

Comptia.Actualtests.SY0-301.v2013-11-26.by.NANCY.943q

Number: SY0-301
Passing Score: 750
Time Limit: 90 min
File Version: 22.5



<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?

- 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).



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

- 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

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 78

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 79

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 80

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 81

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 82

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 83

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 84

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 85

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 86

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 87

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 88

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 89

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 90

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 91

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 92**

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 93**

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 94**

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 95

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 96

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 97

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 98

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 99

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 100

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 101

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 102

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 103

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 104

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 105

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 106

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 107

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 108

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 109

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 110

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 111

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 112

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 113

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 114

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 115

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 116

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 117

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 118

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 119

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 120

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 121

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 122

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 123

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 124

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 125

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 126

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 127

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 128

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 129

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 130

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 131

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 132

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 133

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 134

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 135

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 136

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 137

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 138

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 139

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 140

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 141

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 142

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 143

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 144

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 145

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 146

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 147

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. RIPEMD
- C. WEP
- D. LEAP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 148

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 149

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 150

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 151

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 152

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 153

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 154

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 155

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 156

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 157

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 158

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 159

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 160

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 161

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 162

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 163

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 164

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 165

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 166

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 167

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 168

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 169

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 170

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 171

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 172

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 173

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 174

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 175

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 176

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 177

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 178

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 179

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 180

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 181

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 182

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 183

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 184

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 185

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 186

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 187

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 188

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 189

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 190

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 191

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 192

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 193

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 194

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 195

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 196

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 197

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 198

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 199

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 200

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 201

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 202

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 203

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 204

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 205

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 206

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 207

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 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 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 209

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 210

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 211

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 212

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 213

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 214

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 215

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 216

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 217

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 218

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 219

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 220

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 221

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 222

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 223

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 224

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 225

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 226

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 227

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 228

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 229

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 230

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 231

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 232

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 233

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 234

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 235

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 236

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 237

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 238

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 239

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 240

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 241

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 242

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 243

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 244

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 245**

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 246**

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 247**

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 248

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 249

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 250

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 251

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 252

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 253

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 254

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 255

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 256

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 257

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 258

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 259

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 260

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 261

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 262

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 263

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 264

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 265

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 266

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 267

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 268

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 269

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 270

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 271

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 272

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 273

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 274

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 275

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 276

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 277

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 278

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 279

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 280

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 281

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 282

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 283

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 284

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 285

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 286

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 287

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 288

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 289

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 290

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 291

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 292

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 293

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 294

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 295

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 296

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 297

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 298

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 299

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 300

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 301

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 302

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 303

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 304

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 305

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 306

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 307

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 308

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 309

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 310

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 311

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 312

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 313

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 314

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 315

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 316

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 317

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 318

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 319

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 320

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 321

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 322

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 323

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 324

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 325

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 326

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 327

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 328

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 329

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 330

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 331

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 332

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 333

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 334

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 335

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 336

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 337

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 338

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 339

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 340

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 341

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 342

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 343

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 344

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 345

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 346

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 347

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 348

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 349

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 350

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 351

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 352

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 353

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 354

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 355

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 356

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 357

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 358

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 359

A username provides which of the following?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 360

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 361

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 362

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 363

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 364

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 365

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 366

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 367

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 368

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 369**

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
- C. FTP
- D. HTTPS

Correct Answer: B

Section: (none)

Explanation**Explanation/Reference:****QUESTION 370**

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 371**

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 372**

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 373

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 374

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 375

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 376

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 377

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 378

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 379

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 380

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 381

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 382

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 383

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 384

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 385

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 386

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 387

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 388

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 389

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 390

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 391

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 392

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 393

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 394

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 395

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 396

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 397

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 398

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 399

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 400

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 401

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 402

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 403

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 404

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 405

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 406

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 407

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 408

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 409

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 410

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 411

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 412

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 413

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 414

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 415

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 416

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 417

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 418

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 419

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 420

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 421

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 422

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 423

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 424

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 425

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 426

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 427

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 428

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 429

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 430

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 431

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 432

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 433

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 434

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 435

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 436

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 437

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 438

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 439

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 440

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 441

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 442

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 443

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 444

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 445

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 446

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 447

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 448

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 449

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 450

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 451

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 452

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 453

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 454

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 455

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 456

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 457

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 458

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 459

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 460

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 461

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 462

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 463

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 464

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 465

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 466

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 467

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 468

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 469

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 470

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 471

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 472

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 473

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 474

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 475

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 476

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 477

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 478

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 479

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 480

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 481

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 482

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 483

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 484

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 485

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 486

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 487

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 488

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 489

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 490

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 491

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 492

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 493

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 494

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 495

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 496

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 497

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 498

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 499

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 500**

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 501**

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 502**

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 503**

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 504

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 505

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 506

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 507

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 508

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 509

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 510

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 511

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 512

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 513

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 514

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 515

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 516

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 517

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 518

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 519

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 520

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 521

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 522

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 523

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 524

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 525

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 526

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 527

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 528

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 529

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 530

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 531

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 532

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 533

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 534

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 535

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 536

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 537

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 538

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 539

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 540

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 541

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 542

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 543

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 544

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 545

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 546

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 547

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 548

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



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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 549

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 550

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 551

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 552

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 553

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 554

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 555

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 556

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 557

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 558

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 559

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 560

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 561

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 562

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 563

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 564

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 565

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 566

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 567

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 568

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 569

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 570

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 571

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 572

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 573

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 574

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 575

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 576

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 577

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 578

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 579

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 580

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 581

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 582

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 583

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 584

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 585

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 586

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 587

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 588

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 589

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 590

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 591

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 592

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 593

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 594

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 595

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 596

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 597

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 598

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 599

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 600

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 601

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 602

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 603

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 604

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 605

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 606

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 607

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 608

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 609

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 610

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 611

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 612

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 613

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 614

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 615

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 616

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 617

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 618

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 619

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 620

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 621

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 622

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 623

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 624

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 625

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 626

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 627

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 628

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 629

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 630

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 631

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 632

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 633

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 634

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 635

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 636

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 637

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 638

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 639

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 640

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 641

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 642

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 643

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:

QUESTION 644

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 645

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 646

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 647

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 648

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 649

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 650

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:

QUESTION 651

Which of the following must be kept secret for a public key infrastructure to remain secure?

- A. Certificate Authority
- B. Certificate revocation list

- C. Public key ring
- D. Private key

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 652

Which of the following devices is BEST suited to protect an HTTP-based application that is susceptible to injection attacks?

- A. Protocol filter
- B. Load balancer
- C. NIDS
- D. Layer 7 firewall

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 653

Which of the following is best practice to put at the end of an ACL?

- A. Implicit deny
- B. Time of day restrictions
- C. Implicit allow
- D. SNMP string

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 654

An achievement in providing worldwide Internet security was the signing of certificates associated with which of the following protocols?

- A. TCP/IP
- B. SSL
- C. SCP
- D. SSH

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 655

A Chief Information Security Officer (CISO) wants to implement two-factor authentication within the company. Which of the following would fulfill the CISO's requirements?

- A. Username and password
- B. Retina scan and fingerprint scan
- C. USB token and PIN
- D. Proximity badge and token

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 656

Which of the following can a security administrator implement on mobile devices that will help prevent unwanted people from viewing the data if the device is left unattended?

- A. Screen lock
- B. Voice encryption
- C. GPS tracking
- D. Device encryption

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 657

Which of the following security concepts can prevent a user from logging on from home during the weekends?

- A. Time of day restrictions
- B. Multifactor authentication
- C. Implicit deny
- D. Common access card

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 658

Which of the following would provide the STRONGEST encryption?

- A. Random one-time pad
- B. DES with a 56-bit key
- C. AES with a 256-bit key

D. RSA with a 1024-bit key

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 659

During a server audit, a security administrator does not notice abnormal activity. However, a network security analyst notices connections to unauthorized ports from outside the corporate network. Using specialized tools, the network security analyst also notices hidden processes running. Which of the following has MOST likely been installed on the server?

- A. SPIM
- B. Backdoor
- C. Logic bomb
- D. Rootkit

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 660

A security administrator wants to ensure that the message the administrator sends out to their Chief Financial Officer (CFO) does not get changed in route. Which of the following is the administrator MOST concerned with?

- A. Data confidentiality
- B. High availability
- C. Data integrity
- D. Business continuity

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 661

Which of the following can be performed when an element of the company policy cannot be enforced by technical means?

- A. Develop a set of standards
- B. Separation of duties
- C. Develop a privacy policy
- D. User training

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 662

Timestamps and sequence numbers act as countermeasures against which of the following types of attacks?

- A. Smurf
- B. DoS
- C. Vishing
- D. Replay

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 663

Which of the following would be used as a secure substitute for Telnet?

- A. SSH
- B. SFTP
- C. SSL
- D. HTTPS

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 664

Which of the following is described as an attack against an application using a malicious file?

- A. Client side attack
- B. Spam
- C. Impersonation attack
- D. Phishing attack

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 665

Which of the following assessment techniques would a security administrator implement to ensure that systems and software are developed properly?

- A. Baseline reporting
- B. Input validation
- C. Determine attack surface

D. Design reviews

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 666

Which of the following would a security administrator implement in order to identify a problem between two applications that are not communicating properly?

- A. Protocol analyzer
- B. Baseline report
- C. Risk assessment
- D. Vulnerability scan

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 667

Which of the following would a security administrator implement in order to identify change from the standard configuration on a server?

- A. Penetration test
- B. Code review
- C. Baseline review
- D. Design review

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 668

Which of the following tools would a security administrator use in order to identify all running services throughout an organization?

- A. Architectural review
- B. Penetration test
- C. Port scanner
- D. Design review

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 669

Which of the following protocols provides transport security for virtual terminal emulation?

- A. TLS
- B. SSH
- C. SCP
- D. S/MIME

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 670

Based on information leaked to industry websites, business management is concerned that unauthorized employees are accessing critical project information for a major, well-known new product. To identify any such users, the security administrator could:

- A. Set up a honeypot and place false project documentation on an unsecure share.
- B. Block access to the project documentation using a firewall.
- C. Increase antivirus coverage of the project servers.
- D. Apply security updates and harden the OS on all project servers.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 671

A set of standardized system images with a pre-defined set of applications is used to build end-user workstations. The security administrator has scanned every workstation to create a current inventory of all applications that are installed on active workstations and is documenting which applications are out-of-date and could be exploited. The security administrator is determining the:

- A. Attack surface.
- B. Application hardening effectiveness.
- C. Application baseline.
- D. OS hardening effectiveness.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 672

A perimeter survey finds that the wireless network within a facility is easily reachable outside of the physical perimeter. Which of the following should be adjusted to mitigate this risk?

- A. CCMP

- B. MAC filter
- C. SSID broadcast
- D. Power level controls

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 673

Which of the following would verify that a threat does exist and security controls can easily be bypassed without actively testing an application?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 674

Connections using point-to-point protocol authenticate using which of the following? (Select TWO).

- A. RIPEMD
- B. PAP
- C. CHAP
- D. RC4
- E. Kerberos

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 675

Which of the following will help prevent smurf attacks?

- A. Allowing necessary UDP packets in and out of the network
- B. Disabling directed broadcast on border routers
- C. Disabling unused services on the gateway firewall
- D. Flash the BIOS with the latest firmware

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 676

An advantage of virtualizing servers, databases, and office applications is:

- A. Centralized management.
- B. Providing greater resources to users.
- C. Stronger access control.
- D. Decentralized management.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 677

A major security risk with co-mingling of hosts with different security requirements is:

- A. Security policy violations.
- B. Zombie attacks.
- C. Password compromises.
- D. Privilege creep.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 678

Which of the following attacks targets high level executives to gain company information?

- A. Phishing
- B. Whaling
- C. Vishing
- D. Spoofing

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 679

Which of the following can be used as an equipment theft deterrent?

- A. Screen locks
- B. GPS tracking
- C. Cable locks
- D. Whole disk encryption

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 680

At the outside break area, an employee, Ann, asked another employee to let her into the building because her badge is missing. Which of the following does this describe?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 681

A company that has a mandatory vacation policy has implemented which of the following controls?

- A. Risk control
- B. Privacy control
- C. Technical control
- D. Physical control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 682

Which of the following is the MOST intrusive type of testing against a production system?

- A. White box testing
- B. War dialing
- C. Vulnerability testing
- D. Penetration testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 683

The IT department has installed new wireless access points but discovers that the signal extends far into the

parking lot. Which of the following actions should be taken to correct this?

- A. Disable the SSID broadcasting
- B. Configure the access points so that MAC filtering is not used
- C. Implement WEP encryption on the access points
- D. Lower the power for office coverage only

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 684

The helpdesk reports increased calls from clients reporting spikes in malware infections on their systems. Which of the following phases of incident response is MOST appropriate as a FIRST response?

- A. Recovery
- B. Follow-up
- C. Validation
- D. Identification
- E. Eradication
- F. Containment

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 685

Which of the following protocols would be used to verify connectivity between two remote devices at the HIGHEST level of the OSI model?

- A. ICMP
- B. IPSec
- C. SCP
- D. TCP

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 686

Which of the following devices would be MOST useful to ensure availability when there are a large number of requests to a certain website?

- A. Protocol analyzer
- B. Load balancer
- C. VPN concentrator

D. Web security gateway

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 687

Which of the following uses port 22 by default? (Select THREE).

- A. SSH
- B. SSL
- C. TLS
- D. SFTP
- E. SCP
- F. FTPS
- G. SMTP
- H. SNMP

Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 688

Ann, a software developer, has installed some code to reactivate her account one week after her account has been disabled. Which of the following is this an example of? (Select TWO).

- A. Rootkit
- B. Logic Bomb
- C. Botnet
- D. Backdoor
- E. Spyware

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 689

The string:

' or 1=1-- -

represents which of the following?

- A. Bluejacking
- B. Rogue access point
- C. SQL Injection

D. Client-side attacks

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 690

Joe, an administrator, installs a web server on the Internet that performs credit card transactions for customer payments. Joe also sets up a second web server that looks like the first web server. However, the second server contains fabricated files and folders made to look like payments were processed on this server but really were not. Which of the following is the second server?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 691

Which of the following can Joe, a security administrator, implement on his network to capture attack details that are occurring while also protecting his production network?

- A. Security logs
- B. Protocol analyzer
- C. Audit logs
- D. Honeypot

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 692

Ann, a security technician, is reviewing the IDS log files. She notices a large number of alerts for multicast packets from the switches on the network. After investigation, she discovers that this is normal activity for her network. Which of the following BEST describes these results?

- A. True negatives
- B. True positives
- C. False positives
- D. False negatives

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 693

Joe, a security analyst, asks each employee of an organization to sign a statement saying that they understand how their activities may be monitored. Which of the following BEST describes this statement? (Select TWO).

- A. Acceptable use policy
- B. Risk acceptance policy
- C. Privacy policy
- D. Email policy
- E. Security policy

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 694

A process in which the functionality of an application is tested without any knowledge of the internal mechanisms of the application is known as:

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 695

Which of the following tools would allow Ann, the security administrator, to be able to BEST quantify all traffic on her network?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 696

Which of the following should an administrator implement to research current attack methodologies?

- A. Design reviews
- B. Honeypot
- C. Vulnerability scanner
- D. Code reviews

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 697

Which of the following consists of peer assessments that help identify security threats and vulnerabilities?

- A. Risk Assessment
- B. Code reviews
- C. Baseline reporting
- D. Alarms

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 698

Ann is starting a disaster recovery program. She has gathered specifics and team members for a meeting on site. Which of the following types of tests is this?

- A. Structured walk through
- B. Full Interruption test
- C. Check list test
- D. Table top exercise

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 699

An internal auditing team would like to strengthen the password policy to support special characters. Which of the following types of password controls would achieve this goal?

- A. Add reverse encryption
- B. Password complexity
- C. Increase password length
- D. Allow single sign on

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 700

Which of the following can be implemented in hardware or software to protect a web server from cross-site scripting attacks?

- A. Intrusion Detection System
- B. Flood Guard Protection
- C. Web Application Firewall
- D. URL Content Filter

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 701

Ann, the software security engineer, works for a major software vendor. Which of the following practices should be implemented to help prevent race conditions, buffer overflows, and other similar vulnerabilities prior to each production release?

