SY0-501.exam.210q

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

SY0-501

CompTIA Security+ Certification Exam

Exam A

QUESTION 1

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: ACG
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following encryption methods does PKI typically use to securely project keys?

A. Elliptic curve
B. Digital signatures

C. Asymmetric
D. Obfuscation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
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

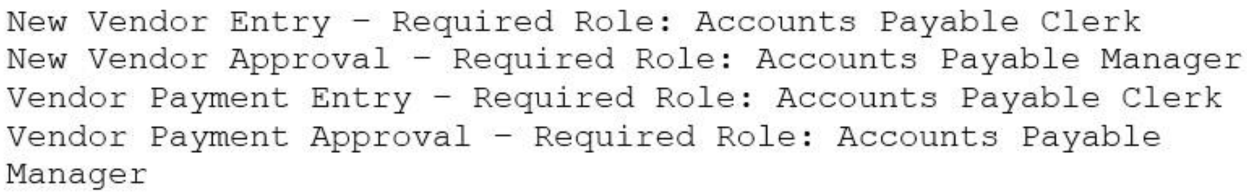
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

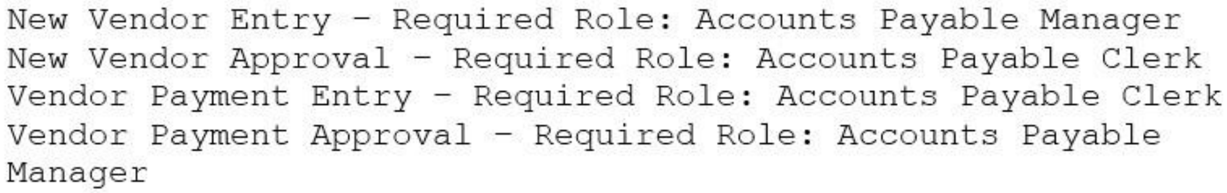
QUESTION 4
An organization's internal auditor discovers that large sums of money have recently been paid to a vendor that management does not recognize. The IT security department is asked to investigate the organizations the organization's ERP system to determine how the accounts payable module has been used to make these vendor payments.
The IT security department finds the following security configuration for the accounts payable module:

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

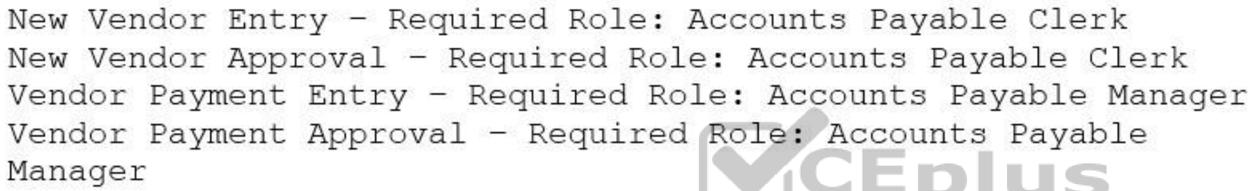
Which of the following changes to the security configuration of the accounts payable module would BEST mitigate the risk?



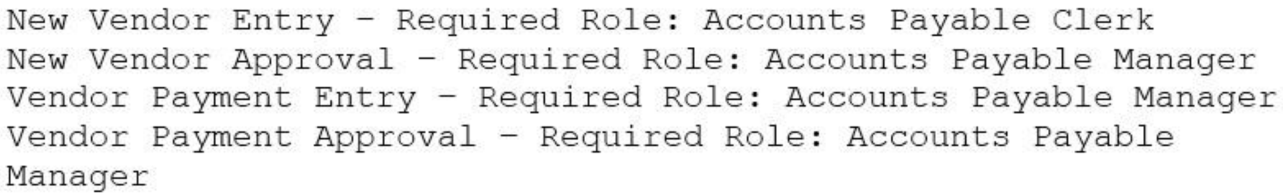
New Vendor Entry – Required Role: Accounts Payable Clerk
New Vendor Approval – Required Role: Accounts Payable Manager
Vendor Payment Entry – Required Role: Accounts Payable Clerk
Vendor Payment Approval – Required Role: Accounts Payable
Manager



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



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



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

A.

B.

C.

D.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5

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 6

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:

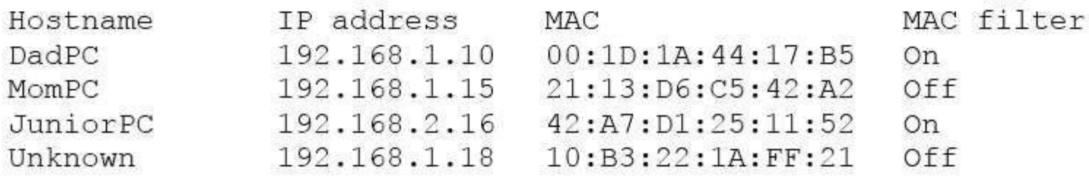
QUESTION 7
An organization finds that most help desk calls are regarding account lockout due to a variety of applications running on different systems. Management is looking for a solution to reduce the number of account lockouts while improving security. Which of the following is the BEST solution for 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 8
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 9
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 10

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 11

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 12

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: D
Section: (none)
Explanation

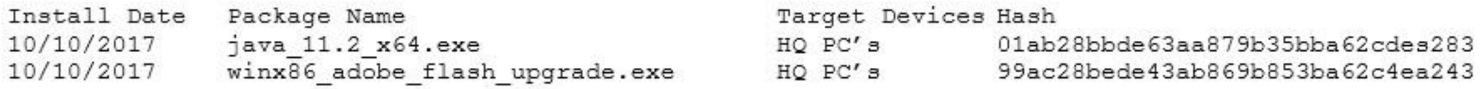
Explanation/Reference:

QUESTION 13

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 14
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 15
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 16
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 17
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 18
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 19
A company's user lockout policy is enabled after five unsuccessful login attempts. The help desk notices a user is repeatedly locked out over the course of a workweek. Upon contacting the user, the help desk discovers the user is on vacation and does not have network access. Which of the following types of attacks are
MOST likely occurring? (Select two.)

