



SY0-501.310q

SY0-501

SY0-501

CompTIA Security+ Certification Exam

Score: 800/1000

Version:

Time Limit: 120 Minutes

Exam A (310 questions)

Question 1

Ann, a customer, is reporting that several important files are missing from her workstation. She recently received communication from an unknown party who is requesting funds to restore the files. Which of the following attacks has occurred?

- ☐ Ransomware
- ☐ Keylogger
- ☐ Buffer overflow
- ☐ Rootkit

Question 2

A security analyst is reviewing an assessment report that includes software versions, running services, supported encryption algorithms, and permission settings. Which of the following produced the report?

- ☐ Vulnerability scanner
- ☐ Protocol analyzer
- ☐ Network mapper
- ☐ Web inspector

Question 3

An employer requires that employees use a key-generating app on their smartphones to log into corporate applications. In terms of authentication of an individual, this type of access policy is BEST defined as:

- ☐ Something you have.
- ☐ Something you know.
- ☐ Something you do.
- ☐ Something you are.

Question 4

An analyst wants to implement a more secure wireless authentication for office access points. Which of the following technologies allows for encrypted authentication of wireless clients over TLS?

- ☐ PEAP
- ☐ EAP
- ☐ WPA2
- ☐ RADIUS

Question 5

Joe a website administrator believes he owns the intellectual property for a company invention and has been replacing image files on the company's public facing website in the DMZ. Joe is using steganography to hide stolen data.

Which of the following controls can be implemented to mitigate this type of inside threat?

- ☐ Digital signatures
- ☐ File integrity monitoring
- ☐ Access controls
- ☐ Change management
- ☐ Stateful inspection firewall

Question 6

Recently several employees were victims of a phishing email that appeared to originate from the company president. The email claimed the employees would be disciplined if they did not click on a malicious link in the message.

Which of the following principles of social engineering made this attack successful?

- ☐ Authority
- ☐ Spamming
- ☐ Social proof
- ☐ Scarcity

Question 7

A Chief Security Officer (CSO) has been unsuccessful in attempts to access the website for a potential partner (www.example.net).

Which of the following rules is preventing the CSO from accessing the site?

Blocked sites: *.nonews.com, *.rumorhasit.net, *.mars?

- ☐ Rule 1: deny from inside to outside source any destination any service smtp
- ☐ Rule 2: deny from inside to outside source any destination any service ping
- ☐ Rule 3: deny from inside to outside source any destination {blocked sites} service http-https
- ☐ Rule 4: deny from any to any source any destination any service any

Question 8

After a recent internal breach, a company decided to regenerate and reissue all certificates used in the transmission of confidential information. The company places the greatest importance on confidentiality and non-repudiation, and decided to generate dual key pairs for each client. Which of the following BEST describes how the company will use these certificates?

- ☐ One key pair will be used for encryption and decryption. The other will be used to digitally sign the data.
- ☐ One key pair will be used for encryption. The other key pair will provide extended validation.
- ☐ Data will be encrypted once by each key, doubling the confidentiality and non-repudiation strength.
- ☐ One key pair will be used for internal communication, and the other will be used for external communication.

Question 9

Malware that changes its binary pattern on specific dates at specific times to avoid detection is known as a (n):

- ☐ armored virus
- ☐ logic bomb
- ☐ polymorphic virus
- ☐ Trojan

Question 10

A security administrator is developing controls for creating audit trails and tracking if a PHI data breach is to occur. The administrator has been given the following requirements:

All access must be correlated to a user account.
All user accounts must be assigned to a single individual.
User access to the PHI data must be recorded.
Anomalies in PHI data access must be reported.
Logs and records cannot be deleted or modified.

Which of the following should the administrator implement to meet the above requirements? (Select three.)

- ☐ Eliminate shared accounts.
- ☐ Create a standard naming convention for accounts.
- ☐ Implement usage auditing and review.
- ☐ Enable account lockout thresholds.
- ☐ Copy logs in real time to a secured WORM drive.
- ☐ Implement time-of-day restrictions.
- ☐ Perform regular permission audits and reviews.

Question 11

Which of the following is the main difference an XSS vulnerability and a CSRF vulnerability?

- ☐ XSS needs the attacker to be authenticated to the trusted server.
- ☐ XSS does not need the victim to be authenticated to the trusted server.
- ☐ CSRF needs the victim to be authenticated to the trusted server.
- ☐ CSRF does not need the victim to be authenticated to the trusted server.
- ☐ CSRF does not need the attacker to be authenticated to the trusted server.

Question 12

Due to regulatory requirements, a security analyst must implement full drive encryption on a Windows file server.

Which of the following should the analyst implement on the system to BEST meet this requirement? (Choose two.)

- ☐ Enable and configure EFS on the file system.
- ☐ Ensure the hardware supports TPM, and enable it in the BIOS.
- ☐ Ensure the hardware supports VT-X, and enable it in the BIOS.
- ☐ Enable and configure BitLocker on the drives.
- ☐ Enable and configure DFS across the file system.

Question 13

A Security Officer on a military base needs to encrypt several smart phones that will be going into the field.

Which of the following encryption solutions should be deployed in this situation?

- ☐ Elliptic curve
- ☐ One-time pad
- ☐ 3DES
- ☐ AES-256

Question 14

Which of the following is the GREATEST risk to a company by allowing employees to physically bring their personal smartphones to work?

- ☐ Taking pictures of proprietary information and equipment in restricted areas.
- ☐ Installing soft token software to connect to the company's wireless network.
- ☐ Company cannot automate patch management on personally-owned devices.
- ☐ Increases the attack surface by having more target devices on the company's campus

Question 15

A new intern in the purchasing department requires read access to shared documents. Permissions are normally controlled through a group called "Purchasing", however, the purchasing group permissions allow write access.

Which of the following would be the BEST course of action?

- ☐ Modify all the shared files with read only permissions for the intern.
- ☐ Create a new group that has only read permissions for the files.
- ☐ Remove all permissions for the shared files.
- ☐ Add the intern to the "Purchasing" group.

Question 16

A security program manager wants to actively test the security posture of a system. The system is not yet in production and has no uptime requirement or active user base.

Which of the following methods will produce a report which shows vulnerabilities that were actually exploited?

- ☐ Peer review
- ☐ Component testing
- ☐ Penetration testing
- ☐ Vulnerability testing

Question 17

As part of a new BYOD rollout, a security analyst has been asked to find a way to securely store company data on personal devices.

Which of the following would BEST help to accomplish this?

- ☐ Require the use of an eight-character PIN.
- ☐ Implement containerization of company data.
- ☐ Require annual AUP sign-off.
- ☐ Use geofencing tools to unlock devices while on the premises.

Question 18

A security analyst accesses corporate web pages and inputs random data in the forms. The response received includes the type of database used and SQL commands that the database accepts. Which of the following should the security analyst use to prevent this vulnerability?

- ☐ Application fuzzing
- ☐ Error handling
- ☐ Input validation
- ☐ Pointer dereference

Question 19

A company is using a mobile device deployment model in which employees use their personal devices for work at their own discretion. Some of the problems the company is encountering include the following:

There is no standardization.

Employees ask for reimbursement for their devices.

Employees do not replace their devices often enough to keep them running efficiently.

The company does not have enough control over the devices.

Which of the following is a deployment model that would help the company overcome these problems?

- ☐ BYOD
- ☐ VDI
- ☐ COPE
- ☐ CYOD

Question 20

A security administrator is creating a subnet on one of the corporate firewall interfaces to use as a DMZ which is expected to accommodate at most 14 physical hosts.

Which of the following subnets would BEST meet the requirements?

- ☐ 192.168.0.16 255.25.255.248
- ☐ 192.168.0.16/28
- ☐ 192.168.1.50 255.255.25.240
- ☐ 192.168.2.32/27

Question 21

A company wants to host a publicly available server that performs the following functions:

Evaluates MX record lookup

Can perform authenticated requests for A and AAA records

Uses RRSIG

Which of the following should the company use to fulfill the above requirements?

- ☐ DNSSEC
- ☐ SFTP
- ☐ nslookup
- ☐ dig
- ☐ LDAPS

Question 22

An organization's primary datacenter is experiencing a two-day outage due to an HVAC malfunction. The node located in the datacenter has lost power and is no longer operational, impacting the ability of all users to connect to the alternate datacenter. Which of the following BIA concepts BEST represents the risk described in this scenario?

- ☐ SPoF
- ☐ RTO
- ☐ MTBF
- ☐ MTTR

Question 23

A security analyst is attempting to break into a client's secure network. The analyst was not given prior information about the client, except for a block of public IP addresses that are currently in use. After network enumeration, the analyst's NEXT step is to perform:

- ☐ a risk analysis.
- ☐ a vulnerability assessment.
- ☐ a gray-box penetration test.
- ☐ an external security audit.
- ☐ a red team exercise.

Question 24

A security analyst is doing a vulnerability assessment on a database server. A scanning tool returns the following information:

```
Database:      CustomerAccess1
Column:        Password
Data type:     MD5 Hash
Salted?:       No
```

There have been several security breaches on the web server that accesses this database. The security team is instructed to mitigate the impact of any possible breaches. The security team is also instructed to improve the security on this database by making it less vulnerable to offline attacks. Which of the following would BEST accomplish these goals? (Choose two.)

- ☐ Start using salts to generate MD5 password hashes
- ☐ Generate password hashes using SHA-256
- ☐ Force users to change passwords the next time they log on
- ☐ Limit users to five attempted logons before they are locked out
- ☐ Require the web server to only use TLS 1.2 encryption

Question 25

A security analyst is attempting to identify vulnerabilities in a customer's web application without impacting the system or its data.

Which of the following BEST describes the vulnerability scanning concept performed?

- ☐ Aggressive scan
- ☐ Passive scan
- ☐ Non-credentialed scan
- ☐ Compliance scan

Question 26

Which of the following threats has sufficient knowledge to cause the MOST danger to an organization?

- ☐ Competitors
- ☐ Insiders
- ☐ Hacktivists
- ☐ Script kiddies

Question 27

A company is developing a new secure technology and requires computers being used for development to be isolated. Which of the following should be implemented to provide the MOST secure environment?

- ☐ A perimeter firewall and IDS
- ☐ An air gapped computer network
- ☐ A honeypot residing in a DMZ
- ☐ An ad hoc network with NAT
- ☐ A bastion host

Question 28

A user of the wireless network is unable to gain access to the network. The symptoms are:

- 1.) Unable to connect to both internal and Internet resources
- 2.) The wireless icon shows connectivity but has no network access

The wireless network is WPA2 Enterprise and users must be a member of the wireless security group to authenticate.

Which of the following is the MOST likely cause of the connectivity issues?

- ☐ The wireless signal is not strong enough
- ☐ A remote DDoS attack against the RADIUS server is taking place
- ☐ The user's laptop only supports WPA and WEP
- ☐ The DHCP scope is full
- ☐ The dynamic encryption key did not update while the user was offline

Question 29

A manager wants to distribute a report to several other managers within the company. Some of them reside in remote locations that are not connected to the domain but have a local server. Because there is sensitive data within the report and the size of the report is beyond the limit of the email attachment size, emailing the report is not an option. Which of the following protocols should be implemented to distribute the report securely? (Select three.)

- ☐ S/MIME
- ☐ SSH
- ☐ SNMPv3
- ☐ FTPS
- ☐ SRTP
- ☐ HTTPS
- ☐ LDAPS

Question 30

Which of the following is the proper order for logging a user into a system from the first step to the last step?

- ☐ Identification, authentication, authorization
- ☐ Identification, authorization, authentication
- ☐ Authentication, identification, authorization
- ☐ Authentication, identification, authorization
- ☐ Authorization, identification, authentication

Question 31

Corporations choose to exceed regulatory framework standards because of which of the following incentives?

- ☐ It improves the legal defensibility of the company.
- ☐ It gives a social defense that the company is not violating customer privacy laws.
- ☐ It proves to investors that the company takes APT cyber actors seriously
- ☐ It results in overall industrial security standards being raised voluntarily.

Question 32

Which of the following cryptographic attacks would salting of passwords render ineffective?

- ☐ Brute force
- ☐ Dictionary
- ☐ Rainbow tables
- ☐ Birthday

Question 33

A company offers SaaS, maintaining all customers' credentials and authenticating locally. Many large customers have requested the company offer some form of federation with their existing authentication infrastructures.

Which of the following would allow customers to manage authentication and authorizations from within their existing organizations?

- ☐ Implement SAML so the company's services may accept assertions from the customers' authentication servers.
- ☐ Provide customers with a constrained interface to manage only their users' accounts in the company's active directory server.
- ☐ Provide a system for customers to replicate their users' passwords from their authentication service to the company's.
- ☐ Use SOAP calls to support authentication between the company's product and the customers' authentication servers.

Question 34

HOTSPOT

A newly purchased corporate WAP needs to be configured in the MOST secure manner possible.

INSTRUCTIONS

Please click on the below items on the network diagram and configure them accordingly:

WAP

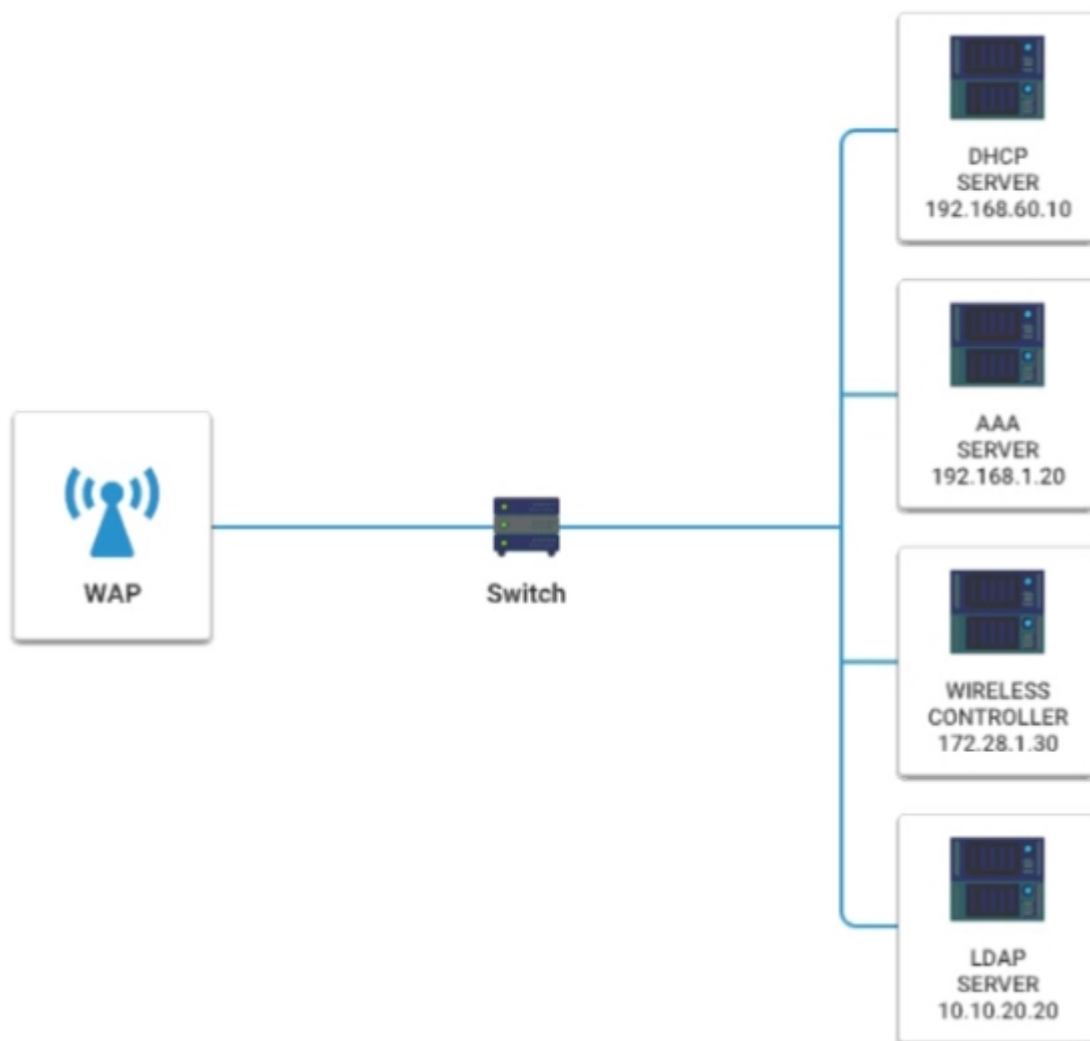
DHCP Server

AAA Server

Wireless Controller

LDAP Server

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



The image displays two screenshots of a 'Wireless Access Point' configuration interface. The left screenshot shows the 'Basic Wireless Settings' tab. It includes a 'Wireless Network Mode' dropdown menu with options 'MIXED', 'B ONLY', and 'G ONLY'; a 'Wireless Network Name (SSID)' text field with 'DEFAULT'; a 'Wireless Channel' dropdown menu with options 1 through 11; and a 'Wireless SSID Broadcast' section with 'enable' and 'disable' radio buttons. The right screenshot shows the 'Wireless Security' tab. It features a 'Security Mode' dropdown menu with options 'Disabled', 'WEP', 'WPA Enterprise', 'WPA Personal', 'WPA2 Enterprise', 'WPA2 Personal', and 'RADIUS'. Both screenshots have 'Cancel Changes' and 'Save Settings' buttons at the bottom.