- A. Product baseline report
- B. Input validation
- C. Patch regression testing
- D. Code review

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 702

Ann, a security analyst, is preparing for an upcoming security audit. To ensure that she identifies unapplied security controls and patches without attacking or compromising the system, Ann would use which of the following?

- A. Vulnerability scanning
- B. SQL injection
- C. Penetration testing
- D. Antivirus update

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 703

Ann, the security administrator, received a report from the security technician, that an unauthorized new user

account was added to the server over two weeks ago. Which of the following could have mitigated this event?

- A. Routine log audits
- B. Job rotation
- C. Risk likelihood assessment
- D. Separation of duties

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 704

Which of the following ports should be opened on a firewall to allow for NetBIOS communication? (Select TWO).

- A. 110
- B. 137
- C. 139
- D. 143
- E. 161
- F. 443

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 705

Joe, the systems administrator, is setting up a wireless network for his team's laptops only and needs to prevent other employees from accessing it. Which of the following would BEST address this?

- A. Disable default SSID broadcasting.
- B. Use WPA instead of WEP encryption.
- C. Lower the access point's power settings.
- D. Implement MAC filtering on the access point.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 706

After Ann, a user, logs into her banking websites she has access to her financial institution mortgage, credit card, and brokerage websites as well. Which of the following is being described?

- A. Trusted OS
- B. Mandatory access control
- C. Separation of duties

D. Single sign-on

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 707

Which of the following means of wireless authentication is easily vulnerable to spoofing?

- A. MAC Filtering
- B. WPA - LEAP
- C. WPA - PEAP
- D. Enabled SSID

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 708

Which of the following is a way to implement a technical control to mitigate data loss in case of a mobile device theft?

- A. Disk encryption
- B. Encryption policy
- C. Solid state drive
- D. Mobile device policy

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 709

The BEST methods for a web developer to prevent the website application code from being vulnerable to cross-site request forgery (XSRF) is to: (Select TWO).

- A. Permit redirection to Internet-facing web URLs.
- B. Ensure all HTML tags are enclosed in angle brackets, e.g., "<" and ">".
- C. Validate and filter input on the server side and client side.
- D. Use a web proxy to pass website requests between the user and the application.
- E. Restrict and sanitize use of special characters in input and URLs.

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 710

When an order was submitted via the corporate website, an administrator noted special characters (e.g., “;--” and “or 1=1 --”) were input instead of the expected letters and numbers. Which of the following is the MOST likely reason for the unusual results?

- A. The user is attempting to hijack the web server session using an open-source browser.
- B. The user has been compromised by a cross-site scripting attack (XSS) and is part of a botnet performing DDoS attacks.
- C. The user is attempting to fuzz the web server by entering foreign language characters which are incompatible with the website.
- D. The user is sending malicious SQL injection strings in order to extract sensitive company or customer data via the website.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 711

When a communications plan is developed for disaster recovery and business continuity plans, the MOST relevant items to include would be: (Select TWO).

- A. Methods and templates to respond to press requests, institutional and regulatory reporting requirements.
- B. Methods to exchange essential information to and from all response team members, employees, suppliers, and customers.
- C. Developed recovery strategies, test plans, post-test evaluation and update processes.
- D. Defined scenarios by type and scope of impact and dependencies, with quantification of loss potential.
- E. Methods to review and report on system logs, incident response, and incident handling.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 712

Key elements of a business impact analysis should include which of the following tasks?

- A. Develop recovery strategies, prioritize recovery, create test plans, post-test evaluation, and update processes.
- B. Identify institutional and regulatory reporting requirements, develop response teams and communication trees, and develop press release templates.
- C. Employ regular preventive measures such as patch management, change management, antivirus and vulnerability scans, and reports to management.
- D. Identify critical assets systems and functions, identify dependencies, determine critical downtime limit, define scenarios by type and scope of impact, and quantify loss potential.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 713

End-user awareness training for handling sensitive personally identifiable information would include secure storage and transmission of customer:

- A. Date of birth.
- B. First and last name.
- C. Phone number.
- D. Employer name.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 714

Jane, a security administrator, needs to implement a secure wireless authentication method that uses a remote RADIUS server for authentication. Which of the following authentication methods should Jane use?

- A. WPA2-PSK
- B. WEP-PSK
- C. CCMP
- D. LEAP

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 715

Which of the following risk mitigation strategies will allow Ann, a security analyst, to enforce least privilege principles?

- A. User rights reviews
- B. Incident management
- C. Risk based controls
- D. Annual loss expectancy

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 716

The security officer is preparing a read-only USB stick with a document of important personal phone numbers, vendor contacts, an MD5 program, and other tools to provide to employees. At which of the following points in an incident should the officer instruct employees to use this information?

- A. Business Impact Analysis
- B. First Responder
- C. Damage and Loss Control
- D. Contingency Planning

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 717

To ensure proper evidence collection, which of the following steps should be preformed FIRST?

- A. Take hashes from the live system
- B. Review logs
- C. Capture the system image
- D. Copy all compromised files

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 718

Joe, the security administrator, has determined that one of his web servers is under attack. Which of the following can help determine where the attack originated from?

- A. Capture system image
- B. Record time offset
- C. Screenshots
- D. Network sniffing

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 719

Joe, the system administrator, is performing an overnight system refresh of hundreds of user computers. The refresh has a strict timeframe and must have zero downtime during business hours. Which of the following should Joe take into consideration?

- A. A disk-based image of every computer as they are being replaced.
- B. A plan that skips every other replaced computer to limit the area of affected users.
- C. An offsite contingency server farm that can act as a warm site should any issues appear.
- D. A back-out strategy planned out anticipating any unforeseen problems that may arise.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 720

A program displays:

ERROR: this program has caught an exception and will now terminate.

Which of the following is MOST likely accomplished by the program's behavior?

- A. Operating system's integrity is maintained
- B. Program's availability is maintained
- C. Operating system's scalability is maintained
- D. User's confidentiality is maintained

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 721

A security administrator wants to deploy a physical security control to limit an individual's access into a sensitive area. Which of the following should be implemented?

- A. Guards
- B. CCTV
- C. Bollards
- D. Spike strip

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 722

A network administrator uses an RFID card to enter the datacenter, a key to open the server rack, and a username and password to logon to a server. These are examples of which of the following?

- A. Multifactor authentication
- B. Single factor authentication
- C. Separation of duties
- D. Identification

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 723

Which of the following results in datacenters with failed humidity controls? (Select TWO).

- A. Excessive EMI
- B. Electrostatic charge
- C. Improper ventilation
- D. Condensation
- E. Irregular temperature

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 724

An online store wants to protect user credentials and credit card information so that customers can store their credit card information and use their card for multiple separate transactions. Which of the following database designs provides the BEST security for the online store?

- A. Use encryption for the credential fields and hash the credit card field
- B. Encrypt the username and hash the password
- C. Hash the credential fields and use encryption for the credit card field
- D. Hash both the credential fields and the credit card field

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 725

A network administrator is configuring access control for the sales department which has high employee turnover. Which of the following is BEST suited when assigning user rights to individuals in the sales department?

- A. Time of day restrictions
- B. Group based privileges
- C. User assigned privileges
- D. Domain admin restrictions

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 726

A security administrator is reviewing the below output from a password auditing tool:

P@ss.

@pW1.

S3cU4

Which of the following additional policies should be implemented based on the tool's output?

- A. Password age
- B. Password history
- C. Password length
- D. Password complexity

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 727

Joe, a user, in a coffee shop is checking his email over a wireless network. An attacker records the temporary credentials being passed to Joe's browser. The attacker later uses the credentials to impersonate Joe and creates SPAM messages. Which of the following attacks allows for this impersonation?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 728

A security architect wishes to implement a wireless network with connectivity to the company's internal network. Before they inform all employees that this network is being put in place, the architect wants to roll it out to a small test segment. Which of the following allows for greater secrecy about this network during this initial phase of implementation?

- A. Disabling SSID broadcasting
- B. Implementing WPA2 - TKIP
- C. Implementing WPA2 - CCMP
- D. Filtering test workstations by MAC address

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 729

Digital certificates can be used to ensure which of the following? (Select TWO).

- A. Availability

- B. Confidentiality
- C. Verification
- D. Authorization
- E. Non-repudiation

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 730

A network administrator is looking for a way to automatically update company browsers so they import a list of root certificates from an online source. This online source will then be responsible for tracking which certificates are to be trusted or not trusted. Which of the following BEST describes the service that should be implemented to meet these requirements?

- A. Trust model
- B. Key escrow
- C. OCSP
- D. PKI

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 731

A security administrator has concerns about new types of media which allow for the mass distribution of personal comments to a select group of people. To mitigate the risks involved with this media, employees should receive training on which of the following?

- A. Peer to Peer
- B. Mobile devices
- C. Social networking
- D. Personally owned devices

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 732

A network administrator is responsible for securing applications against external attacks. Every month, the underlying operating system is updated. There is no process in place for other software updates. Which of the following processes could MOST effectively mitigate these risks?

- A. Application hardening
- B. Application change management
- C. Application patch management

D. Application firewall review

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 733

The software developer is responsible for writing the code and promoting from the development network to the quality network. The network administrator is responsible for promoting code to the production application servers. Which of the following practices are they following to ensure application integrity?

- A. Job rotation
- B. Implicit deny
- C. Least privilege
- D. Separation of duties

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 734

A software developer is responsible for writing the code on an accounting application. Another software developer is responsible for developing code on a system in human resources. Once a year they have to switch roles for several weeks. Which of the following practices is being implemented?

- A. Mandatory vacations
- B. Job rotation
- C. Least privilege
- D. Separation of duties

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 735

A quality assurance analyst is reviewing a new software product for security, and has complete access to the code and data structures used by the developers. This is an example of which of the following types of testing?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 736

The security consultant is assigned to test a client's new software for security, after logs show targeted attacks from the Internet. To determine the weaknesses, the consultant has no access to the application program interfaces, code, or data structures. This is an example of which of the following types of testing?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 737

Which of the following types of cryptography should be used when minimal overhead is necessary for a mobile device?

- A. Block cipher
- B. Elliptical curve cryptography
- C. Diffie-Hellman algorithm
- D. Stream cipher

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 738

The server administrator has noted that most servers have a lot of free disk space and low memory utilization. Which of the following statements will be correct if the server administrator migrates to a virtual server environment?

- A. The administrator will need to deploy load balancing and clustering.
- B. The administrator may spend more on licensing but less on hardware and equipment.
- C. The administrator will not be able to add a test virtual environment in the data center.
- D. Servers will encounter latency and lowered throughput issues.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 739

Which of the following implementation steps would be appropriate for a public wireless hot-spot?

- A. Reduce power level
- B. Disable SSID broadcast
- C. Open system authentication
- D. MAC filter

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 740

Configuring key/value pairs on a RADIUS server is associated with deploying which of the following?

- A. WPA2-Enterprise wireless network
- B. DNS secondary zones
- C. Digital certificates
- D. Intrusion detection system

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 741

Which of the following preventative controls would be appropriate for responding to a directive to reduce the attack surface of a specific host?

- A. Installing anti-malware
- B. Implementing an IDS
- C. Taking a baseline configuration
- D. Disabling unnecessary services

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 742

A security analyst performs the following activities: monitors security logs, installs surveillance cameras and analyzes trend reports. Which of the following job responsibilities is the analyst performing? (Select TWO).

- A. Detect security incidents
- B. Reduce attack surface of systems
- C. Implement monitoring controls
- D. Hardening network devices
- E. Prevent unauthorized access

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 743

A certificate used on an ecommerce web server is about to expire. Which of the following will occur if the certificate is allowed to expire?

- A. The certificate will be added to the Certificate Revocation List (CRL).
- B. Clients will be notified that the certificate is invalid.
- C. The ecommerce site will not function until the certificate is renewed.
- D. The ecommerce site will no longer use encryption.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 744

An administrator needs to segment internal traffic between layer 2 devices within the LAN. Which of the following types of network design elements would MOST likely be used?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 745

The security administrator needs to restrict traffic on a layer 3 device to support FTP from a new remote site. Which of the following secure network administration principles will need to be implemented?

- A. Implicit deny
- B. VLAN management
- C. Port security
- D. Access control lists

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 746

After a network outage, a PC technician is unable to ping various network devices. The network administrator verifies that those devices are working properly and can be accessed securely. Which of the following is the

MOST likely reason the PC technician is unable to ping those devices?

- A. ICMP is being blocked
- B. SSH is not enabled
- C. DNS settings are wrong
- D. SNMP is not configured properly

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 747

Which of the following ports is used for SSH, by default?

- A. 23
- B. 32
- C. 12
- D. 22

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 748

The security administrator has been tasked to update all the access points to provide a more secure connection. All access points currently use WPA TKIP for encryption. Which of the following would be configured to provide more secure connections?

- A. WEP
- B. WPA2 CCMP
- C. Disable SSID broadcast and increase power levels
- D. MAC filtering

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 749

After a recent security breach, the network administrator has been tasked to update and backup all router and switch configurations. The security administrator has been tasked to enforce stricter security policies. All users were forced to undergo additional user awareness training. All of these actions are due to which of the following types of risk mitigation strategies?

- A. Change management
- B. Implementing policies to prevent data loss
- C. User rights and permissions review

D. Lessons learned

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 750

Various network outages have occurred recently due to unapproved changes to network and security devices. All changes were made using various system credentials. The security analyst has been tasked to update the security policy. Which of the following risk mitigation strategies would also need to be implemented to reduce the number of network outages due to unauthorized changes?

- A. User rights and permissions review
- B. Configuration management
- C. Incident management
- D. Implement security controls on Layer 3 devices

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 751

Which of the following concepts is used by digital signatures to ensure integrity of the data?

- A. Non-repudiation
- B. Hashing
- C. Transport encryption
- D. Key escrow

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 752

A security analyst discovered data such as images and word documents hidden within different types of files. Which of the following cryptographic concepts describes what was discovered?

- A. Symmetric encryption
- B. Non-repudiation
- C. Steganography
- D. Hashing

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 753

Which of the following concepts describes the use of a one way transformation in order to validate the integrity of a program?

- A. Hashing
- B. Key escrow
- C. Non-repudiation
- D. Steganography

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 754

A network administrator has been tasked with securing the WLAN. Which of the following cryptographic products would be used to provide the MOST secure environment for the WLAN?

- A. WPA2 CCMP
- B. WPA
- C. WPA with MAC filtering
- D. WPA2 TKIP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 755

Recent data loss on financial servers due to security breaches forced the system administrator to harden their systems. Which of the following algorithms with transport encryption would be implemented to provide the MOST secure web connections to manage and access these servers?

- A. SSL
- B. TLS
- C. HTTP
- D. FTP

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 756

Which of the following provides a static record of all certificates that are no longer valid?

- A. Private key
- B. Recovery agent

- C. CRLs
- D. CA

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 757

A company requires that a user's credentials include providing something they know and something they are in order to gain access to the network. Which of the following types of authentication is being described?

- A. Biometrics
- B. Kerberos
- C. Token
- D. Two-factor

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 758

A company wants to ensure that all credentials for various systems are saved within a central database so that users only have to login once for access to all systems. Which of the following would accomplish this?

- A. Multi-factor authentication
- B. Smart card access
- C. Same Sign-On
- D. Single Sign-On

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 759

A server with the IP address of 10.10.2.4 has been having intermittent connection issues. The logs show repeated connection attempts from the following IP:

10.10.3.23

These attempts are overloading the server to the point that it cannot respond to traffic. Which of the following attacks is occurring?

- A. Xmas
- B. DDoS
- C. DoS
- D. XSS

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 760

Physical documents must be incinerated after a set retention period is reached. Which of the following attacks does this action remediate?

- A. Shoulder Surfing
- B. Dumpster Diving
- C. Phishing
- D. Impersonation

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 761

All executive officers have changed their monitor location so it cannot be easily viewed when passing by their offices. Which of the following attacks does this action remediate?

- A. Dumpster Diving
- B. Impersonation
- C. Shoulder Surfing
- D. Whaling

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 762

Which of the following protocols is vulnerable to man-in-the-middle attacks by NOT using end to end TLS encryption?