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

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
QUESTION 20
Ann. An employee in the payroll department, has contacted the help desk citing multiple issues with her device, including:

- Slow performance
- Word documents, PDFs, and images no longer opening
- A pop-up

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
An administrator is replacing a wireless router. The configuration of the old wireless router was not documented before it stopped functioning. The equipment connecting to the wireless network uses older legacy equipment that was manufactured prior to the release of the 802.11i standard. Which of the following configuration options should the administrator select for the new wireless router?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 22
An application team is performing a load-balancing test for a critical application during off-hours and has requested access to the load balancer to review which servers are up without having the administrator on call. The security analyst is hesitant to give the application team full access due to other critical applications running on the load balancer. Which of the following is the BEST solution for security analyst to process the request?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Which of the following cryptographic attacks would salting of passwords render ineffective?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
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 25
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 26
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 27

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 28

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 29

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:

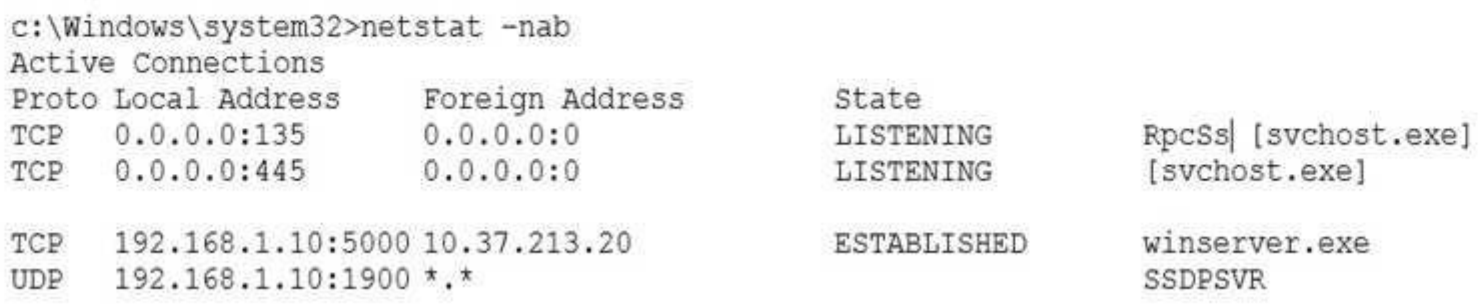
QUESTION 30
Which of the following specifically describes the exploitation of an interactive process to access otherwise restricted areas of the OS?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
After a user reports stow computer performance, a systems administrator detects a suspicious file, which was installed as part of a freeware software package.
The systems administrator reviews the output below:



```
c:\Windows\system32>netstat -nab
Active Connections
Proto Local Address      Foreign Address         State               
TCP   0.0.0.0:135        0.0.0.0:0               LISTENING        RpcSs| [svchost.exe]
TCP   0.0.0.0:445        0.0.0.0:0               LISTENING        [svchost.exe]

TCP   192.168.1.10:5000  10.37.213.20            ESTABLISHED      winserver.exe
UDP   192.168.1.10:1900  *.*                                      SSDPSVR
```

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
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 33
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 34
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 35
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:

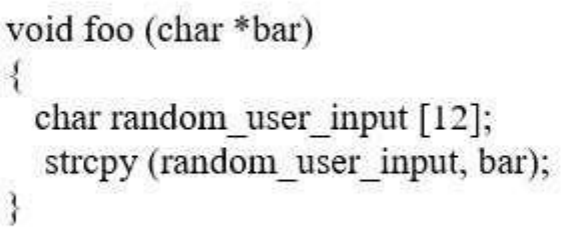
QUESTION 36
Which of the following occurs when the security of a web application relies on JavaScript for input validation?

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 37
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 overflowD. Backdoor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
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 39
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 40
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 41
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:

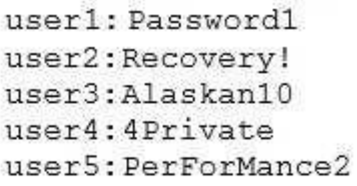
QUESTION 42
A security analyst is hardening a web server, which should allow a secure certificate-based session using the organization's PKI infrastructure. The web server should also utilize the latest security techniques and standards. Given this set of requirements, which of the following techniques 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 43
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 44

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 45

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 46
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 47
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 48

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?

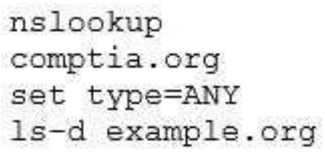
A. The firewall should be configured to prevent user traffic form matching the implicit deny rule.
B. The firewall should be configured with access lists to allow inbound and outbound traffic.
C. The firewall should be configured with port security to allow traffic.
D. The firewall should be configured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

Correct Answer: A
Section: (none)
Explanation

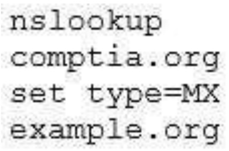
Explanation/Reference:

QUESTION 49

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



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

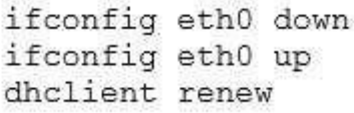


```
nslookup
comptia.org
set type=MX
example.org
```

B.

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

D. `ipconfig /flushDNS`

E. 

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

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50

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

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51

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

A. ISA
B. NDA
C. MOU

D. SLA

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53

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

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

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54

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

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55

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

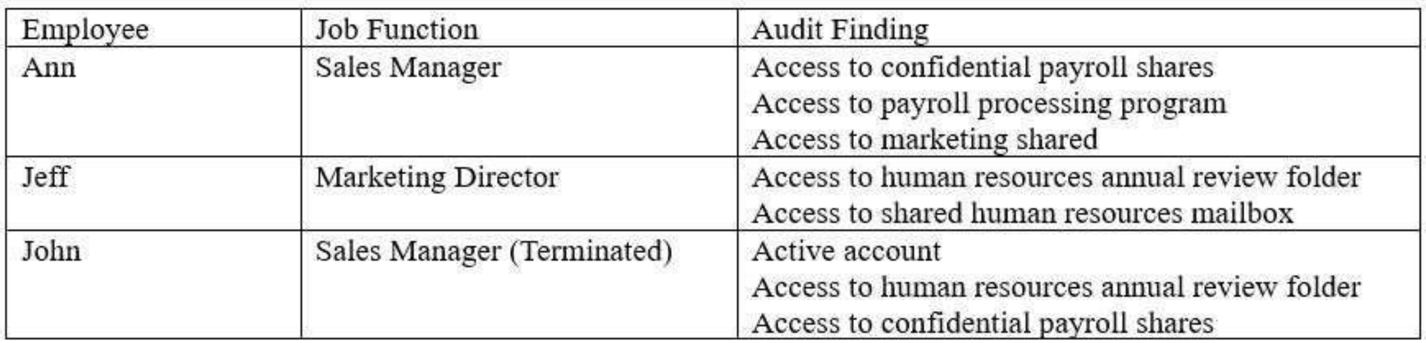
A. CCM
B. CBC
C. GCM
D. DSA
E. CFB

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56

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



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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