Question 35

A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website. During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine.

Which of the following describes the type of attack the proxy has been legitimately programmed to perform?

- ☐ Transitive access
- ☐ Spoofing
- ☐ Man-in-the-middle
- ☐ Replay

Question 36

A computer on a company network was infected with a zero-day exploit after an employee accidentally opened an email that contained malicious content. The employee recognized the email as malicious and was attempting to delete it, but accidentally opened it.

Which of the following should be done to prevent this scenario from occurring again in the future?

- ☐ Install host-based firewalls on all computers that have an email client installed
- ☐ Set the email program default to open messages in plain text
- ☐ Install end-point protection on all computers that access web email
- ☐ Create new email spam filters to delete all messages from that sender

Question 37

Which of the following security controls does an iris scanner provide?

- ☐ Logical
- ☐ Administrative
- ☐ Corrective
- ☐ Physical
- ☐ Detective
- ☐ Deterrent

Question 38

A help desk is troubleshooting user reports that the corporate website is presenting untrusted certificate errors to employees and customers when they visit the website. Which of the following is the MOST likely cause of this error, provided the certificate has not expired?

- ☐ The certificate was self signed, and the CA was not imported by employees or customers
- ☐ The root CA has revoked the certificate of the intermediate CA
- ☐ The valid period for the certificate has passed, and a new certificate has not been issued
- ☐ The key escrow server has blocked the certificate from being validated

Question 39

An incident response manager has started to gather all the facts related to a SIEM alert showing multiple systems may have been compromised.

The manager has gathered these facts:

The breach is currently indicated on six user PCs

One service account is potentially compromised

Executive management has been notified

In which of the following phases of the IRP is the manager currently working?

- ☐ Recovery
- ☐ Eradication
- ☐ Containment
- ☐ Identification

Question 40

An application developer is designing an application involving secure transports from one service to another that will pass over port 80 for a request.

Which of the following secure protocols is the developer MOST likely to use?

- ☐ FTPS
- ☐ SFTP
- ☐ SSL
- ☐ LDAPS
- ☐ SSH

Question 41

An organization's file server has been virtualized to reduce costs. Which of the following types of backups would be MOST appropriate for the particular file server?

- ☐ Snapshot
- ☐ Full
- ☐ Incremental
- ☐ Differential

Question 42

The computer resource center issued smartphones to all first-level and above managers. The managers have the ability to install mobile tools. Which of the following tools should be implemented to control the types of tools the managers install?

- ☐ Download manager
- ☐ Content manager
- ☐ Segmentation manager
- ☐ Application manager

Question 43

Joe, the security administrator, sees this in a vulnerability scan report:

"The server 10.1.2.232 is running Apache 2.2.20 which may be vulnerable to a mod_cgi exploit."

Joe verifies that the mod_cgi module is not enabled on 10.1.2.232. This message is an example of:

- ☐ a threat.
- ☐ a risk.
- ☐ a false negative.
- ☐ a false positive.

Question 44

Every morning, a systems administrator monitors failed login attempts on the company's log management server. The administrator notices the DBAdmin account has five failed username and/or password alerts during a ten-minute window. The systems administrator determines the user account is a dummy account used to attract attackers.

Which of the following techniques should the systems administrator implement?

- ☐ Role-based access control
- ☐ Honeypot
- ☐ Rule-based access control
- ☐ Password cracker

Question 45

An organization wishes to provide better security for its name resolution services. Which of the following technologies BEST supports the deployment of DNSSEC at the organization?

- ☐ LDAP
- ☐ TPM
- ☐ TLS
- ☐ SSL
- ☐ PKI

Question 46

Which of the following can be provided to an AAA system for the identification phase?

- ☐ Username
- ☐ Permissions
- ☐ One-time token
- ☐ Private certificate

Question 47

A company wants to provide centralized authentication for its wireless system. The wireless authentication system must integrate with the directory back end. Which of the following is a AAA solution that will provide the required wireless authentication?

- ☐ TACACS+
- ☐ MSCHAPv2
- ☐ RADIUS
- ☐ LDAP

Question 48

A software development manager is taking over an existing software development project. The team currently suffers from poor communication due to a long delay between requirements documentation and feature delivery. This gap is resulting in an above average number of security-related bugs making it into production.

Which of the following development methodologies is the team MOST likely using now?

- ☐ Agile
- ☐ Waterfall
- ☐ Scrum
- ☐ Spiral

Question 49

A security analyst wants to harden the company's VoIP PBX. The analyst is worried that credentials may be intercepted and compromised when IP phones authenticate with the PBX. Which of the following would best prevent this from occurring?

- ☐ Implement SRTP between the phones and the PBX.
- ☐ Place the phones and PBX in their own VLAN.
- ☐ Restrict the phone connections to the PBX.
- ☐ Require SIPS on connections to the PBX.

Question 50

An analyst is part of a team that is investigating a potential breach of sensitive data at a large financial services organization. The organization suspects a breach occurred when proprietary data was disclosed to the public. The team finds servers were accessed using shared credentials that have been in place for some time. In addition, the team discovers undocumented firewall rules, which provided unauthorized external access to a server. Suspecting the activities of a malicious insider threat, which of the following was MOST likely to have been utilized to exfiltrate the proprietary data?

- ☐ Keylogger
- ☐ Botnet
- ☐ Crypto-malware
- ☐ Backdoor
- ☐ Ransomware
- ☐ DLP

Question 51

A security analyst is investigating a security breach. Upon inspection of the audit an access logs, the analyst notices the host was accessed and the `/etc/passwd` file was modified with a new entry for username "gotcha" and user ID of 0. Which of the following are the MOST likely attack vector and tool the analyst should use to determine if the attack is still ongoing? (Select TWO)

- ☐ Logic bomb
- ☐ Backdoor
- ☐ Keylogger
- ☐ Netstat
- ☐ Tracert
- ☐ Ping

Question 52

A security administrator wishes to implement a secure a method of file transfer when communicating with outside organizations.

Which of the following protocols would BEST facilitate secure file transfers? (Select TWO)

- ☐ SCP
- ☐ TFTP
- ☐ SNMP
- ☐ FTP
- ☐ SMTP
- ☐ FTPS

Question 53

Which of the following encryption methods does PKI typically use to securely protect keys?

- ☐ Elliptic curve
- ☐ Digital signatures
- ☐ Asymmetric
- ☐ Obfuscation

Question 54

A penetration tester is conducting an assessment on Comptia.org and runs the following command from a coffee shop while connected to the public Internet: `c:\nslookup -querytype=MX comptia.org`
Server: Unknown

Address: 198.51.100.45

comptia.org MX preference=10, mail exchanger = 92.68.102.33
comptia.org MX preference=20, mail exchanger = exchg1.comptia.org
exchg1.comptia.org internet address = 192.168.102.67

Which of the following should the penetration tester conclude about the command output?

- ☐ The public/private views on the Comptia.org DNS servers are misconfigured.
- ☐ Comptia.org is running an older mail server, which may be vulnerable to exploits.
- ☐ The DNS SPF records have not been updated for Comptia.org.
- ☐ 192.168.102.67 is a backup mail server that may be more vulnerable to attack.

Question 55

Users report the following message appears when browsing to the company's secure site: This website cannot be trusted. Which of the following actions should a security analyst take to resolve these messages? (Select two.)

- ☐ Verify the certificate has not expired on the server.
- ☐ Ensure the certificate has a .pfx extension on the server.
- ☐ Update the root certificate into the client computer certificate store.
- ☐ Install the updated private key on the web server.
- ☐ Have users clear their browsing history and relaunch the session.

Question 56

Ann, an employee in the payroll department, has contacted the help desk citing multiple issues with her device, including:

Slow performance

Word documents, PDFs, and images no longer opening

A pop-up

Ann states the issues began after she opened an invoice that a vendor emailed to her. Upon opening the invoice, she had to click several security warnings to view it in her word processor. With which of the following is the device MOST likely infected?

- ☐ Spyware
- ☐ Crypto-malware
- ☐ Rootkit
- ☐ Backdoor

Question 57

Which of the following technologies employ the use of SAML? (Select two.)

- ☐ Single sign-on
- ☐ Federation
- ☐ LDAP
- ☐ Secure token
- ☐ RADIUS

Question 58

A vulnerability scanner that uses its running service's access level to better assess vulnerabilities across multiple assets within an organization is performing a:

- ☐ Credentialed scan.
- ☐ Non-intrusive scan.
- ☐ Privilege escalation test.
- ☐ Passive scan.

Question 59

A technician needs to implement a system which will properly authenticate users by their username and password only when the users are logging in from a computer in the office building. Any attempt to authenticate from a location other than the office building should be rejected.

Which of the following MUST the technician implement?

- ☐ Dual factor authentication
- ☐ Transitive authentication
- ☐ Single factor authentication
- ☐ Biometric authentication

Question 60

A security administrator is reviewing the following network capture:

```
192.168.20.43:2043 -> 10.234.66.21:80  
POST "192.168.20.43 https://www.banksite.com<ENTER>JoeUsr<BackSPACE>erPassword<ENTER>"
```

Which of the following malware is MOST likely to generate the above information?

- ☐ Keylogger
- ☐ Ransomware
- ☐ Logic bomb
- ☐ Adware

Question 61

While performing surveillance activities, an attacker determines that an organization is using 802.1X to secure LAN access.

Which of the following attack mechanisms can the attacker utilize to bypass the identified network security?

- ☐ MAC spoofing
- ☐ Pharming
- ☐ Xmas attack
- ☐ ARP poisoning

Question 62

A company has a data classification system with definitions for “Private” and “Public”. The company’s security policy outlines how data should be protected based on type. The company recently added the data type “Proprietary”.

Which of the following is the MOST likely reason the company added this data type?

- ☐ Reduced cost
- ☐ More searchable data
- ☐ Better data classification
- ☐ Expanded authority of the privacy officer

Question 63

A security administrator is implementing a new WAF solution and has placed some of the web servers behind the WAF, with the WAF set to audit mode. When reviewing the audit logs of external requests and posts to the web servers, the administrator finds the following entry:

```
Context Details for Signature 20000018334
Context: Parameter
Actual Parameter Name: Account_Name
Parameter Value: SELECT * FROM Users WHERE Username='1' OR '1'='1' AND Password='1' OR '1'='1'
```

Based on this data, which of the following actions should the administrator take?

- ☐ Alert the web server administrators to a misconfiguration.
- ☐ Create a blocking policy based on the parameter values.
- ☐ Change the parameter name ‘Account_Name’ identified in the log.
- ☐ Create an alert to generate emails for abnormally high activity.

Question 64

Which of the following is a compensating control that will BEST reduce the risk of weak passwords?

- ☐ Requiring the use of one-time tokens
- ☐ Increasing password history retention count
- ☐ Disabling user accounts after exceeding maximum attempts
- ☐ Setting expiration of user passwords to a shorter time

Question 65

A company wants to ensure that the validity of publicly trusted certificates used by its web server can be determined even during an extended internet outage.

Which of the following should be implemented?

- ☐ Recovery agent
- ☐ Ocsf
- ☐ CrI
- ☐ Key escrow

Question 66

A company is developing a new system that will unlock a computer automatically when an authorized user sits in front of it, and then lock the computer when the user leaves. The user does not have to perform any action for this process to occur. Which of the following technologies provides this capability?

- ☐ Facial recognition
- ☐ Fingerprint scanner
- ☐ Motion detector
- ☐ Smart cards

Question 67

A security administrator has been asked to implement a VPN that will support remote access over IPSEC.

Which of the following is an encryption algorithm that would meet this requirement?

- ☐ MD5
- ☐ AES
- ☐ UDP
- ☐ PKI

Question 68

When trying to log onto a company's new ticketing system, some employees receive the following message: Access denied: too many concurrent sessions. The ticketing system was recently installed on a small VM with only the recommended hardware specifications. Which of the following is the MOST likely cause for this error message?

- ☐ Network resources have been exceeded.
- ☐ The software is out of licenses.
- ☐ The VM does not have enough processing power.
- ☐ The firewall is misconfigured.

Question 69

Which of the following are MOST susceptible to birthday attacks?

- ☐ Hashed passwords
- ☐ Digital certificates
- ☐ Encryption passwords
- ☐ One time passwords

Question 70

After an identified security breach, an analyst is tasked to initiate the IR process. Which of the following is the NEXT step the analyst should take?

- ☐ Recovery
- ☐ Identification
- ☐ Preparation
- ☐ Documentation
- ☐ Escalation

Question 71

A company has a security policy that specifies all endpoint computing devices should be assigned a unique identifier that can be tracked via an inventory management system. Recent changes to airline security regulations have cause many executives in the company to travel with mini tablet devices instead of laptops. These tablet devices are difficult to tag and track. An RDP application is used from the tablet to connect into the company network.

Which of the following should be implemented in order to meet the security policy requirements?

- ☐ Virtual desktop infrastructure (VDI)
- ☐ WS-security and geo-fencing
- ☐ A hardware security module (HSM)
- ☐ RFID tagging system
- ☐ MDM software
- ☐ Security Requirements Traceability Matrix (SRTM)

Question 72

A dumpster diver recovers several hard drives from a company and is able to obtain confidential data from one of the hard drives. The company then discovers its information is posted online. Which of the following methods would have MOST likely prevented the data from being exposed?

- ☐ Removing the hard drive from its enclosure
- ☐ Using software to repeatedly rewrite over the disk space
- ☐ Using Blowfish encryption on the hard drives
- ☐ Using magnetic fields to erase the data

Question 73

The availability of a system has been labeled as the highest priority. Which of the following should be focused on the MOST to ensure the objective?

- ☐ Authentication
- ☐ HVAC
- ☐ Full-disk encryption
- ☐ File integrity checking

Question 74

A company is deploying smartphones for its mobile salesforce. These devices are for personal and business use but are owned by the company. Sales personnel will save new customer data via a custom application developed for the company. This application will integrate with the contact information stored in the smartphones and will populate new customer records onto it.

