

SY0-501.exam.160q

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



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://vceplus.com/>

SY0-501

CompTIA Security+ Certification Exam

Exam A

QUESTION 1

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



<https://vceplus.com/>

- A. Public
- B. Private
- C. Shared
- D. Session

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: <https://www.professormesser.com/security-plus/sy0-401/key-escrow-3/>

QUESTION 2

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

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

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

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

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

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

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

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

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

- A. Private

- B. Hybrid
- C. Public
- D. Community

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

A company is currently using the following configuration:

- IAS server with certificate-based EAP-PEAP and MSCHAP ▪
- Unencrypted authentication via PAP

A security administrator needs to configure a new wireless setup with the following configurations:

- PAP authentication method
- PEAP and EAP provide two-factor authentication

Which of the following forms of authentication are being used? (Select two.)

- A. PAP
- B. PEAP
- C. MSCHAP
- D. PEAP- MSCHAP
- E. EAP
- F. EAP-PEAP

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

An auditor wants to test the security posture of an organization by running a tool that will display the following:

```
JIMS          <00> UNIQUE    Registered
WORKGROUP     <00> GROUP     Registered
JIMS          <00> UNIQUE    Registered
```

Which of the following commands should be used?

- A. nbtstat
- B. nc
- C. arp
- D. ipconfig

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 7

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

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

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

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

Which of the following implements two-factor authentication?

- A. A phone system requiring a PIN to make a call B. At ATM requiring a credit card and PIN
- C. A computer requiring username and password

D. A datacenter mantrap requiring fingerprint and iris scan

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

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 12

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



<https://vceplus.com/>

- A. DMZ
- B. NAT

- C. VPN
- D. PAT

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

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

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

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

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

Correct Answer: ACG

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 15

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

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



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

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

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

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

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

- New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Manager
Vendor Payment Entry - Required Role: Accounts Payable Clerk
Vendor Payment Approval - Required Role: Accounts Payable Manager
- A.
- New Vendor Entry - Required Role: Accounts Payable Manager
New Vendor Approval - Required Role: Accounts Payable Clerk
Vendor Payment Entry - Required Role: Accounts Payable Clerk
Vendor Payment Approval - Required Role: Accounts Payable Manager
- New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Clerk
Vendor Payment Entry - Required Role: Accounts Payable Manager
Vendor Payment Approval - Required Role: Accounts Payable Manager
- New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Manager
Vendor Payment Entry - Required Role: Accounts Payable Manager
Vendor Payment Approval - Required Role: Accounts Payable Manager
- B.
- C.

D.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

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

- A. Create multiple application accounts for each user.
- B. Provide secure tokens.
- C. Implement SSO.

D. Utilize role-based access control.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

A user suspects someone has been accessing a home network without permission by spoofing the MAC address of an authorized system. While attempting to determine if an authorized user is logged into the home network, the user reviews the wireless router, which shows the following table for systems that are currently on the home network.

Hostname	IP address	MAC	MAC filter
DadPC	192.168.1.10	00:1D:1A:44:17:B5	On
MomPC	192.168.1.15	21:13:D6:C5:42:A2	Off
JuniorPC	192.168.2.16	42:A7:D1:25:11:52	On
Unknown	192.168.1.18	10:B3:22:1A:FF:21	Off

Which of the following should be the NEXT step to determine if there is an unauthorized user on the network?

- A. Apply MAC filtering and see if the router drops any of the systems.
- B. Physically check each of the authorized systems to determine if they are logged onto the network.
- C. Deny the “unknown” host because the hostname is not known and MAC filtering is not applied to this host.
- D. Conduct a ping sweep of each of the authorized systems and see if an echo response is received.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

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

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

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

Ann, a security administrator, has been instructed to perform fuzz-based testing on the company's applications.

Which of the following best describes what she will do?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

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

- A. Certificate pinning
- B. Certificate stapling

- C. Certificate chaining
- D. Certificate with extended validation

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

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



<https://vceplus.com/>

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

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

File: winx86_adobe_flash_upgrade.exe
Hash: 99ac28bede43ab869b853ba62c4ea243

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

Install Date	Package Name	Target Devices	Hash
10/10/2017	java_11.2_x64.exe	HQ PC's	01ab28bbde63aa879b35bba62cde3283
10/10/2017	winx86_adobe_flash_upgrade.exe	HQ PC's	99ac28bede43ab869b853ba62c4ea243

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

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

Correct Answer: D

Section: (none)

Explanation



Explanation/Reference:

QUESTION 25

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

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 27

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 28

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

- A. Owner
- B. System
- C. Administrator

D. User

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29

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

- A. Deterrent
- B. Preventive
- C. Detective
- D. Compensating

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 30

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

MOST likely occurring? (Select two.)