- A. HTTPS
- B. WEP
- C. WPA
- D. WPA 2

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 763

A security administrator has been tasked with setting up a new internal wireless network that must use end to end TLS. Which of the following may be used to meet this objective?

- A. WPA
- B. HTTPS
- C. WEP
- D. WPA 2

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 764

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 techniques are used above? (Select TWO).

- A. Blue snarfing
- B. Evil twin
- C. Packet sniffing
- D. War dialing
- E. Rogue access point

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 765

A server administrator notes that a legacy application often stops running due to a memory error. When reviewing the debugging logs, they notice code being run calling an internal process to exploit the machine. Which of the following attacks does this describe?

- A. Zero-day
- B. Buffer overflow
- C. Cross site scripting
- D. Malicious add-on

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 766

Key cards at a bank are not tied to individuals, but rather to organizational roles. After a break in, it becomes apparent that extra efforts must be taken to successfully pinpoint who exactly enters secure areas. Which of the following security measures can be put in place to mitigate the issue until a new key card system can be installed?

- A. Bollards
- B. Video surveillance
- C. Proximity readers
- D. Fencing

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 767

After running into the data center with a vehicle, attackers were able to enter through the hole in the building and steal several key servers in the ensuing chaos. Which of the following security measures can be put in place to mitigate the issue from occurring in the future?

- A. Fencing
- B. Proximity readers
- C. Video surveillance
- D. Bollards

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 768

Which of the following ciphers would be BEST used to encrypt streaming video?

- A. RSA
- B. RC4
- C. SHA1
- D. 3DES

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 769

A CA is compromised and attacks start distributing maliciously signed software updates. Which of the following can be used to warn users about the malicious activity?

- A. Key escrow
- B. Private key verification
- C. Public key verification
- D. Certificate revocation list

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 770

After encrypting all laptop hard drives, an executive officer's laptop has trouble booting to the operating system. Now that it is successfully encrypted the helpdesk cannot retrieve the data. Which of the following can be used to decrypt the information for retrieval?

- A. Recovery agent
- B. Private key
- C. Trust models
- D. Public key

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 771

Which of the following devices is MOST likely being used when processing the following?

1 PERMIT IP ANY ANY EQ 80

2 DENY IP ANY ANY

- A. Firewall
- B. NIPS
- C. Load balancer
- D. URL filter

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 772

The security administrator at ABC company received the following log information from an external party:

10:45:01 EST, SRC 10.4.3.7:3056, DST 8.4.2.1:80, ALERT, Directory traversal

10:45:02 EST, SRC 10.4.3.7:3057, DST 8.4.2.1:80, ALERT, Account brute force

10:45:03 EST, SRC 10.4.3.7:3058, DST 8.4.2.1:80, ALERT, Port scan

The external party is reporting attacks coming from abc-company.com. Which of the following is the reason the ABC company's security administrator is unable to determine the origin of the attack?

- A. A NIDS was used in place of a NIPS.
- B. The log is not in UTC.
- C. The external party uses a firewall.
- D. ABC company uses PAT.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 773

A user attempting to log on to a workstation for the first time is prompted for the following information before being granted access: username, password, and a four-digit security pin that was mailed to him during account registration. This is an example of which of the following?

- A. Dual-factor authentication
- B. Multifactor authentication
- C. Single factor authentication
- D. Biometric authentication

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 774

The security administrator is implementing a malware storage system to archive all malware seen by the company into a central database. The malware must be categorized and stored based on similarities in the code. Which of the following should the security administrator use to identify similar malware?

- A. TwoFish
- B. SHA-512
- C. Fuzzy hashes
- D. HMAC

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 775

The security administrator installed a newly generated SSL certificate onto the company web server. Due to a mis-configuration of the website, a downloadable file containing one of the pieces of the key was available to the public. It was verified that the disclosure did not require a reissue of the certificate. Which of the following was MOST likely compromised?

- A. The file containing the recovery agent's keys.
- B. The file containing the public key.
- C. The file containing the private key.
- D. The file containing the server's encrypted passwords.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 776

After analyzing and correlating activity from multiple sensors, the security administrator has determined that a group of very well organized individuals from an enemy country is responsible for various attempts to breach the company network, through the use of very sophisticated and targeted attacks. Which of the following is this an example of?

- A. Privilege escalation
- B. Advanced persistent threat
- C. Malicious insider threat
- D. Spear phishing

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 777

Which of the following was launched against a company based on the following IDS log?

```
122.41.15.252 - - [21/May/2012:00:17:20 +1200] "GET
/index.php?username=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAA HTTP/1.1" 200 2731 "http://www.company.com/cgi-
bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1; Hotbar 4.4.7.0)"
```

- A. SQL injection
- B. Buffer overflow attack
- C. XSS attack
- D. Online password crack

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 778

The security administrator is analyzing a user's history file on a Unix server to determine if the user was attempting to break out of a rootjail. Which of the following lines in the user's history log shows evidence that the user attempted to escape the rootjail?

- A. `cd ../../../../bin/bash`
- B. `whoami`
- C. `ls /root`
- D. `sudo -u root`

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 779

A software development company has hired a programmer to develop a plug-in module to an existing proprietary application. After completing the module, the developer needs to test the entire application to ensure that the module did not introduce new vulnerabilities. Which of the following is the developer performing when testing the application?

- A. Black box testing
- B. White box testing
- C. Gray box testing
- D. Design review

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 780

A security administrator must implement all requirements in the following corporate policy:

- Passwords shall be protected against offline password brute force attacks.
- Passwords shall be protected against online password brute force attacks.

Which of the following technical controls must be implemented to enforce the corporate policy? (Select THREE).

- A. Account lockout
- B. Account expiration
- C. Screen locks
- D. Password complexity
- E. Minimum password lifetime
- F. Minimum password length

Correct Answer: ADF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 781

Which of the following is a best practice for error and exception handling?

- A. Log detailed exception but display generic error message
- B. Display detailed exception but log generic error message
- C. Log and display detailed error and exception messages
- D. Do not log or display error or exception messages

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 782

A merchant acquirer has the need to store credit card numbers in a transactional database in a high performance environment. Which of the following BEST protects the credit card data?

- A. Database field encryption
- B. File-level encryption
- C. Data loss prevention system
- D. Full disk encryption

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 783

A team of firewall administrators have access to a 'master password list' containing service account passwords. Which of the following BEST protects the master password list?

- A. File encryption
- B. Password hashing
- C. USB encryption
- D. Full disk encryption

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 784

An SSL/TLS private key is installed on a corporate web proxy in order to inspect HTTPS requests. Which of the following describes how this private key should be stored so that it is protected from theft?

- A. Implement full disk encryption
- B. Store on encrypted removable media
- C. Utilize a hardware security module
- D. Store on web proxy file system

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 785

An insurance company requires an account recovery process so that information created by an employee can be accessed after that employee is no longer with the firm. Which of the following is the BEST approach to implement this process?

- A. Employee is required to share their password with authorized staff prior to leaving the firm
- B. Passwords are stored in a reversible form so that they can be recovered when needed
- C. Authorized employees have the ability to reset passwords so that the data is accessible
- D. All employee data is exported and imported by the employee prior to them leaving the firm

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 786

A small company has a website that provides online customer support. The company requires an account recovery process so that customers who forget their passwords can regain access. Which of the following is the BEST approach to implement this process?

- A. Replace passwords with hardware tokens which provide two-factor authentication to the online customer support site.
- B. Require the customer to physically come into the company's main office so that the customer can be authenticated prior to their password being reset.
- C. Web-based form that identifies customer by another mechanism and then emails the customer their forgotten password.
- D. Web-based form that identifies customer by another mechanism, sets a temporary password and forces a password change upon first login.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 787

A bank has a fleet of aging payment terminals used by merchants for transactional processing. The terminals currently support single DES but require an upgrade in order to be compliant with security standards. Which of the following is likely to be the simplest upgrade to the aging terminals which will improve in-transit protection of transactional data?

- A. AES
- B. 3DES
- C. RC4
- D. WPA2

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 788

A new MPLS network link has been established between a company and its business partner. The link provides logical isolation in order to prevent access from other business partners. Which of the following should be applied in order to achieve confidentiality and integrity of all data across the link?

- A. MPLS should be run in IPVPN mode.
- B. SSL/TLS for all application flows.
- C. IPSec VPN tunnels on top of the MPLS link.
- D. HTTPS and SSH for all application flows.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 789

Which of the following authentication services should be replaced with a more secure alternative?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 790

A financial company requires a new private network link with a business partner to cater for real-time and batched data flows. Which of the following activities should be performed by the IT security staff member prior to establishing the link?

- A. Baseline reporting
- B. Design review
- C. Code review
- D. SLA reporting

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 791

A customer has provided an email address and password to a website as part of the login process. Which of the following BEST describes the email address?

- A. Identification
- B. Authorization
- C. Access control
- D. Authentication

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 792

Which of the following is designed to ensure high availability of web based applications?

- A. Proxies
- B. Load balancers
- C. URL filtering
- D. Routers

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 793

After a number of highly publicized and embarrassing customer data leaks as a result of social engineering attacks by phone, the Chief Information Officer (CIO) has decided user training will reduce the risk of another data leak. Which of the following would be MOST effective in reducing data leaks in this situation?

- A. Information Security Awareness
- B. Social Media and BYOD
- C. Data Handling and Disposal
- D. Acceptable Use of IT Systems

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 794

Human Resources (HR) would like executives to undergo only two specific security training programs a year. Which of the following provides the BEST level of security training for the executives? (Select TWO).

- A. Acceptable use of social media
- B. Data handling and disposal
- C. Zero day exploits and viruses
- D. Phishing threats and attacks

- E. Clean desk and BYOD
- F. Information security awareness

Correct Answer: DF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 795

Which of the following provides data the best fault tolerance at the LOWEST cost?

- A. Load balancing
- B. Clustering
- C. Server virtualization
- D. RAID 6

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 796

The librarian wants to secure the public Internet kiosk PCs at the back of the library. Which of the following would be the MOST appropriate? (Select TWO).

- A. Device encryption
- B. Antivirus
- C. Privacy screen
- D. Cable locks
- E. Remote wipe

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 797

Which of the following functions provides an output which cannot be reversed and converts data into a string of characters?

- A. Hashing
- B. Stream ciphers
- C. Steganography
- D. Block ciphers

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 798

Which of the following encrypts data a single bit at a time?

- A. Stream cipher
- B. Steganography
- C. 3DES
- D. Hashing

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 799

A system administrator wants to enable WPA2 CCMP. Which of the following is the only encryption used?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 800

Which of the following is used to verify data integrity?

- A. SHA
- B. 3DES
- C. AES
- D. RSA

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 801

Two programmers write a new secure application for the human resources department to store personal identifiable information. The programmers make the application available to themselves using an uncommon port along with an ID and password only they know. This is an example of which of the following?

- A. Root Kit
- B. Spyware

- C. Logic Bomb
- D. Backdoor

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 802

Everyone in the accounting department has the ability to print and sign checks. Internal audit has asked that only one group of employees may print checks while only two other employees may sign the checks. Which of the following concepts would enforce this process?

- A. Separation of Duties
- B. Mandatory Vacations
- C. Discretionary Access Control
- D. Job Rotation

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 803

The security department has implemented a new laptop encryption product in the environment. The product requires one user name and password at the time of boot up and also another password after the operating system has finished loading. This setup is using which of the following authentication types?

- A. Two-factor authentication
- B. Single sign-on
- C. Multifactor authentication
- D. Single factor authentication

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 804

The Human Resources department has a parent shared folder setup on the server. There are two groups that have access, one called managers and one called staff. There are many sub folders under the parent shared folder, one is called payroll. The parent folder access control list propagates all subfolders and all subfolders inherit the parent permission. Which of the following is the quickest way to prevent the staff group from gaining access to the payroll folder?

- A. Remove the staff group from the payroll folder
- B. Implicit deny on the payroll folder for the staff group
- C. Implicit deny on the payroll folder for the managers group
- D. Remove inheritance from the payroll folder

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 805

The finance department works with a bank which has recently had a number of cyber attacks. The finance department is concerned that the banking website certificates have been compromised. Which of the following can the finance department check to see if any of the bank's certificates are still valid?

- A. Bank's CRL
- B. Bank's private key
- C. Bank's key escrow
- D. Bank's recovery agent

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 806

Which of the following are examples of network segmentation? (Select TWO).

- A. IDS
- B. IaaS
- C. DMZ
- D. Subnet
- E. IPS

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 807

Which of the following provides the strongest authentication security on a wireless network?

- A. MAC filter
- B. WPA2
- C. WEP
- D. Disable SSID broadcast

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 808

Which of the following provides the BEST explanation regarding why an organization needs to implement IT security policies?

- A. To ensure that false positives are identified
- B. To ensure that staff conform to the policy
- C. To reduce the organizational risk
- D. To require acceptable usage of IT systems

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 809

An incident response team member needs to perform a forensics examination but does not have the required hardware. Which of the following will allow the team member to perform the examination with minimal impact to the potential evidence?

- A. Using a software file recovery disc
- B. Mounting the drive in read-only mode
- C. Imaging based on order of volatility
- D. Hashing the image after capture

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 810

Which of the following allows an organization to store a sensitive PKI component with a trusted third party?

- A. Trust model
- B. Public Key Infrastructure
- C. Private key
- D. Key escrow

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 811

Which of the following security devices can be replicated on a Linux based computer using IP tables to inspect and properly handle network based traffic?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 812

A software firm posts patches and updates to a publicly accessible FTP site. The software firm also posts digitally signed checksums of all patches and updates. The firm does this to address:

- A. Integrity of downloaded software.
- B. Availability of the FTP site.
- C. Confidentiality of downloaded software.
- D. Integrity of the server logs.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 813

An administrator has successfully implemented SSL on srv4.comptia.com using wildcard certificate *.comptia.com, and now wishes to implement SSL on srv5.comptia.com. Which of the following files should be copied from srv4 to accomplish this?

- A. certificate, private key, and intermediate certificate chain
- B. certificate, intermediate certificate chain, and root certificate
- C. certificate, root certificate, and certificate signing request
- D. certificate, public key, and certificate signing request

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 814

When reviewing security logs, an administrator sees requests for the AAAA record of www.comptia.com. Which of the following BEST describes this type of record?

- A. DNSSEC record
- B. IPv4 DNS record
- C. IPSEC DNS record
- D. IPv6 DNS record

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 815

Which of the following practices reduces the management burden of access management?

- A. Password complexity policies
- B. User account audit
- C. Log analysis and review
- D. Group based privileges

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 816

Which of the following helps to apply the proper security controls to information?

- A. Data classification
- B. Deduplication
- C. Clean desk policy
- D. Encryption

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 817

Which of the following describes purposefully injecting extra input during testing, possibly causing an application to crash?

- A. Input validation
- B. Exception handling
- C. Application hardening
- D. Fuzzing

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 818

Which of the following types of security services are used to support authentication for remote users and devices?

- A. Biometrics
- B. HSM
- C. RADIUS
- D. TACACS

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 819

A Chief Information Security Officer (CISO) is tasked with outsourcing the analysis of security logs. These will need to still be reviewed on a regular basis to ensure the security of the company has not been breached. Which of the following cloud service options would support this requirement?

- A. SaaS
- B. MaaS
- C. IaaS
- D. PaaS

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 820

A security administrator needs a locally stored record to remove the certificates of a terminated employee. Which of the following describes a service that could meet these requirements?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 821

A security analyst informs the Chief Executive Officer (CEO) that a security breach has just occurred. This results in the Risk Manager and Chief Information Officer (CIO) being caught unaware when the CEO asks for further information. Which of the following strategies should be implemented to ensure the Risk Manager and CIO are not caught unaware in the future?

- A. Procedure and policy management
- B. Chain of custody management
- C. Change management
- D. Incident management

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 822

Which of the following relies on the use of shared secrets to protect communication?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 823

A security administrator wants to test the reliability of an application which accepts user provided parameters. The administrator is concerned with data integrity and availability. Which of the following should be implemented to accomplish this task?