The customer application's data is encrypted at rest, and the application's connection to the back office system is considered secure. The Chief Information Security Officer (CISO) has concerns that customer contact information may be accidentally leaked due to the limited security capabilities of the devices and the planned controls.

Which of the following will be the MOST efficient security control to implement to lower this risk?

- ☐ Implement a mobile data loss agent on the devices to prevent any user manipulation with the contact information.
- ☐ Restrict screen capture features on the devices when using the custom application and the contact information.
- ☐ Restrict contact information storage dataflow so it is only shared with the customer application.
- ☐ Require complex passwords for authentication when accessing the contact information.

Question 75

A security analyst is hardening an authentication server. One of the primary requirements is to ensure there is mutual authentication and delegation. Given these requirements, which of the following technologies should the analyst recommend and configure?

- ☐ LDAP services
- ☐ Kerberos services
- ☐ NTLM services
- ☐ CHAP services

Question 76

A global gaming console manufacturer is launching a new gaming platform to its customers.

Which of the following controls reduces the risk created by malicious gaming customers attempting to circumvent control by way of modifying consoles?

- ☐ Firmware version control
- ☐ Manual software upgrades
- ☐ Vulnerability scanning
- ☐ Automatic updates
- ☐ Network segmentation
- ☐ Application firewalls

Question 77

Which of the following is an important step to take BEFORE moving any installation packages from a test environment to production?

- ☐ Roll back changes in the test environment
- ☐ Verify the hashes of files
- ☐ Archive and compress the files
- ☐ Update the secure baseline

Question 78

A company wants to ensure confidential data from storage media is sanitized in such a way that the drive cannot be reused. Which of the following method should the technician use?

- ☐ Shredding
- ☐ Wiping
- ☐ Low-level formatting
- ☐ Repartitioning
- ☐ Overwriting

Question 79

Which of the following must be intact for evidence to be admissible in court?

- ☐ Chain of custody
- ☐ Order of volatility
- ☐ Legal hold
- ☐ Preservation

Question 80

The Chief Executive Officer (CEO) of a major defense contracting company is traveling overseas for a conference. The CEO will be taking a laptop.

Which of the following should the security administrator implement to ensure confidentiality of the data if the laptop were to be stolen or lost during the trip?

- ☐ Remote wipe
- ☐ Full device encryption
- ☐ BIOS password
- ☐ GPS tracking

Question 81

A manager suspects that an IT employee with elevated database access may be knowingly modifying financial transactions for the benefit of a competitor. Which of the following practices should the manager implement to validate the concern?

- ☐ Separation of duties
- ☐ Mandatory vacations
- ☐ Background checks
- ☐ Security awareness training

Question 82

A technician must configure a firewall to block external DNS traffic from entering a network.

Which of the following ports should they block on the firewall?

- ☐ 53
- ☐ 110
- ☐ 143
- ☐ 443

Question 83

A security engineer wants to add SSL to the public web server. Which of the following would be the FIRST step to implement the SSL certificate?

- ☐ Download the web certificate
- ☐ Install the intermediate certificate
- ☐ Generate a CSR
- ☐ Encrypt the private key

Question 84

A customer calls a technician and needs to remotely connect to a web server to change some code manually. The technician needs to configure the user's machine with protocols to connect to the Unix web server, which is behind a firewall. Which of the following protocols does the technician MOST likely need to configure?

- ☐ SSH
- ☐ SFTP
- ☐ HTTPS
- ☐ SNMP

Question 85

An incident responder receives a call from a user who reports a computer is exhibiting symptoms consistent with a malware infection. Which of the following steps should the responder perform NEXT?

- ☐ Capture and document necessary information to assist in the response.
- ☐ Request the user capture and provide a screenshot or recording of the symptoms.
- ☐ Use a remote desktop client to collect and analyze the malware in real time.
- ☐ Ask the user to back up files for later recovery.

Question 86

In determining when it may be necessary to perform a credentialed scan against a system instead of a non-credentialed scan, which of the following requirements is MOST likely to influence this decision?

- ☐ The scanner must be able to enumerate the host OS of devices scanned.
- ☐ The scanner must be able to footprint the network.
- ☐ The scanner must be able to check for open ports with listening services.
- ☐ The scanner must be able to audit file system permissions

Question 87

Which of the following BEST explains why sandboxing is a best practice for testing software from an untrusted vendor prior to an enterprise deployment?

- ☐ It allows the software to run in an unconstrained environment with full network access.
- ☐ It eliminates the possibility of privilege escalation attacks against the local VM host.
- ☐ It facilitates the analysis of possible malware by allowing it to run until resources are exhausted.
- ☐ It restricts the access of the software to a contained logical space and limits possible damage.

Question 88

A new firewall has been placed into service at an organization. However, a configuration has not been entered on the firewall. Employees on the network segment covered by the new firewall report they are unable to access the network. Which of the following steps should be completed to BEST resolve the issue?

- ☐ The firewall should be configured to prevent user traffic from matching the implicit deny rule.
- ☐ The firewall should be configured with access lists to allow inbound and outbound traffic.
- ☐ The firewall should be configured with port security to allow traffic.
- ☐ The firewall should be configured to include an explicit deny rule.

Question 89

During a lessons learned meeting regarding a previous incident, the security team receives a follow-up action item with the following requirements:

Allow authentication from within the United States anytime

Allow authentication if the user is accessing email or a shared file system

Do not allow authentication if the AV program is two days out of date

Do not allow authentication if the location of the device is in two specific countries

Given the requirements, which of the following mobile deployment authentication types is being utilized?

- ☐ Geofencing authentication
- ☐ Two-factor authentication
- ☐ Context-aware authentication
- ☐ Biometric authentication

Question 90

A company is terminating an employee for misbehavior. Which of the following steps is MOST important in the process of disengagement from this employee?

- ☐ Obtain a list of passwords used by the employee.
- ☐ Generate a report on outstanding projects the employee handled.
- ☐ Have the employee surrender company identification.
- ☐ Have the employee sign an NDA before departing.

Question 91

A network administrator wants to implement a method of securing internal routing. Which of the following should the administrator implement?

- ☐ DMZ
- ☐ NAT
- ☐ VPN
- ☐ PAT

Question 92

Two users need to send each other emails over unsecured channels. The system should support the principle of non-repudiation. Which of the following should be used to sign the user's certificates?

- ☐ RA
- ☐ CA
- ☐ CRL
- ☐ CSR

Question 93

An attacker wearing a building maintenance uniform approached a company's receptionist asking for access to a secure area. The receptionist asks for identification, a building access badge and checks the company's list approved maintenance personnel prior to granting physical access to the secure area.

The controls used by the receptionist are in place to prevent which of the following types of attacks?

- ☐ Tailgating
- ☐ Shoulder surfing
- ☐ Impersonation
- ☐ Hoax

Question 94

A chief Financial Officer (CFO) has asked the Chief Information Officer (CISO) to provide responses to a recent audit report detailing deficiencies in the organization security controls. The CFO would like to know ways in which the organization can improve its authorization controls.

Given the request by the CFO, which of the following controls should the CISO focus on in the report? (Select Three)

- ☐ Password complexity policies
- ☐ Hardware tokens
- ☐ Biometric systems
- ☐ Role-based permissions
- ☐ One time passwords
- ☐ Separation of duties
- ☐ Multifactor authentication
- ☐ Single sign-on
- ☐ Least privilege

Question 95

A product manager is concerned about continuing operations at a facility located in a region undergoing significant political unrest. After consulting with senior management, a decision is made to suspend operations at the facility until the situation stabilizes.

Which of the following risk management strategies BEST describes management's response?

- ☐ Deterrence
- ☐ Mitigation
- ☐ Avoidance
- ☐ Acceptance

Question 96

A penetration tester finds that a company's login credentials for the email client were being sent in clear text. Which of the following should be done to provide encrypted logins to the email server?

- ☐ Enable IPsec and configure SMTP.
- ☐ Enable SSH and LDAP credentials.
- ☐ Enable MIME services and POP3.
- ☐ Enable an SSL certificate for IMAP services.

Question 97

A security engineer is faced with competing requirements from the networking group and database administrators. The database administrators would like ten application servers on the same subnet for ease of administration, whereas the networking group would like to segment all applications from one another.

Which of the following should the security administrator do to rectify this issue?

- ☐ Recommend performing a security assessment on each application, and only segment the applications with the most vulnerability
- ☐ Recommend classifying each application into like security groups and segmenting the groups from one another
- ☐ Recommend segmenting each application, as it is the most secure approach
- ☐ Recommend that only applications with minimal security features should be segmented to protect them

Question 98

An organization is using a tool to perform a source code review. Which of the following describes the case in which the tool incorrectly identifies the vulnerability?

- ☐ False negative
- ☐ True negative
- ☐ False positive
- ☐ True positive

Question 99

A network administrator is brute forcing accounts through a web interface. Which of the following would provide the BEST defense from an account password being discovered?

- ☐ Password history
- ☐ Account lockout
- ☐ Account expiration
- ☐ Password complexity

Question 100

A senior incident response manager receives a call about some external IPs communicating with internal computers during off hours. Which of the following types of malware is MOST likely causing this issue?

- ☐ Botnet
- ☐ Ransomware
- ☐ Polymorphic malware
- ☐ Armored virus

Question 101

Joe, a user, has been trying to send Ann, a different user, an encrypted document via email. Ann has not received the attachment but is able to receive the header information.

Which of the following is MOST likely preventing Ann from receiving the encrypted file?

- ☐ Unencrypted credentials
- ☐ Authentication issues
- ☐ Weak cipher suite
- ☐ Permission issues

Question 102

Which of the following network vulnerability scan indicators BEST validates a successful, active scan?

- ☐ The scan job is scheduled to run during off-peak hours.
- ☐ The scan output lists SQL injection attack vectors.
- ☐ The scan data identifies the use of privileged-user credentials.
- ☐ The scan results identify the hostname and IP address.

Question 103

A systems administrator is reviewing the following information from a compromised server:

Process	DEP	Local Address	Remote Address
LSASS	YES	0.0.0.0	10.210.100.62
APACHE	NO	0.0.0.0	10.130.210.20
MySQL	NO	127.0.0.1	127.0.0.1
TFTP	YES	191.168.1.10	10.34.221.96

Given the above information, which of the following processes was MOST likely exploited via a remote buffer overflow attack?

- ☐ Apache
- ☐ LSASS
- ☐ MySQL
- ☐ TFTP

Question 104

Given the log output:

```
Max 15 00:15:23.431 CRT: #SEC_LOGIN-5-LOGIN_SUCCESS:
Login Success [user: msmith] [Source: 10.0.12.45]
[localport: 23] at 00:15:23:431 CET Sun Mar 15 2015
```

Which of the following should the network administrator do to protect data security?

- ☐ Configure port security for logons
- ☐ Disable telnet and enable SSH
- ☐ Configure an AAA server
- ☐ Disable password and enable RSA authentication

Question 105

Which of the following are the MAIN reasons why a systems administrator would install security patches in a staging environment before the patches are applied to the production server? (Select two.)

- ☐ To prevent server availability issues
- ☐ To verify the appropriate patch is being installed
- ☐ To generate a new baseline hash after patching
- ☐ To allow users to test functionality
- ☐ To ensure users are trained on new functionality

Question 106

A member of the admins group reports being unable to modify the "changes" file on a server. The permissions on the file are as follows:

```
Permissions User Group File
-rwxrw-r-- Admins Admins changes
```

Based on the output above, which of the following BEST explains why the user is unable to modify the "changes" file?

- ☐ The SELinux mode on the server is set to "enforcing."
- ☐ The SELinux mode on the server is set to "permissive."
- ☐ An ACL has been added to the permissions for the file.
- ☐ The admins group does not have adequate permissions to access the file.

Question 107

A forensic investigator has run into difficulty recovering usable files from a SAN drive. Which of the following SAN features might have caused the problem?

- ☐ Storage multipaths
- ☐ Deduplication
- ☐ iSCSI initiator encryption
- ☐ Data snapshots

Question 108

A security team wants to establish an Incident Response plan. The team has never experienced an incident.

Which of the following would BEST help them establish plans and procedures?

- ☐ Table top exercises
- ☐ Lessons learned
- ☐ Escalation procedures
- ☐ Recovery procedures

Question 109

The Chief Security Officer (CISO) at a multinational banking corporation is reviewing a plan to upgrade the entire corporate IT infrastructure. The architecture consists of a centralized cloud environment hosting the majority of data, small server clusters at each corporate location to handle the majority of customer transaction processing, ATMs, and a new mobile banking application accessible from smartphones, tablets, and the Internet via HTTP. The corporation does business having varying data retention and privacy laws.

Which of the following technical modifications to the architecture and corresponding security controls should be implemented to provide the MOST complete protection of data?

- ☐ Revoke exiting root certificates, re-issue new customer certificates, and ensure all transactions are digitally signed to minimize fraud, implement encryption for data in-transit between data centers
- ☐ Ensure all data is encryption according to the most stringent regulatory guidance applicable, implement encryption for data in-transit between data centers, increase data availability by replicating all data, transaction data, logs between each corporate location
- ☐ Store customer data based on national borders, ensure end-to end encryption between ATMs, end users, and servers, test redundancy and COOP plans to ensure data is not inadvertently shifted from one legal jurisdiction to another with more stringent regulations
- ☐ Install redundant servers to handle corporate customer processing, encrypt all customer data to ease the transfer from one country to another, implement end-to-end encryption between mobile applications and the cloud.

Question 110

A user clicked an email link that led to a website than infected the workstation with a virus. The virus encrypted all the network shares to which the user had access. The virus was not deleted or blocked by the company's email filter, website filter, or antivirus. Which of the following describes what occurred?

- ☐ The user's account was over-privileged.
- ☐ Improper error handling triggered a false negative in all three controls.
- ☐ The email originated from a private email server with no malware protection.
- ☐ The virus was a zero-day attack.

Question 111

A security analyst is testing both Windows and Linux systems for unauthorized DNS zone transfers within a LAN on comptia.org from example.org. Which of the following commands should the security analyst use? (Select two.)

- ☐ `nslookup
comptia.org
set type=ANY
ls-d example.org
nslookup
comptia.org
set type=MX
example.org`
- ☐ `dig -axfr comptia.org @example.org`
- ☐ `ipconfig /flushDNS
ifconfig eth0 down
ifconfig eth0 up
dhclient renew`
- ☐ `dig @example.org comptia.org`

Question 112

An organization has hired a penetration tester to test the security of its ten web servers. The penetration tester is able to gain root/administrative access in several servers by exploiting vulnerabilities associated with the implementation of SMTP, POP, DNS, FTP, Telnet, and IMAP.

Which of the following recommendations should the penetration tester provide to the organization to better protect their web servers in the future?

- ☐ Use a honeypot
- ☐ Disable unnecessary services
- ☐ Implement transport layer security
- ☐ Increase application event logging

Question 113

A new mobile application is being developed in-house. Security reviews did not pick up any major flaws, however vulnerability scanning results show fundamental issues at the very end of the project cycle.

Which of the following security activities should also have been performed to discover vulnerabilities earlier in the lifecycle?

- ☐ Architecture review
- ☐ Risk assessment
- ☐ Protocol analysis
- ☐ Code review

Question 114

An external contractor, who has not been given information about the software or network architecture, is conducting a penetration test. Which of the following BEST describes the test being performed?

- ☐ Black box
- ☐ White box
- ☐ Passive reconnaissance
- ☐ Vulnerability scan

Question 115

When designing a web based client server application with single application server and database cluster backend, input validation should be performed:

- ☐ On the client
- ☐ Using database stored procedures
- ☐ On the application server
- ☐ Using HTTPS

Question 116

An analyst is using a vulnerability scanner to look for common security misconfigurations on devices. Which of the following might be identified by the scanner? (Select TWO).