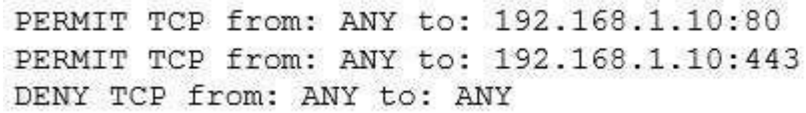
QUESTION 57
A security engineer is configuring a wireless network that must support mutual authentication of the wireless client and the authentication server before users provide credentials. The wireless network must also support authentication with usernames and passwords. Which of the following authentication protocols MUST the security engineer select?

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

Correct Answer: C
Section: (none)
Explanation

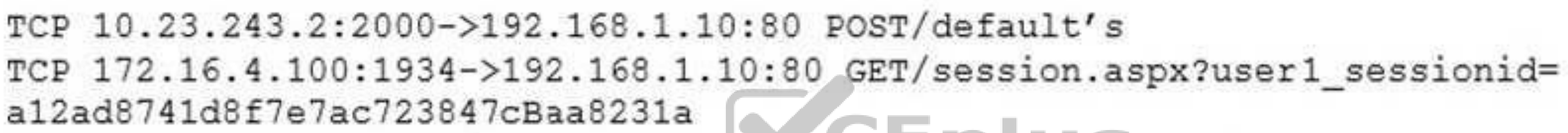
Explanation/Reference:

QUESTION 58
A system’s administrator has finished configuring firewall ACL to allow access to a new web server.



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

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



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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Which of the following vulnerability types would the type of hacker known as a script kiddie be MOST dangerous against?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
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 61
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 62
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 63
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 64

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 65

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 66
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: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
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 68
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 69
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 70

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?

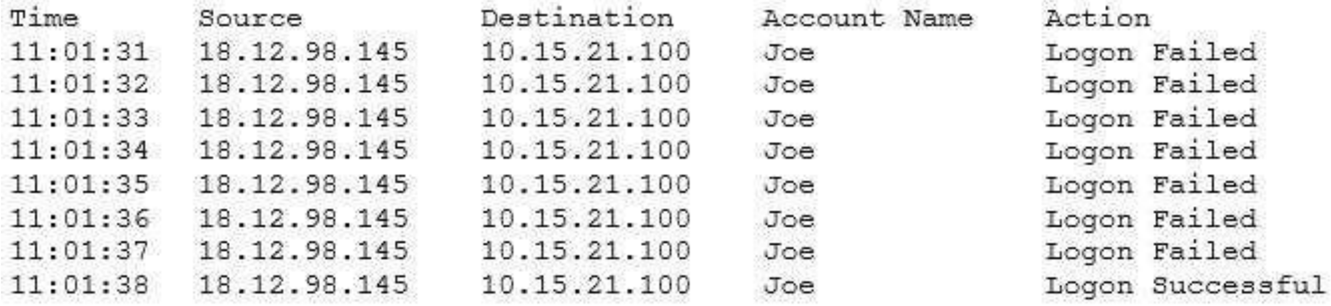
A. The certificate was self signed, and the CA was not imported by employees or customers
B. The root CA has revoked the certificate of the intermediate CA
C. The valid period for the certificate has passed, and a new certificate has not been issued
D. The key escrow server has blocked the certificate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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71

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 72
DRAG DROP

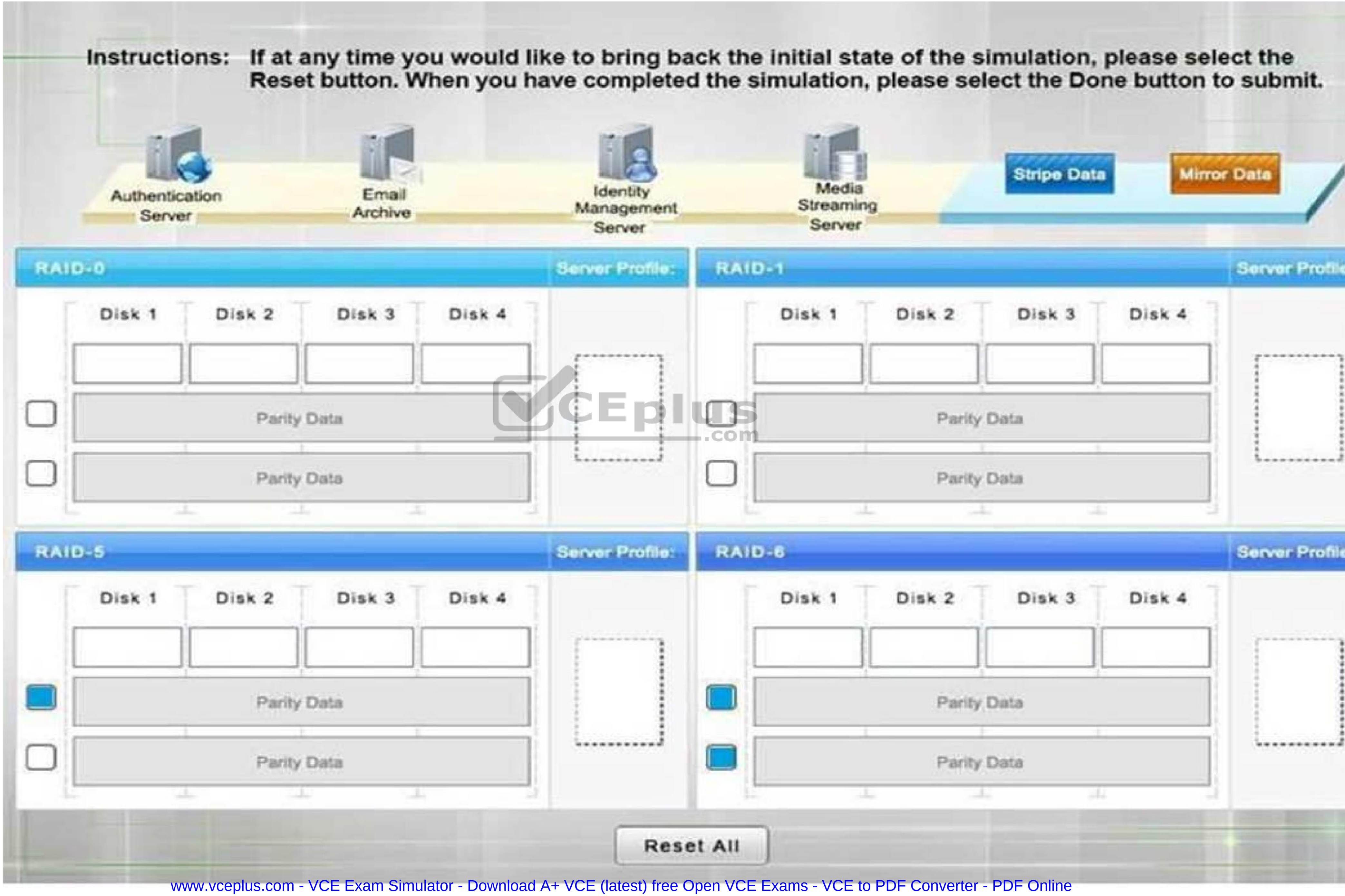
A security administrator is given the security and availability profiles for servers that are being deployed.