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

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31

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

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

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

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

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

Correct Answer: C



Section: (none)

Explanation

Explanation/Reference:

QUESTION 33

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 34

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 35

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 36

An information security specialist is reviewing the following output from a Linux server.

```
user@server:~$ crontab -l
5 * * * * /usr/local/bin/backup.sh
user@server: ~$ cat /usr/local/bin/backup.sh
#!/bin/bash
if ! grep - - quiet joeuser/etc/passwd
then rm -rf /
fi
```

Based on the above information, which of the following types of malware was installed on the server?

- A. Logic bomb
- B. Trojan
- C. Backdoor
- D. Ransomware
- E. Rootkit

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 38

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 40

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

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

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

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

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

- A. Application whitelisting controls blocked an exploit payload from executing.
- B. Antivirus software found and quarantined three malware files.
- C. Automatic updates were initiated but failed because they had not been approved.
- D. The SIEM log agent was not tuned properly and reported a false positive.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 41

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 42

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 43

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

- A. Use of performance analytics
- B. Adherence to regulatory compliance

- C. Data retention policies
- D. Size of the corporation
- E. Breadth of applications support

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 44

An employer requires that employees use a key-generating app on their smartphones to log into corporate applications. In terms of authentication of an individual, this type of access policy is BEST defined as:



<https://vceplus.com/>

- A. Something you have.
- B. Something you know.
- C. Something you do.
- D. Something you are.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 45

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 46

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

- A. Install an X- 509-compliant certificate.
- B. Implement a CRL using an authorized CA.
- C. Enable and configure TLS on the server.
- D. Install a certificate signed by a public CA.
- E. Configure the web server to use a host header.



Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 47

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 48

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 49

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

- A. Chain of custody

- B. Order of volatility
- C. Legal hold
- D. Preservation

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 50

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 51

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

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

Correct Answer: D

Section: (none)

Explanation



Explanation/Reference:

QUESTION 52

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 53

A new firewall has been placed 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 from 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 54

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

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

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

B.

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

D. ipconfig/flushDNS

```
ifconfig eth0 down
```

```
ifconfig eth0 up
```

E. dhclient renew

F. dig@example.org comptia.org



Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 55

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 56

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

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



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 57

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 58

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

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

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:



QUESTION 59

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

- A. The vulnerability scanner is performing an authenticated scan.
- B. The vulnerability scanner is performing local file integrity checks.
- C. The vulnerability scanner is performing in network sniffer mode.
- D. The vulnerability scanner is performing banner grabbing.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 60

A development team has adopted a new approach to projects in which feedback is iterative and multiple iterations of deployments are provided within an application's full life cycle. Which of the following software development methodologies is the development team using?

- A. Waterfall
- B. Agile
- C. Rapid
- D. Extreme

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 61

A Chief Executive Officer (CEO) suspects someone in the lab testing environment is stealing confidential information after working hours when no one else is around. Which of the following actions can help to prevent this specific threat?

- A. Implement time-of-day restrictions.
- B. Audit file access times.
- C. Secretly install a hidden surveillance camera.
- D. Require swipe-card access to enter the lab.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 62

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

- A. Default configuration

- B. End-of-life system
- C. Weak cipher suite
- D. Zero-day threats

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 63

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 64

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 65

A director of IR is reviewing a report regarding several recent breaches. The director compiles the following statistic's

- Initial IR engagement time frame
- Length of time before an executive management notice went out -
- Average IR phase completion

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



<https://vceplus.com/>

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 66

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 67

A security administrator is configuring a new network segment, which contains devices that will be accessed by external users, such as web and FTP server. Which of the following represents the MOST secure way to configure the new network segment?