- ☐ The firewall is disabled on workstations.
- ☐ SSH is enabled on servers.
- ☐ Browser homepages have not been customized.
- ☐ Default administrator credentials exist on networking hardware.
- ☐ The OS is only set to check for updates once a day.

Question 117

Which of the following are considered among the BEST indicators that a received message is a hoax? (Choose two.)

- ☐ Minimal use of uppercase letters in the message
- ☐ Warnings of monetary loss to the receiver
- ☐ No valid digital signature from a known security organization
- ☐ Claims of possible damage to computer hardware
- ☐ Embedded URLs

Question 118

Which of the following specifically describes the exploitation of an interactive process to access otherwise restricted areas of the OS?

- ☐ Privilege escalation
- ☐ Pivoting
- ☐ Process affinity
- ☐ Buffer overflow

Question 119

The process of applying a salt and cryptographic hash to a password then repeating the process many times is known as which of the following?

- ☐ Collision resistance
- ☐ Rainbow table
- ☐ Key stretching
- ☐ Brute force attack

Question 120

Which of the following BEST describes an attack where communications between two parties are intercepted and forwarded to each party with neither party being aware of the interception and potential modification to the communications?

- ☐ Spear phishing
- ☐ Man-in-the-middle
- ☐ URL hijacking
- ☐ Transitive access

Question 121

A security analyst has been asked to perform a review of an organization's software development lifecycle. The analyst reports that the lifecycle does not contain a phase in which team members evaluate and provide critical feedback of another developer's code.

Which of the following assessment techniques is BEST described in the analyst's report?

- ☐ Architecture evaluation
- ☐ Baseline reporting
- ☐ Whitebox testing
- ☐ Peer review

Question 122

A company determines that it is prohibitively expensive to become compliant with new credit card regulations. Instead, the company decides to purchase insurance to cover the cost of any potential loss. Which of the following is the company doing?

- ☐ Transferring the risk
- ☐ Accepting the risk
- ☐ Avoiding the risk
- ☐ Migrating the risk

Question 123

The firewall administrator is adding a new certificate for the company's remote access solution. The solution requires that the uploaded file contain the entire certificate chain for the certificate to load properly. The administrator loads the company certificate and the root CA certificate into the file. The file upload is rejected.

Which of the following is required to complete the certificate chain?

- ☐ Certificate revocation list
- ☐ Intermediate authority
- ☐ Recovery agent
- ☐ Root of trust

Question 124

DRAG DROP

A security administrator is given the security and availability profiles for servers that are being deployed.

Match each RAID type with the correct configuration and MINIMUM number of drives.

Review the server profiles and match them with the appropriate RAID type based on integrity, availability, I/O, storage requirements. Instructions:

All drive definitions can be dragged as many times as necessary

Not all placeholders may be filled in the RAID configuration boxes

If parity is required, please select the appropriate number of paritycheckboxes

Server profiles may be dragged only once

If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

Instructions: If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit.

Authentication Server Email Archive Identity Management Server Media Streaming Server **Stripe Data** **Mirror Data**

RAID-0	Server Profile:	RAID-1	Server Profile:
Disk 1 Disk 2 Disk 3 Disk 4 ☐ Parity Data ☐ Parity Data		Disk 1 Disk 2 Disk 3 Disk 4 ☐ Parity Data ☐ Parity Data	
RAID-5	Server Profile:	RAID-6	Server Profile:
Disk 1 Disk 2 Disk 3 Disk 4 ☒ Parity Data ☐ Parity Data		Disk 1 Disk 2 Disk 3 Disk 4 ☒ Parity Data ☒ Parity Data	

Reset All

Question 125

Management wishes to add another authentication factor in addition to fingerprints and passwords in order to have three-factor authentication. Which of the following would BEST satisfy this request?

- ☐ Retinal scan
- ☐ Passphrase
- ☐ Token fob
- ☐ Security question

Question 126

Which of the following is the LEAST secure hashing algorithm?

- ☐ SHA1
- ☐ RIPEMD
- ☐ MD5
- ☐ DES

Question 127

Which of the following are methods to implement HA in a web application server environment? (Select two.)

- ☐ Load balancers
- ☐ Application layer firewalls
- ☐ Reverse proxies
- ☐ VPN concentrators
- ☐ Routers

Question 128

The chief security officer (CSO) has issued a new policy that requires that all internal websites be configured for HTTPS traffic only. The network administrator has been tasked to update all internal sites without incurring additional costs.

Which of the following is the best solution for the network administrator to secure each internal website?

- ☐ Use certificates signed by the company CA
- ☐ Use a signing certificate as a wild card certificate
- ☐ Use certificates signed by a public ca
- ☐ Use a self-signed certificate on each internal server

Question 129

A security analyst is working on a project that requires the implementation of a stream cipher. Which of the following should the analyst use?

- ☐ Hash function
- ☐ Elliptic curve
- ☐ Symmetric algorithm
- ☐ Public key cryptography

Question 130

A security administrator suspects that a DDoS attack is affecting the DNS server. The administrator accesses a workstation with the hostname of workstation01 on the network and obtains the following output from the ipconfig command:

IP Address	Subnet Mask	Default Gateway	DNS Server Address
192.168.1.26	255.255.255.0	192.168.1.254	192.168.1.254

The administrator successfully pings the DNS server from the workstation. Which of the following commands should be issued from the workstation to verify the DDoS attack is no longer occurring?

- ☐ dig www.google.com
- ☐ dig 192.168.1.254
- ☐ dig workstation01.com
- ☐ dig 192.168.1.26

Question 131

A security analyst is investigating a potential breach. Upon gathering, documenting, and securing the evidence, which of the following actions is the NEXT step to minimize the business impact?

- ☐ Launch an investigation to identify the attacking host
- ☐ Initiate the incident response plan
- ☐ Review lessons learned captured in the process
- ☐ Remove malware and restore the system to normal operation

Question 132

A security analyst conducts a manual scan on a known hardened host that identifies many non-compliant items.

Which of the following BEST describe why this has occurred? (Select TWO)

- ☐ Privileged-user certificated were used to scan the host
- ☐ Non-applicable plugins were selected in the scan policy
- ☐ The incorrect audit file was used
- ☐ The output of the report contains false positives
- ☐ The target host has been compromised

Question 133

A buffer overflow can result in:

- ☐ loss of data caused by unauthorized command execution.
- ☐ privilege escalation caused by TPN override.
- ☐ reduced key strength due to salt manipulation.
- ☐ repeated use of one-time keys.

Question 134

An incident involving a workstation that is potentially infected with a virus has occurred. The workstation may have sent confidential data to an unknown internet server.

Which of the following should a security analyst do FIRST?

- ☐ Make a copy of everything in memory on the workstation.
- ☐ Turn off the workstation.
- ☐ Consult information security policy.
- ☐ Run a virus scan.

Question 135

A copy of a highly confidential salary report was recently found on a printer in the IT department. The human resources department does not have this specific printer mapped to its devices, and it is suspected that an employee in the IT department browsed to the share where the report was located and printed it without authorization. Which of the following technical controls would be the BEST choice to immediately prevent this from happening again?

- ☐ Implement a DLP solution and classify the report as confidential, restricting access only to human resources staff
- ☐ Restrict access to the share where the report resides to only human resources employees and enable auditing
- ☐ Have all members of the IT department review and sign the AUP and disciplinary policies
- ☐ Place the human resources computers on a restricted VLAN and configure the ACL to prevent access from the IT department

Question 136

A procedure differs from a policy in that it:

- ☐ is a high-level statement regarding the company's position on a topic.
- ☐ sets a minimum expected baseline of behavior.
- ☐ provides step-by-step instructions for performing a task.
- ☐ describes adverse actions when violations occur.

Question 137

To help prevent one job role from having sufficient access to create, modify, and approve payroll data, which of the following practices should be employed?

- ☐ Least privilege
- ☐ Job rotation
- ☐ Background checks
- ☐ Separation of duties

Question 138

A security administrator suspects a MITM attack aimed at impersonating the default gateway is underway. Which of the following tools should the administrator use to detect this attack? (Select two.)

- ☐ Ping
- ☐ Ipconfig
- ☐ Tracert
- ☐ Netstat
- ☐ Dig
- ☐ Nslookup

Question 139

Which of the following can affect electrostatic discharge in a network operations center?

- ☐ Fire suppression
- ☐ Environmental monitoring
- ☐ Proximity card access
- ☐ Humidity controls

Question 140

An organization is comparing and contrasting migration from its standard desktop configuration to the newest version of the platform. Before this can happen, the Chief Information Security Officer (CISO) voices the need to evaluate the functionality of the newer desktop platform to ensure interoperability with existing software in use by the organization. In which of the following principles of architecture and design is the CISO engaging?

- ☐ Dynamic analysis
- ☐ Change management
- ☐ Baselineing
- ☐ Waterfalling

Question 141

A company's loss control department identifies theft as a recurring loss type over the past year. Based on the department's report, the Chief Information Officer (CIO) wants to detect theft of datacenter equipment.

Which of the following controls should be implemented?

- ☐ Biometrics
- ☐ Cameras
- ☐ Motion detectors
- ☐ Mantraps

Question 142

A datacenter manager has been asked to prioritize critical system recovery priorities.

Which of the following is the MOST critical for immediate recovery?

- ☐ Communications software
- ☐ Operating system software
- ☐ Weekly summary reports to management
- ☐ Financial and production software

Question 143

While troubleshooting a client application connecting to the network, the security administrator notices the following error: Certificate is not valid.

Which of the following is the BEST way to check if the digital certificate is valid?

- ☐ PKI
- ☐ CRL
- ☐ CSR
- ☐ IPSec

Question 144

A security architect has convened a meeting to discuss an organization's key management policy. The organization has a reliable internal key management system, and some argue that it would be best to manage the cryptographic keys internally as opposed to using a solution from a third party. The company should use:

- ☐ the current internal key management system.
- ☐ a third-party key management system that will reduce operating costs.
- ☐ risk benefits analysis results to make a determination.
- ☐ a software solution including secure key escrow capabilities.

Question 145

A bank uses a wireless network to transmit credit card purchases to a billing system.

Which of the following would be MOST appropriate to protect credit card information from being accessed by unauthorized individuals outside of the premises?

- ☐ Air gap
- ☐ Infrared detection
- ☐ Faraday cage
- ☐ Protected distributions

Question 146

Which of the following penetration testing concepts is being used when an attacker uses public Internet databases to enumerate and learn more about a target?

- ☐ Reconnaissance
- ☐ Initial exploitation
- ☐ Pivoting
- ☐ Vulnerability scanning
- ☐ White box testing

Question 147

The Chief Information Security Officer (CISO) is asking for ways to protect against zero-day exploits. The CISO is concerned that an unrecognized threat could compromise corporate data and result in regulatory fines as well as poor corporate publicity. The network is mostly flat, with split staff/guest wireless functionality.

Which of the following equipment **MUST** be deployed to guard against unknown threats?

- ☐ Cloud-based antivirus solution, running as local admin, with push technology for definition updates
- ☐ Implementation of an off-site datacenter hosting all company data, as well as deployment of VDI for all client computing needs
- ☐ Host-based heuristic IPS, segregated on a management VLAN, with direct control of the perimeter firewall ACLs
- ☐ Behavior-based IPS with a communication link to a cloud-based vulnerability and threat feed

Question 148

After correctly configuring a new wireless enabled thermostat to control the temperature of the company's meeting room, Joe, a network administrator determines that the thermostat is not connecting to the internet-based control system. Joe verifies that the thermostat received the expected network parameters and it is associated with the AP. Additionally, the other wireless mobile devices connected to the same wireless network are functioning properly. The network administrator verified that the thermostat works when tested at his residence.

Which of the following is the **MOST** likely reason the thermostat is not connecting to the internet?

- ☐ The company implements a captive portal
- ☐ The thermostat is using the incorrect encryption algorithm
- ☐ the WPA2 shared key is incorrect
- ☐ The company's DHCP server scope is full

Question 149

Which of the following implements two-factor authentication?

- ☐ A phone system requiring a PIN to make a call
- ☐ At ATM requiring a credit card and PIN
- ☐ A computer requiring username and password
- ☐ A datacenter mantrap requiring fingerprint and iris scan

Question 150

During a third-party audit, it is determined that a member of the firewall team can request, approve, and implement a new rule-set on the firewall.

Which of the following will the audit team most likely recommend during the audit out brief?

- ☐ Discretionary access control for the firewall team
- ☐ Separation of duties policy for the firewall team
- ☐ Least privilege for the firewall team
- ☐ Mandatory access control for the firewall team

Question 151

A supervisor in your organization was demoted on Friday afternoon. The supervisor had the ability to modify the contents of a confidential database, as well as other managerial permissions. On Monday morning, the database administrator reported that log files indicated that several records were missing from the database.

Which of the following risk mitigation strategies should have been implemented when the supervisor was demoted?

- ☐ Incident management
- ☐ Routine auditing
- ☐ IT governance
- ☐ Monthly user rights reviews

Question 152

Which of the following attack types BEST describes a client-side attack that is used to manipulate an HTML iframe with JavaScript code via a web browser?

- ☐ Buffer overflow
- ☐ MITM
- ☐ XSS
- ☐ SQLi

Question 153

An employee uses RDP to connect back to the office network.

If RDP is misconfigured, which of the following security exposures would this lead to?

- ☐ A virus on the administrator's desktop would be able to sniff the administrator's username and password.
- ☐ Result in an attacker being able to phish the employee's username and password.
- ☐ A social engineering attack could occur, resulting in the employee's password being extracted.
- ☐ A man in the middle attack could occur, resulting the employee's username and password being captured.

Question 154

An information system owner has supplied a new requirement to the development team that calls for increased non-repudiation within the application. After undergoing several audits, the owner determined that current levels of non-repudiation were insufficient.

Which of the following capabilities would be MOST appropriate to consider implementing in response to the new requirement?

- ☐ Transitive trust
- ☐ Symmetric encryption
- ☐ Two-factor authentication
- ☐ Digital signatures
- ☐ One-time passwords

Question 155

A wireless network uses a RADIUS server that is connected to an authenticator, which in turn connects to a supplicant. Which of the following represents the authentication architecture in use?

- ☐ Open systems authentication
- ☐ Captive portal
- ☐ RADIUS federation
- ☐ 802.1x

Question 156

A company was recently audited by a third party. The audit revealed the company's network devices were transferring files in the clear. Which of the following protocols should the company use to transfer files?

- ☐ HTTPS
- ☐ LDAPS
- ☐ SCP
- ☐ SNMPv3

Question 157

Which of the following would enhance the security of accessing data stored in the cloud? (Select TWO)

- ☐ Block level encryption
- ☐ SAML authentication
- ☐ Transport encryption
- ☐ Multifactor authentication
- ☐ Predefined challenge questions
- ☐ Hashing

Question 158

A forensic expert is given a hard drive from a crime scene and is asked to perform an investigation. Which of the following is the FIRST step the forensic expert needs to take the chain of custody?

- ☐ Make a forensic copy
- ☐ Create a hash of the hard drive
- ☐ Recover the hard drive data
- ☐ Update the evidence log

Question 159

An administrator intends to configure an IPSec solution that provides ESP with integrity protection, but not confidentiality protection.

Which of the following AES modes of operation would meet this integrity-only requirement?

- ☐ HMAC
- ☐ PCBC
- ☐ CBC
- ☐ GCM
- ☐ CFB

Question 160

Which of the following methods minimizes the system interaction when gathering information to conduct a vulnerability assessment of a router?

- ☐ Download the configuration
- ☐ Run a credentialed scan.
- ☐ Conduct the assessment during downtime
- ☐ Change the routing to bypass the router.