- A. Secure coding
- B. Fuzzing
- C. Exception handling
- D. Input validation

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 824

Which of the following concepts is a term that directly relates to customer privacy considerations?

- A. Data handling policies
- B. Personally identifiable information
- C. Information classification
- D. Clean desk policies

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 825

Which of the following is a Data Loss Prevention (DLP) strategy and is MOST useful for securing data in use?

- A. Email scanning
- B. Content discovery

- C. Database fingerprinting
- D. Endpoint protection

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 826

Which of the following is a concern when encrypting wireless data with WEP?

- A. WEP displays the plain text entire key when wireless packet captures are reassembled
- B. WEP implements weak initialization vectors for key transmission
- C. WEP uses a very weak encryption algorithm
- D. WEP allows for only four pre-shared keys to be configured

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 827

A security administrator is tasked with calculating the total ALE on servers. In a two year period of time, a company has to replace five servers. Each server replacement has cost the company \$4,000 with downtime costing \$3,000. Which of the following is the ALE for the company?

- A. \$7,000
- B. \$10,000
- C. \$17,500
- D. \$35,000

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 828

ABC company has a lot of contractors working for them. The provisioning team does not always get notified that a contractor has left the company. Which of the following policies would prevent contractors from having access to systems in the event a contractor has left?

- A. Annual account review
- B. Account expiration policy
- C. Account lockout policy
- D. Account disablement

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 829

The practice of marking open wireless access points is called which of the following?

- A. War dialing
- B. War chalking
- C. War driving
- D. Evil twin

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 830

Multi-tenancy is a concept found in which of the following?

- A. Full disk encryption
- B. Removable media
- C. Cloud computing
- D. Data loss prevention

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 831

Which of the following is a common coding error in which boundary checking is not performed?

- A. Input validation
- B. Fuzzing
- C. Secure coding
- D. Cross-site scripting

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 832

While previously recommended as a security measure, disabling SSID broadcast is not effective against most attackers because network SSIDs are:

- A. no longer used to authenticate to most wireless networks.
- B. contained in certain wireless packets in plaintext.

- C. contained in all wireless broadcast packets by default.
- D. no longer supported in 802.11 protocols.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 833

One of the most consistently reported software security vulnerabilities that leads to major exploits is:

- A. Lack of malware detection.
- B. Attack surface decrease.
- C. Inadequate network hardening.
- D. Poor input validation.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 834

Public key certificates and keys that are compromised or were issued fraudulently are listed on which of the following?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 835

One of the most basic ways to protect the confidentiality of data on a laptop in the event the device is physically stolen is to implement which of the following?

- A. File level encryption with alphanumeric passwords
- B. Biometric authentication and cloud storage
- C. Whole disk encryption with two-factor authentication
- D. BIOS passwords and two-factor authentication

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 836

Users report that after downloading several applications, their systems' performance has noticeably decreased. Which of the following would be used to validate programs prior to installing them?

- A. Whole disk encryption
- B. SSH
- C. Telnet
- D. MD5

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 837

Ann, 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 she notices several pictures of the employee's pets are on the hard drive and on a cloud storage network. When Ann 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 838

A malicious user is sniffing a busy encrypted wireless network waiting for an authorized client to connect to it. Only after an authorized client has connected and the hacker was able to capture the client handshake with the AP can the hacker begin a brute force attack to discover the encryption key. Which of the following attacks is taking place?

- A. IV attack
- B. WEP cracking
- C. WPA cracking
- D. Rogue AP

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 839

Which of the following protocols is used by IPv6 for MAC address resolution?

- A. NDP
- B. ARP
- C. DNS
- D. NCP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 840

Which of the following provides dedicated hardware-based cryptographic functions to an operating system and its applications running on laptops and desktops?

- A. TPM
- B. HSM
- C. CPU
- D. FPU

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 841

Which of the following tests a number of security controls in the least invasive manner?

- A. Vulnerability scan
- B. Threat assessment
- C. Penetration test
- D. Ping sweep

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 842

When using PGP, which of the following should the end user protect from compromise? (Select TWO).

- A. Private key
- B. CRL details
- C. Public key
- D. Key password
- E. Key escrow

F. Recovery agent

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 843

Which of the following disaster recovery strategies has the highest cost and shortest recovery time?

- A. Warm site
- B. Hot site
- C. Cold site
- D. Co-location site

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 844

In the case of a major outage or business interruption, the security office has documented the expected loss of earnings, potential fines and potential consequence to customer service. Which of the following would include the MOST detail on these objectives?

- A. Business Impact Analysis
- B. IT Contingency Plan
- C. Disaster Recovery Plan
- D. Continuity of Operations

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 845

After visiting a website, a user receives an email thanking them for a purchase which they did not request. Upon investigation the security administrator sees the following source code in a pop-up window:

```
<HTML>
```

```
<body onload="document.getElementById('badForm').submit()">
```

```
<form id="badForm" action="shoppingsite.company.com/purchase.php" method="post"
```

```
<input name="Perform Purchase" value="Perform Purchase" />
```

```
</form></body></HTML>
```

Which of the following has MOST likely occurred?

- A. SQL injection
- B. Cookie stealing
- C. XSRF
- D. XSS

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 846

Which of the following ports should be used by a system administrator to securely manage a remote server?

- A. 22
- B. 69
- C. 137
- D. 445

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 847

Which of the following ports is used to securely transfer files between remote UNIX systems?

- A. 21
- B. 22
- C. 69
- D. 445

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 848

Which of the following is a security benefit of providing additional HVAC capacity or increased tonnage in a datacenter?

- A. Increased availability of network services due to higher throughput
- B. Longer MTBF of hardware due to lower operating temperatures
- C. Higher data integrity due to more efficient SSD cooling
- D. Longer UPS run time due to increased airflow

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 849

Fuzzing is a security assessment technique that allows testers to analyze the behavior of software applications under which of the following conditions?

- A. Unexpected input
- B. Invalid output
- C. Parameterized input
- D. Valid output

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 850

Which of the following types of wireless attacks would be used specifically to impersonate another WAP in order to gain unauthorized information from mobile users?

- A. IV attack
- B. Evil twin
- C. War driving
- D. Rogue access point

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 851

Which of the following types of application attacks would be used to identify malware causing security breaches that have NOT yet been identified by any trusted sources?

- A. Zero-day
- B. LDAP injection
- C. XML injection
- D. Directory traversal

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 852

Which of the following is built into the hardware of most laptops but is not setup for centralized management by default?

- A. Whole disk encryption

- B. TPM encryption
- C. USB encryption
- D. Individual file encryption

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 853

Which of the following is true about the recovery agent?

- A. It can decrypt messages of users who lost their private key.
- B. It can recover both the private and public key of federated users.
- C. It can recover and provide users with their lost or private key.
- D. It can recover and provide users with their lost public key.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 854

Which of the following MOST specifically defines the procedures to follow when scheduled system patching fails resulting in system outages?

- A. Risk transference
- B. Change management
- C. Configuration management
- D. Access control revalidation

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 855

A review of the company's network traffic shows that most of the malware infections are caused by users visiting gambling and gaming websites. The security manager wants to implement a solution that will block these websites, scan all web traffic for signs of malware, and block the malware before it enters the company network. Which of the following is suited for this purpose?

- A. ACL
- B. IDS
- C. UTM
- D. Firewall

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 856

Which of the following would the security engineer set as the subnet mask for the servers below to utilize host addresses on separate broadcast domains?

Server 1: 192.168.100.6

Server 2: 192.168.100.9

Server 3: 192.169.100.20

- A. /24
- B. /27
- C. /28
- D. /29
- E. /30

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 857

Which of the following offerings typically allows the customer to apply operating system patches?

- A. Software as a service
- B. Public Clouds
- C. Cloud Based Storage
- D. Infrastructure as a service

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 858

A technician is unable to manage a remote server. Which of the following ports should be opened on the firewall for remote server management? (Select TWO).

- A. 22
- B. 135
- C. 137
- D. 143
- E. 443
- F. 3389

Correct Answer: AF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 859

Which of the following network design elements allows for many internal devices to share one public IP address?

- A. DNAT
- B. PAT
- C. DNS
- D. DMZ

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 860

When designing a new network infrastructure, a security administrator requests that the intranet web server be placed in an isolated area of the network for security purposes. Which of the following design elements would be implemented to comply with the security administrator's request?

- A. DMZ
- B. Cloud services
- C. Virtualization
- D. Sandboxing

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 861

Which of the following components of an all-in-one security appliance would MOST likely be configured in order to restrict access to peer-to-peer file sharing websites?

- A. Spam filter
- B. URL filter
- C. Content inspection
- D. Malware inspection

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 862

At an organization, unauthorized users have been accessing network resources via unused network wall jacks. Which of the following would be used to stop unauthorized access?

- A. Configure an access list.
- B. Configure spanning tree protocol.
- C. Configure port security.
- D. Configure loop protection.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 863

Users report that they are unable to access network printing services. The security technician checks the router access list and sees that web, email, and secure shell are allowed. Which of the following is blocking network printing?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 864

Joe, a security administrator, believes that a network breach has occurred in the datacenter as a result of a misconfigured router access list, allowing outside access to an SSH server. Which of the following should Joe search for in the log files?

- A. Failed authentication attempts
- B. Network ping sweeps
- C. Host port scans
- D. Connections to port 22

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 865

Which of the following firewall types inspects Ethernet traffic at the MOST levels of the OSI model?

- A. Packet Filter Firewall
- B. Stateful Firewall
- C. Proxy Firewall

D. Application Firewall

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 866

A security analyst needs to logon to the console to perform maintenance on a remote server. Which of the following protocols would provide secure access?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 867

The network administrator has been tasked to rebuild a compromised web server. The administrator is to remove the malware and install all the necessary updates and patches. This represents which of the following stages of the Incident Handling Response?

- A. Lessons Learned
- B. Plan of action
- C. Eradication
- D. Reconstitution

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 868

Management has been informed of an increased number of tailgating violations into the server room. Which of the following is the BEST method of preventing future violations?

- A. Security Guards
- B. Man Traps
- C. Proximity Cards
- D. Biometrics authentication

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 869

Ann, a newly hired human resource employee, sent out confidential emails with digital signatures, to an unintended group. Which of the following would prevent her from denying accountability?

- A. Email Encryption
- B. Steganography
- C. Non Repudiation
- D. Access Control

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 870

Ann would like to forward some Personal Identifiable Information to her HR department by email, but she is worried about the confidentiality of the information. Which of the following will accomplish this task securely?

- A. Digital Signatures
- B. Hashing
- C. Secret Key
- D. Encryption

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 871

Ann, a technician, is attempting to establish a remote terminal session to an end user's computer using Kerberos authentication, but she cannot connect to the destination machine. Which of the following default ports should Ann ensure is open?

- A. 22
- B. 139
- C. 443
- D. 3389

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 872

Concurrent use of a firewall, content filtering, antivirus software and an IDS system would be considered components of:

- A. Redundant systems.

- B. Separation of duties.
- C. Layered security.
- D. Application control.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 873

A company is trying to limit the risk associated with the use of unapproved USB devices to copy documents. Which of the following would be the BEST technology control to use in this scenario?

- A. Content filtering
- B. IDS
- C. Audit logs
- D. DLP

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 874

A company's employees were victims of a spear phishing campaign impersonating the CEO. The company would now like to implement a solution to improve the overall security posture by assuring their employees that email originated from the CEO. Which of the following controls could they implement to BEST meet this goal?

- A. Spam filter
- B. Digital signatures
- C. Antivirus software
- D. Digital certificates

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 875

Which of the following is a security risk regarding the use of public P2P as a method of collaboration?

- A. Data integrity is susceptible to being compromised.
- B. Monitoring data changes induces a higher cost.
- C. Users are not responsible for data usage tracking.
- D. Limiting the amount of necessary space for data storage.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 876

The method to provide end users of IT systems and applications with requirements related to acceptable use, privacy, new threats and trends, and use of social networking is:

- A. Security awareness training.
- B. BYOD security training.
- C. Role-based security training.
- D. Legal compliance training.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 877

After an audit, it was discovered that the security group memberships were not properly adjusted for employees' accounts when they moved from one role to another. Which of the following has the organization failed to properly implement? (Select TWO).

- A. Mandatory access control enforcement.
- B. User rights and permission reviews.
- C. Technical controls over account management.
- D. Account termination procedures.
- E. Management controls over account management.
- F. Incident management and response plan.

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 878

A security technician wishes to gather and analyze all Web traffic during a particular time period. Which of the following represents the BEST approach to gathering the required data?

- A. Configure a VPN concentrator to log all traffic destined for ports 80 and 443.
- B. Configure a proxy server to log all traffic destined for ports 80 and 443.
- C. Configure a switch to log all traffic destined for ports 80 and 443.
- D. Configure a NIDS to log all traffic destined for ports 80 and 443.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 879

A security administrator suspects that an increase in the amount of TFTP traffic on the network is due to unauthorized file transfers, and wants to configure a firewall to block all TFTP traffic. Which of the following would accomplish this task?

- A. Deny TCP port 68
- B. Deny TCP port 69
- C. Deny UDP port 68
- D. Deny UCP port 69

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 880

A company determines a need for additional protection from rogue devices plugging into physical ports around the building. Which of the following provides the highest degree of protection from unauthorized wired network access?

- A. Intrusion Prevention Systems
- B. MAC filtering
- C. Flood guards
- D. 802.1x

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 881

The Chief Technical Officer (CTO) is worried about an increased amount of malware detected on end user's workstations. Which of the following technologies should be recommended to detect such anomalies?

- A. NIDS
- B. Web content filter
- C. Host-based IDS
- D. Web application firewall

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 882

The network security engineer just deployed an IDS on the network, but the Chief Technical Officer (CTO) has concerns that the device is only able to detect known anomalies. Which of the following types of IDS has been deployed?

- A. Signature Based IDS

- B. Heuristic IDS
- C. Behavior Based IDS
- D. Anomaly Based IDS

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 883

Joe, a newly hired employee, has a corporate workstation that has been compromised due to several visits to P2P sites. Joe insisted that he was not aware of any company policy that prohibits the use of such web sites. Which of the following is the BEST method to deter employees from the improper use of the company's information systems?

- A. Acceptable Use Policy
- B. Privacy Policy
- C. Security Policy
- D. Human Resource Policy

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 884

A compromised workstation utilized in a Distributed Denial of Service (DDOS) attack has been removed from the network and an image of the hard drive has been created. However, the system administrator stated that the system was left unattended for several hours before the image was created. In the event of a court case, which of the following is likely to be an issue with this incident?

- A. Eye Witness
- B. Data Analysis of the hard drive
- C. Chain of custody
- D. Expert Witness

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 885

The Chief Technical Officer (CTO) has tasked The Computer Emergency Response Team (CERT) to develop and update all Internal Operating Procedures and Standard Operating Procedures documentation in order to successfully respond to future incidents. Which of the following stages of the Incident Handling process is the team working on?

- A. Lessons Learned
- B. Eradication
- C. Recovery

D. Preparation

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 886

Company XYZ recently salvaged company laptops and removed all hard drives, but the Chief Information Officer (CIO) is concerned about disclosure of confidential information. Which of the following is the MOST secure method to dispose of these hard drives?

- A. Degaussing
- B. Physical Destruction
- C. Lock up hard drives in a secure safe
- D. Wipe

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 887

During which of the following phases of the Incident Response process should a security administrator define and implement general defense against malware?

- A. Lessons Learned
- B. Preparation
- C. Eradication
- D. Identification

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 888

A company has recently implemented a high density wireless system by having a junior technician install two new access points for every access point already deployed. Users are now reporting random wireless disconnections and slow network connectivity. Which of the following is the MOST likely cause?

- A. The old APs use 802.11a
- B. Users did not enter the MAC of the new APs
- C. The new APs use MIMO
- D. A site survey was not conducted

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 889

A company provides secure wireless Internet access for visitors and vendors working onsite. Some of the vendors using older technology report that they are unable to access the wireless network after entering the correct network information. Which of the following is the MOST likely reason for this issue?

- A. The SSID broadcast is disabled.
- B. The company is using the wrong antenna type.
- C. The MAC filtering is disabled on the access point.
- D. The company is not using strong enough encryption.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 890

A company is looking to reduce the likelihood of employees in the finance department being involved with money laundering. Which of the following controls would BEST mitigate this risk?