1. Match each RAID type with the correct configuration and MINIMUM number of drives.
2. Review the server profiles and match them with the appropriate RAID type based on integrity, availability, I/O, storage requirements. Instructions:

▪ All drive definitions can be dragged as many times as necessary
▪ Not all placeholders may be filled in the RAID configuration boxes
▪ If parity is required, please select the appropriate number of parity checkboxes ▪
Server profiles may be dragged only once

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

Select and Place:



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.

RAID-0 — Server Profile:

Disk 1	Disk 2	Disk 3	Disk 4

□ Parity Data

□ Parity Data

RAID-1 — Server Profile

Disk 1	Disk 2	Disk 3	Disk 4

□ Parity Data

□ Parity Data

RAID-5 — Server Profile:

Disk 1	Disk 2	Disk 3	Disk 4

☑ Parity Data

□ Parity Data

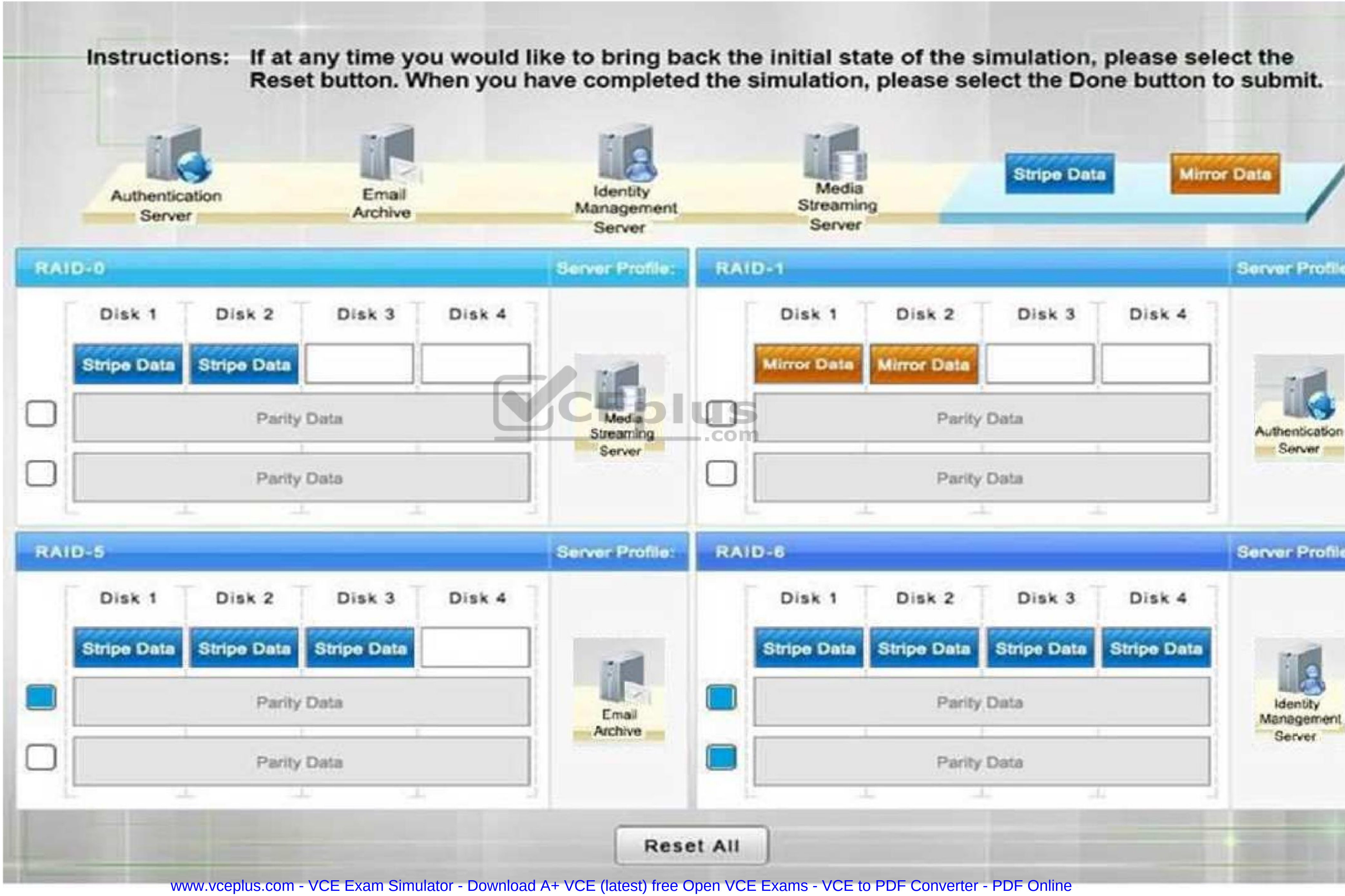
RAID-6 — Server Profile

Disk 1	Disk 2	Disk 3	Disk 4

☑ Parity Data

☑ Parity Data

Correct Answer:



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.

