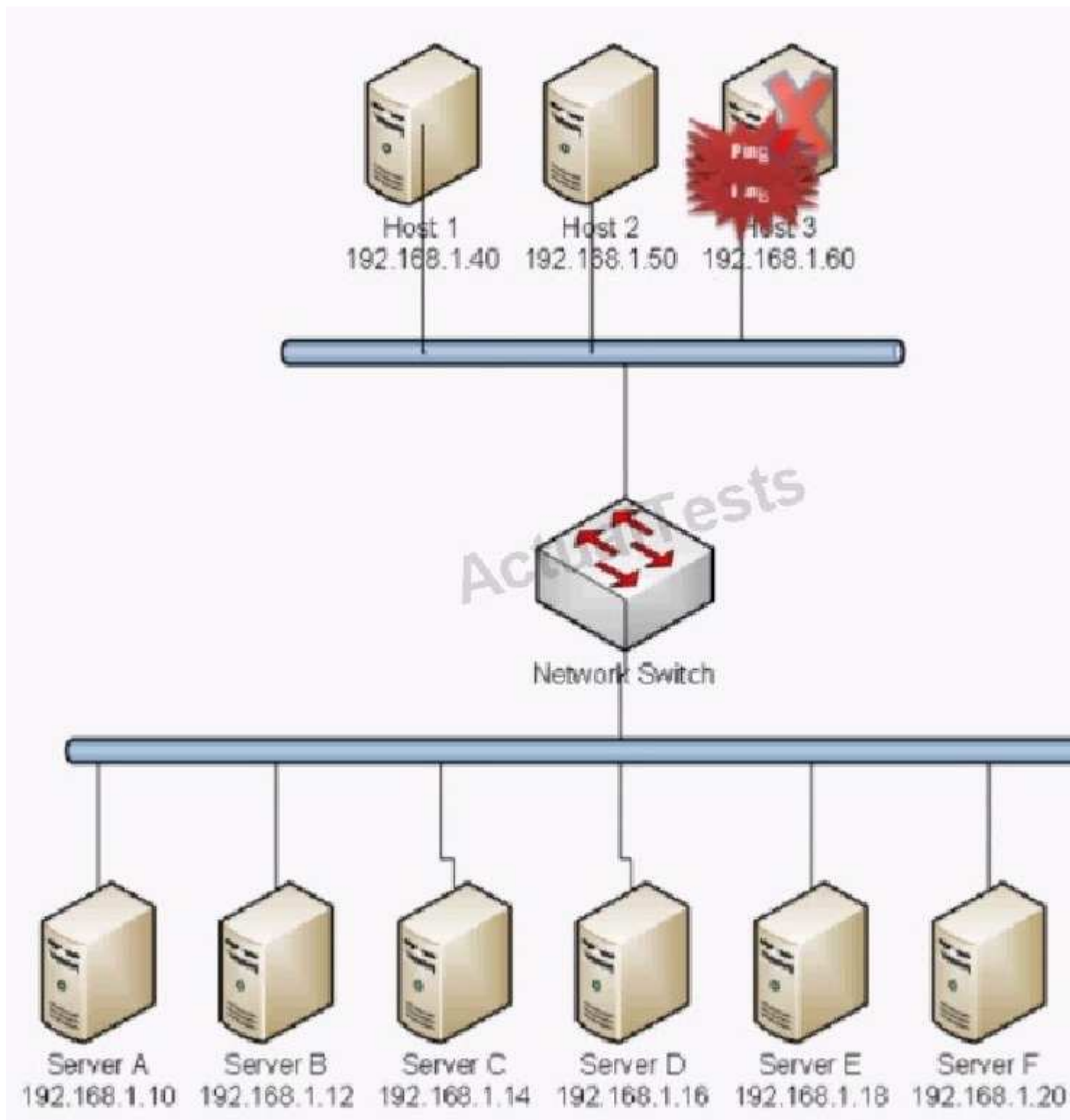
-- Exhibit











-- Exhibit --

Which of the following BEST describes the type of attack that is occurring?

