

SY0-501.exam.178q

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

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?



<https://vceplus.com/>

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 2

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 3**

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 4**

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 5

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 6

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

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: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

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

- A. LDAP
- B. TPM
- C. TLS
- D. SSL
- E. PKI



Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

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 10

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



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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

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 13

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. <https://docs.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview> **QUESTION 14**

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

- A. Botnet
- B. Ransomware
- C. Polymorphic malware
- D. Armored virus

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 15

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

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

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

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 17

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

The systems administrator reviews the output below:



```
c:\Windows\system32>netstat -nab
Active Connections
Proto Local Address          Foreign Address        State
TCP    0.0.0.0:135             0.0.0.0:0              LISTENING
TCP    0.0.0.0:445             0.0.0.0:0              LISTENING
TCP    192.168.1.10:5000      10.37.213.20          ESTABLISHED
UDP    192.168.1.10:1900      *.*
```

Proto	Local Address	Foreign Address	State	Process
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	RpcSs [svchost.exe]
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	[svchost.exe]
TCP	192.168.1.10:5000	10.37.213.20	ESTABLISHED	winserver.exe
UDP	192.168.1.10:1900	*,*		SSDPSVR

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

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: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 19

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 20

When systems, hardware, or software are not supported by the original vendor, it is a vulnerability known as:

- A. system sprawl
- B. end-of-life systems
- C. resource exhaustion
- D. a default configuration

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

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

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

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

A company wants to host a publicity 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?



<https://vceplus.com/>

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



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

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 24

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 25

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 26

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 27

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 28

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 29

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 30

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

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



Which of the following vulnerabilities is present?

- A. Bad memory pointer
- B. Buffer overflow
- C. Integer overflowD. Backdoor

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

A wireless network uses a RADIUS server that is connected to an authenticator, which in turn connects to a supplicant. Which of the following represents the authentication architecture in use?

- A. Open systems authentication
- B. Captive portal
- C. RADIUS federation
- D. 802.1x



Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 33

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 34

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 35

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 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
- 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

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:

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 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 42

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?



<https://vceplus.com/>

- 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 43

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 44

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 45

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 46

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

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

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 47

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:

QUESTION 48

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 49

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 50

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?

- 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 51

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
- D. VPN concentrators
- E. Routers

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:



QUESTION 52

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 53

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 54

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:

QUESTION 55

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 56

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

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

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 57

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 58

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

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

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

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

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 59

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

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



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 60

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 61

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 62

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 63

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 64

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?



<https://vceplus.com/>

- 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 65

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 66

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 67

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

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

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 68**

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 69

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 70

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 71

A user is presented with the following items during the new-hire onboarding process:

- Laptop
- Secure USB drive

- Hardware OTP token
- External high-capacity HDD
- Password complexity policy
- Acceptable use policy
- HASP key
- Cable lock

Which of the following is one component of multifactor authentication?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 72

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 73

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 74

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 75

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 76

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 77

A company's AUP requires:

- Passwords must meet complexity requirements.
 - Passwords are changed at least once every six months. ▪
- Passwords must be at least eight characters long.

An auditor is reviewing the following report:

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

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 78

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 79

A security analyst notices anomalous activity coming from several workstations in the organizations. Upon identifying and containing the issue, which of the following should the security analyst do NEXT?

- A. Document and lock the workstations in a secure area to establish chain of custody
- B. Notify the IT department that the workstations are to be reimaged and the data restored for reuse
- C. Notify the IT department that the workstations may be reconnected to the network for the users to continue working
- D. Document findings and processes in the after-action and lessons learned report

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 80

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 81

An information security analyst needs to work with an employee who can answer questions about how data for a specific system is used in the business. The analyst should seek out an employee who has the role of:

- A. steward
- B. owner
- C. privacy officer
- D. systems administrator

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 82

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 83

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 84

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 85

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 86

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 87

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 88

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.



<https://vceplus.com/>

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 89

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

Which of the following would correct the deficiencies?

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

Correct Answer: C



Section: (none)

Explanation

Explanation/Reference:

QUESTION 90

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

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

- A. Revision control system
- B. Client side exception handling
- C. Server side validation
- D. Server hardening

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 91

An attacker discovers a new vulnerability in an enterprise application. The attacker takes advantage of the vulnerability by developing new malware. After installing the malware, the attacker is provided with access to the infected machine.

Which of the following is being described?

- A. Zero-day exploit
- B. Remote code execution
- C. Session hijacking
- D. Command injection

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 92

A security administrator returning from a short vacation receives an account lock-out message when attempting to log into the computer. After getting the account unlocked the security administrator immediately notices a large amount of emails alerts pertaining to several different user accounts being locked out during the past three days. The security administrator uses system logs to determine that the lock-outs were due to a brute force attack on all accounts that has been previously logged into that machine.