RAID-0 — Server Profile: Media Streaming Server

Disk 1	Disk 2	Disk 3	Disk 4
Stripe Data	Stripe Data		

□ Parity Data

□ Parity Data

RAID-1 — Server Profile: Authentication Server

Disk 1	Disk 2	Disk 3	Disk 4
Mirror Data	Mirror Data		

□ Parity Data

□ Parity Data

RAID-5 — Server Profile: Email Archive

Disk 1	Disk 2	Disk 3	Disk 4
Stripe Data	Stripe Data	Stripe Data	

☑ Parity Data

□ Parity Data

RAID-6 — Server Profile: Identity Management Server

Disk 1	Disk 2	Disk 3	Disk 4
Stripe Data	Stripe Data	Stripe Data	Stripe Data

☑ Parity Data

☑ Parity Data

Section: (none)
Explanation

Explanation/Reference:
Explanation:
RAID-0 is known as striping. It is not a fault tolerant solution but does improve disk performance for read/write operations. Striping requires a minimum of two disks and does not use parity.
RAID-0 can be used where performance is required over fault tolerance, such as a media streaming server.
RAID-1 is known as mirroring because the same data is written to two disks so that the two disks have identical data. This is a fault tolerant solution that halves the storage space. A minimum of two disks are used in mirroring and does not use parity. RAID-1 can be used where fault tolerance is required over performance, such as on an authentication server. RAID-5 is a fault tolerant solution that uses parity and striping. A minimum of three disks are required for RAID-5 with one disk's worth of space being used for parity information. However, the parity information is distributed across all the disks. RAID-5 can recover from a sing disk failure. RAID-6 is a fault tolerant solution that uses dual parity and striping. A minimum of four disks are required for RAID-6. Dual parity allows RAID-6 to recover from the simultaneous failure of up to two disks. Critical data should be stored on a RAID-6 system.

http://www.adaptec.com/en-us/solutions/raid_levels.html

QUESTION 73
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 74
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 75
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 76
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 77
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 78
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 79
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: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
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 81
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 82
A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website. During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine.

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83

Which of the following use the SSH protocol?

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

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85

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

A. MTBF
B. ALE

C. SLA
D. ARO

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
A Security Officer on a military base needs to encrypt several smart phones that will be going into the field.

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
An organization relies heavily on an application that has a high frequency of security updates. At present, the security team only updates the application on the first Monday of each month, even though the security updates are released as often as twice a week.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
A security technician would like to obscure sensitive data within a file so that it can be transferred without causing suspicion.

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

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 91
A supervisor in your organization was demoted on Friday afternoon. The supervisor had the ability to modify the contents of a confidential database, as well as other managerial permissions. On Monday morning, the database administrator reported that log files indicated that several records were missing from the database.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Which of the following attack types is being carried out where a target is being sent unsolicited messages via Bluetooth?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 93
Joe is exchanging encrypted email with another party. Joe encrypts the initial email with a key. When Joe receives a response, he is unable to decrypt the response with the same key he used initially.

Which of the following would explain the situation?

A. An ephemeral key was used for one of the messages
B. A stream cipher was used for the initial email; a block cipher was used for the reply
C. Out-of-band key exchange has taken place

D. Asymmetric encryption is being used

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:
Explanation:
Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes.

QUESTION 94
Recently several employees were victims of a phishing email that appeared to originate from the company president. The email claimed the employees would be disciplined if they did not click on a malicious link in the message.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Which of the following is the LEAST secure hashing algorithm?

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

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Phishing emails frequently take advantage of high-profile catastrophes reported in the news.

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
New magnetic locks were ordered for an entire building. In accordance with company policy, employee safety is the top priority.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99

An administrator discovers the following log entry on a server:

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

Which of the following attacks is being attempted?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Which of the following would verify that a threat does exist and security controls can easily be bypassed without actively testing an application?

A. Protocol analyzer
B. Vulnerability scan
C. Penetration test
D. Port scanner

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 102
Which of the following technologies would be MOST appropriate to utilize when testing a new software patch before a company-wide deployment?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 103
A system administrator needs to implement 802.1x whereby when a user logs into the network, the authentication server communicates to the network switch and assigns the user to the proper VLAN.

Which of the following protocols should be used?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
A security administrator receives notice that a third-party certificate authority has been compromised, and new certificates will need to be issued.

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
A company wants to host a publicly available server that performs the following functions:

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 106
A security administrator is developing training for corporate users on basic security principles for personal email accounts.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
A company researched the root cause of a recent vulnerability in its software. It was determined that the vulnerability was the result of two updates made in the last release. Each update alone would not have resulted in the vulnerability.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109

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

Which of the following should be implemented?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110

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

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

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

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

QUESTION 111
A security program manager wants to actively test the security posture of a system. The system is not yet in production and has no uptime requirement or active user base.

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

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 112
A new intern in the purchasing department requires read access to shared documents. Permissions are normally controlled through a group called "Purchasing", however, the purchasing group permissions allow write access.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113