- A. Implement privacy policies
- B. Enforce mandatory vacations
- C. Implement a security policy
- D. Enforce time of day restrictions

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 891

A company recently experienced data loss when a server crashed due to a midday power outage. Which of the following should be used to prevent this from occurring again?

- A. Recovery procedures
- B. EMI shielding
- C. Environmental monitoring
- D. Redundancy

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 892

Joe, a security administrator, is concerned with users tailgating into the restricted areas. Given a limited budget, which of the following would BEST assist Joe with detecting this activity?

- A. Place a full-time guard at the entrance to confirm user identity.
- B. Install a camera and DVR at the entrance to monitor access.
- C. Revoke all proximity badge access to make users justify access.
- D. Install a motion detector near the entrance.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 893

It is important to staff who use email messaging to provide PII to others on a regular basis to have confidence that their messages are not intercepted or altered during transmission. They are concerned about which of the following types of security control?

- A. Integrity
- B. Safety
- C. Availability
- D. Confidentiality

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 894

A security manager requires fencing around the perimeter, and cipher locks on all entrances. The manager is concerned with which of the following security controls?

- A. Integrity
- B. Availability
- C. Confidentiality
- D. Safety

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 895

A security engineer is reviewing log data and sees the output below:

POST: /payload.php HTTP/1.1

HOST: localhost

Accept: */*

Referrer: http://localhost/

HTTP/1.1 403 Forbidden

Connection: close

Log: Access denied with 403. Pattern matches form bypass

Which of the following technologies was MOST likely being used to generate this log?

- A. Host-based Intrusion Detection System
- B. Web application firewall
- C. Network-based Intrusion Detection System
- D. Stateful Inspection Firewall
- E. URL Content Filter

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 896

A security team has identified that the wireless signal is broadcasting into the parking lot. To reduce the risk of an attack against the wireless network from the parking lot, which of the following controls should be used? (Select TWO).

- A. Antenna placement
- B. Interference
- C. Use WEP
- D. Single Sign on
- E. Disable the SSID
- F. Power levels

Correct Answer: AF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 897

An organization does not have adequate resources to administer its large infrastructure. A security administrator wishes to integrate the security controls of some of the network devices in the organization. Which of the following methods would BEST accomplish this goal?

- A. Unified Threat Management
- B. Virtual Private Network
- C. Single sign on
- D. Role-based management

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 898

Which of the following would allow the organization to divide a Class C IP address range into several ranges?

- A. DMZ
- B. Virtual LANs
- C. NAT
- D. Subnetting

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 899

A company's legacy server requires administration using Telnet. Which of the following protocols could be used to secure communication by offering encryption at a lower OSI layer? (Select TWO).

- A. IPv6
- B. SFTP
- C. IPSec
- D. SSH
- E. IPv4

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 900

Joe, the Chief Technical Officer (CTO), is concerned about new malware being introduced into the corporate network. He has tasked the security engineers to implement a technology that is capable of alerting the team when unusual traffic is on the network. Which of the following types of technologies will BEST address this scenario?

- A. Application Firewall
- B. Anomaly Based IDS
- C. Proxy Firewall
- D. Signature IDS

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 901

A security administrator wishes to increase the security of the wireless network. Which of the following BEST

addresses this concern?

- A. Change the encryption from TKIP-based to CCMP-based.
- B. Set all nearby access points to operate on the same channel.
- C. Configure the access point to use WEP instead of WPA2.
- D. Enable all access points to broadcast their SSIDs.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 902

Which of the following describes the purpose of an MOU?

- A. Define interoperability requirements
- B. Define data backup process
- C. Define onboard/offboard procedure
- D. Define responsibilities of each party

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 903

The system administrator has deployed updated security controls for the network to limit risk of attack. The security manager is concerned that controls continue to function as intended to maintain appropriate security posture. Which of the following risk mitigation strategies is MOST important to the security manager?

- A. User permissions
- B. Policy enforcement
- C. Routine audits
- D. Change management

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 904

The security manager received a report that an employee was involved in illegal activity and has saved data to a workstation's hard drive. During the investigation, local law enforcement's criminal division confiscates the hard drive as evidence. Which of the following forensic procedures is involved?

- A. Chain of custody
- B. System image
- C. Take hashes
- D. Order of volatility

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 905

Environmental control measures include which of the following?

- A. Access list
- B. Lighting
- C. Motion detection
- D. EMI shielding

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 906

Which of the following is the BEST concept to maintain required but non-critical server availability?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 907

Prior to leaving for an extended vacation, Joe uses his mobile phone to take a picture of his family in the house living room. Joe posts the picture on a popular social media site together with the message: "Heading to our two weeks vacation to Italy." Upon returning home, Joe discovers that the house was burglarized. Which of the following is the MOST likely reason the house was burglarized if nobody knew Joe's home address?

- A. Joe has enabled the device access control feature on his mobile phone.
- B. Joe's home address can be easily found using the TRACEROUTE command.
- C. The picture uploaded to the social media site was geo-tagged by the mobile phone.
- D. The message posted on the social media site informs everyone the house will be empty.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 908

Which of the following technical controls helps to prevent Smartphones from connecting to a corporate network?

- A. Application white listing
- B. Remote wiping
- C. Acceptable use policy
- D. Mobile device management

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 909

The Chief Risk Officer is concerned about the new employee BYOD device policy and has requested the security department implement mobile security controls to protect corporate data in the event that a device is lost or stolen. The level of protection must not be compromised even if the communication SIM is removed from the device. Which of the following BEST meets the requirements? (Select TWO).

- A. Asset tracking
- B. Screen-locks
- C. Geo-tagging
- D. Patch management
- E. Device encryption

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 910

A way to assure data at-rest is secure even in the event of loss or theft is to use:

- A. Full device encryption.
- B. Special permissions on the file system.
- C. Trusted Platform Module integration.
- D. Access Control Lists.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 911

Which of the following would prevent a user from installing a program on a company-owned mobile device?

- A. White-listing
- B. Access control lists

- C. Geotagging
- D. Remote wipe

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 912

Which of the following can be used to maintain a higher level of security in a SAN by allowing isolation of mis-configurations or faults?

- A. VLAN
- B. Protocol security
- C. Port security
- D. VSAN

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 913

The act of magnetically erasing all of the data on a disk is known as:

- A. Wiping
- B. Dissolution
- C. Scrubbing
- D. Degaussing

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 914

LDAP and Kerberos are commonly used for which of the following?

- A. To perform queries on a directory service
- B. To store usernames and passwords for Federated Identity
- C. To sign SSL wildcard certificates for subdomains
- D. To utilize single sign-on capabilities

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 915

A recent audit has revealed weaknesses in the process of deploying new servers and network devices. Which of the following practices could be used to increase the security posture during deployment? (Select TWO).

- A. Deploy a honeypot
- B. Disable unnecessary services
- C. Change default passwords
- D. Implement an application firewall
- E. Penetration testing

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 916

Joe, a network security engineer, has visibility to network traffic through network monitoring tools. However, he's concerned that a disgruntled employee may be targeting a server containing the company's financial records. Which of the following security mechanism would be MOST appropriate to confirm Joe's suspicion?

- A. HIDS
- B. HIPS
- C. NIPS
- D. NIDS

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 917

Ann, a security administrator, wishes to replace their RADIUS authentication with a more secure protocol, which can utilize EAP. Which of the following would BEST fit her objective?

- A. CHAP
- B. SAML
- C. Kerberos
- D. Diameter

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 918

Joe analyzed the following log and determined the security team should implement which of the following as a mitigation method against further attempts?

Host 192.168.1.123

[00:00:01]Successful Login: 015 192.168.1.123 : local

[00:00:03]Unsuccessful Login: 022 214.34.56.006 :RDP 192.168.1.124

[00:00:04]UnSuccessful Login: 010 214.34.56.006 :RDP 192.168.1.124

[00:00:07]UnSuccessful Login: 007 214.34.56.006 :RDP 192.168.1.124

[00:00:08]UnSuccessful Login: 003 214.34.56.006 :RDP 192.168.1.124

- A. Reporting
- B. IDS
- C. Monitor system logs
- D. Hardening

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 919

A computer supply company is located in a building with three wireless networks. The system security team implemented a quarterly security scan and saw the following. Which of the following is this an example of?

SSID State Channel Level

Computer AreUs1 connected 1 70dbm

Computer AreUs2 connected 5 80dbm

Computer AreUs3 connected 3 75dbm

Computer AreUs4 connected 6 95dbm

- A. Rouge access point
- B. Near field communication
- C. Jamming
- D. Packet sniffing

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 920

Joe, a technician at the local power plant, notices that several turbines had ramp up in cycles during the week. Further investigation by the system engineering team determined that a timed .exe file had been uploaded to the system control console during a visit by international contractors. Which of the following actions should Joe recommend?

- A. Create a VLAN for the SCADA
- B. Enable PKI for the MainFrame

- C. Implement patch management
- D. Implement stronger WPA2 Wireless

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 921

A system administrator has been instructed by the head of security to protect their data at-rest. Which of the following would provide the strongest protection?

- A. Prohibiting removable media
- B. Incorporating a full-disk encryption system
- C. Biometric controls on data center entry points
- D. A host-based intrusion detection system

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 922

An Information Systems Security Officer (ISSO) has been placed in charge of a classified peer-to-peer network that cannot connect to the Internet. The ISSO can update the antivirus definitions manually, but which of the following steps is MOST important?

- A. A full scan must be run on the network after the DAT file is installed.
- B. The signatures must have a hash value equal to what is displayed on the vendor site.
- C. The definition file must be updated within seven days.
- D. All users must be logged off of the network prior to the installation of the definition file.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 923

Ann has taken over as the new head of the IT department. One of her first assignments was to implement AAA in preparation for the company's new telecommuting policy. When she takes inventory of the organizations existing network infrastructure, she makes note that it is a mix of several different vendors. Ann knows she needs a method of secure centralized access to the company's network resources. Which of the following is the BEST service for Ann to implement?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 924

A group policy requires users in an organization to use strong passwords that must be changed every 15 days. Joe and Ann were hired 16 days ago. When Joe logs into the network, he is prompted to change his password; when Ann logs into the network, she is not prompted to change her password. Which of the following BEST explains why Ann is not required to change her password?

- A. Ann's user account has administrator privileges.
- B. Joe's user account was not added to the group policy.
- C. Ann's user account was not added to the group policy.
- D. Joe's user account was inadvertently disabled and must be re-created.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 925

A new web server has been provisioned at a third party hosting provider for processing credit card transactions. The security administrator runs the netstat command on the server and notices that ports 80, 443, and 3389 are in a 'listening' state. No other ports are open. Which of the following services should be disabled to ensure secure communications?

- A. HTTPS
- B. HTTP
- C. RDP
- D. TELNET

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 926

Several employee accounts appear to have been cracked by an attacker. Which of the following should the security administrator implement to mitigate password cracking attacks? (Select TWO).

- A. Increase password complexity
- B. Deploy an IDS to capture suspicious logins
- C. Implement password history
- D. Implement monitoring of logins
- E. Implement password expiration
- F. Increase password length

Correct Answer: AF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 927

Human Resources suspects an employee is accessing the employee salary database. The administrator is asked to find out who it is. In order to complete this task, which of the following is a security control that should be in place?

- A. Shared accounts should not be in use
- B. Account lockout should be enabled
- C. Privileges should be assigned to groups rather than individuals
- D. Time of day restrictions should be in use

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 928

A cafe provides laptops for Internet access to their customers. The cafe is located in the center corridor of a busy shopping mall. The company has experienced several laptop thefts from the cafe during peak shopping hours of the day. Corporate has asked that the IT department provide a solution to eliminate laptop theft. Which of the following would provide the IT department with the BEST solution?

- A. Attach cable locks to each laptop
- B. Require each customer to sign an AUP
- C. Install a GPS tracking device onto each laptop
- D. Install security cameras within the perimeter of the cafe

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 929

An auditor's report discovered several accounts with no activity for over 60 days. The accounts were later identified as contractors' accounts who would be returning in three months and would need to resume the activities. Which of the following would mitigate and secure the auditor's finding?

- A. Disable unnecessary contractor accounts and inform the auditor of the update.
- B. Reset contractor accounts and inform the auditor of the update.
- C. Inform the auditor that the accounts belong to the contractors.
- D. Delete contractor accounts and inform the auditor of the update.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 930

A company hired Joe, an accountant. The IT administrator will need to create a new account for Joe. The company uses groups for ease of management and administration of user accounts. Joe will need network access to all directories, folders and files within the accounting department. Which of the following configurations will meet the requirements?

- A. Create a user account and assign the user account to the accounting group.
- B. Create an account with role-based access control for accounting.
- C. Create a user account with password reset and notify Joe of the account creation.
- D. Create two accounts: a user account and an account with full network administration rights.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 931

Ann, the network administrator, has learned from the helpdesk that employees are accessing the wireless network without entering their domain credentials upon connection. Once the connection is made, they cannot reach any internal resources, while wired network connections operate smoothly. Which of the following is MOST likely occurring?

- A. A user has plugged in a personal access point at their desk to connect to the network wirelessly.
- B. The company is currently experiencing an attack on their internal DNS servers.
- C. The company's WEP encryption has been compromised and WPA2 needs to be implemented instead.
- D. An attacker has installed an access point nearby in an attempt to capture company information.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 932

Ann works at a small company and she is concerned that there is no oversight in the finance department; specifically, that Joe writes, signs and distributes paychecks, as well as other expenditures. Which of the following controls can she implement to address this concern?

- A. Mandatory vacations
- B. Time of day restrictions
- C. Least privilege
- D. Separation of duties

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 933

A hospital IT department wanted to secure its doctor's tablets. The IT department wants operating system level security and the ability to secure the data from alteration. Which of the following methods would MOST likely

work?

- A. Cloud storage
- B. Removal Media
- C. TPM
- D. Wiping

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



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

QUESTION 934

Customers' credit card information was stolen from a popular video streaming company. A security consultant determined that the information was stolen, while in transit, from the gaming consoles of a particular vendor. Which of the following methods should the company consider to secure this data in the future?

- A. Application firewalls
- B. Manual updates
- C. Firmware version control
- D. Encrypted TCP wrappers

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 935

A new intern was assigned to the system engineering department, which consists of the system architect and system software developer's teams. These two teams have separate privileges. The intern requires privileges to view the system architectural drawings and comment on some software development projects. Which of the following methods should the system administrator implement?

- A. Group base privileges
- B. Generic account prohibition
- C. User access review
- D. Credential management

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 936

A system security analyst using an enterprise monitoring tool notices an unknown internal host exfiltrating files to several foreign IP addresses. Which of the following would be an appropriate mitigation technique?

- A. Disabling unnecessary accounts
- B. Rogue machine detection
- C. Encrypting sensitive files
- D. Implementing antivirus

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 937

One of the system administrators at a company is assigned to maintain a secure computer lab. The administrator has rights to configure machines, install software, and perform user account maintenance. However, the administrator cannot add new computers to the domain, because that requires authorization from the Information Assurance Officer. This is an example of which of the following?

- A. Mandatory access
- B. Rule-based access control
- C. Least privilege
- D. Job rotation

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 938

Which of the following common access control models is commonly used on systems to ensure a "need to know" based on classification levels?

- A. Role Based Access Controls
- B. Mandatory Access Controls
- C. Discretionary Access Controls
- D. Access Control List

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 939

A company's security administrator wants to manage PKI for internal systems to help reduce costs. Which of the following is the FIRST step the security administrator should take?

- A. Install a registration server.
- B. Generate shared public and private keys.

- C. Install a CA.
- D. Establish a key escrow policy.