Question 161

A technician has installed new vulnerability scanner software on a server that is joined to the company domain. The vulnerability scanner is able to provide visibility over the patch posture of all company's clients.

Which of the following is being used?

- ☐ Gray box vulnerability testing
- ☐ Passive scan
- ☐ Credentialed scan
- ☐ Bypassing security controls

Question 162

Joe a computer forensic technician responds to an active compromise of a database server. Joe first collects information in memory, then collects network traffic and finally conducts an image of the hard drive.

Which of the following procedures did Joe follow?

- ☐ Order of volatility
- ☐ Chain of custody
- ☐ Recovery procedure
- ☐ Incident isolation

Question 163

A security analyst is reviewing patches on servers. One of the servers is reporting the following error message in the WSUS management console:

The computer has not reported status in 30 days.

Given this scenario, which of the following statements BEST represents the issue with the output above?

- ☐ The computer in question has not pulled the latest ACL policies for the firewall.
- ☐ The computer in question has not pulled the latest GPO policies from the management server.
- ☐ The computer in question has not pulled the latest antivirus definitions from the antivirus program.
- ☐ The computer in question has not pulled the latest application software updates.

Question 164

Which of the following solutions should an administrator use to reduce the risk from an unknown vulnerability in a third-party software application?

- ☐ Sandboxing
- ☐ Encryption
- ☐ Code signing
- ☐ Fuzzing

Question 165

A datacenter recently experienced a breach. When access was gained, an RF device was used to access an air-gapped and locked server rack. Which of the following would BEST prevent this type of attack?

- ☐ Faraday cage
- ☐ Smart cards
- ☐ Infrared detection
- ☐ Alarms

Question 166

A database backup schedule consists of weekly full backups performed on Saturday at 12:00 a.m. and daily differential backups also performed at 12:00 a.m. If the database is restored on Tuesday afternoon, which of the following is the number of individual backups that would need to be applied to complete the database recovery?

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4

Question 167

Which of the following would allow for the QUICKEST restoration of a server into a warm recovery site in a case in which server data mirroring is not enabled?

- ☐ Full backup
- ☐ Incremental backup
- ☐ Differential backup
- ☐ Snapshot

Question 168

Which of the following techniques can be bypass a user or computer's web browser privacy settings? (Select Two)

- ☐ SQL injection
- ☐ Session hijacking
- ☐ Cross-site scripting
- ☐ Locally shared objects
- ☐ LDAP injection

Question 169

User from two organizations, each with its own PKI, need to begin working together on a joint project. Which of the following would allow the users of the separate PKIs to work together without connection errors?

- ☐ Trust model
- ☐ Stapling
- ☐ Intermediate CA
- ☐ Key escrow

Question 170

A security analyst reviews the following output:

```
File name: somefile.pdf
File MD5: E289F21CD33E4F57890DDEA5CF267ED2
File size: 1.9 Mb
Created by: Jan Smith
Deleted by: Jan Smith
Date deleted: October 01, 2015 8:43:21 EST
```

The analyst loads the hash into the SIEM to discover if this hash is seen in other parts of the network. After inspecting a large number of files, the security analyst reports the following:

```
File hash: E289F21CD33E4F57890DDEA5CF267ED2
Files found: somestuff.xls, somefile.pdf, nofile.doc
```

Which of the following is the MOST likely cause of the hash being found in other areas?

- ☐ Jan Smith is an insider threat
- ☐ There are MD5 hash collisions
- ☐ The file is encrypted
- ☐ Shadow copies are present

Question 171

After attempting to harden a web server, a security analyst needs to determine if an application remains vulnerable to SQL injection attacks.

Which of the following would BEST assist the analyst in making this determination?

- ☐ tracert
- ☐ Fuzzer
- ☐ nslookup
- ☐ Nmap
- ☐ netcat

Question 172

Which of the following BEST describes a network-based attack that can allow an attacker to take full control of a vulnerable host?

- ☐ Remote exploit
- ☐ Amplification
- ☐ Sniffing
- ☐ Man-in-the-middle

Question 173

A user is presented with the following items during the new-hire onboarding process:

- Laptop
- Secure USB drive
- Hardware OTP token
- External high-capacity HDD
- Password complexity policy
- Acceptable use policy
- HASP key
- Cable lock

Which of the following is one component of multifactor authentication?

- ☐ Secure USB drive
- ☐ Cable lock
- ☐ Hardware OTP token
- ☐ HASP key

Question 174

An administrator has configured a new Linux server with the FTP service. Upon verifying that the service was configured correctly, the administrator has several users test the FTP service. Users report that they are able to connect to the FTP service and download their personal files, however, they cannot transfer new files to the server.

Which of the following will most likely fix the uploading issue for the users?

- ☐ Create an ACL to allow the FTP service write access to user directories
- ☐ Set the Boolean selinux value to allow FTP home directory uploads
- ☐ Reconfigure the ftp daemon to operate without utilizing the PSAV mode
- ☐ Configure the FTP daemon to utilize PAM authentication pass through user permissions

Question 175

Which of the following controls allows a security guard to perform a post-incident review?

- ☐ Detective
- ☐ Preventive
- ☐ Corrective
- ☐ Deterrent

Question 176

An organization identifies a number of hosts making outbound connections to a known malicious IP over port TCP 80. The organization wants to identify the data being transmitted and prevent future connections to this IP.

Which of the following should the organization do to achieve this outcome?

- ☐ Use a protocol analyzer to reconstruct the data and implement a web-proxy.
- ☐ Deploy a web-proxy and then blacklist the IP on the firewall.
- ☐ Deploy a web-proxy and implement IPS at the network edge.
- ☐ Use a protocol analyzer to reconstruct the data and blacklist the IP on the firewall.

Question 177

A company is planning to encrypt the files in several sensitive directories of a file server with a symmetric key. Which of the following could be used?

- ☐ RSA
- ☐ TwoFish
- ☐ Diffie-Helman
- ☐ NTLMv2
- ☐ RIPEMD

Question 178

A business sector is highly competitive, and safeguarding trade secrets and critical information is paramount. On a seasonal basis, an organization employs temporary hires and contractor personnel to accomplish its mission objectives. The temporary and contract personnel require access to network resources only when on the clock.

Which of the following account management practices are the BEST ways to manage these accounts?

- ☐ Employ time-of-day restrictions.
- ☐ Employ password complexity.
- ☐ Employ a random key generator strategy.
- ☐ Employ an account expiration strategy.
- ☐ Employ a password lockout policy

Question 179

Company XYZ has decided to make use of a cloud-based service that requires mutual, certificate-based authentication with its users. The company uses SSL-inspecting IDS at its network boundary and is concerned about the confidentiality of the mutual authentication.

Which of the following model prevents the IDS from capturing credentials used to authenticate users to the new service or keys to decrypt that communication?

- ☐ Use of OATH between the user and the service and attestation from the company domain
- ☐ Use of active directory federation between the company and the cloud-based service
- ☐ Use of smartcards that store x.509 keys, signed by a global CA
- ☐ Use of a third-party, SAML-based authentication service for attestation

Question 180

A Chief Information Security Officer (CISO) has tasked a security analyst with assessing the security posture of an organization and which internal factors would contribute to a security compromise. The analyst performs a walk-through of the organization and discovers there are multiple instances of unlabeled optical media on office desks. Employees in the vicinity either do not claim ownership or disavow any knowledge concerning who owns the media. Which of the following is the MOST immediate action to be taken?

- ☐ Confiscate the media and dispose of it in a secure manner as per company policy.
- ☐ Confiscate the media, insert it into a computer, find out what is on the disc, and then label it and return it to where it was found.
- ☐ Confiscate the media and wait for the owner to claim it. If it is not claimed within one month, shred it.
- ☐ Confiscate the media, insert it into a computer, make a copy of the disc, and then return the original to where it was found.

Question 181

A security administrator is tasked with conducting an assessment made to establish the baseline security posture of the corporate IT infrastructure. The assessment must report actual flaws and weaknesses in the infrastructure. Due to the expense of hiring outside consultants, the testing must be performed using in-house or cheaply available resource. There cannot be a possibility of any requirement being damaged in the test.

Which of the following has the administrator been tasked to perform?

- ☐ Risk transference
- ☐ Penetration test
- ☐ Threat assessment
- ☐ Vulnerability assessment

Question 182

A security administrator has configured a RADIUS and a TACACS+ server on the company's network. Network devices will be required to connect to the TACACS+ server for authentication and send accounting information to the RADIUS server. Given the following information:

RADIUS IP: 192.168.20.45

TACACS+ IP: 10.23.65.7

Which of the following should be configured on the network clients? (Select two.)

- ☐ Accounting port: TCP 389
- ☐ Accounting port: UDP 1812
- ☐ Accounting port: UDP 1813
- ☐ Authentication port: TCP 49
- ☐ Authentication port: TCP 88
- ☐ Authentication port: UDP 636

Question 183

A network administrator needs to allocate a new network for the R&D group. The network must not be accessible from the Internet regardless of the network firewall or other external misconfigurations. Which of the following settings should the network administrator implement to accomplish this?

- ☐ Configure the OS default TTL to 1
- ☐ Use NAT on the R&D network
- ☐ Implement a router ACL
- ☐ Enable protected ports on the switch

Question 184

Company A agrees to provide perimeter protection, power, and environmental support with measurable goals for Company B, but will not be responsible for user authentication or patching of operating systems within the perimeter.

Which of the following is being described?

- ☐ Service level agreement
- ☐ Memorandum of understanding
- ☐ Business partner agreement
- ☐ Interoperability agreement

Question 185

Joe, a salesman, was assigned to a new project that requires him to travel to a client site. While waiting for a flight, Joe, decides to connect to the airport wireless network without connecting to a VPN, and he sends confidential emails to fellow colleagues. A few days later, the company experiences a data breach. Upon investigation, the company learns Joe's emails were intercepted. Which of the following MOST likely caused the data breach?

- ☐ Policy violation
- ☐ Social engineering
- ☐ Insider threat
- ☐ Zero-day attack

Question 186

An application team is performing a load-balancing test for a critical application during off-hours and has requested access to the load balancer to review which servers are up without having the administrator on call. The security analyst is hesitant to give the application team full access due to other critical applications running on the load balancer. Which of the following is the BEST solution for security analyst to process the request?

- ☐ Give the application team administrator access during off-hours.
- ☐ Disable other critical applications before granting the team access.
- ☐ Give the application team read-only access.
- ☐ Share the account with the application team.

Question 187

A web server, which is configured to use TLS with AES-GCM-256, SHA-384, and ECDSA, recently suffered an information loss breach.

Which of the following is MOST likely the cause?

- ☐ Insufficient key bit length
- ☐ Weak cipher suite
- ☐ Unauthenticated encryption method
- ☐ Poor implementation

Question 188

A security administrator is reviewing the following PowerShell script referenced in the Task Scheduler on a database server:

```
$members = GetADGroupMemeber -Identity "Domain Admins" -Recursive | Select - ExpandProperty  
name  
if ($members -notcontains "JohnDoe"){  
Remove-Item -path C:\Database -recurse -force  
}
```

Which of the following did the security administrator discover?

- ☐ Ransomware
- ☐ Backdoor
- ☐ Logic bomb
- ☐ Trojan

Question 189

While reviewing the monthly internet usage it is noted that there is a large spike in traffic classified as "unknown" and does not appear to be within the bounds of the organizations Acceptable Use Policy.

Which of the following tool or technology would work BEST for obtaining more information on this traffic?

- ☐ Firewall logs
- ☐ IDS logs
- ☐ Increased spam filtering
- ☐ Protocol analyzer

Question 190

Which of the following differentiates a collision attack from a rainbow table attack?

- ☐ A rainbow table attack performs a hash lookup
- ☐ A rainbow table attack uses the hash as a password
- ☐ In a collision attack, the hash and the input data are equivalent
- ☐ In a collision attack, the same input results in different hashes

Question 191

A help desk technician receives a phone call from an individual claiming to be an employee of the organization and requesting assistance to access a locked account. The help desk technician asks the individual to provide proof of identity before access can be granted. Which of the following types of attack is the caller performing?

- ☐ Phishing
- ☐ Shoulder surfing
- ☐ Impersonation
- ☐ Dumpster diving

Question 192

Six months into development, the core team assigned to implement a new internal piece of software must convene to discuss a new requirement with the stake holders. A stakeholder identified a missing feature critical to the organization, which must be implemented. The team needs to validate the feasibility of the newly introduced requirement and ensure it does not introduce new vulnerabilities to the software and other applications that will integrate with it.

Which of the following BEST describes what the company?

- ☐ The system integration phase of the SDLC
- ☐ The system analysis phase of SSDSLC
- ☐ The system design phase of the SDLC
- ☐ The system development phase of the SDLC

Question 193

An administrator thinks the UNIX systems may be compromised, but a review of system log files provides no useful information. After discussing the situation with the security team, the administrator suspects that the attacker may be altering the log files and removing evidence of intrusion activity.

Which of the following actions will help detect attacker attempts to further alter log files?

- ☐ Enable verbose system logging
- ☐ Change the permissions on the user's home directory
- ☐ Implement remote syslog
- ☐ Set the bash_history log file to "read only"

Question 194

Joe is exchanging encrypted email with another party. Joe encrypts the initial email with a key. When Joe receives a response, he is unable to decrypt the response with the same key he used initially.

Which of the following would explain the situation?

- ☐ An ephemeral key was used for one of the messages
- ☐ A stream cipher was used for the initial email; a block cipher was used for the reply
- ☐ Out-of-band key exchange has taken place
- ☐ Asymmetric encryption is being used

Question 195

Which of the following is commonly used for federated identity management across multiple organizations?

- ☐ SAML
- ☐ Active Directory
- ☐ Kerberos
- ☐ LDAP

Question 196

A network administrator wants to ensure that users do not connect any unauthorized devices to the company network. Each desk needs to connect a VoIP phone and computer.

Which of the following is the BEST way to accomplish this?

- ☐ Enforce authentication for network devices
- ☐ Configure the phones on one VLAN, and computers on another
- ☐ Enable and configure port channels
- ☐ Make users sign an Acceptable use Agreement

Question 197

A security administrator learns that PII, which was gathered by the organization, has been found in an open forum. As a result, several C-level executives found their identities were compromised, and they were victims of a recent whaling attack.

Which of the following would prevent these problems in the future? (Select TWO).

- ☐ Implement a reverse proxy.
- ☐ Implement an email DLP.
- ☐ Implement a spam filter.
- ☐ Implement a host-based firewall.
- ☐ Implement a HIDS.

Question 198

A network technician is setting up a segmented network that will utilize a separate ISP to provide wireless access to the public area for a company. Which of the following wireless security methods should the technician implement to provide basic accountability for access to the public network?

- ☐ Pre-shared key
- ☐ Enterprise
- ☐ Wi-Fi Protected setup
- ☐ Captive portal

Question 199

The help desk is receiving numerous password change alerts from users in the accounting department. These alerts occur multiple times on the same day for each of the affected users' accounts.

Which of the following controls should be implemented to curtail this activity?

- ☐ Password Reuse
- ☐ Password complexity
- ☐ Password History
- ☐ Password Minimum age

Question 200

An analyst receives an alert from the SIEM showing an IP address that does not belong to the assigned network can be seen sending packets to the wrong gateway.

Which of the following network devices is misconfigured and which of the following should be done to remediate the issue?

- ☐ Firewall; implement an ACL on the interface
- ☐ Router; place the correct subnet on the interface
- ☐ Switch; modify the access port to trunk port
- ☐ Proxy; add the correct transparent interface

Question 201

Which of the following precautions MINIMIZES the risk from network attacks directed at multifunction printers, as well as the impact on functionality at the same time?