Which of the following can be implemented to reduce the likelihood of this attack going undetected?

- A. Password complexity rules
- B. Continuous monitoring
- C. User access reviews
- D. Account lockout policies

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 93

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

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 94

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

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 95

Company policy requires the use of passphrases instead of passwords.

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 96

During a routine audit, it is discovered that someone has been using a stale administrator account to log into a seldom used server. The person has been using the server to view inappropriate websites that are prohibited to end users.

Which of the following could best prevent this from occurring again?

- A. Credential management
- B. Group policy management
- C. Acceptable use policy
- D. Account expiration policy

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 97

Which of the following should identify critical systems and components?

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



Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 98

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 99

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 100

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.

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 101

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 area.

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 102

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?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 103

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

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 104

Which of the following use the SSH protocol?

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

Correct Answer: BF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 105

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

- A. Taking pictures of proprietary information and equipment in restricted areas.
- B. Installing soft token software to connect to the company's wireless network.

- C. Company cannot automate patch management on personally-owned devices.
- D. Increases the attack surface by having more target devices on the company's campus

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 106

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

- A. MTBF
- B. ALE
- C. SLA
- D. ARO

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 107

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

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 108

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

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 109

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

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 110

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



<https://vceplus.com/>

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

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

Correct Answer: B

Section: (none)

Explanation



Explanation/Reference:

QUESTION 111

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

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

QUESTION 112

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

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

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

Correct Answer: D

Section: (none)

Explanation



Explanation/Reference:

QUESTION 113

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 114

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 115

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 116

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 117

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 118

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 119

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 120

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

QUESTION 121

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

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



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

QUESTION 122

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

Which of the following protocols should be used?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 123

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

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

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



Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 124

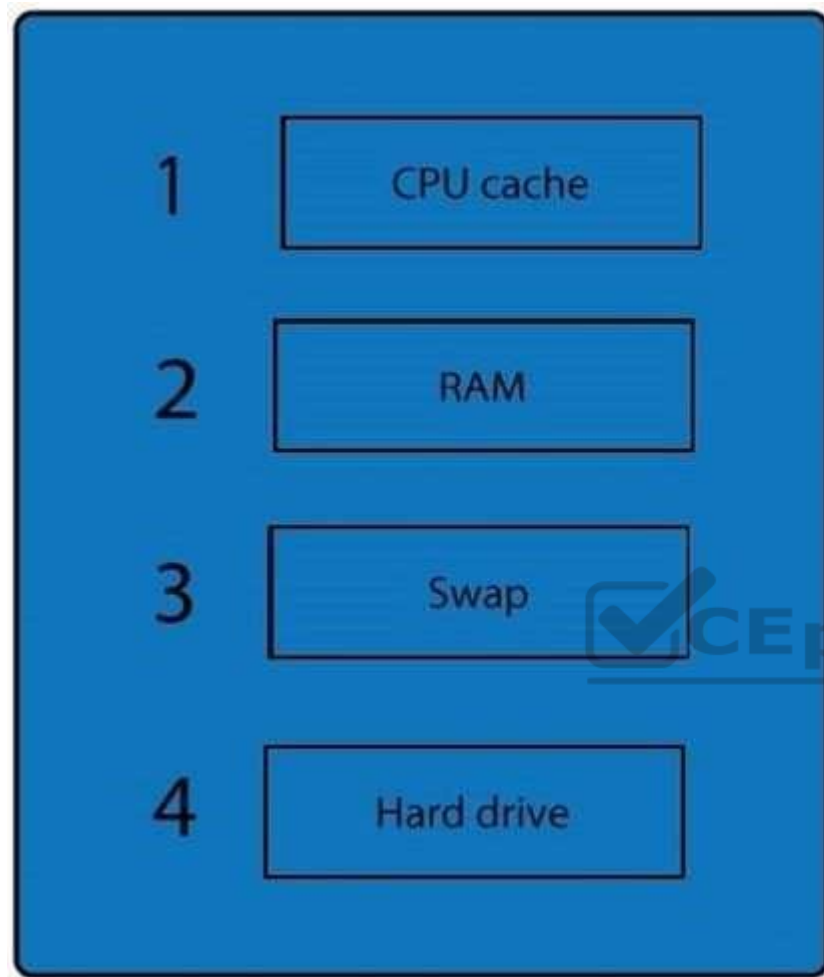
DRAG DROP

A forensic analyst is asked to respond to an ongoing network attack on a server. Place the items in the list below in the correct order in which the forensic analyst should preserve them.

Select and Place:

1	<input type="text"/>	RAM
2	<input type="text"/>	CPU cache
3	<input type="text"/>	Swap
4	<input type="text"/>	Hard drive

Correct Answer:



Section: (none)

Explanation

Explanation/Reference:

Explanation:

When dealing with multiple issues, address them in order of volatility (OOV); always deal with the most volatile first. Volatility can be thought of as the amount of time that you have to collect certain data before a window of opportunity is gone. Naturally, in an investigation you want to collect everything, but some data will exist longer than others, and you cannot possibly collect all of it once. As an example, the OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and printouts.