Correct Answer: C

Section: (none)

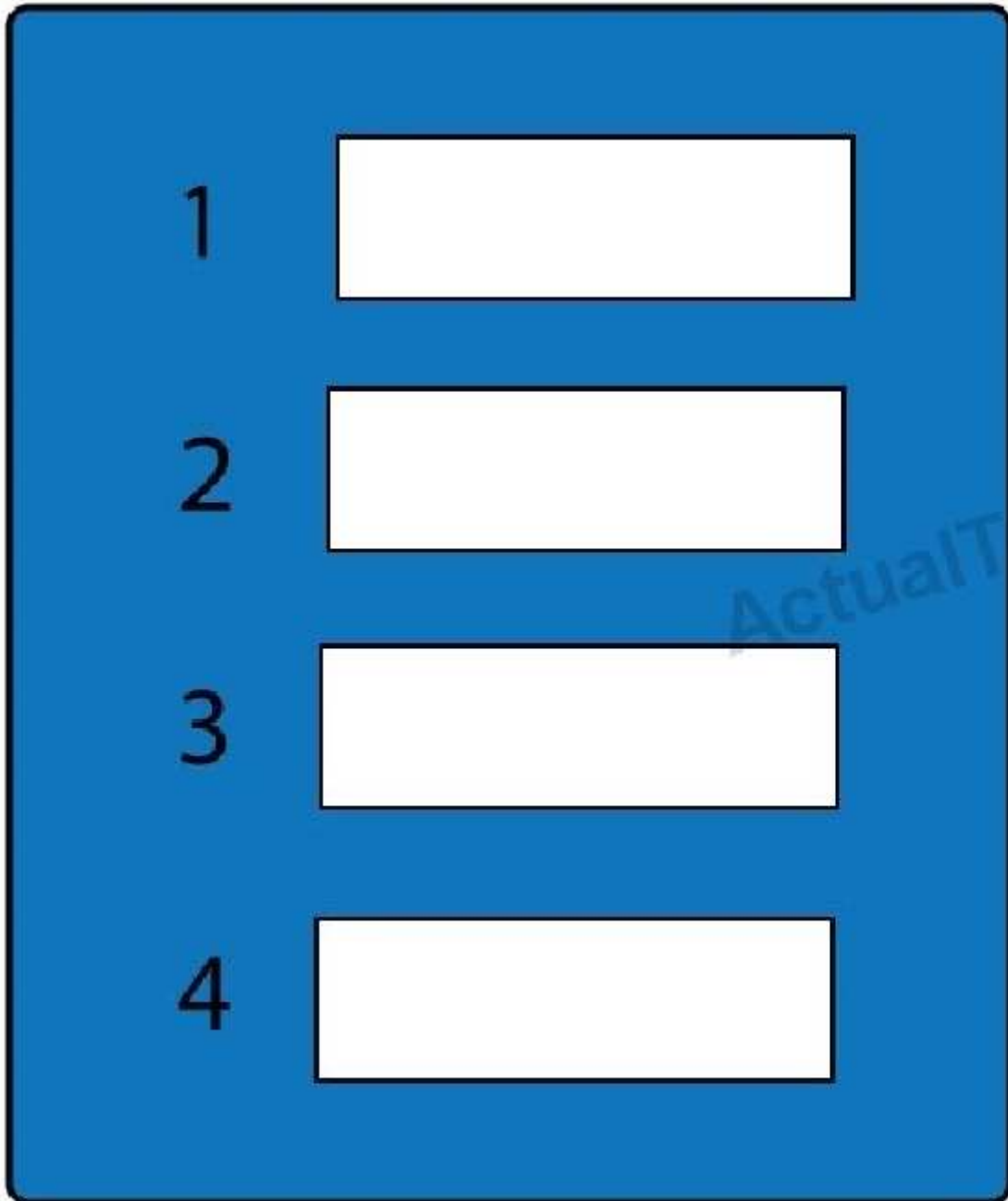
Explanation

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

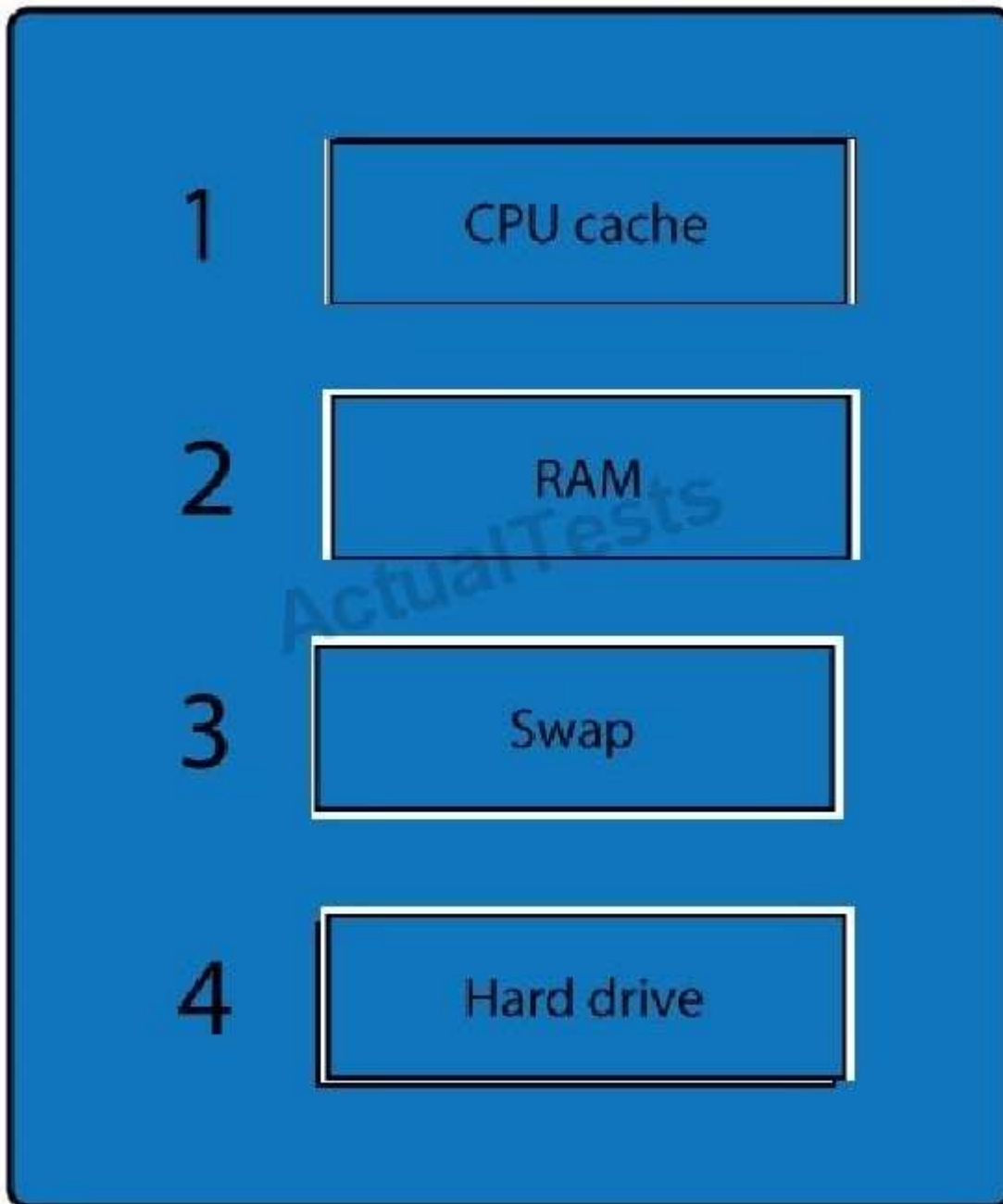
- A.
- B.
- C.
- D.

Correct Answer:

Section: (none)

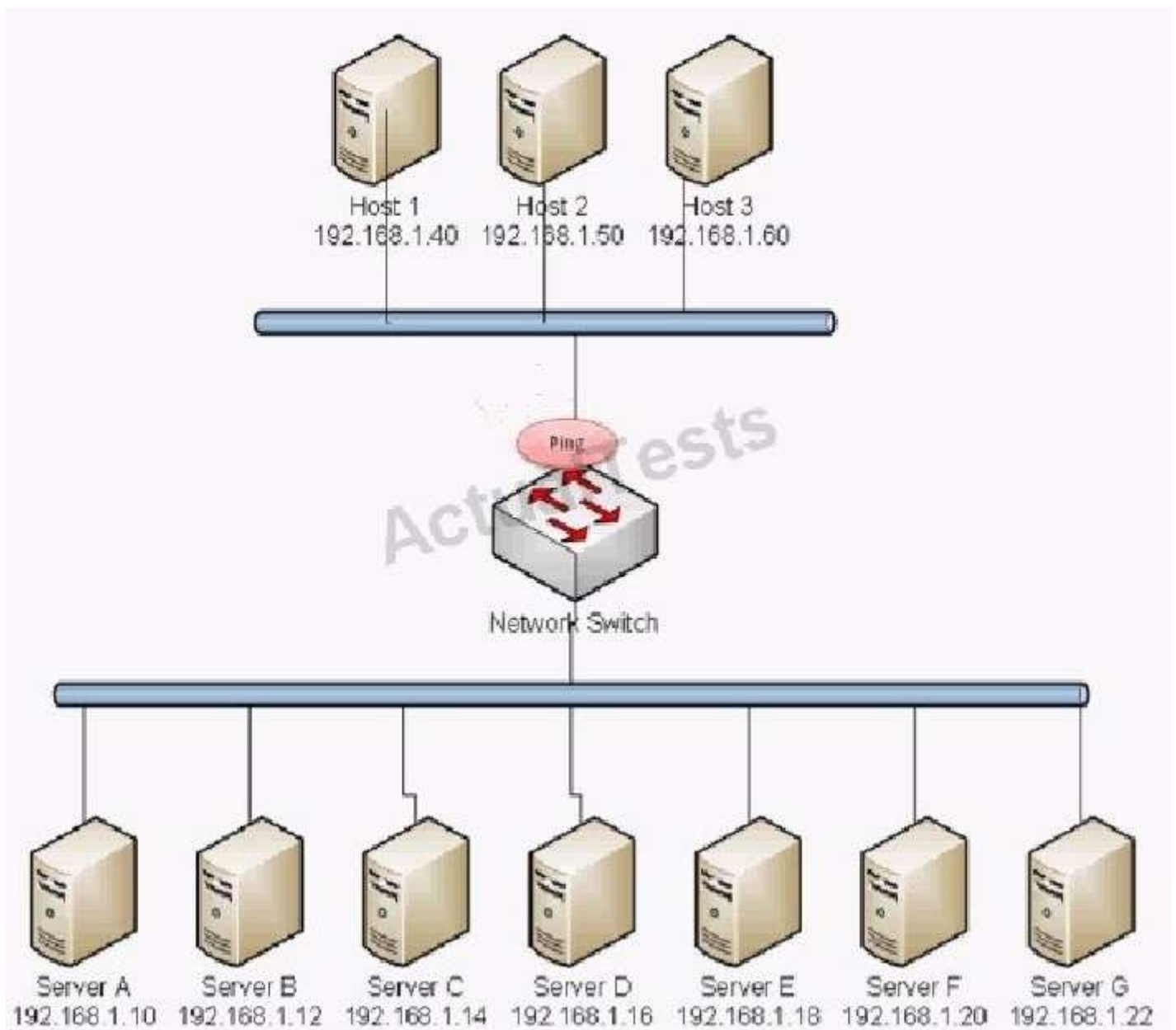
Explanation

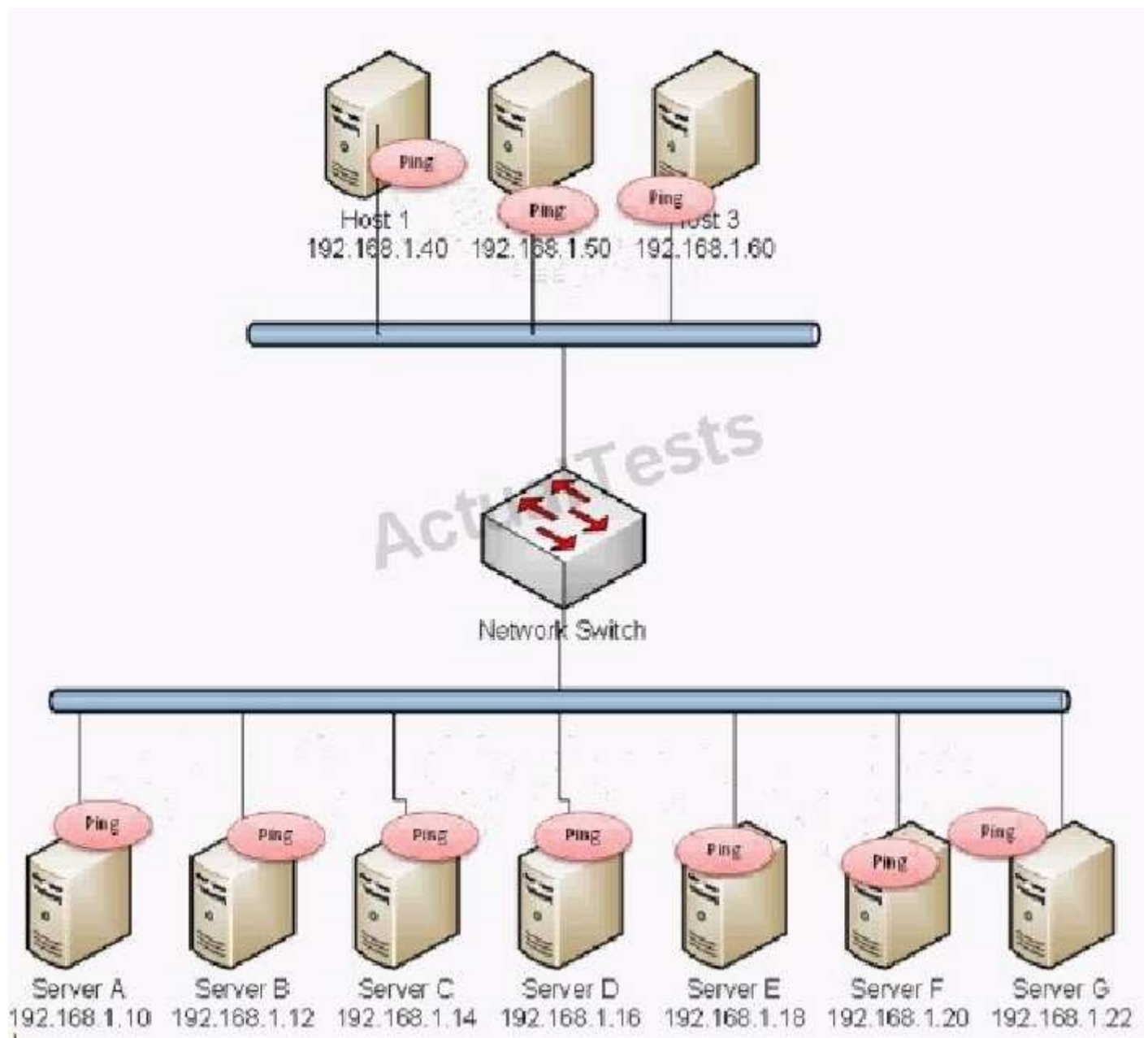
Explanation/Reference:

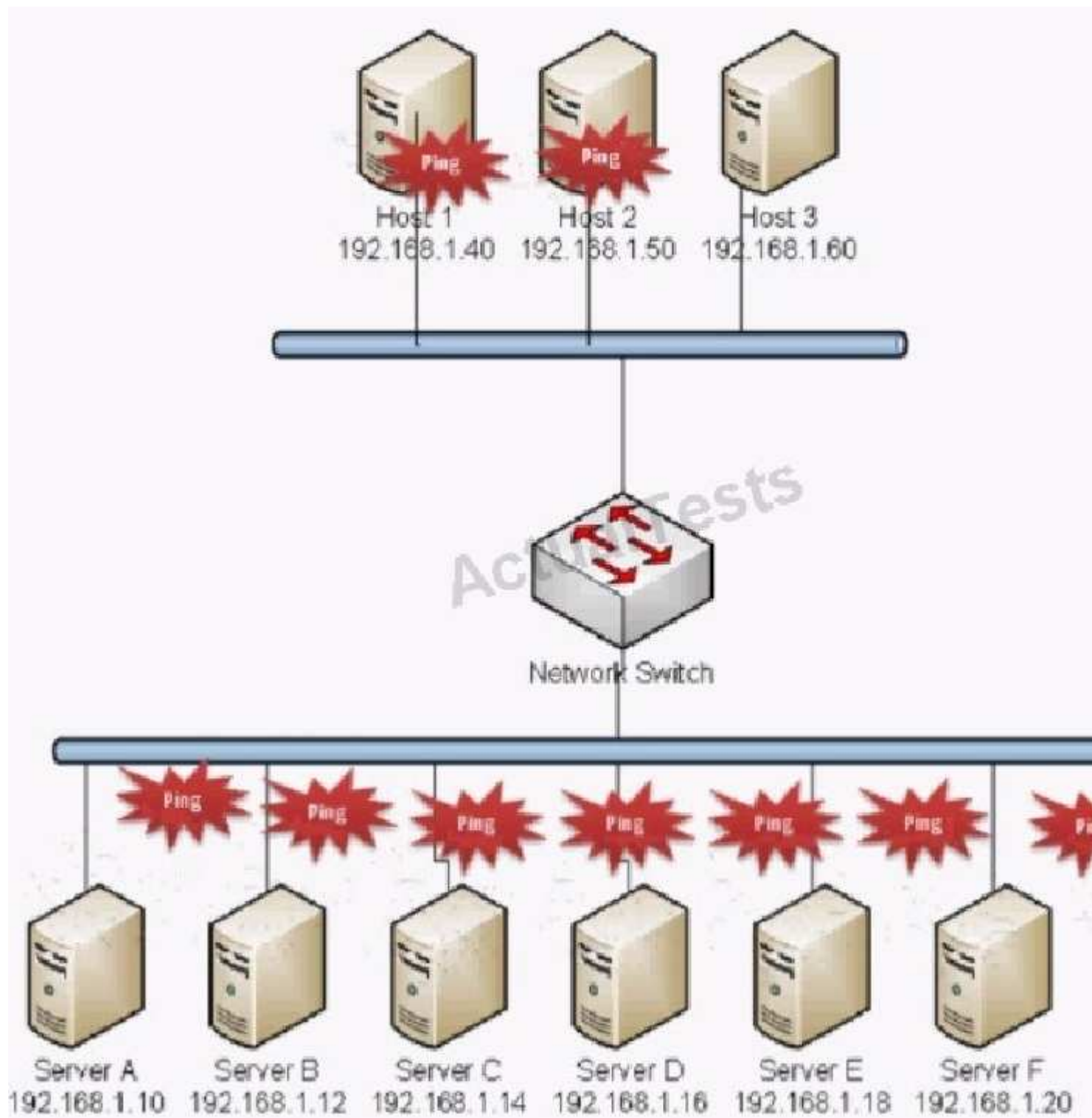


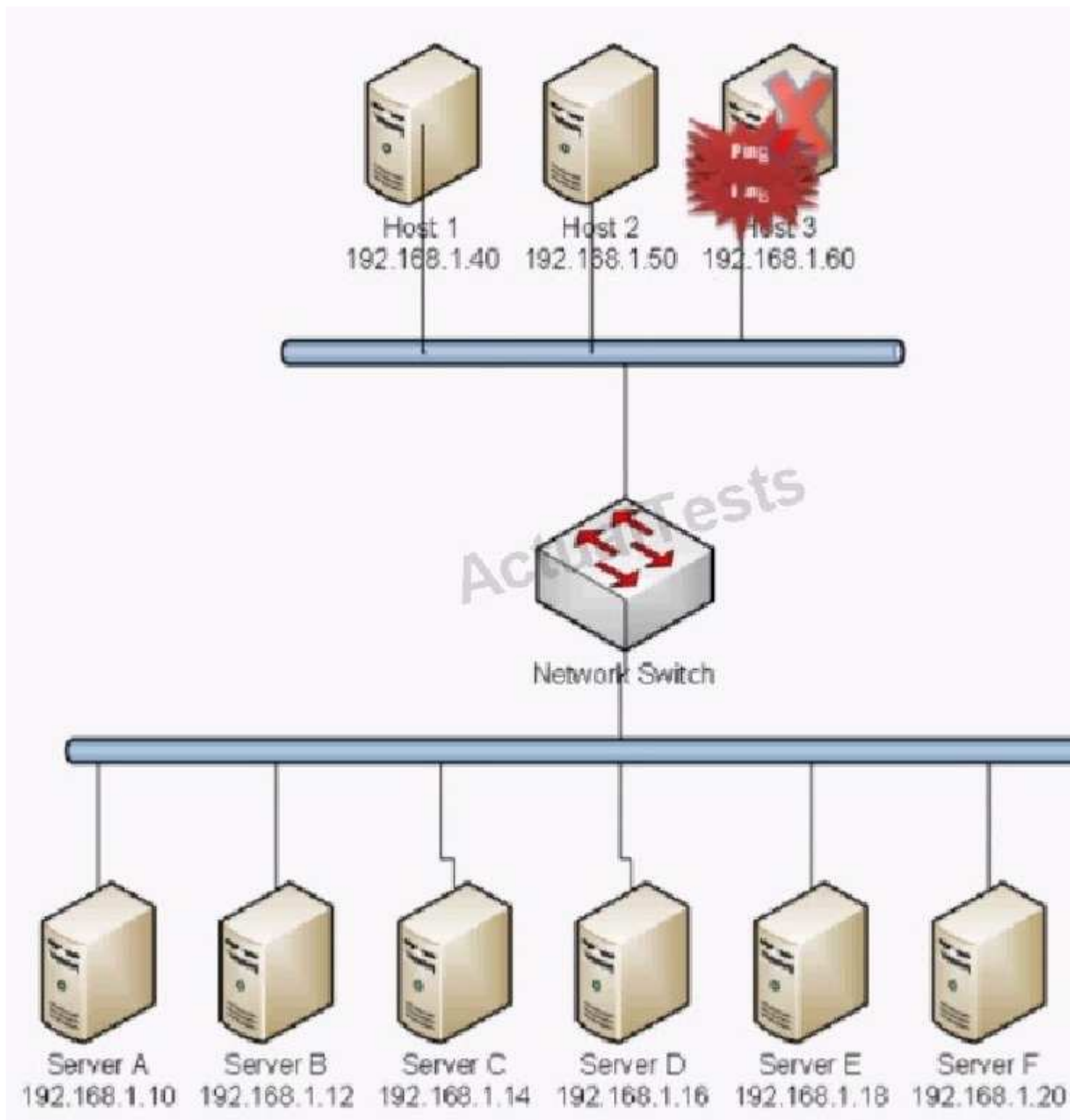
QUESTION 2

-- 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)

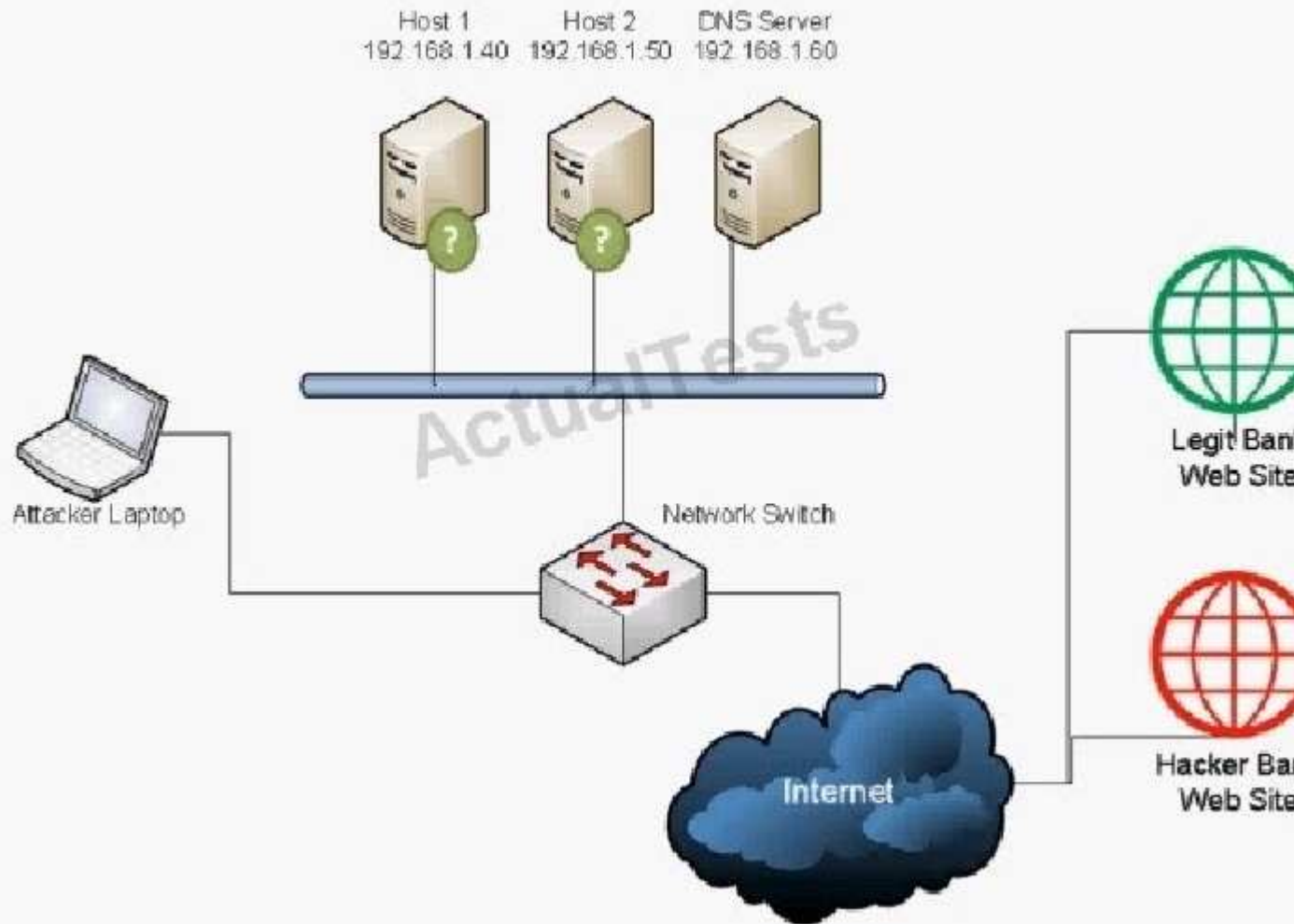
Explanation

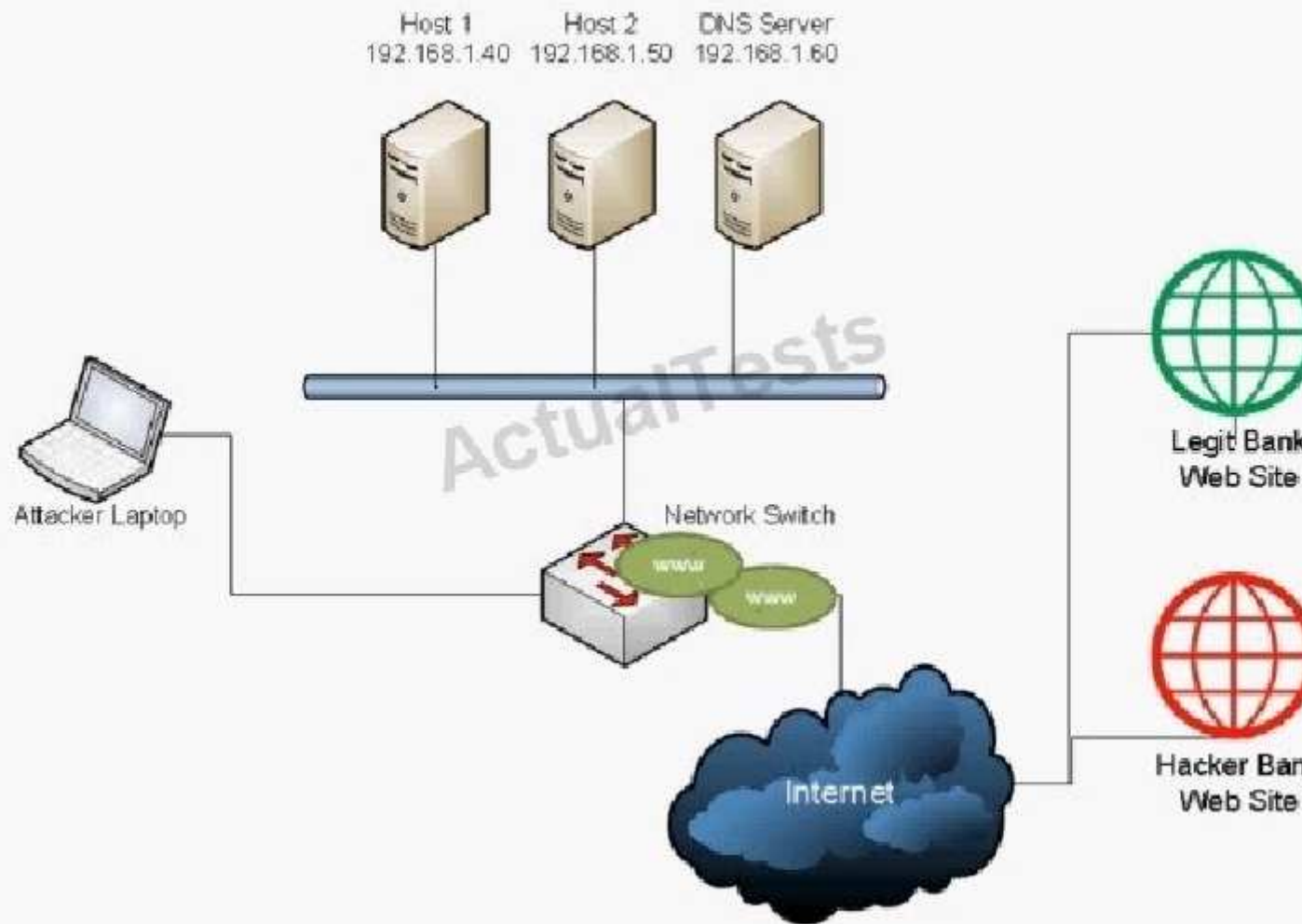
Explanation/Reference:

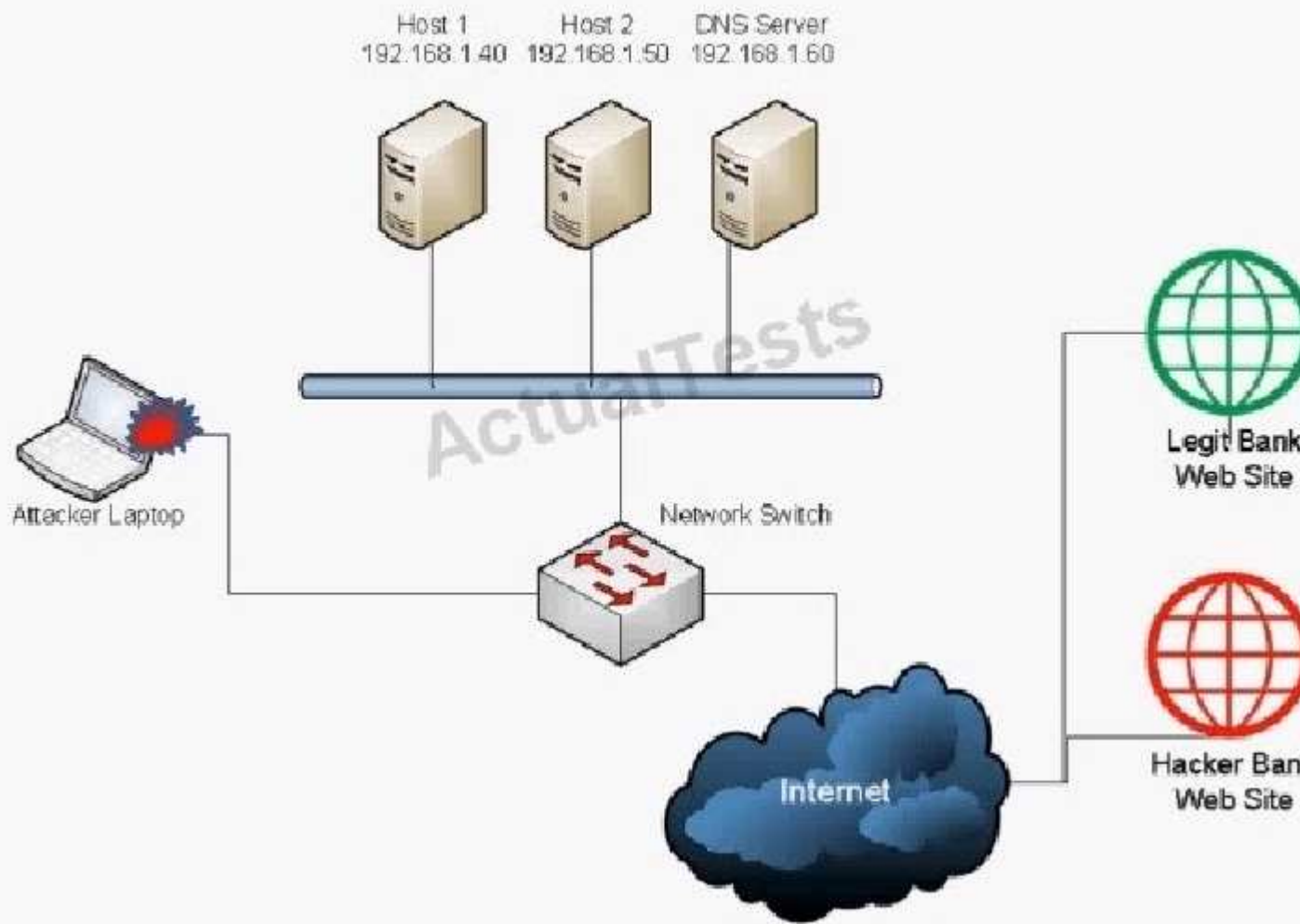
FTP	21
Telnet	23
SMTP	25
SNMP	161
SCP	22
TFTP	69