- ☐ Isolating the systems using VLANs
- ☐ Installing a software-based IPS on all devices
- ☐ Enabling full disk encryption
- ☐ Implementing a unique user PIN access functions

Question 202

A systems administrator is configuring a system that uses data classification labels.

Which of the following will the administrator need to implement to enforce access control?

- ☐ Discretionary access control
- ☐ Mandatory access control
- ☐ Role-based access control
- ☐ Rule-based access control

Question 203

A user needs to send sensitive information to a colleague using PKI.

Which of the following concepts apply when a sender encrypts the message hash with the sender's private key? (Select TWO)

- ☐ Non-repudiation
- ☐ Email content encryption
- ☐ Steganography
- ☐ Transport security
- ☐ Message integrity

Question 204

Malicious traffic from an internal network has been detected on an unauthorized port on an application server.

Which of the following network-based security controls should the engineer consider implementing?

- ☐ ACLs
- ☐ HIPS
- ☐ NAT
- ☐ MAC filtering

Question 205

Which of the following is a document that contains detailed information about actions that include how something will be done, when the actions will be performed, and penalties for failure?

- ☐ MOU
- ☐ ISA
- ☐ BPA
- ☐ SLA

Question 206

Which of the following is the BEST way for home users to mitigate vulnerabilities associated with IoT devices on their home networks?

- ☐ Power off the devices when they are not in use,
- ☐ Prevent IoT devices from contacting the Internet directly.
- ☐ Apply firmware and software updates upon availability.
- ☐ Deploy a bastion host on the home network.

Question 207

Adhering to a layered security approach, a controlled access facility employs security guards who verify the authorization of all personnel entering the facility. Which of the following terms BEST describes the security control being employed?

- ☐ Administrative
- ☐ Corrective
- ☐ Deterrent
- ☐ Compensating

Question 208

An organization relies heavily on an application that has a high frequency of security updates. At present, the security team only updates the application on the first Monday of each month, even though the security updates are released as often as twice a week.

Which of the following would be the BEST method of updating this application?

- ☐ Configure testing and automate patch management for the application.
- ☐ Configure security control testing for the application.
- ☐ Manually apply updates for the application when they are released.
- ☐ Configure a sandbox for testing patches before the scheduled monthly update.

Question 209

A stock trading company had the budget for enhancing its secondary datacenter approved. Since the main site is a hurricane-affected area and the disaster recovery site is 100 mi (161 km) away, the company wants to ensure its business is always operational with the least amount of man hours needed. Which of the following types of disaster recovery sites should the company implement?

- ☐ Hot site
- ☐ Warm site
- ☐ Cold site
- ☐ Cloud-based site

Question 210

When attackers use a compromised host as a platform for launching attacks deeper into a company's network, it is said that they are:

- ☐ escalating privilege
- ☐ becoming persistent
- ☐ fingerprinting
- ☐ pivoting

Question 211

Audit logs from a small company's vulnerability scanning software show the following findings:

Destinations scanned:

- Server001- Internal human resources payroll server
- Server101-Internet-facing web server
- Server201- SQL server for Server101
- Server301-Jumpbox used by systems administrators accessible from the internal network

Validated vulnerabilities found:

- Server001- Vulnerable to buffer overflow exploit that may allow attackers to install software
- Server101- Vulnerable to buffer overflow exploit that may allow attackers to install software
- Server201-OS updates not fully current
- Server301- Accessible from internal network without the use of jumpbox
- Server301-Vulnerable to highly publicized exploit that can elevate user privileges

Assuming external attackers who are gaining unauthorized information are of the highest concern, which of the following servers should be addressed FIRST?

- ☐ Server001
- ☐ Server101
- ☐ Server201
- ☐ Server301

Question 212

A security administrator must implement a system to ensure that invalid certificates are not used by a custom developed application. The system must be able to check the validity of certificates even when internet access is unavailable.

Which of the following MUST be implemented to support this requirement?

- ☐ CSR
- ☐ OCSP
- ☐ CRL
- ☐ SSH

Question 213

An information security analyst needs to work with an employee who can answer questions about how data for a specific system is used in the business. The analyst should seek out an employee who has the role of:

- ☐ steward
- ☐ owner
- ☐ privacy officer
- ☐ systems administrator

Question 214

A security analyst is mitigating a pass-the-hash vulnerability on a Windows infrastructure. Given the requirement, which of the following should the security analyst do to MINIMIZE the risk?

- ☐ Enable CHAP
- ☐ Disable NTLM
- ☐ Enable Kerberos
- ☐ Disable PAP

Question 215

A security analyst has received the following alert snippet from the HIDS appliance:

PROTOCOL	SIG	SRC . PORT	DST . PORT
TCP	XMAS SCAN	192.168.1.1:1091	192.168.1.2:8891
TCP	XMAS SCAN	192.168.1.1:649	192.168.1.2:9001
TCP	XMAS SCAN	192.168.1.1:2264	192.168.1.2:6455
TCP	XMAS SCAN	192.168.1.1:3464	192.168.1.2:8744

Given the above logs, which of the following is the cause of the attack?

- ☐ The TCP ports on destination are all open
- ☐ FIN, URG, and PSH flags are set in the packet header
- ☐ TCP MSS is configured improperly
- ☐ There is improper Layer 2 segmentation

Question 216

Before an infection was detected, several of the infected devices attempted to access a URL that was similar to the company name but with two letters transposed. Which of the following BEST describes the attack vector used to infect the devices?

- ☐ Cross-site scripting
- ☐ DNS poisoning
- ☐ Typo squatting
- ☐ URL hijacking

Question 217

A security analyst has set up a network tap to monitor network traffic for vulnerabilities. Which of the following techniques would BEST describe the approach the analyst has taken?

- ☐ Compliance scanning
- ☐ Credentialed scanning
- ☐ Passive vulnerability scanning
- ☐ Port scanning

Question 218

A software development company needs to share information between two remote servers, using encryption to protect it. A programmer suggests developing a new encryption protocol, arguing that using an unknown protocol with secure, existing cryptographic algorithm libraries will provide strong encryption without being susceptible to attacks on other known protocols.

Which of the following summarizes the BEST response to the programmer's proposal?

- ☐ The newly developed protocol will only be as secure as the underlying cryptographic algorithms used.
- ☐ New protocols often introduce unexpected vulnerabilities, even when developed with otherwise secure and tested algorithm libraries.
- ☐ A programmer should have specialized training in protocol development before attempting to design a new encryption protocol.
- ☐ The obscurity value of unproven protocols against attacks often outweighs the potential for introducing new vulnerabilities.

Question 219

An organization requires users to provide their fingerprints to access an application. To improve security, the application developers intend to implement multifactor authentication. Which of the following should be implemented?

- ☐ Use a camera for facial recognition
- ☐ Have users sign their name naturally
- ☐ Require a palm geometry scan
- ☐ Implement iris recognition

Question 220

When configuring settings in a mandatory access control environment, which of the following specifies the subjects that can access specific data objects?

- ☐ Owner
- ☐ System
- ☐ Administrator
- ☐ User

Question 221

A botnet has hit a popular website with a massive number of GRE-encapsulated packets to perform a DDoS attack. News outlets discover a certain type of refrigerator was exploited and used to send outbound packets to the website that crashed. To which of the following categories does the refrigerator belong?

- ☐ SoC
- ☐ ICS
- ☐ IoT
- ☐ MFD

Question 222

A security technician would like to obscure sensitive data within a file so that it can be transferred without causing suspicion.

Which of the following technologies would BEST be suited to accomplish this?

- ☐ Transport Encryption
- ☐ Stream Encryption
- ☐ Digital Signature
- ☐ Steganography

Question 223

As part of the SDLC, a third party is hired to perform a penetration test. The third party will have access to the source code, integration tests, and network diagrams. Which of the following BEST describes the assessment being performed?

- ☐ Black box
- ☐ Regression
- ☐ White box
- ☐ Fuzzing

Question 224

A company's user lockout policy is enabled after five unsuccessful login attempts. The help desk notices a user is repeatedly locked out over the course of a workweek. Upon contacting the user, the help desk discovers the user is on vacation and does not have network access. Which of the following types of attacks are MOST likely occurring? (Select two.)

- ☐ Replay
- ☐ Rainbow tables
- ☐ Brute force
- ☐ Pass the hash
- ☐ Dictionary

Question 225

An administrator has concerns regarding the traveling sales team who works primarily from smart phones.

Given the sensitive nature of their work, which of the following would BEST prevent access to the data in case of loss or theft?

- ☐ Enable screensaver locks when the phones are not in use to prevent unauthorized access
- ☐ Configure the smart phones so that the stored data can be destroyed from a centralized location
- ☐ Configure the smart phones so that all data is saved to removable media and kept separate from the device
- ☐ Enable GPS tracking on all smart phones so that they can be quickly located and recovered

Question 226

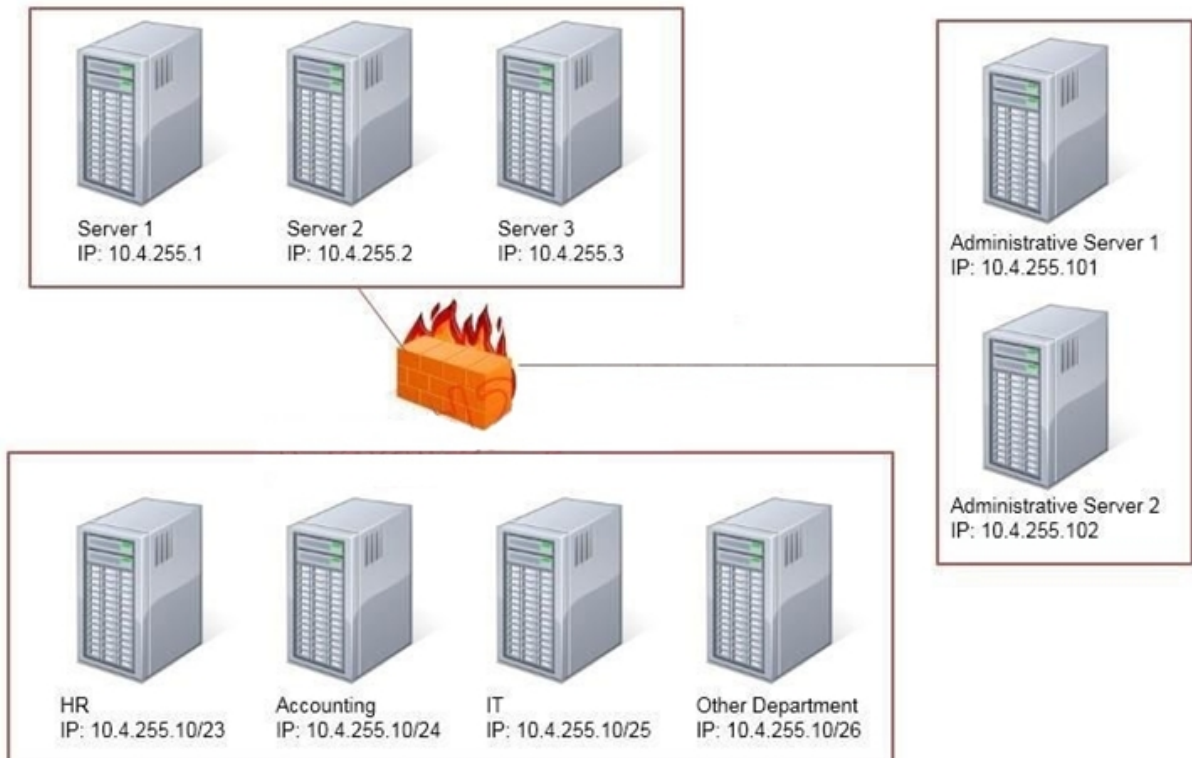
SIMULATION

Task: Configure the firewall (fill out the table) to allow these four rules:

Only allow the Accounting computer to have HTTPS access to the Administrative server.

Only allow the HR computer to be able to communicate with the Server2 System over SCP.

Allow the IT computer to have access to both the AdministrativeServer 1 and Administrative Server 2



Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny

Question 227

A vice president at a manufacturing organization is concerned about desktops being connected to the network. Employees need to log onto the desktops' local account to verify that a product is being created within specifications; otherwise, the desktops should be as isolated as possible. Which of the following is the BEST way to accomplish this?

- ☐ Put the desktops in the DMZ.
- ☐ Create a separate VLAN for the desktops.
- ☐ Air gap the desktops.
- ☐ Join the desktops to an ad-hoc network.

Question 228

A company recently replaced its unsecure email server with a cloud-based email and collaboration solution that is managed and insured by a third party. Which of the following actions did the company take regarding risks related to its email and collaboration services?

- ☐ Transference
- ☐ Acceptance
- ☐ Mitigation
- ☐ Deterrence

Question 229

In an effort to reduce data storage requirements, some company devices to hash every file and eliminate duplicates. The data processing routines are time sensitive so the hashing algorithm is fast and supported on a wide range of systems.

Which of the following algorithms is BEST suited for this purpose?

- ☐ MD5
- ☐ SHA
- ☐ RIPEMD
- ☐ AES

Question 230

An audit has revealed that database administrators are also responsible for auditing database changes and backup logs.

Which of the following access control methodologies would BEST mitigate this concern?

- ☐ Time of day restrictions
- ☐ Principle of least privilege
- ☐ Role-based access control
- ☐ Separation of duties

Question 231

A company's AUP requires:

Passwords must meet complexity requirements.

Passwords are changed at least once every six months.

Passwords must be at least eight characters long.

An auditor is reviewing the following report:

Username	Last login	Last changed
Carol	2 hours	90 days
David	2 hours	30 days
Ann	1 hour	247 days
Joe	0.5 hours	7 days

Which of the following controls should the auditor recommend to enforce the AUP?

- ☐ Account lockout thresholds
- ☐ Account recovery
- ☐ Password expiration
- ☐ Prohibit password reuse

Question 232

A bank is experiencing a DoS attack against an application designed to handle 500 IP-based sessions. In addition, the perimeter router can only handle 1Gbps of traffic.

Which of the following should be implemented to prevent a DoS attacks in the future?

- ☐ Deploy multiple web servers and implement a load balancer
- ☐ Increase the capacity of the perimeter router to 10 Gbps
- ☐ Install a firewall at the network to prevent all attacks
- ☐ Use redundancy across all network devices and services

Question 233

A security administrator is evaluating three different services: radius, diameter, and Kerberos.

Which of the following is a feature that is UNIQUE to Kerberos?

- ☐ It provides authentication services
- ☐ It uses tickets to identify authenticated users
- ☐ It provides single sign-on capability
- ☐ It uses XML for cross-platform interoperability

Question 234

An employee receives an email, which appears to be from the Chief Executive Officer (CEO), asking for a report of security credentials for all users.

Which of the following types of attack is MOST likely occurring?

- ☐ Policy violation
- ☐ Social engineering
- ☐ Whaling
- ☐ Spear phishing

Question 235

A security analyst is hardening a web server, which should allow a secure certificate-based session using the organization's PKI infrastructure. The web server should also utilize the latest security techniques and standards. Given this set of requirements, which of the following techniques should the analyst implement to BEST meet these requirements? (Select two.)

- ☐ Install an X- 509-compliant certificate.
- ☐ Implement a CRL using an authorized CA.
- ☐ Enable and configure TLS on the server.
- ☐ Install a certificate signed by a public CA.
- ☐ Configure the web server to use a host header.

Question 236

A security administrator needs an external vendor to correct an urgent issue with an organization's physical access control system (PACS). The PACS does not currently have internet access because it is running a legacy operation system.

Which of the following methods should the security administrator select the best balances security and efficiency?