- A. Smurf Attack
- B. Man in the middle
- C. Backdoor

- D. Replay
- E. Spear Phishing
- F. Xmas Attack
- G. Blue Jacking
- H. Ping of Death

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### **QUESTION 3**

**DRAG DROP**

Drag and drop the correct protocol to its default port.

FTP	<input type="text"/>	161
Telnet	<input type="text"/>	22
SMTP	<input type="text"/>	21
SNMP	<input type="text"/>	69
SCP	<input type="text"/>	25
TFTP	<input type="text"/>	23

- A.
- B.
- C.
- D.

Correct Answer:

Section: (none)

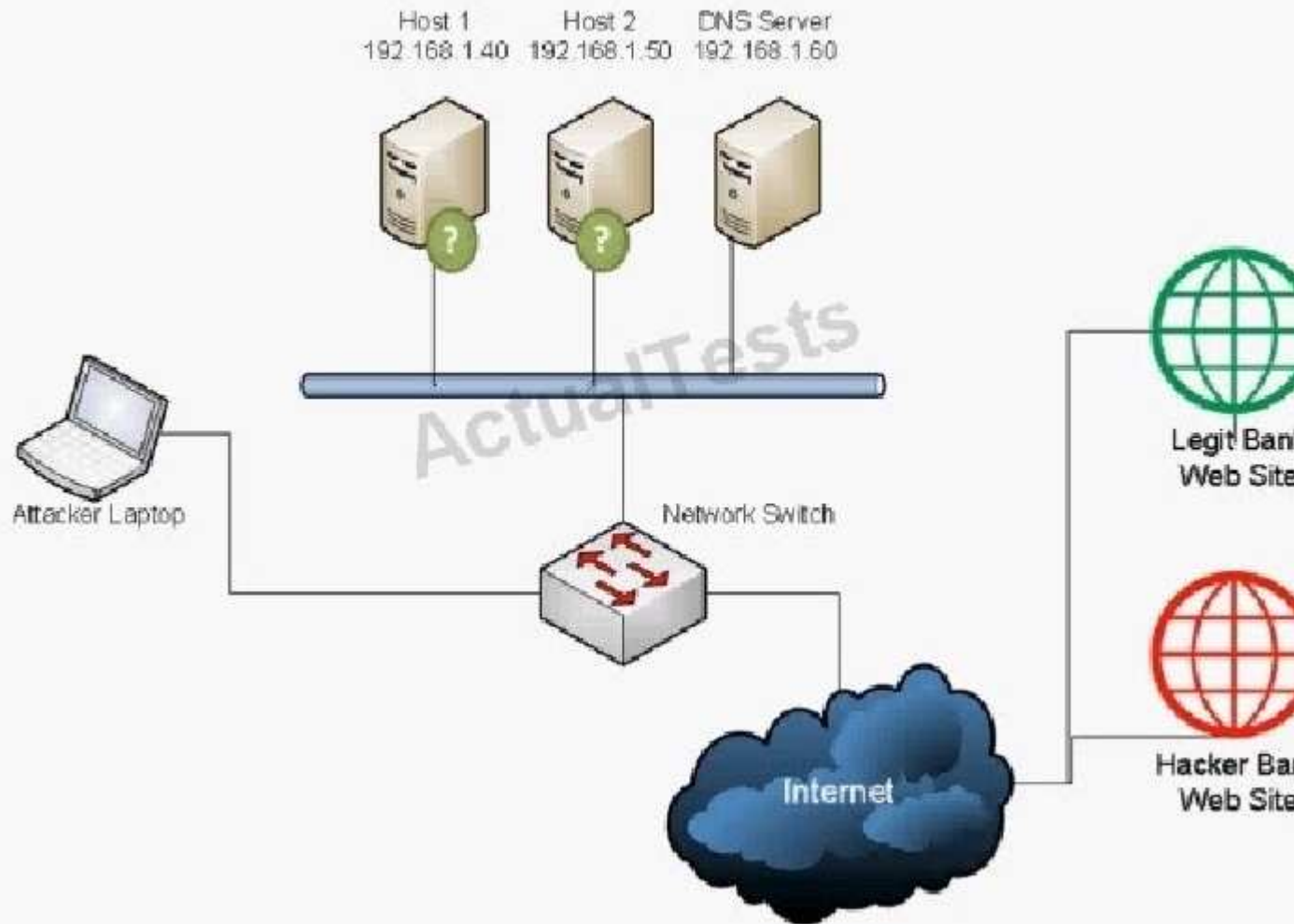
Explanation

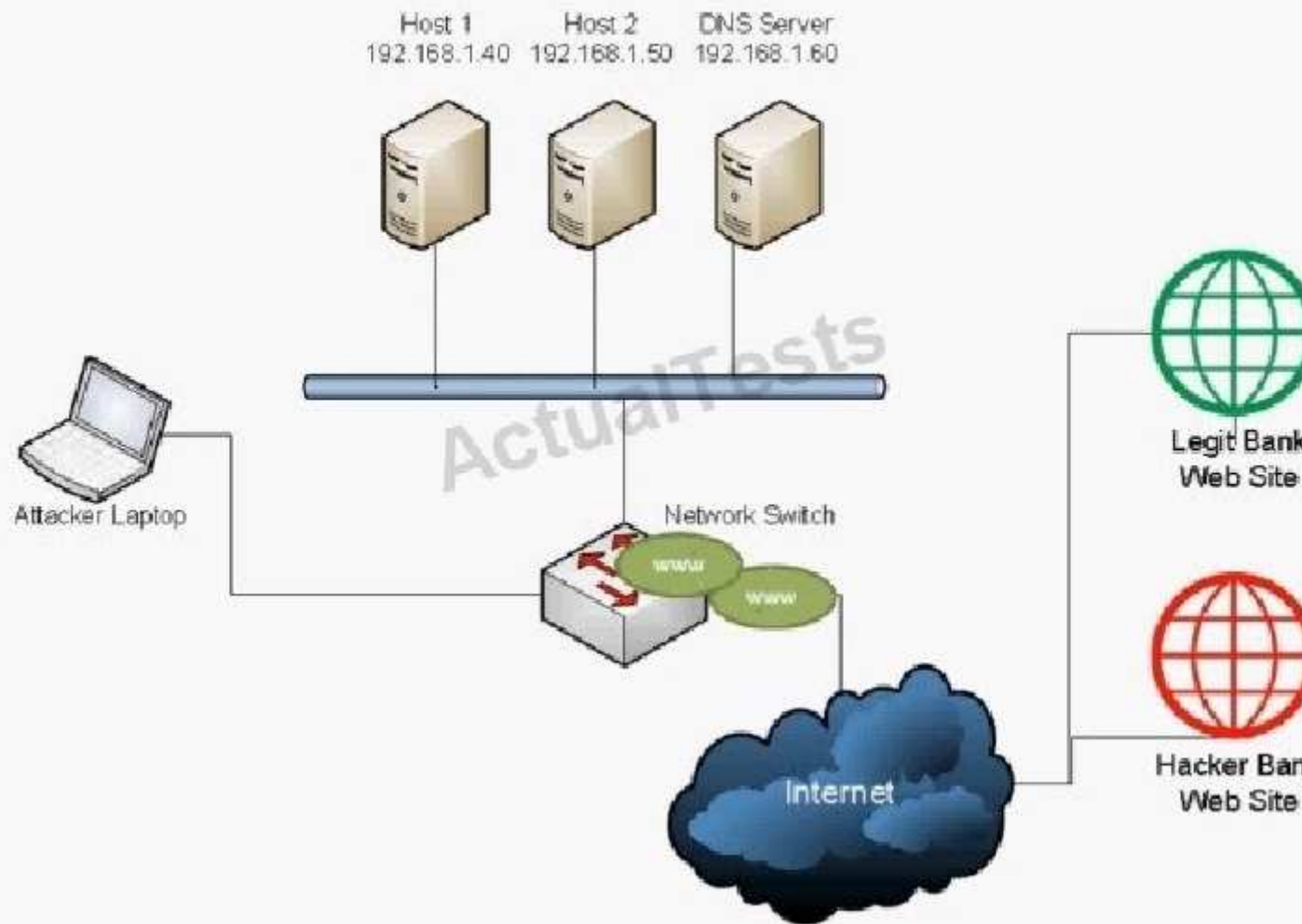
Explanation/Reference:

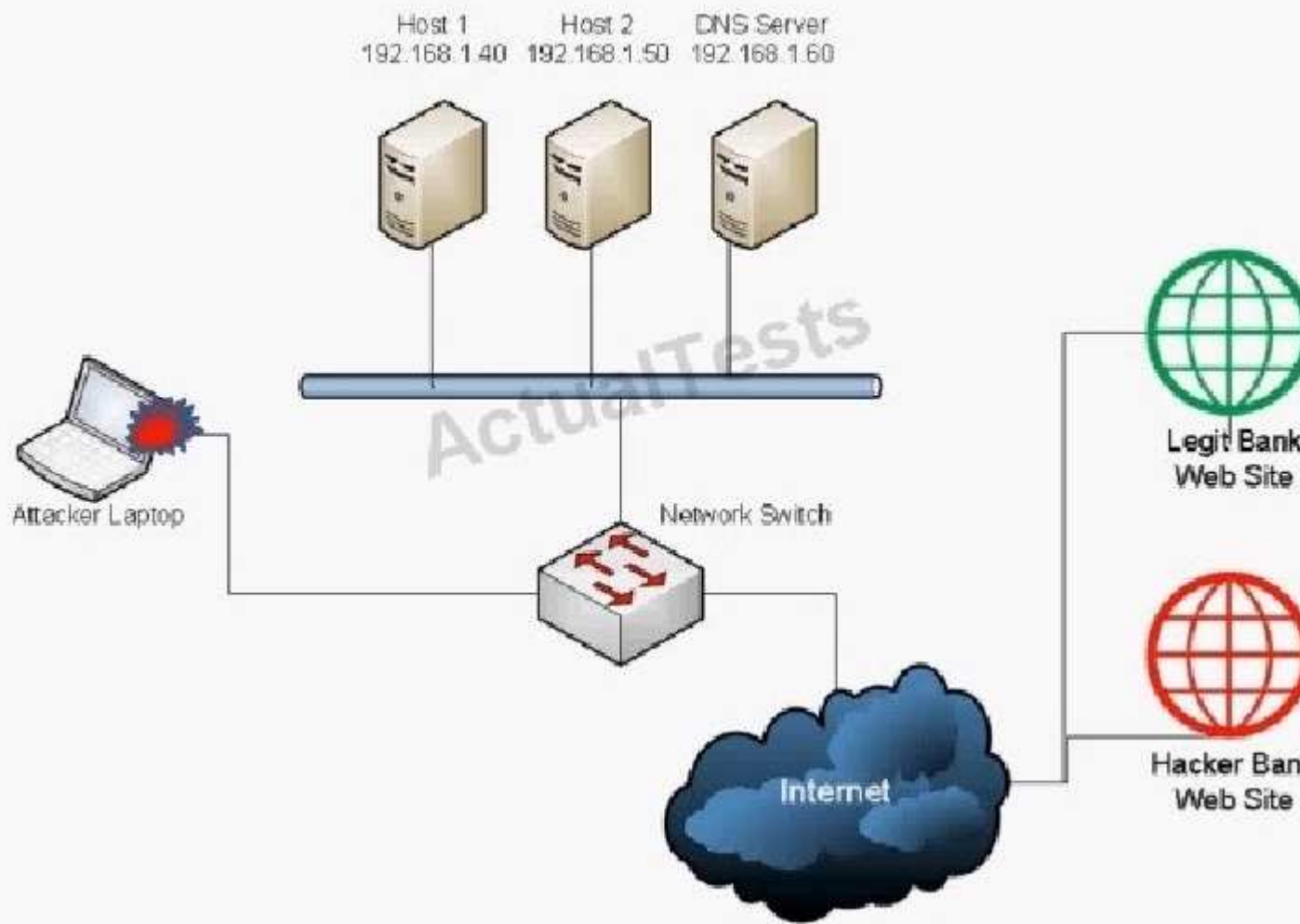
FTP	21
Telnet	23
SMTP	25
SNMP	161
SCP	22
TFTP	69