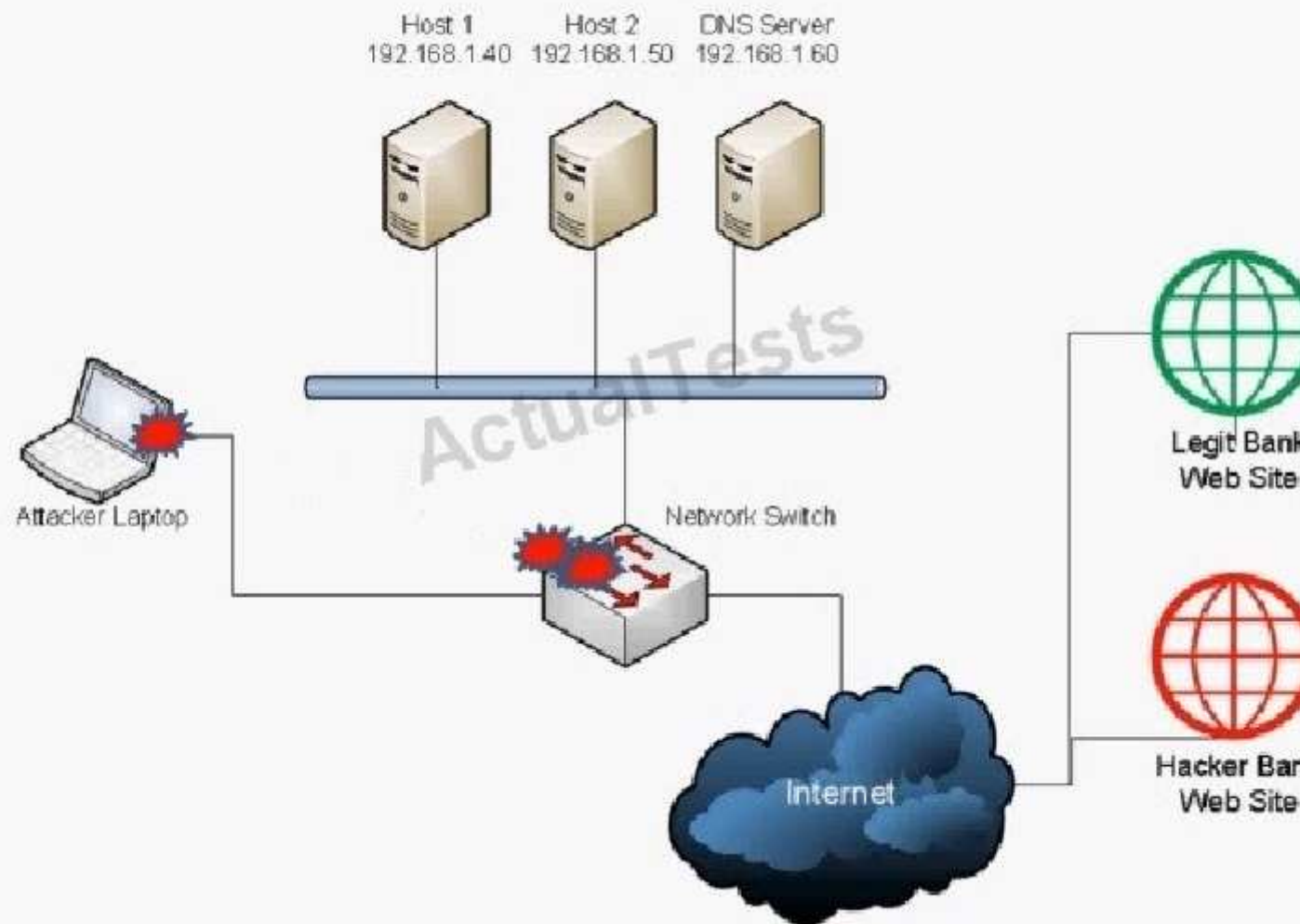
QUESTION 4

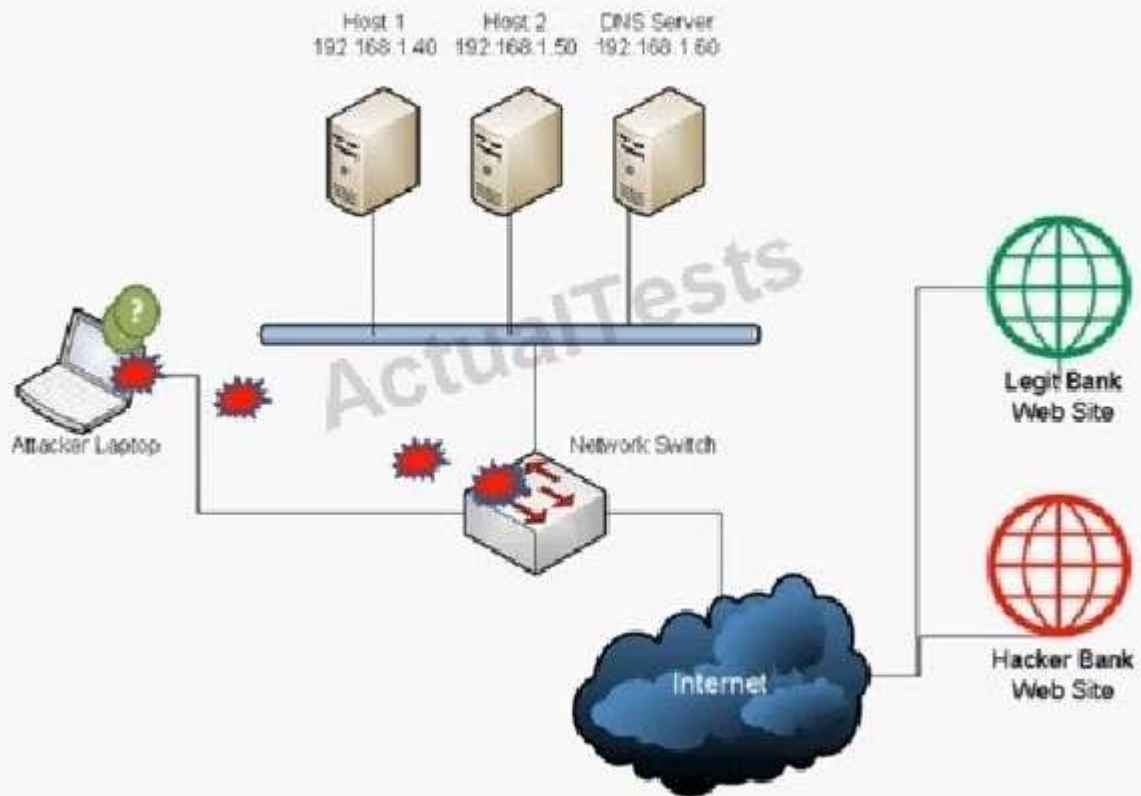
-- Exhibit

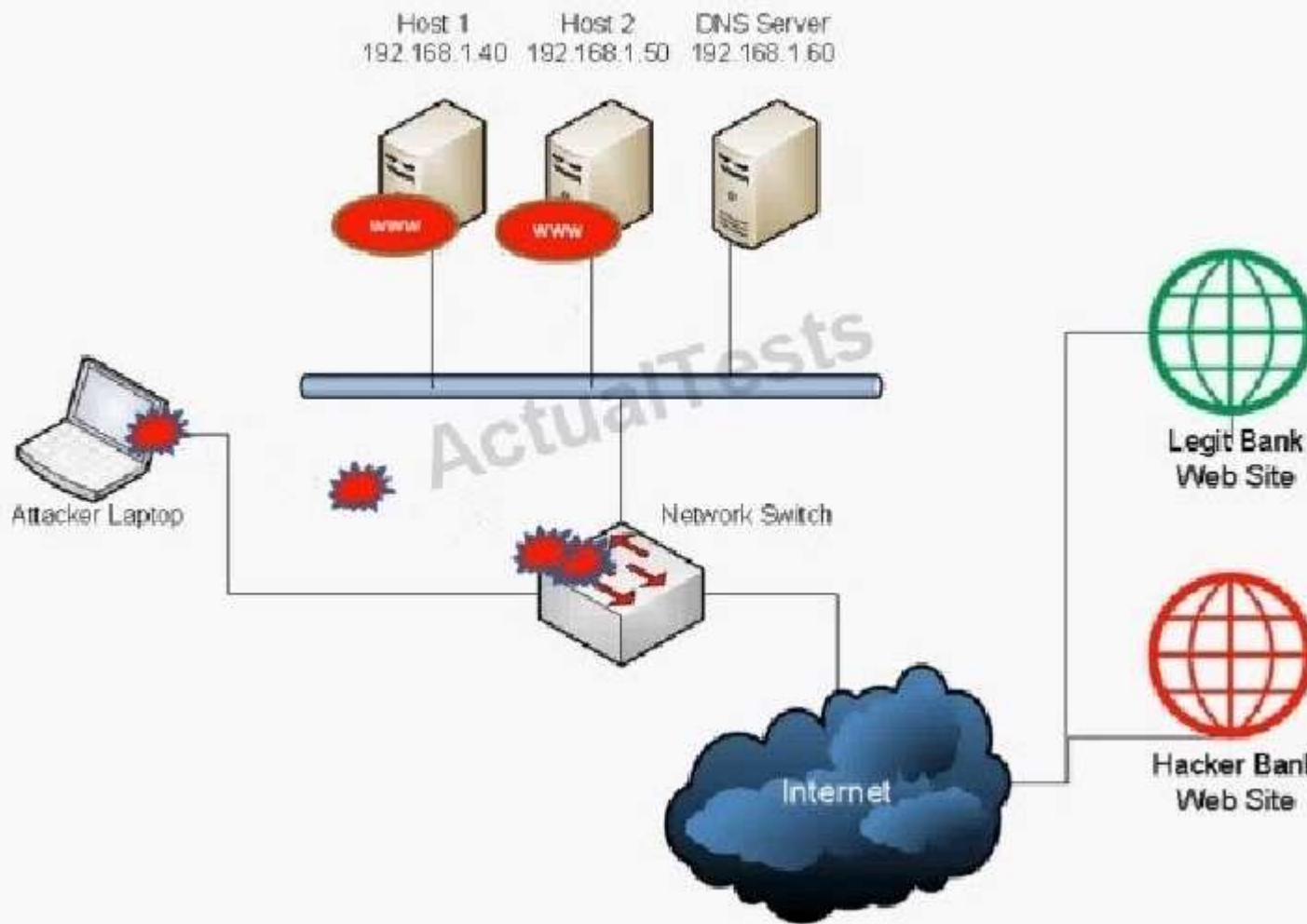


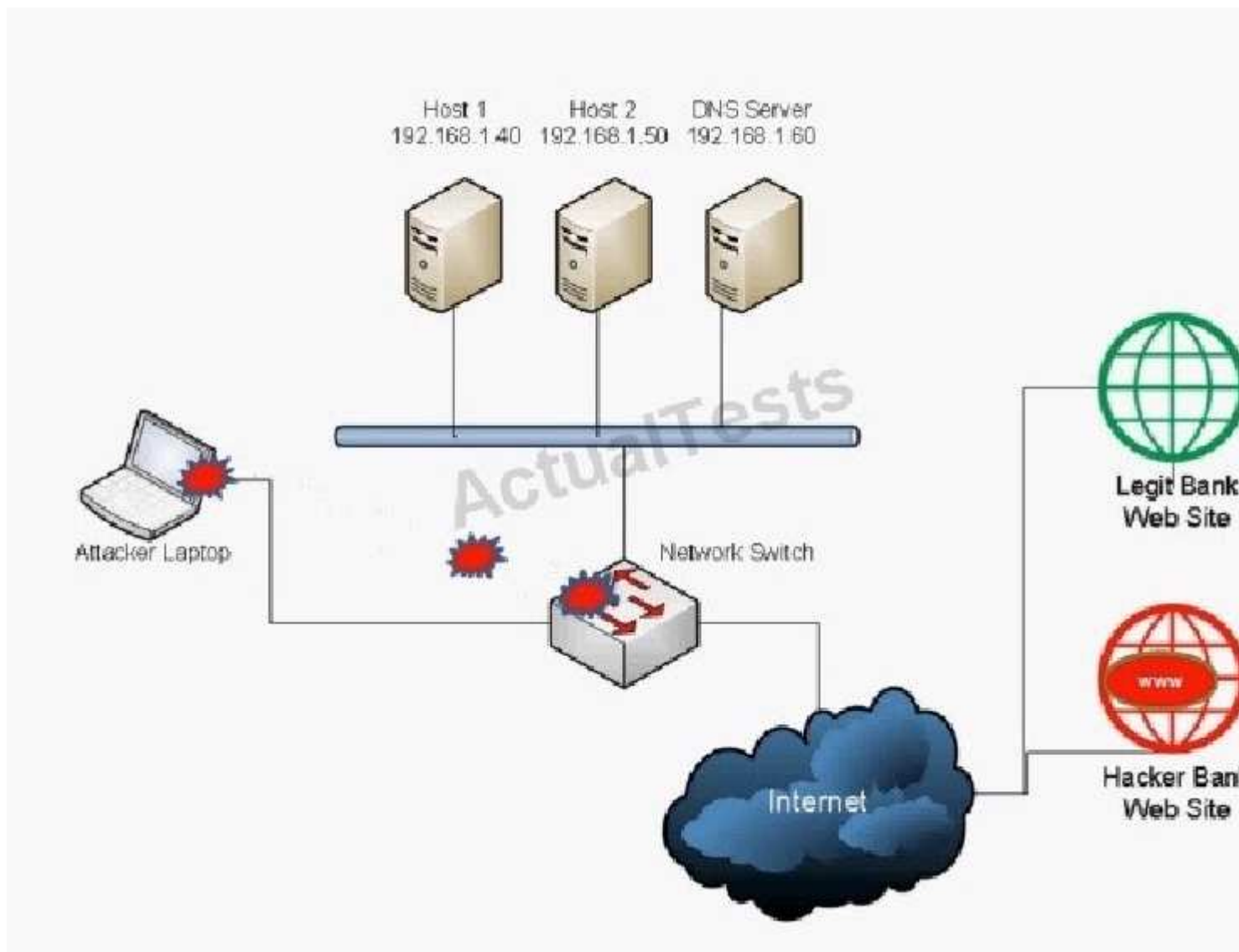












-- Exhibit --

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/>