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

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

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

Correct Answer: C
Section: (none)
Explanation

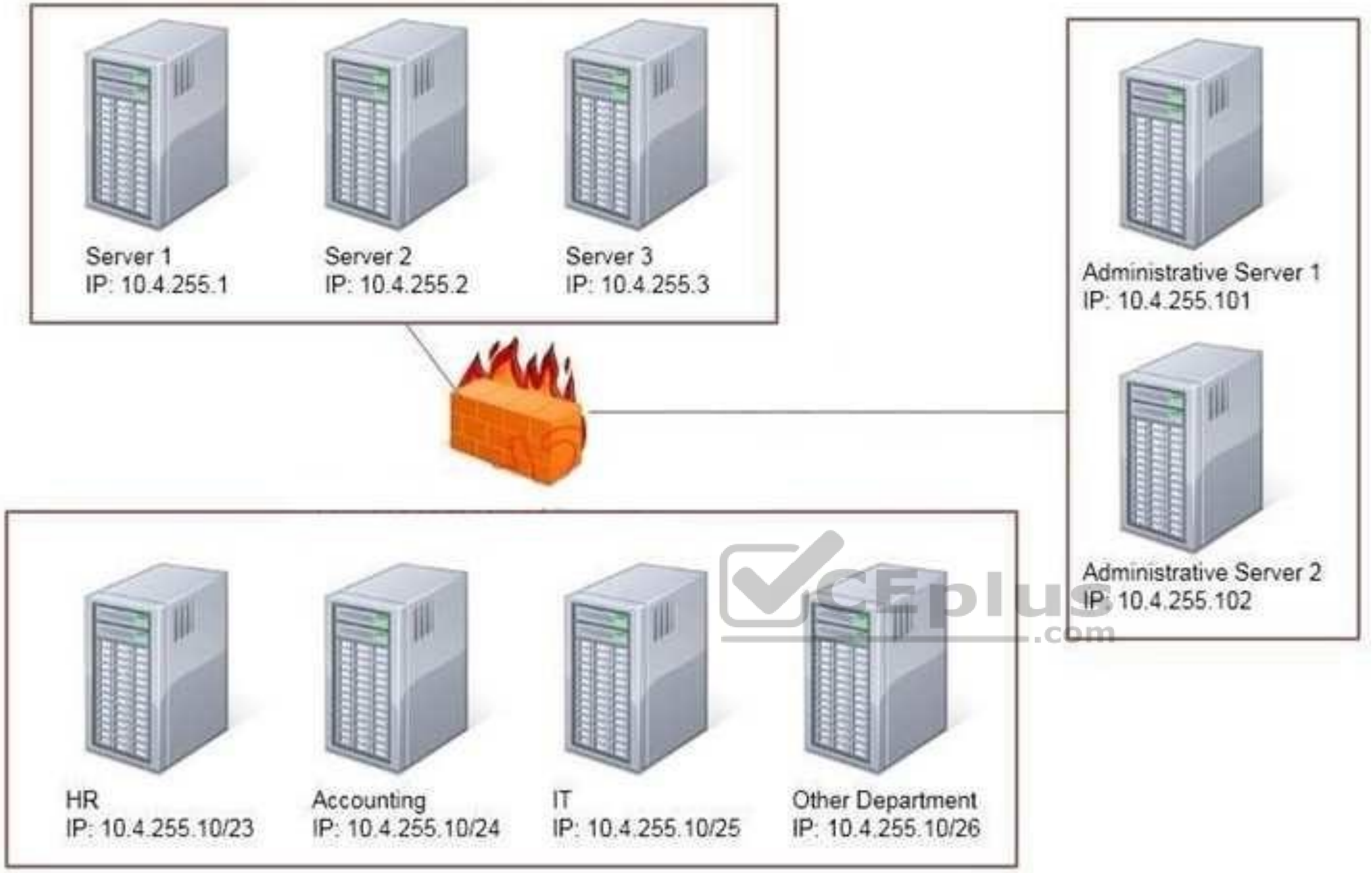
Explanation/Reference:

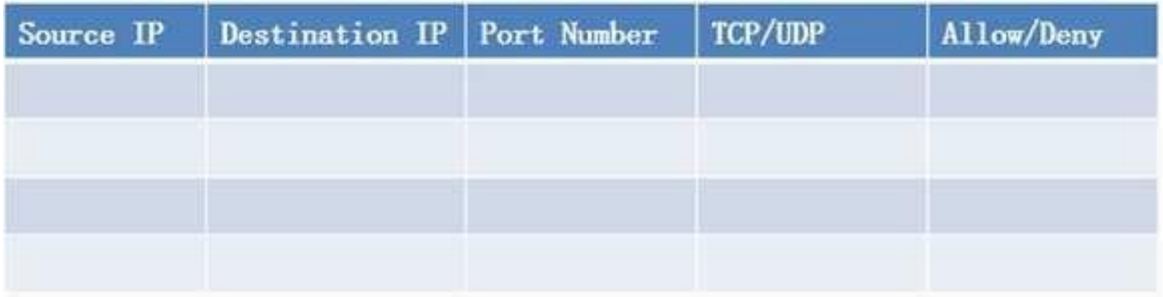
QUESTION 114

SIMULATION

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

- Only allow the Accounting computer to have HTTPS access to the Administrative server.
- Only allow the HR computer to be able to communicate with the Server 2 System over SCP.
- Allow the IT computer to have access to both the Administrative Server 1 and Administrative Server 2



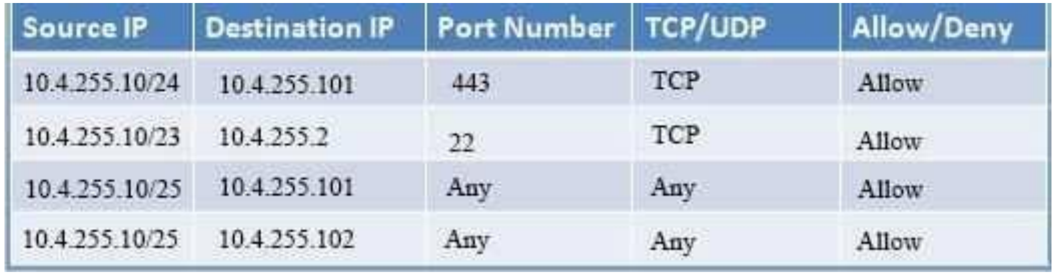


Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny

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

Explanation/Reference:
Explanation:

Use the following answer for this simulation task.
Below table has all the answers required for this question.



Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny
10.4.255.10/24	10.4.255.101	443	TCP	Allow
10.4.255.10/23	10.4.255.2	22	TCP	Allow
10.4.255.10/25	10.4.255.101	Any	Any	Allow
10.4.255.10/25	10.4.255.102	Any	Any	Allow

Firewall rules act like ACLs, and they are used to dictate what traffic can pass between the firewall and the internal network. Three possible actions can be taken based on the rule's criteria:

Block the connection Allow the connection
Allow the connection only if it is secured

TCP is responsible for providing a reliable, one-to-one, connection-oriented session. TCP establishes a connection and ensures that the other end receives any packets sent.
Two hosts communicate packet results with each other. TCP also ensures that packets are decoded and sequenced properly. This connection is persistent during the session.
When the session ends, the connection is torn down.
UDP provides an unreliable connectionless communication method between hosts. UDP is considered a best-effort protocol, but it's considerably faster than TCP.
The sessions don't establish a synchronized session like the kind used in TCP, and UDP doesn't guarantee error-free communications.
The primary purpose of UDP is to send small packets of information.
The application is responsible for acknowledging the correct reception of the data. Port 22 is used by both SSH and SCP with UDP.
Port 443 is used for secure web connections? HTTPS and is a TCP port.
Thus to make sure only the Accounting computer has HTTPS access to the Administrative server you should use TCP port 443 and set the rule to allow communication between 10.4.255.10/24 (Accounting) and 10.4.255.101 (Administrative server1) Thus to make sure that only the HR computer has access to Server2 over SCP you need use of TCP port 22 and set the rule to allow communication between 10.4.255.10/23 (HR) and 10.4.255.2 (server2)

Thus to make sure that the IT computer can access both the Administrative servers you need to use a port and accompanying port number and set the rule to allow communication between: 10.4.255.10.25 (IT computer) and 10.4.255.101 (Administrative server1)
10.4.255.10.25 (IT computer) and 10.4.255.102 (Administrative server2)

QUESTION 115
Which of the following BEST describes an attack where communications between two parties are intercepted and forwarded to each party with neither party being aware of the interception and potential modification to the communications?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
Which of the following are MOST susceptible to birthday attacks?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
Joe a computer forensic technician responds to an active compromise of a database server. Joe first collects information in memory, then collects network traffic and finally conducts an image of the hard drive.