- ☐ Temporarily permit outbound internet access for the pacs so desktop sharing can be set up
- ☐ Have the external vendor come onsite and provide access to the PACS directly
- ☐ Set up VPN concentrator for the vendor and restrict access to the PACS using desktop sharing
- ☐ Set up a web conference on the administrator's pc; then remotely connect to the pacs

Question 237

Joe, an employee, wants to show his colleagues how much he knows about smartphones. Joe demonstrates a free movie application that he installed from a third party on his corporate smartphone. Joe's colleagues were unable to find the application in the app stores. Which of the following allowed Joe to install the application? (Select two.)

- ☐ Near-field communication.
- ☐ Rooting/jailbreaking
- ☐ Ad-hoc connections
- ☐ Tethering
- ☐ Sideloaded

Question 238

An incident response analyst at a large corporation is reviewing proxy data log. The analyst believes a malware infection may have occurred. Upon further review, the analyst determines the computer responsible for the suspicious network traffic is used by the Chief Executive Officer (CEO).

Which of the following is the best NEXT step for the analyst to take?

- ☐ Call the CEO directly to ensure awareness of the event
- ☐ Run a malware scan on the CEO's workstation
- ☐ Reimage the CEO's workstation
- ☐ Disconnect the CEO's workstation from the network

Question 239

A business has recently deployed laptops to all sales employees. The laptops will be used primarily from home offices and while traveling, and a high amount of wireless mobile use is expected.

To protect the laptops while connected to untrusted wireless networks, which of the following would be the BEST method for reducing the risk of having the laptops compromised?

- ☐ MAC filtering
- ☐ Virtualization
- ☐ OS hardening
- ☐ Application white-listing

Question 240

Which of the following is a deployment concept that can be used to ensure only the required OS access is exposed to software applications?

- ☐ Staging environment
- ☐ Sandboxing
- ☐ Secure baseline
- ☐ Trusted OS

Question 241

After a user reports slow computer performance, a systems administrator detects a suspicious file, which was installed as part of a freeware software package.

The systems administrator reviews the output below:

```
c:\Windows\system32>netstat -nab
Active Connections
Proto Local Address      Foreign Address    State              Process
TCP    0.0.0.0:135        0.0.0.0:0          LISTENING          RpcSs [svchost.exe]
TCP    0.0.0.0:445        0.0.0.0:0          LISTENING          [svchost.exe]
TCP    192.168.1.10:5000  10.37.213.20      ESTABLISHED        winserver.exe
UDP    192.168.1.10:1900 *. *               SSDPSVR
```

Based on the above information, which of the following types of malware was installed on the user's computer?

- ☐ RAT
- ☐ Keylogger
- ☐ Spyware
- ☐ Worm
- ☐ Bot

Question 242

A security analyst is investigating a suspected security breach and discovers the following in the logs of the potentially compromised server:

Time	Source	Destination	Account Name	Action
11:01:31	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:32	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:33	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:34	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:35	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:36	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:37	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:38	18.12.98.145	10.15.21.100	Joe	Logon Successful

Which of the following would be the BEST method for preventing this type of suspected attack in the future?

- ☐ Implement password expirations
- ☐ Implement restrictions on shared credentials
- ☐ Implement account lockout settings
- ☐ Implement time-of-day restrictions on this server

Question 243

An administrator is configuring access to information located on a network file server named "Bowman". The files are located in a folder named "BalkFiles". The files are only for use by the "Matthews" division and should be read-only. The security policy requires permissions for shares to be managed at the file system layer and also requires those permissions to be set according to a least privilege model. Security policy for this data type also dictates that administrator-level accounts on the system have full access to the files.

The administrator configures the file share according to the following table:

Share permissions

1	Everyone	Full control
---	----------	--------------

File system permissions

2	Bowman\Users	Modify	Inherited
3	Domain\Matthews	Read	Not inherited
4	Bowman\System	Full control	Inherited
5	Bowman\Administrators	Full control	Not inherited

Which of the following rows has been misconfigured?

- ☐ Row 1
- ☐ Row 2
- ☐ Row 3
- ☐ Row 4
- ☐ Row 5

Question 244

Which of the following is the appropriate network structure used to protect servers and services that must be provided to external clients without completely eliminating access for internal users?

- ☐ NAC
- ☐ VLAN
- ☐ DMZ
- ☐ Subnet

Question 245

A security analyst is inspecting the results of a recent internal vulnerability scan that was performed against intranet services.

The scan reports include the following critical-rated vulnerability: Title: Remote Command Execution vulnerability in web server Rating: Critical (CVSS 10.0)

Threat actor: any remote user of the web server

Confidence: certain

Recommendation: apply vendor patches

Which of the following actions should the security analyst perform FIRST?

- ☐ Escalate the issue to senior management.
- ☐ Apply organizational context to the risk rating.
- ☐ Organize for urgent out-of-cycle patching.
- ☐ Exploit the server to check whether it is a false positive.

Question 246

A security manager is creating an account management policy for a global organization with sales personnel who must access corporate network resources while traveling all over the world.

Which of the following practices is the security manager MOST likely to enforce with the policy? (Select TWO)

- ☐ Time-of-day restrictions
- ☐ Password complexity
- ☐ Location-based authentication
- ☐ Group-based access control
- ☐ Standard naming convention

Question 247

A Chief Information Officer (CIO) asks the company's security specialist if the company should spend any funds on malware protection for a specific server. Based on a risk assessment, the ARO value of a malware infection for a server is 5 and the annual cost for the malware protection is \$2500.

Which of the following SLE values warrants a recommendation against purchasing the malware protection?

- ☐ \$500
- ☐ \$1000
- ☐ \$2000
- ☐ \$2500

Question 248

Attackers have been using revoked certificates for MITM attacks to steal credentials from employees of Company.com.

Which of the following options should Company.com implement to mitigate these attacks?

- ☐ Captive portal
- ☐ OCSP stapling
- ☐ Object identifiers
- ☐ Key escrow
- ☐ Extended validation certificate

Question 249

A group of non-profit agencies wants to implement a cloud service to share resources with each other and minimize costs. Which of the following cloud deployment models BEST describes this type of effort?

- ☐ Public
- ☐ Hybrid
- ☐ Community
- ☐ Private

Question 250

An organization's internal auditor discovers that large sums of money have recently been paid to a vendor that management does not recognize. The IT security department is asked to investigate the organizations the organization's ERP system to determine how the accounts payable module has been used to make these vendor payments.

The IT security department finds the following security configuration for the accounts payable module:

New Vendor Entry – Required Role: Accounts Payable Clerk

New Vendor Approval – Required Role: Accounts Payable Clerk

Vendor Payment Entry – Required Role: Accounts Payable Clerk

Vendor Payment Approval – Required Role: Accounts Payable Manager

Which of the following changes to the security configuration of the accounts payable module would BEST mitigate the risk?



New Vendor Entry – Required Role: Accounts Payable Clerk
 New Vendor Approval – Required Role: Accounts Payable Manager
 Vendor Payment Entry – Required Role: Accounts Payable Clerk
 Vendor Payment Approval – Required Role: Accounts Payable Manager



New Vendor Entry – Required Role: Accounts Payable Manager
 New Vendor Approval – Required Role: Accounts Payable Clerk
 Vendor Payment Entry – Required Role: Accounts Payable Clerk
 Vendor Payment Approval – Required Role: Accounts Payable Manager



New Vendor Entry – Required Role: Accounts Payable Clerk
 New Vendor Approval – Required Role: Accounts Payable Clerk
 Vendor Payment Entry – Required Role: Accounts Payable Manager
 Vendor Payment Approval – Required Role: Accounts Payable Manager



New Vendor Entry – Required Role: Accounts Payable Clerk
 New Vendor Approval – Required Role: Accounts Payable Manager
 Vendor Payment Entry – Required Role: Accounts Payable Manager
 Vendor Payment Approval – Required Role: Accounts Payable Manager

Question 251

Which of the following use the SSH protocol?

- ☐ Stelnet
- ☐ SCP
- ☐ SNMP
- ☐ FTPS
- ☐ SSL
- ☐ SFTP

Question 252

A network administrator is creating a new network for an office. For security purposes, each department should have its resources isolated from every other department but be able to communicate back to central servers. Which of the following architecture concepts would BEST accomplish this?

- ☐ Air gapped network
- ☐ Load balanced network
- ☐ Network address translation
- ☐ Network segmentation

Question 253

After a merger between two companies a security analyst has been asked to ensure that the organization's systems are secured against infiltration by any former employees that were terminated during the transition.

Which of the following actions are MOST appropriate to harden applications against infiltration by former employees? (Select TWO)

- ☐ Monitor VPN client access
- ☐ Reduce failed login out settings
- ☐ Develop and implement updated access control policies
- ☐ Review and address invalid login attempts
- ☐ Increase password complexity requirements
- ☐ Assess and eliminate inactive accounts

Question 254

A remote user (User1) is unable to reach a newly provisioned corporate windows workstation. The system administrator has been given the following log files from the VPN, corporate firewall and workstation host.

```
VPN log:
[2015-03-25 08:00.23 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.29 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.40 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:01.11 CST-6: VPN-Server-1: User1 5.5.5.5 authentication succeeded.]
[2015-03-25 09:01.35 CST-6: VPN-Server-1: User1 5.5.5.5 disconnected. Idle timeout.]
Corporate firewall log:
[2015-03-25 14:01.12 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.13 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.14 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.15 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.16 CST: d administrator has been given the following
[2015-03-25 14:01.16 CST: accepted 5.5.5.5(1025) -> 10.1.1.5(3389)]
[2015-03-25 14:01.17 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.18 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
Workstation host firewall log:
[2015-03-21 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-22 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-23 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-24 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-25 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-25 09:01.17 CST-5: 5.5.5.5 -> 10.1.1.5(msrdp) (action=drop)]
[2015-03-26 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
```

Which of the following is preventing the remote user from being able to access the workstation?

- ☐ Network latency is causing remote desktop service request to time out
- ☐ User1 has been locked out due to too many failed passwords
- ☐ Lack of network time synchronization is causing authentication mismatches
- ☐ The workstation has been compromised and is accessing known malware sites
- ☐ The workstation host firewall is not allowing remote desktop connections

Question 255

Which of the following would meet the requirements for multifactor authentication?

- ☐ Username, PIN, and employee ID number
- ☐ Fingerprint and password
- ☐ Smart card and hardware token
- ☐ Voice recognition and retina scan

Question 256

An employee workstation with an IP address of 204.211.38.211/24 reports it is unable to submit print jobs to a network printer at 204.211.38.52/24 after a firewall upgrade. The active firewall rules are as follows:

IP Address	Protocol	Port Number	Action
204.211.38.1/24	ALL	ALL	Permit
204.211.38.211/24	ALL	ALL	Permit
204.211.38.52/24	UDP	631	Permit
204.211.38.52/24	TCP	25	Deny

Assuming port numbers have not been changed from their defaults, which of the following should be modified to allow printing to the network printer?

- ☐ The permit statement for 204.211.38.52/24 should be changed to TCP port 631 instead of UDP
- ☐ The deny statement for 204.211.38.52/24 should be changed to a permit statement
- ☐ The permit statement for 204.211.38.52/24 should be changed to UDP port 443 instead of 631
- ☐ The permit statement for 204.211.38.211/24 should be changed to TCP port 631 only instead of ALL

Question 257

A company is performing an analysis of the corporate enterprise network with the intent of identifying what will cause losses in revenue, referrals, and/or reputation when out of commission. Which of the following is an element of a BIA that is being addressed?

- ☐ Mission-essential function
- ☐ Single point of failure
- ☐ backup and restoration plans
- ☐ Identification of critical systems

Question 258

A security auditor is putting together a report for the Chief Executive Officer (CEO) on personnel security and its impact on the security posture of the whole organization. Which of the following would be the MOST important factor to consider when it comes to personnel security?

- ☐ Insider threats
- ☐ Privilege escalation
- ☐ Hacktivist
- ☐ Phishing through social media
- ☐ Corporate espionage

Question 259

Legal authorities notify a company that its network has been compromised for the second time in two years. The investigation shows the attackers were able to use the same vulnerability on different systems in both attacks.

Which of the following would have allowed the security team to use historical information to protect against the second attack?

- ☐ Key risk indicators
- ☐ Lessons learned
- ☐ Recovery point objectives
- ☐ Tabletop exercise

Question 260

After a routine audit, a company discovers that engineering documents have been leaving the network on a particular port. The company must allow outbound traffic on this port, as it has a legitimate business use. Blocking the port would cause an outage. Which of the following technology controls should the company implement?

- ☐ NAC
- ☐ Web proxy
- ☐ DLP
- ☐ ACL

Question 261

Which of the following types of penetration test will allow the tester to have access only to password hashes prior to the penetration test?

- ☐ Black box
- ☐ Gray box
- ☐ Credentialed
- ☐ White box

Question 262

Joe, a security administrator, needs to extend the organization's remote access functionality to be used by staff while travelling. Joe needs to maintain separate access control functionalities for internal, external, and VOIP services. Which of the following represents the BEST access technology for Joe to use?

- ☐ RADIUS
- ☐ TACACS+
- ☐ Diameter
- ☐ Kerberos

Question 263

Ann, a user, reports she is unable to access an application from her desktop. A security analyst verifies Ann's access and checks the SIEM for any errors. The security analyst reviews the log file from Ann's system and notices the following output:

```
2017-08-21 10:48:12 DROPTCP 172.20.89.232 239.255.255.255 443
1900 250 ----- RECEIVE 2017-08-21 10:48:12 DROPUDP
192.168.72.205 239.255.255.255 443 1900 250 ----- RECEIVE
```

Which of the following is MOST likely preventing Ann from accessing the application from the desktop?

- ☐ Web application firewall
- ☐ DLP
- ☐ Host-based firewall
- ☐ UTM
- ☐ Network-based firewall

Question 264

Two users need to securely share encrypted files via email. Company policy prohibits users from sharing credentials or exchanging encryption keys.

Which of the following can be implemented to enable users to share encrypted data while abiding by company policies?

- ☐ Key escrow
- ☐ Digital signatures
- ☐ PKI
- ☐ Hashing

Question 265

An organization has several production-critical SCADA supervisory systems that cannot follow the normal 30- day patching policy.

Which of the following BEST maximizes the protection of these systems from malicious software?

- ☐ Configure a firewall with deep packet inspection that restricts traffic to the systems.
- ☐ Configure a separate zone for the systems and restrict access to known ports.
- ☐ Configure the systems to ensure only necessary applications are able to run.
- ☐ Configure the host firewall to ensure only the necessary applications have listening ports

Question 266

A high-security defense installation recently begun utilizing large guard dogs that bark very loudly and excitedly at the slightest provocation. Which of the following types of controls does this BEST describe?

- ☐ Deterrent
- ☐ Preventive
- ☐ Detective
- ☐ Compensating

Question 267

An administrator discovers the following log entry on a server:

```
Nov 12 2013 00:23:45 httpd[2342]: GET  
/app2/prod/proc/process.php?input=change;cd%20../../../../etc;cat%20shadow
```

Which of the following attacks is being attempted?

- ☐ Command injection
- ☐ Password attack
- ☐ Buffer overflow
- ☐ Cross-site scripting

Question 268

Confidential emails from an organization were posted to a website without the organization's knowledge. Upon investigation, it was determined that the emails were obtained from an internal actor who sniffed the emails in plain text.

Which of the following protocols, if properly implemented, would have MOST likely prevented the emails from being sniffed? (Select TWO)

- ☐ Secure IMAP
- ☐ DNSSEC
- ☐ S/MIME
- ☐ SMTPS
- ☐ HTTPS

Question 269

A mobile device user is concerned about geographic positioning information being included in messages sent between users on a popular social network platform. The user turns off the functionality in the application, but wants to ensure the application cannot re-enable the setting without the knowledge of the user.

Which of the following mobile device capabilities should the user disable to achieve the stated goal?

- ☐ Device access control
- ☐ Location based services
- ☐ Application control
- ☐ GEO-Tagging

Question 270

A network administrator adds an ACL to allow only HTTPS connections form host 192.168.2.3 to web server 192.168.5.2. After applying the rule, the host is unable to access the server. The network administrator runs the output and notices the configuration below:

```
accesslist 102 permit tcp host 192.168.2.6 eq 3389 host 192.168.5.2
accesslist 102 deny ip any any log
accesslist 102 permit tcp host 192.168.2.3 eq 443 host 192.168.5.2
```

Which of the following rules would be BEST to resolve the issue?

- ☐

```
accesslist 102 permit tcp host 192.168.2.3 host 192.168.5.2 eq 443
accesslist 102 permit tcp host 192.168.2.6 host 192.168.5.2 eq 3389
accesslist 102 deny ip any any log
```
- ☐

```
accesslist 102 permit tcp host 192.168.2.6 host 192.168.5.2 eq 3389
accesslist 102 deny ip any any log
accesslist 102 permit tcp host 192.168.2.3 host 192.168.5.2 eq 443
```
- ☐

```
accesslist 102 permit tcp host 192.168.2.3 eq 443 host 192.168.5.2
accesslist 102 deny ip any any log
accesslist 102 permit tcp host 192.168.2.6 eq 3389 host 192.168.5.2
```
- ☐

```
accesslist 102 permit tcp host 192.168.2.3 host 192.168.5.2
accesslist 102 permit tcp host 192.168.2.6 eq 3389 host 192.168.5.2
accesslist 102 deny ip any any log
```

Question 271

A security engineer is configuring a wireless network with EAP-TLS. Which of the following activities is a requirement for this configuration?

- ☐ Setting up a TACACS+ server
- ☐ Configuring federation between authentication servers
- ☐ Enabling TOTP
- ☐ Deploying certificates to endpoint devices

Question 272

Following the successful response to a data-leakage incident, the incident team lead facilitates an exercise that focuses on continuous improvement of the organization's incident response capabilities. Which of the following activities has the incident team lead executed?

- ☐ Lessons learned review
- ☐ Root cause analysis
- ☐ Incident audit
- ☐ Corrective action exercise

Question 273

Which of the following is the summary of loss for a given year?

- ☐ MTBF
- ☐ ALE
- ☐ SLA
- ☐ ARO

Question 274

A company hires a consulting firm to crawl its Active Directory network with a non-domain account looking for unpatched systems. Actively taking control of systems is out of scope, as is the creation of new administrator accounts. For which of the following is the company hiring the consulting firm?

- ☐ Vulnerability scanning
- ☐ Penetration testing
- ☐ Application fuzzing
- ☐ User permission auditing

Question 275

Which of the following delineates why it is important to perform egress filtering and monitoring on Internet connected security zones of interfaces on a firewall?

- ☐ Egress traffic is more important than ingress traffic for malware prevention
- ☐ To rebalance the amount of outbound traffic and inbound traffic
- ☐ Outbound traffic could be communicating to known botnet sources
- ☐ To prevent DDoS attacks originating from external network

Question 276

An in-house penetration tester has been asked to evade a new DLP system. The tester plans to exfiltrate data through steganography.

Discovery of which of the following would help catch the tester in the act?

- ☐ Abnormally high numbers of outgoing instant messages that contain obfuscated text
- ☐ Large-capacity USB drives on the tester's desk with encrypted zip files
- ☐ Outgoing emails containing unusually large image files
- ☐ Unusual SFTP connections to a consumer IP address

Question 277

A company stores highly sensitive data files used by the accounting system on a server file share. The accounting system uses a service account named accounting-svc to access the file share. The data is protected with a full disk encryption, and the permissions are set as follows:

File system permissions: Users = Read Only

Share permission: accounting-svc = Read Only

Given the listed protections are in place and unchanged, to which of the following risks is the data still subject?

- ☐ Exploitation of local console access and removal of data
- ☐ Theft of physical hard drives and a breach of confidentiality
- ☐ Remote exfiltration of data using domain credentials
- ☐ Disclosure of sensitive data to third parties due to excessive share permissions

Question 278

A Chief Information Officer (CIO) drafts an agreement between the organization and its employees. The agreement outlines ramifications for releasing information without consent and/or approvals. Which of the following BEST describes this type of agreement?

- ☐ ISA
- ☐ NDA
- ☐ MOU
- ☐ SLA

Question 279

A department head at a university resigned on the first day of the spring semester. It was subsequently determined that the department head deleted numerous files and directories from the server-based home directory while the campus was closed. Which of the following policies or procedures could have prevented this from occurring?

- ☐ Time-of-day restrictions
- ☐ Permission auditing and review
- ☐ Offboarding
- ☐ Account expiration

Question 280

Which of the following are used to substantially increase the computation time required to crack a password? (Choose two.)

- ☐ BCrypt
- ☐ Substitution cipher
- ☐ ECDHE
- ☐ PBKDF2
- ☐ Diffie-Hellman

Question 281

A security analyst captures forensic evidence from a potentially compromised system for further investigation. The evidence is documented and securely stored to FIRST:

- ☐ maintain the chain of custody.
- ☐ preserve the data.
- ☐ obtain a legal hold.
- ☐ recover data at a later time.

Question 282

A systems administrator has implemented multiple websites using host headers on the same server. The server hosts two websites that require encryption and other websites where encryption is optional. Which of the following should the administrator implement to encrypt web traffic for the required websites?

- ☐ Extended domain validation
- ☐ TLS host certificate
- ☐ OCSP stapling
- ☐ Wildcard certificate

Question 283

Which of the following cryptography algorithms will produce a fixed-length, irreversible output?

- ☐ AES
- ☐ 3DES
- ☐ RSA
- ☐ MD5

Question 284

A new security policy in an organization requires that all file transfers within the organization be completed using applications that provide secure transfer. Currently, the organization uses FTP and HTTP to transfer files.

Which of the following should the organization implement in order to be compliant with the new policy?

- ☐ Replace FTP with SFTP and replace HTTP with TLS
- ☐ Replace FTP with FTPS and replaces HTTP with TFTP
- ☐ Replace FTP with SFTP and replace HTTP with Telnet
- ☐ Replace FTP with FTPS and replaces HTTP with IPSec

Question 285

Which of the following attack types is being carried out where a target is being sent unsolicited messages via Bluetooth?

- ☐ War chalking
- ☐ Bluejacking
- ☐ Bluesnarfing
- ☐ Rogue tethering

Question 286

A consumer purchases an exploit from the dark web. The exploit targets the online shopping cart of a popular website, allowing the shopper to modify the price of an item as checkout. Which of the following BEST describes this type of user?

- ☐ Insider
- ☐ Script kiddie
- ☐ Competitor
- ☐ Hacktivist
- ☐ APT

Question 287

Which of the following describes the maximum amount of time a mission essential function can operate without the systems it depends on before significantly impacting the organization?

- ☐ MTBF
- ☐ MTTR
- ☐ RTO
- ☐ RPO

Question 288

A company researched the root cause of a recent vulnerability in its software. It was determined that the vulnerability was the result of two updates made in the last release. Each update alone would not have resulted in the vulnerability.

In order to prevent similar situations in the future, the company should improve which of the following?

- ☐ Change management procedures
- ☐ Job rotation policies
- ☐ Incident response management
- ☐ Least privilege access controls

Question 289

Ann is the IS manager for several new systems in which the classification of the systems' data are being decided. She is trying to determine the sensitivity level of the data being processed. Which of the following people should she consult to determine the data classification?

- ☐ Steward
- ☐ Custodian
- ☐ User
- ☐ Owner

Question 290

An organization is providing employees on the shop floor with computers that will log their time based on when they sign on and off the network.

Which of the following account types should the employees receive?

- ☐ Shared account
- ☐ Privileged account
- ☐ User account
- ☐ Service account

Question 291

A small- to medium-sized company wants to block the use of USB devices on its network. Which of the following is the MOST cost-effective way for the security analyst to prevent this?

- ☐ Implement a DLP system
- ☐ Apply a GPO
- ☐ Conduct user awareness training
- ☐ Enforce the AUP.

Question 292

A system administrator wants to implement an internal communication system that will allow employees to send encrypted messages to each other. The system must also support non-repudiation. Which of the following implements all these requirements?

- ☐ Bcrypt
- ☐ Blowfish
- ☐ PGP
- ☐ SHA

Question 293

An auditor is reviewing the following output from a password-cracking tool:

```
user1: Password1
user2: Recovery!
user3: Alaskan10
user4: 4Private
user5: PerForMance2
```

Which of the following methods did the auditor MOST likely use?

- ☐ Hybrid
- ☐ Dictionary
- ☐ Brute force
- ☐ Rainbow table

Question 294

A small company's Chief Executive Officer (CEO) has asked its Chief Security Officer (CSO) to improve the company's security posture quickly with regard to targeted attacks.

Which of the following should the CSO conduct FIRST?

- ☐ Survey threat feeds from services inside the same industry.
- ☐ Purchase multiple threat feeds to ensure diversity and implement blocks for malicious traffic
- ☐ Conduct an internal audit against industry best practices to perform a qualitative analysis.
- ☐ Deploy a UTM solution that receives frequent updates from a trusted industry vendor.

Question 295

A security analyst notices anomalous activity coming from several workstations in the organizations. Upon identifying and containing the issue, which of the following should the security analyst do NEXT?

- ☐ Document and lock the workstations in a secure area to establish chain of custody
- ☐ Notify the IT department that the workstations are to be reimaged and the data restored for reuse
- ☐ Notify the IT department that the workstations may be reconnected to the network for the users to continue working
- ☐ Document findings and processes in the after-action and lessons learned report

Question 296

A security analyst is hardening a WiFi infrastructure.

The primary requirements are the following:

The infrastructure must allow staff to authenticate using the most secure method.

The infrastructure must allow guests to use an "open" WiFi network that logs valid email addresses before granting access to the Internet.

Given these requirements, which of the following statements BEST represents what the analyst should recommend and configure?

- ☐ Configure a captive portal for guests and WPS for staff.
- ☐ Configure a captive portal for staff and WPA for guests.
- ☐ Configure a captive portal for staff and WEP for guests.
- ☐ Configure a captive portal for guest and WPA2 Enterprise for staff

Question 297

A company is deploying a file-sharing protocol access a network and needs to select a protocol for authenticating clients. Management requests that the service be configured in the most secure way possible. The protocol must also be capable of mutual authentication, and support SSO and smart card logons. Which of the following would BEST accomplish this task?

- ☐ Store credentials in LDAP
- ☐ Use NTLM authentication
- ☐ Implement Kerberos
- ☐ Use MSCHAP authentication

Question 298

The help desk received a call after hours from an employee who was attempting to log into the payroll server remotely. When the help desk returned the call the next morning, the employee was able to log into the server remotely without incident. However, the incident occurred again the next evening.

Which of the following BEST describes the cause of the issue?

- ☐ The password expired on the account and needed to be reset
- ☐ The employee does not have the rights needed to access the database remotely
- ☐ Time-of-day restrictions prevented the account from logging in
- ☐ The employee's account was locked out and needed to be unlocked

Question 299

A technician suspects that a system has been compromised. The technician reviews the following log entry:

WARNING- hash mismatch: C:\Window\SysWOW64\user32.dll

WARNING- hash mismatch: C:\Window\SysWOW64\kernel32.dll

Based solely on the above information, which of the following types of malware is MOST likely installed on the system?

- ☐ Rootkit
- ☐ Ransomware
- ☐ Trojan
- ☐ Backdoor

Question 300

While performing a penetration test, the technicians want their efforts to go unnoticed for as long as possible while they gather useful data about the network they are assessing.

Which of the following would be the BEST choice for the technicians?

- ☐ Vulnerability scanner
- ☐ Offline password cracker
- ☐ Packet sniffer
- ☐ Banner grabbing

Question 301

A security administrator is developing training for corporate users on basic security principles for personal email accounts.

Which of the following should be mentioned as the MOST secure way for password recovery?

- ☐ Utilizing a single Q for password recovery
- ☐ Sending a PIN to a smartphone through text message
- ☐ Utilizing CAPTCHA to avoid brute force attacks
- ☐ Use a different e-mail address to recover password

Question 302

A security administrator is trying to eradicate a worm, which is spreading throughout the organization, using an old remote vulnerability in the SMB protocol. The worm uses Nmap to identify target hosts within the company. The administrator wants to implement a solution that will eradicate the current worm and any future attacks that may be using zero-day vulnerabilities.

Which of the following would BEST meet the requirements when implemented?

- ☐ Host-based firewall
- ☐ Enterprise patch management system
- ☐ Network-based intrusion prevention system
- ☐ Application blacklisting
- ☐ File integrity checking

Question 303

A company is investigating a data compromise where data exfiltration occurred. Prior to the investigation, the supervisor terminates an employee as a result of the suspected data loss. During the investigation, the supervisor is absent for the interview, and little evidence can be provided from the role-based authentication system in use by the company.

The situation can be identified for future mitigation as which of the following?

- ☐ Job rotation
- ☐ Log failure
- ☐ Lack of training
- ☐ Insider threat

Question 304

A malicious system continuously sends an extremely large number of SYN packets to a server. Which of the following BEST describes the resulting effect?

- ☐ The server will be unable to server clients due to lack of bandwidth
- ☐ The server's firewall will be unable to effectively filter traffic due to the amount of data transmitted
- ☐ The server will crash when trying to reassemble all the fragmented packets
- ☐ The server will exhaust its memory maintaining half-open connections

Question 305

A member of a digital forensics team, Joe arrives at a crime scene and is preparing to collect system data. Before powering the system off, Joe knows that he must collect the most volatile data first.

Which of the following is the correct order in which Joe should collect the data?

- ☐ CPU cache, paging/swap files, RAM, remote logging data
- ☐ RAM, CPU cache, Remote logging data, paging/swap files
- ☐ Paging/swap files, CPU cache, RAM, remote logging data
- ☐ CPU cache, RAM, paging/swap files, remote logging data

Question 306

A security administrator is trying to encrypt communication. For which of the following reasons should administrator take advantage of the Subject Alternative Name (SAM) attribute of a certificate?

- ☐ It can protect multiple domains
- ☐ It provides extended site validation
- ☐ It does not require a trusted certificate authority
- ☐ It protects unlimited subdomains

Question 307

Users are attempting to access a company's website but are transparently redirected to another websites. The users confirm the URL is correct. Which of the following would BEST prevent this issue in the future?

- ☐ DNSSEC
- ☐ HTTPS
- ☐ IPSec
- ☐ TLS/SSL

Question 308

An administrator is replacing a wireless router. The configuration of the old wireless router was not documented before it stopped functioning. The equipment connecting to the wireless network uses older legacy equipment that was manufactured prior to the release of the 802.11i standard. Which of the following configuration options should the administrator select for the new wireless router?

- ☐ WPA+CCMP
- ☐ WPA2+CCMP
- ☐ WPA+TKIP
- ☐ WPA2+TKIP

Question 309

Joe notices there are several user accounts on the local network generating spam with embedded malicious code.

Which of the following technical control should Joe put in place to BEST reduce these incidents?

- ☐ Account lockout
- ☐ Group Based Privileges
- ☐ Least privilege
- ☐ Password complexity

Question 310

A security administrator receives an alert from a third-party vendor that indicates a certificate that was installed in the browser has been hijacked at the root of a small public CA. The security administrator knows there are at least four different browsers in use on more than a thousand computers in the domain worldwide.

Which of the following solutions would be BEST for the security administrator to implement to most efficiently assist with this issue?

- ☐ SSL
- ☐ CRL
- ☐ PKI
- ☐ ACL