Order of volatility: Capture system images as a snapshot of what exists, look at network traffic and logs, capture any relevant video/screenshots/hashes, record time offset on the systems, talk to witnesses, and track total man-hours and expenses associated with the investigation.

QUESTION 125

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

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

Uses RRSIG

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

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



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

QUESTION 126

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

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

- A. Utilizing a single Qfor password recovery
- B. Sending a PIN to a smartphone through text message

- C. Utilizing CAPTCHA to avoid brute force attacks
- D. Use a different e-mail address to recover password

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 127

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

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

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



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 128

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

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 129

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

Which of the following should be implemented?

- A. Recovery agent
- B. Ocsf
- C. Crl
- D. Key escrow

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 130

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

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 131

The chief security officer (CSO) has issued a new policy that requires that all internal websites be configured for HTTPS traffic only. The network administrator has been tasked to update all internal sites without incurring additional costs.

Which of the following is the best solution for the network administrator to secure each internal website?

- A. Use certificates signed by the company CA
- B. Use a signing certificate as a wild card certificate
- C. Use certificates signed by a public ca
- D. Use a self-signed certificate on each internal server

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

This is a way to update all internal sites without incurring additional costs?

To be a CA (Certificate Authority), you need an infrastructure that consists of considerable operational elements, hardware, software, policy frameworks and practice statements, auditing, security infrastructure and personnel.

QUESTION 132

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

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

QUESTION 133

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



<https://vceplus.com/>

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 134

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 135

During an application design, the development team specifies a LDAP module for single sign-on communication with the company's access control database. This is an example of which of the following?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 136

After a merger, it was determined that several individuals could perform the tasks of a network administrator in the merged organization. Which of the following should have been performed to ensure that employees have proper access?

- A. Time-of-day restrictions
- B. Change management
- C. Periodic auditing of user credentials
- D. User rights and permission review

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 137

A company exchanges information with a business partner. An annual audit of the business partner is conducted against the SLA in order to verify:

- A. Performance and service delivery metrics
- B. Backups are being performed and tested
- C. Data ownership is being maintained and audited
- D. Risk awareness is being adhered to and enforced

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 138

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 139

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 140

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 141

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 142

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 143

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 144

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 145

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 146

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 147

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 148

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 149

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 150

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 151

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 152

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 153

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

- A. Collision resistance

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 154

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



<https://vceplus.com/>

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 155

A security administrator has been asked to implement a VPN that will support remote access over IPSEC.

Which of the following is an encryption algorithm that would meet this requirement?

- A. MD5
- B. AES
- C. UDP
- D. PKI

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 156

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

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 157

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

- A. Fire suppression
- B. Environmental monitoring

- C. Proximity card access
- D. Humidity controls

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 158

A company would like to prevent the use of a known set of applications from being used on company computers. Which of the following should the security administrator implement?

- A. Whitelisting
- B. Anti-malware
- C. Application hardening
- D. Blacklisting
- E. Disable removable media



Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 159

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

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 160

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 161

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 162

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 163

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 164

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 165

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://\"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 166

Which of the following can be used to control specific commands that can be executed on a network infrastructure device?

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

Correct Answer: D

Section: (none)

Explanation



Explanation/Reference:

QUESTION 167

Company XYZ has decided to make use of a cloud-based service that requires mutual, certificate-based authentication with its users. The company uses SSLinspecting IDS at its network boundary and is concerned about the confidentiality of the mutual authentication.

Which of the following model prevents the IDS from capturing credentials used to authenticate users to the new service or keys to decrypt that communication?

- A. Use of OATH between the user and the service and attestation from the company domain
- B. Use of active directory federation between the company and the cloud-based service
- C. Use of smartcards that store x.509 keys, signed by a global CA
- D. Use of a third-party, SAML-based authentication service for attestation

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 168

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 169

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

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 170

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 171

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 172

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

- A. Egress traffic is more important than ingress traffic for malware prevention
- B. To rebalance the amount of outbound traffic and inbound traffic
- C. Outbound traffic could be communicating to known botnet sources

D. To prevent DDoS attacks originating from external network

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 173

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

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

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 174

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 175

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 176

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

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 177

A global gaming console manufacturer is launching a new gaming platform to its customers.

Which of the following controls reduces the risk created by malicious gaming customers attempting to circumvent control by way of modifying consoles?

- A. Firmware version control
- B. Manual software upgrades
- C. Vulnerability scanning
- D. Automatic updates
- E. Network segmentation
- F. Application firewalls

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:



QUESTION 178

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:



<https://vceplus.com/>