QUESTION 4

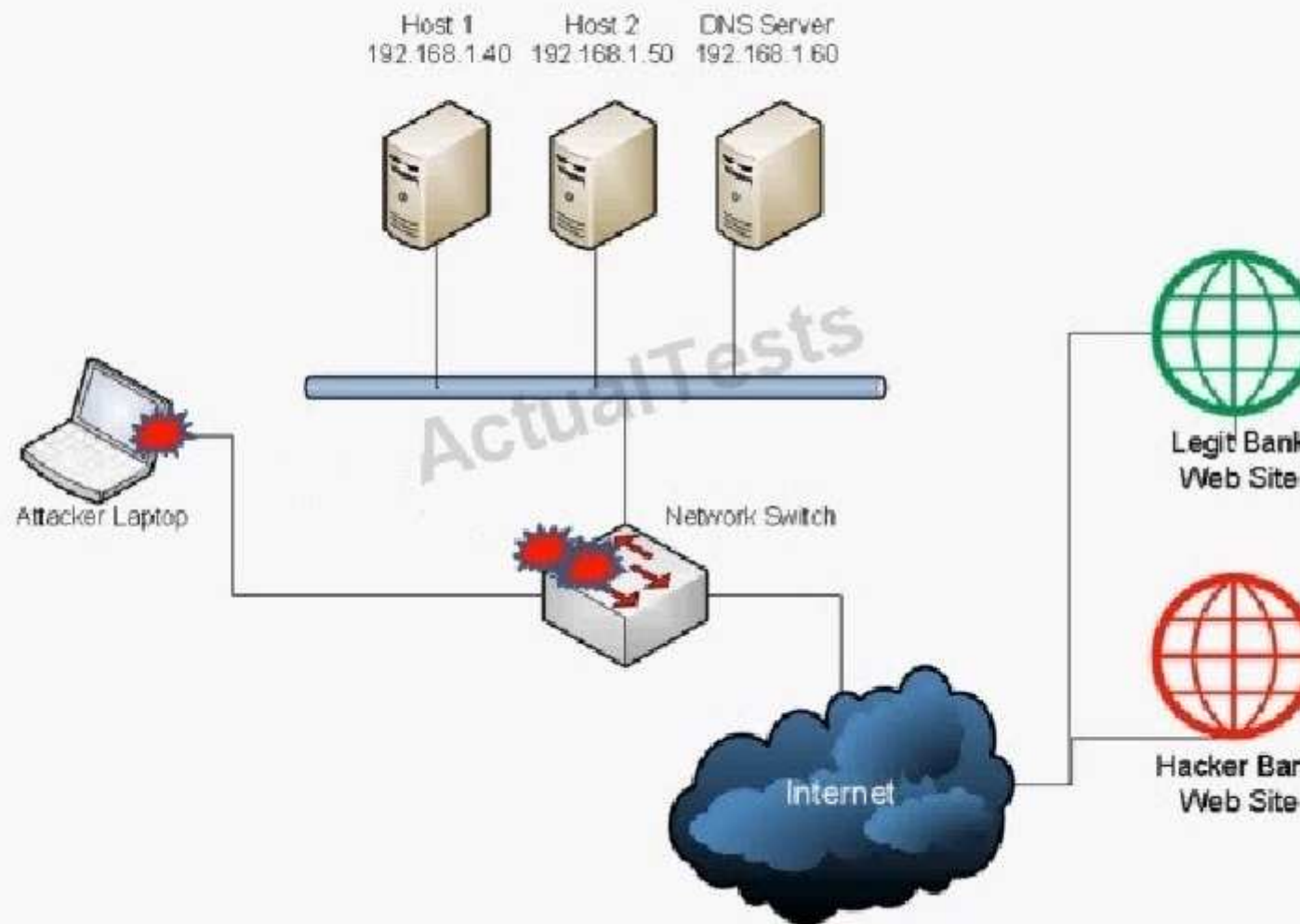
-- Exhibit

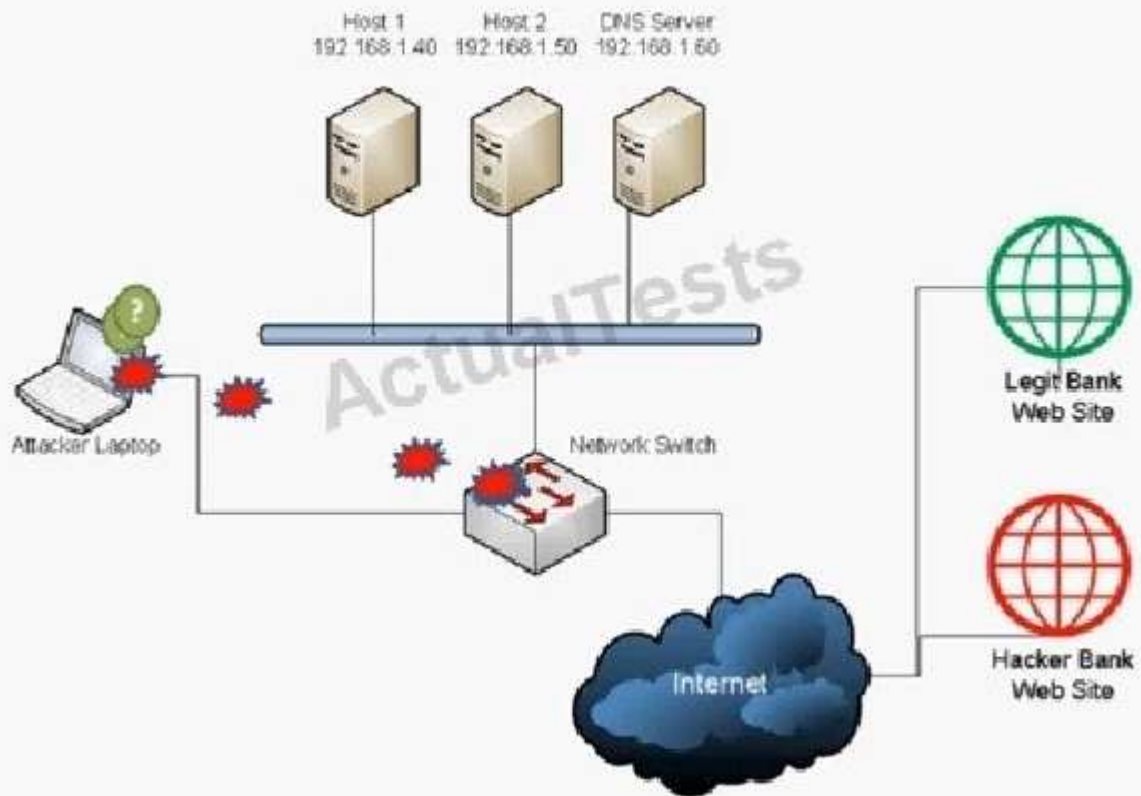


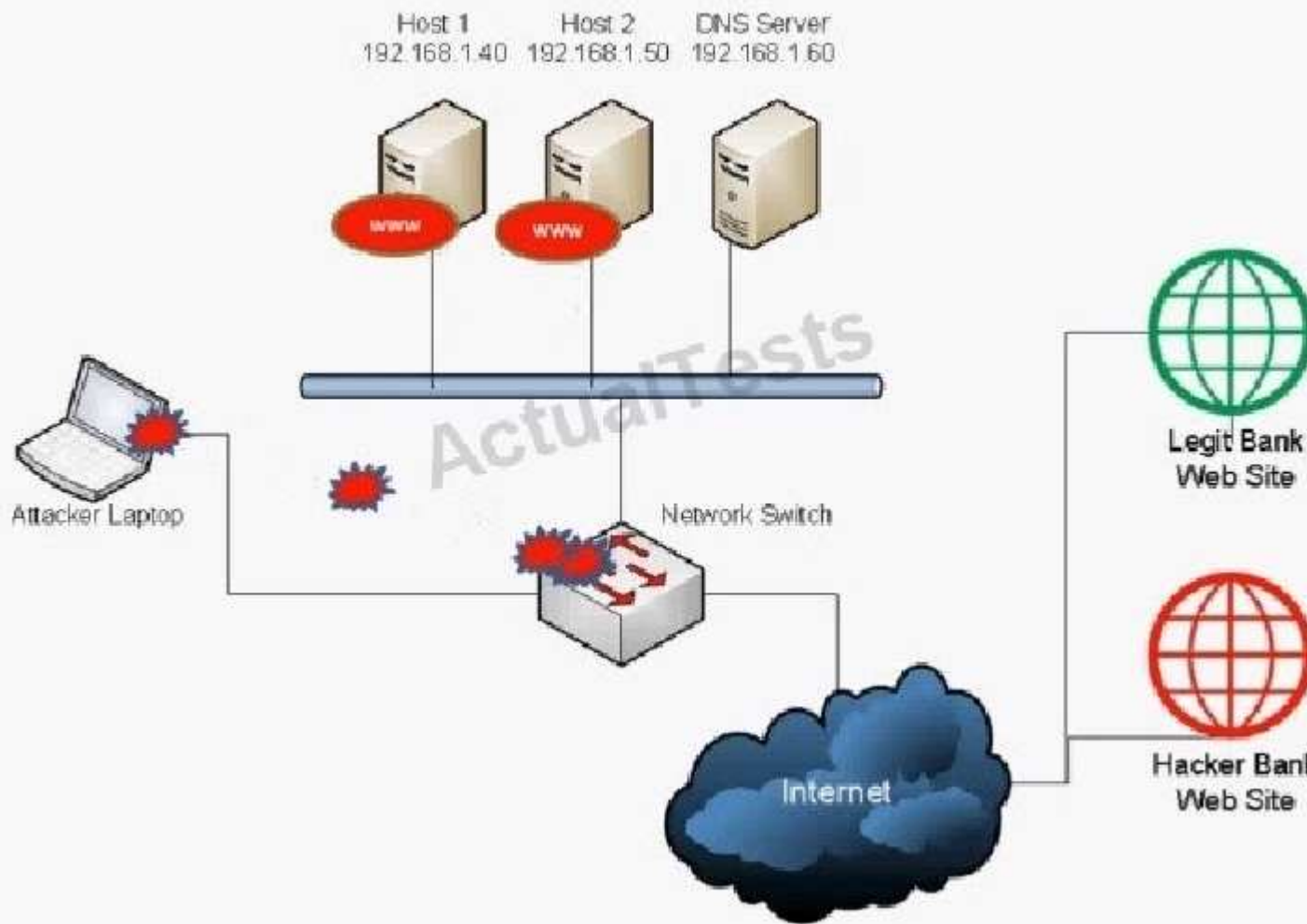


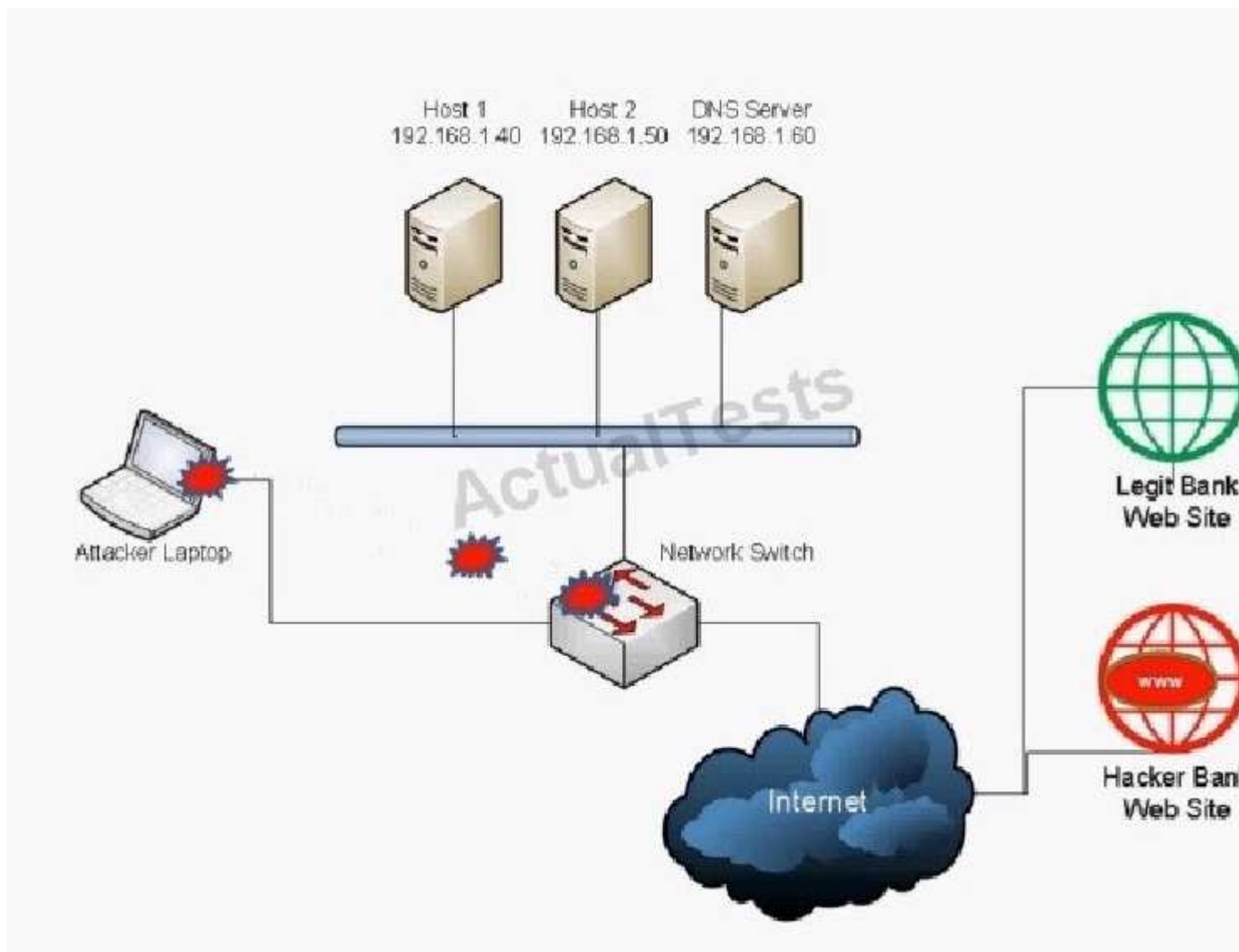












-- Exhibit --

Which of the following BEST describes the type of attack that is occurring? (Select TWO).

- A. DNS spoofing
- B. Man-in-the-middle
- C. Backdoor
- D. Replay
- E. ARP attack
- F. Spear phishing
- G. Xmas attack

**Correct Answer:** AE

**Section:** (none)

**Explanation**

**Explanation/Reference:**



<http://www.gratisexam.com/>