Which of the following procedures did Joe follow?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119

Given the log output:

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
The firewall administrator is adding a new certificate for the company's remote access solution. The solution requires that the uploaded file contain the entire certificate chain for the certificate to load properly. The administrator loads the company certificate and the root CA certificate into the file. The file upload is rejected.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
The Chief Executive Officer (CEO) of a major defense contracting company a traveling overseas for a conference. The CEO will be taking a laptop.

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

A. Remote wipe
B. Full device encryption

C. BIOS password
D. GPS tracking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123

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

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

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

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

QUESTION 124
A product manager is concerned about continuing operations at a facility located in a region undergoing significant political unrest. After consulting with senior management, a decision is made to suspend operations at the facility until the situation stabilizes.

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
Joe notices there are several user accounts on the local network generating spam with embedded malicious code.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126

Two users need to securely share encrypted files via email. Company policy prohibits users from sharing credentials or exchanging encryption keys.
Which of the following can be implemented to enable users to share encrypted data while abiding by company policies?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
Joe a website administrator believes he owns the intellectual property for a company invention and has been replacing image files on the company's public facing website in the DMZ. Joe is using steganography to hide stolen data.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
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 130
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 131
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 132
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 133
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 134
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 135
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 136
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 137
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.

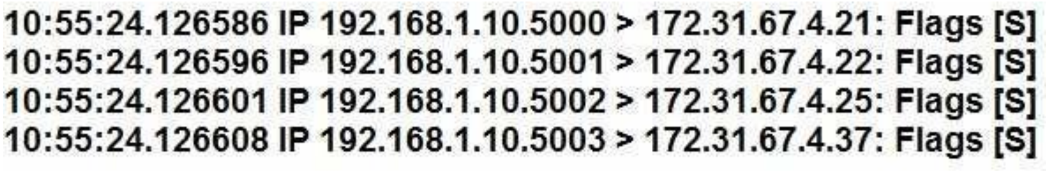
Which of the following should the security administrator configure on the corporate content filter to prevent users from accessing the phishing URL, while at the same time minimizing false positives?

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 138
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 139
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 140

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 141

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 142

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 143

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 144
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 145
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 146
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 147
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 148
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:

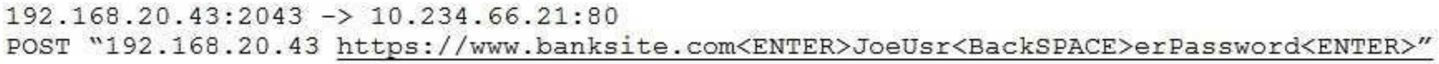
QUESTION 149
A company recently replaced its unsecure email server with a cloud-based email and collaboration solution that is managed and insured by a third party. Which of the following actions did the company take regarding risks related to its email and collaboration services?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
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?

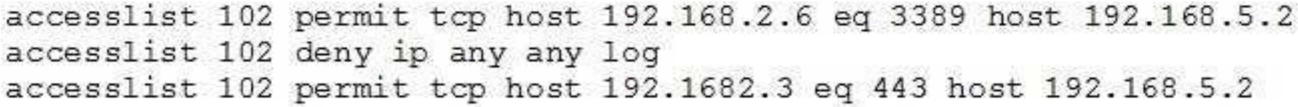
A. Keylogger
B. Ransomware
C. Logic bomb
D. Adware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

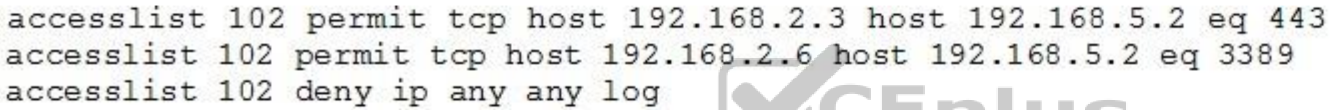
QUESTION 151

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:

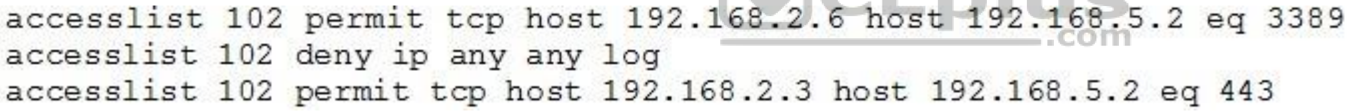


```
accesslist 102 permit tcp host 192.168.2.6 eq 3389 host 192.168.5.2
accesslist 102 deny ip any any log
accesslist 102 permit tcp host 192.1682.3 eq 443 host 192.168.5.2
```

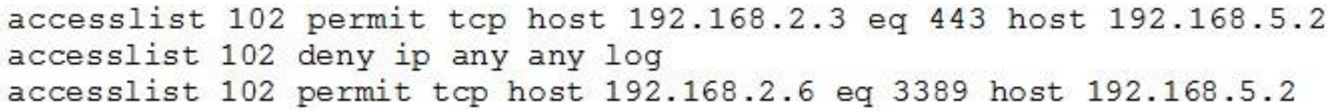
Which of the following rules would be BEST to resolve the issue?



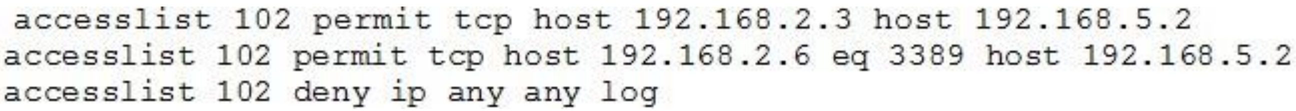
```
accesslist 102 permit tcp host 192.168.2.3 host 192.168.5.2 eq 443
accesslist 102 permit tcp host 192.168.2.6 host 192.168.5.2 eq 3389
accesslist 102 deny ip any any log
```



```
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
```



```
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
```

A.