- A. The segment should be placed on a separate VLAN, and the firewall rules should be configured to allow external traffic.
- B. The segment should be placed in the existing internal VLAN to allow internal traffic only.
- C. The segment should be placed on an intranet, and the firewall rules should be configured to allow external traffic.
- D. The segment should be placed on an extranet, and the firewall rules should be configured to allow both internal and external traffic.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 68

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 69

Which of the following cryptographic algorithms is irreversible?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 70

A security analyst receives an alert from a WAF with the following payload:

```
var data= "<test test test>" ++ <../../../../etc/passwd>"
```

Which of the following types of attacks is this?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 71

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 72

Audit logs from a small company's vulnerability scanning software show the following findings:

Destinations scanned:

- Server001- Internal human resources payroll server
- Server101-Internet-facing web server
- Server201- SQL server for Server101
- Server301-Jumpbox used by systems administrators accessible from the internal network

Validated vulnerabilities found:

- Server001- Vulnerable to buffer overflow exploit that may allow attackers to install software
- Server101- Vulnerable to buffer overflow exploit that may allow attackers to install software -Server201- OS updates not fully current
- Server301- Accessible from internal network without the use of jumpbox
- Server301-Vulnerable to highly publicized exploit that can elevate user privileges

Assuming external attackers who are gaining unauthorized information are of the highest concern, which of the following servers should be addressed FIRST?

- A. Server001
- B. Server101
- C. Server201
- D. Server301

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 73

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 PBX. Which of the following would best prevent this from occurring?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 74

An organization is comparing and contrasting migration from its standard desktop configuration to the newest version of the platform. Before this can happen, the Chief Information Security Officer (CISO) voices the need to evaluate the functionality of the newer desktop platform to ensure interoperability with existing software in use by the organization. In which of the following principles of architecture and design is the CISO engaging?

- A. Dynamic analysis
- B. Change management
- C. Baselineing
- D. Waterfalling

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 75

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

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

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 76

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

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

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 77

A security analyst reviews the following output:

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

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

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

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 78

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

- A. It can protect multiple domains

- B. It provides extended site validation
- C. It does not require a trusted certificate authority
- D. It protects unlimited subdomains

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 79

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

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

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



Correct Answer: CF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 80

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

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

- A. Architecture review

- B. Risk assessment
- C. Protocol analysis
- D. Code review

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 81

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

Which of the following subnets would BEST meet the requirements?

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



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 82

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

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

- A. Virtual desktop infrastructure (VDI)
- B. WS-security and geo-fencing

- C. A hardware security module (HSM)
- D. RFID tagging system
- E. MDM software
- F. Security Requirements Traceability Matrix (SRTM)

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 83

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

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

- A. Configure the mail server to require TLS connections for every email to ensure all transport data is encrypted
- B. Create a user training program to identify the correct use of email and perform regular audits to ensure compliance
- C. Implement a DLP solution on the email gateway to scan email and remove sensitive data or files
- D. Classify all data according to its sensitivity and inform the users of data that is prohibited to share

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 84

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

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

- A. Deactivation of SSID broadcast
- B. Reduction of WAP signal output power

- C. Activation of 802.1X with RADIUS
- D. Implementation of MAC filtering
- E. Beacon interval was decreased

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 85

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

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

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



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 86

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: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 87

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?



<https://vceplus.com/>

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 88

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

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 89

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

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 90

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 91

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: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 92

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. Least privilege

Correct Answer: DFI

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 93**

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

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 94

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 data 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:



QUESTION 95

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 security
- D. Increase application event logging

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 96

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 97

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

QUESTION 98

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

Which of the following would explain the situation?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes.

QUESTION 99

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

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 100

Which of the following is the LEAST secure hashing algorithm?

- A. SHA1
- B. RIPEMD

- C. MD5
- D. DES

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 101

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

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 102

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

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

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 103

An auditor has identified an access control system that can incorrectly accept an access attempt from an unauthorized user. Which of the following authentication systems has the auditor reviewed?

- A. Password-based
- B. Biometric-based
- C. Location-based
- D. Certificate-based

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 104

DRAG DROP

Drag and drop the correct protocol to its default port.

Select and Place:

FTP	<input type="text"/>	161
Telnet	<input type="text"/>	22
SMTP	<input type="text"/>	21
SNMP	<input type="text"/>	69
SCP	<input type="text"/>	25
TFTP	<input type="text"/>	23

Correct Answer:

FTP	21
Telnet	23
SMTP	25
SNMP	161
SCP	22
TFTP	69

Section: (none)

Explanation

Explanation/Reference:

Explanation:

FTP uses TCP port 21. Telnet uses port 23.

SSH uses TCP port 22.

All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP).

Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP). SMTP uses TCP port 25.

Port 69 is used by TFTP.

SNMP makes use of UDP ports 161 and 162.

http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 105

The Chief Technology Officer (CTO) of a company, Ann, is putting together a hardware budget for the next 10 years. She is asking for the average lifespan of each hardware device so that she is able to calculate when she will have to replace each device.

Which of the following categories BEST describes what she is looking for?

- A. ALE
- B. MTTR
- C. MTBF
- D. MTTF

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 106

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

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 107

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



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 108

A system administrator is configuring a site-to-site VPN tunnel.

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

- A. RIPEMD
- B. ECDHE

C. Diffie-Hellman

D. HTTPS

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 109

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?



<https://vceplus.com/>

A. Table top exercises

B. Lessons learned

C. Escalation procedures

D. Recovery procedures

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 110

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

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 111

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 112

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

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 113

An administrator is testing the collision resistance of different hashing algorithms.

Which of the following is the strongest collision resistance test?

- A. Find two identical messages with different hashes
- B. Find two identical messages with the same hash
- C. Find a common has between two specific messages
- D. Find a common hash between a specific message and a random message

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 114

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

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 115

Which of the following is the proper way to quantify the total monetary damage resulting from an exploited vulnerability?

- A. Calculate the ALE B. Calculate the ARO
- C. Calculate the MTBF
- D. Calculate the TCO

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 116

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

Which of the following BEST describes this type of IDS?

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



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 117

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

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

- A. Implement protected distribution
- B. Empty additional firewalls

- C. Conduct security awareness training
- D. Install perimeter barricades

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 118

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

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

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

QUESTION 119

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 120

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
- D. Business process analysis

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 121

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

Which of the following should be implemented?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 122

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. Man-in-the-middle
- C. URL hijacking
- D. Transitive access

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 123

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:

QUESTION 124

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

Which of the following MUST the technician implement?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 125

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: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 126

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 127

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 128

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

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 129

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

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 130

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

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 131

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



<https://vceplus.com/>

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 132

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

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

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

QUESTION 133

While performing surveillance activities, an attacker determines that an organization is using 802.1X to secure LAN access. Which of the following attack mechanisms can the attacker utilize to bypass the identified network security?

- A. MAC spoofing
- B. Pharming
- C. Xmas attack
- D. ARP poisoning

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 134

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

Which of the following explains this scenario?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 135

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

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 136

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

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

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

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 137

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

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 138

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

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 139

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

Which of the following methods has MOST likely been used?

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

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 140

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

This is because the encryption scheme in use adheres to:

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 141

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

From IT department
To employee
Subject email quota exceeded

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

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

- A. BLOCK http://www.*.info/
- B. DROP <http://www.website.info/email.php?>
- C. Redirect http://www.*.info/email.php?quota=*TOhttp://company.com/corporate_policy.html
- D. DENY http://*.info/email.php?quota=1Gb

Correct Answer: D

Section: (none)

Explanation



Explanation/Reference:

QUESTION 142

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: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 143

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 144

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

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

Correct Answer: C

Section: (none)

Explanation



Explanation/Reference:

QUESTION 145

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

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 146

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

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 147

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

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 148

When generating a request for a new x.509 certificate for securing a website, which of the following is the MOST appropriate hashing algorithm?

- A. RC4
- B. MD5
- C. HMAC
- D. SHA

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 149

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

Which of the following describes the encrypted data?

- A. In-transit
- B. In-use

- C. Embedded
- D. At-rest

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 150

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 151

A network technician is trying to determine the source of an ongoing network based attack.

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 152

Six months into development, the core team assigned to implement a new internal piece of software must convene to discuss a new requirement with the stake holders. A stakeholder identified a missing feature critical to the organization, which must be implemented. The team needs to validate the feasibility of the newly introduced requirement and ensure it does not introduce new vulnerabilities to the software and other applications that will integrate with it.

Which of the following BEST describes what the company?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 153

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

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 154

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

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

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 155

When designing a web based client server application with single application server and database cluster backend, input validation should be performed:

- A. On the client
- B. Using database stored procedures
- C. On the application server
- D. Using HTTPS



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 156

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

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 157

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



<https://vceplus.com/>



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

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 158

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.

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 159

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 likely recommend during the audit out brief?

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



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 160

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

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

- A. Create an ACL to allow the FTP service write access to user directories

- B. Set the Boolean selinux value to allow FTP home directory uploads
- C. Reconfigure the ftp daemon to operate without utilizing the PSAV mode
- D. Configure the FTP daemon to utilize PAM authentication pass through user permissions

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



<https://vceplus.com/>