B.

C.

D.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
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 153
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 154
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: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
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 156
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 157
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 158
A security auditor is putting together a report for the Chief Executive Officer (CEO) on personnel security and its impact on the security posture of the whole organization. Which of the following would be the MOST important factor to consider when it comes to personnel security?

A. Insider threats
B. Privilege escalation
C. Hacktivist
D. Phishing through social media
E. Corporate espionage

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
A security administrator wants to configure a company's wireless network in a way that will prevent wireless clients from broadcasting the company's SSID. Which of the following should be configured on the company's access points?

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

Correct Answer: F
Section: (none)
Explanation

Explanation/Reference:
QUESTION 160
A wireless network has the following design requirements:

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

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

A. PEAP
B. PSK
C. Open systems authentication
D. EAP-TLS
E. Captive portals

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
Which of the following strategies should a systems architect use to minimize availability risks due to insufficient storage capacity?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 162
A security engineer wants to implement a site-to-site VPN that will require SSL certificates for mutual authentication. Which of the following should the engineer implement if the design requires client MAC address to be visible across the tunnel?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
After a security incident, management is meeting with involved employees to document the incident and its aftermath.
Which of the following BEST describes this phase of the incident response process?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
A user needs to send sensitive information to a colleague using PKI.

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

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

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
As part of a new BYOD rollout, a security analyst has been asked to find a way to securely store company data on personal devices.
Which of the following would BEST help to accomplish this?

A. Require the use of an eight-character PIN.

B. Implement containerization of company data.
C. Require annual AUP sign-off.
D. Use geofencing tools to unlock devices while on the premises.

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 167
A web server, which is configured to use TLS with AES-GCM-256, SHA-384, and ECDSA, recently suffered an information loss breach.
Which of the following is MOST likely the cause?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
An incident involving a workstation that is potentially infected with a virus has occurred. The workstation may have sent confidential data to an unknown internet server.
Which of the following should a security analyst do FIRST?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
A vice president at a manufacturing organization is concerned about desktops being connected to the network. Employees need to log onto the desktops' local account to verify that a product is being created within specifications; otherwise, the desktops should be as isolated as possible. Which of the following is the BEST way to accomplish this?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
An in-house penetration tester has been asked to evade a new DLP system. The tester plans to exfiltrate data through steganography. Discovery of which of the following would help catch the tester in the act?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
A member of the admins group reports being unable to modify the "changes" file on a server.
The permissions on the file are as follows:

Permissions User Group File

```
-rwxrw-r--+ Admins Admins changes
```

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
A penetration tester is conducting an assessment on Comptia.org and runs the following command from a coffee shop while connected to the public Internet: c:
\nslookup -querytype=MX comptia.org

```
Server: Unknown

Address: 198.51.100.45

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

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

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

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

QUESTION 173
A security analyst is inspecting the results of a recent internal vulnerability scan that was performed against intranet services.
The scan reports include the following critical-rated vulnerability: Title: Remote Command Execution vulnerability in web server Rating: Critical (CVSS 10.0)
Threat actor: any remote user of the web server

Confidence: certain

Recommendation: apply vendor patches

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
Company A agrees to provide perimeter protection, power, and environmental support with measurable goals for Company B, but will not be responsible for user authentication or patching of operating systems within the perimeter. Which of the following is being described?

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

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

QUESTION 175
A company is deploying smartphones for its mobile salesforce. These devices are for personal and business use but are owned by the company. Sales personnel will save new customer data via a custom application developed for the company. This application will integrate with the contact information stored in the smartphones and will populate new customer records onto it.
The customer application's data is encrypted at rest, and the application's connection to the back office system is considered secure. The Chief Information Security Officer (CISO) has concerns that customer contact information may be accidentally leaked due to the limited security capabilities of the devices and the planned controls.

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
The Chief Information Security Officer (CISO) is asking for ways to protect against zero-day exploits. The CISO is concerned that an unrecognized threat could compromise corporate data and result in regulatory fines as well as poor corporate publicity. The network is mostly flat, with split staff/guest wireless functionality. Which of the following equipment MUST be deployed to guard against unknown threats?

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

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

QUESTION 177
An organization has several production-critical SCADA supervisory systems that cannot follow the normal 30- day patching policy.
Which of the following BEST maximizes the protection of these systems from malicious software?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
An organization identifies a number of hosts making outbound connections to a known malicious IP over port TCP 80. The organization wants to identify the data being transmitted and prevent future connections to this IP.
Which of the following should the organization do to achieve this outcome?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 179
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 180
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. Local account
B. Guest account
C. Service account
D. User account

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181

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 182

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 183

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 184
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 185
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 186
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 187
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 case?

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 188

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 189

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

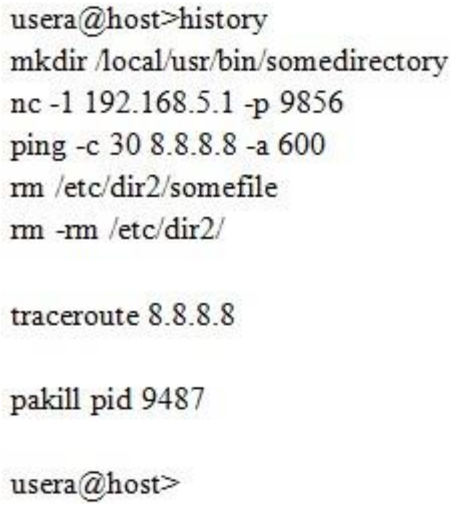
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 190

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 -a 600
rm /etc/dir2/somefile
rm -rm /etc/dir2/

traceroute 8.8.8.8

pakill 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 191
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 192
A security analyst conducts a manual scan on a known hardened host that identifies many non-compliant items.
Which of the following BEST describe why this has occurred? (Select TWO)

A. Privileged-user certificated 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 193

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 194

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 195
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 196
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 197

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 198
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. $1000C. $2000
D. $2500

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 199
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 200
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 201
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 202
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 203
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 204
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 205
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 206

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 207
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 208

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 209
Which of the following is a deployment concept that can be used to ensure only the required OS access is exposed to software applications?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 210
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: