Exam Topic Breakdown

Exam Topic	**Number of Questions**
Topic 1 : Exam Set 1	180
Topic 2 : Exam Set 2	182
Topic 3 : Exam Set 3	111
Topic 4 : Exam Set 4	75
TOTAL	548

Topic 4, Exam Set 4

Question #:1 - (Exam Topic 4)

A security analyst is creating baselines for the server team to follow when hardening new devices for deployment. Which of the following best describes what the analyst is creating?

A. Change management procedure

B. Information security policy

C. Cybersecurity framework

D. Secure configuration guide

Question #:2 - (Exam Topic 4)

An organization is having difficulty correlating events from its individual AV. EDR. DLP. SWG. WAF, MDM. HIPS, and CASB systems. Which of the following is the best way to improve the situation?

A. Remove expensive systems that generate few alerts.

B. Modify the systems to alert only on critical issues.

C. Utilize a SIEM to centralize logs and dashboards.

D. Implement a new syslog/NetFlow appliance.

Question #:3 - (Exam Topic 4)

A cybersecurity analyst reviews the log files from a web server and sees a series of files that indicate a directory traversal attack has occurred. Which of the following is the analyst most likely seeing?

A. http://sample.url.com/<script>Please-Visit-Our-Phishing-Site</script>

B. http://sample.url.com/someotherpageonsite/../../../etc/shadow

C. http://sample.url.com/select-from-database-where-password-null

D. http://redirect.sameple.url.sampleurl.com/malicious-dns-redirect

Question #:4 - (Exam Topic 4)

A vulnerability has been discovered and a known patch to address the vulnerability does not exist. Which of the following controls works best until a proper fix is released?

A. Detective

B. Compensating

C. Deterrent

D. Corrective

Question #:5 - (Exam Topic 4)

Which of the following scenarios best describes a risk reduction technique?

A. A security control objective cannot be met through a technical change, so the company purchases insurance and is no longer concerned about losses from data breaches

B. A security control objective cannot be met through a technical change, so the company implements a pokey to train users on a more secure method of operation

C. A security control objective cannot be met through a technical change, so the company performs regular audits to determine it violations have occurred

D. A security control objective cannot be met through a technical change, so the Chief Information Officer decides to sign off on the risk.

Question #:6 - (Exam Topic 4)

An analyst is concerned about data leaks and wants to restrict access to internet services to authorized users only. The analyst also wants to control the actions each user can perform on each service. Which of the following would be the best technology for the analyst to consider implementing?

A. DLP

B. VPC

C. CASB

D. Content filtering

Question #:7 - (Exam Topic 4)

A company purchased cyber insurance to address items listed on the risk register. Which of the following strategies does this represent?

A. Accept

B. Transfer

C. Mitigate

D. Avoid

Question #:8 - (Exam Topic 4)

A security analyst is investigating an incident to determine what an attacker was able to do on a compromised Laptop. The analyst reviews the following SIEM log:

Host	Event ID	Event source	Description
PC1	865	Microsoft-Windows-SoftwareRestrictionpolicies	C:\asdf234\asdf234.exe was Policies blocked by Group Policy
PC1	4688	Microsoft-Windows-Security Auditing	A new process has been created. New Process Name: powershell.exe Creator Process Name: outlook.exe
PC1	4688	Microsoft-Windows-Security-Auditing	A new process has been created. New Process Name: lat.ps1 Creator Process Name: powershell.exe
PC2	4625	Microsoft-Windows-Security-Auditing	An account failed to log on. LogonType:3 SecurityID:Null SID Workstation Name: PC1 Authentication Package Name: NTLM

Which of the following describes the method that was used to compromise the laptop?

A. An attacker was able to move laterally from PC 1 to PC2 using a pass-the-hash attach

B. An attacker was able to bypass the application approve list by emailing a spreadsheet. attachment with an embedded PowerShell in the file.

C. An attacker was able to install malware to the CAasdf234 folder and use it to gain administrator rights and launch Outlook

D. An attacker was able to phish user credentials successfully from an Outlook user profile

Question #:9 - (Exam Topic 4)

A security analyst was asked to evaluate a potential attack that occurred on a publicly accessible section of the company's website. The malicious actor posted an entry in an attempt to trick users into clicking the following:

https://www.c0mptia.com/contact-us/%3Fname%3D%3Cscript%Ealert(document.cookie)%3C%2Fscript%3E

Which of the following was most likely observed?

A. DLL injection

B. Session replay

C. SQLi

D. xss

Question #:10 - (Exam Topic 4)

A systems administrator set up an automated process that checks for vulnerabilities across the entire environment every morning. Which of the following activities is the systems administrator conducting?

A. Scanning

B. Alerting

C. Reporting

D. Archiving

Question #:11 - (Exam Topic 4)

A company is expanding its threat surface program and allowing individuals to security test the company's internet-facing application. The company will compensate researchers based on the vulnerabilities discovered. Which of the following best describes the program the company is setting up?

A. Open-source intelligence

B. Bug bounty

C. Red team

D. Penetration testing

Question #:12 - (Exam Topic 4)

A security analyst is reviewing SIEM logs during an ongoing attack and notices the following:

```
http://company.com/get  php? f=/etc/passwd

http://company.com/..%2F..%2F..%2F..%2Fetc%2Fshadow

http://company.com/../../../ ../etc/passwd
```

Which of the following best describes the type of attack?

A. SQLi

B. CSRF

C. API attacks

D. Directory traversal

Question #:13 - (Exam Topic 4)

A security analyst has been reading about a newly discovered cyberattack from a known threat actor. Which of the following would best support the analyst's review of the tactics, techniques, and protocols the throat actor was observed using in previous campaigns?

A. Security research publications

B. The MITRE ATT4CK framework

C. The Diamond Model of Intrusion Analysis

D. The Cyber Kill Cham

Question #:14 - (Exam Topic 4)

A Chief Information Security Officer (CISO) wants to explicitly raise awareness about the increase of ransomware-as-a-service in a report to the management team. Which of the following best describes the threat actor in the CISO's report?

A. Insider threat

B. Hacktivist

C. Nation-state

D. Organized crime

Question #:15 - (Exam Topic 4)

An incident response technician collected a mobile device during an investigation. Which of the following should the technician do to maintain the chain of custody?

A. Document the collection and require a sign-off when possession changes.

B. Lock the device in a safe or other secure location to prevent theft or alteration.

C. Place the device in a Faraday cage to prevent corruption of the data.

D. Record the collection in a block chain-protected public ledger.

Question #:16 - (Exam Topic 4)

A security analyst discovers several jpg photos from a cellular phone during a forensics investigation involving a compromised system The analyst runs a forensics tool to gather file metadata Which of the following would be part of the images if all the metadata is still intact?

A. The GSS location

B. When the file was deleted

C. The total number of print jobs

D. The number of copies made

Question #:17 - (Exam Topic 4)

The application development teams have been asked to answer the following questions:

- Does this application receive patches from an external source?
- Does this application contain open-source code?
- Is this application accessible by external users?
- Does this application meet the corporate password standard?

Which of the following are these questions part of?

A. Risk control self-assessment

B. Risk management strategy

C. Risk acceptance

D. Risk matrix

Question #:18 - (Exam Topic 4)

During an incident, an EDR system detects an increase in the number of encrypted outbound connections from multiple hosts. A firewall is also reporting an increase in outbound connections that use random high ports. An analyst plans to review the correlated logs to find the source of the incident. Which of the following tools will best assist the analyst?

A. A vulnerability scanner

B. A NGFW

C. The Windows Event Viewer

D. A SIEM

Question #:19 - (Exam Topic 4)

A host was infected with malware. During the incident response. Joe, a user, reported that he did not receive any emails with links, but he had been browsing the internet all day. Which of the following would most likely show where the malware originated?

A. The DNS logs

B. The web server logs

C. The SIP traffic logs

D. The SNMP logs

Question #:20 - (Exam Topic 4)

An attacker was eavesdropping on a user who was shopping online. The attacker was able to spoof the IP address associated with the shopping site. Later, the user received an email regarding credit card statement with unusual purchases. Which of the following attacks took place?

A. On-path attack

B. Protocol poisoning

C. Domain hijacking

D. Bluejacking

Question #:21 - (Exam Topic 4)

Historically, a company has had issues with users plugging in personally owned removable media devices into corporate computers. As a result, the threat of malware incidents is almost constant. Which of the following would best help prevent the malware from being installed on the computers?

A. AUP

B. NGFW

C. DLP

D. EDR

Question #:22 - (Exam Topic 4)

Server administrators want to configure a cloud solution so that computing memory and processor usage are maximized most efficiently across a number of virtual servers. They also need to avoid potential denial-of-service situations caused by availability. Which of the following should administrators configure to maximize system availability while efficiently utilizing available computing power?

A. Dynamic resource allocation

B. High availability

C. Segmentation

D. Container security

Question #:23 - (Exam Topic 4)

An organization suffered numerous multiday power outages at its current location. The Chief Executive Officer wants to create a disaster recovery strategy to resolve this issue. Which of the following options offer low-cost solutions? (Select two).

A. Warm site

B. Generator

C. Hot site

D. Cold site

E. Cloud backups

F. UPS

Question #:24 - (Exam Topic 4)

Which of the following is an example of risk avoidance?

A. Installing security updates directly in production to expedite vulnerability fixes

B. Buying insurance to prepare for financial loss associated with exploits

C. Not installing new software to prevent compatibility errors

D. Not taking preventive measures to stop the theft of equipment

Question #:25 - (Exam Topic 4)

An organization wants to ensure that proprietary information is not inadvertently exposed during facility tours. Which of the following would the organization implement to mitigate this risk?

A. Clean desk policy

B. Background checks

C. Non-disclosure agreements

D. Social media analysis

Question #:26 - (Exam Topic 4)

When implementing automation with loT devices, which of the following should be considered first to keep the network secure?

A. Z-Wave compatibility

B. Network range

C. Zigbee configuration

D. Communication protocols

Question #:27 - (Exam Topic 4)

Which of the following scenarios describes a possible business email compromise attack?

A. An employee receives a gift card request m an email that has an executive's name m the display held to the email

B. Employees who open an email attachment receive messages demanding payment m order to access files

C. A service desk employee receives an email from the HR director asking for log-in credentials lo a cloud administrator account

D. An employee receives an email with a link to a phishing site that is designed to look like the company's email portal.

Question #:28 - (Exam Topic 4)

A company's Chief Information Security Officer (CISO) recently warned the security manager that the company's Chief Executive Officer (CEO) is planning to publish a controversial opinion article in a national newspaper, which may result in new cyberattacks. Which of the following would be best for the security manager to use in a threat model?

A. Hacktivists

B. White-hat hackers

C. Script kiddies

D. Insider threats

Question #:29 - (Exam Topic 4)

The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, including during a pandemic or crisis. However, the CEO is concerned that some staff members may take advantage of the flexibility and work from high-risk countries while on holiday or outsource work to a third-party organization in another country. The Chief Information Officer believes the company can implement some basic controls to mitigate the majority of the risk. Which of the following would be best to mitigate the CEO's concerns? (Select two).

A. Geolocation

B. Time-of-day restrictions

C. Certificates

D. Tokens

E. Geotagging

F. Role-based access controls

Question #:30 - (Exam Topic 4)

A security architect at a large, multinational organization is concerned about the complexities and overhead of managing multiple encryption keys securely in a multicioud provider environment. The security architect is looking for a solution with reduced latency to allow the incorporation of the organization's existing keys and to maintain consistent, centralized control and management regardless of the data location. Which of the following would best meet the architect's objectives?

A. Trusted Platform Module

B. laaS

C. HSMaas

D. PaaS

Question #:31 - (Exam Topic 4)

The most recent vulnerability scan flagged the domain controller with a critical vulnerability. The systems administrator researched the vulnerability and discovered the domain controller does not run the associated application with the vulnerability. Which of the following steps should the administrator take next?

A. Ensure the scan engine is configured correctly.

B. Apply a patch to the domain controller.

C. Research the CVE.

D. Document this as a false positive.

Question #:32 - (Exam Topic 4)

A large financial services firm recently released information regarding a security breach within its corporate network that began several years before. During the time frame in which the breach occurred, indicators show an attacker gained administrative access to the network through a file downloaded from a social media site and subsequently installed it without the user's knowledge. Since the compromise, the attacker was able to take command and control of the computer systems anonymously while obtaining sensitive corporate and personal employee information. Which of the following methods did the attacker most likely use to gain access?

A. A bol

B. A fileless virus

C. A logic bomb

D. A RAT

Question #:33 - (Exam Topic 4)

Which of the following exercises should an organization use to improve its incident response process?

A. Tabletop

B. Replication

C. Failover

D. Recovery

Question #:34 - (Exam Topic 4)

Which of the following threat vectors would appear to be the most legitimate when used by a malicious actor to impersonate a company?

A. Phone call

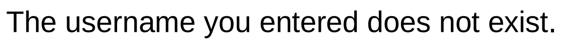
B. Instant message

C. Email

D. Text message

Question #:35 - (Exam Topic 4)

An attacker is attempting to harvest user credentials on a client's website. A security analyst notices multiple attempts of random usernames and passwords. When the analyst types in a random username and password, the logon screen displays the following message:



The username you entered does not exist.

Which of the following should the analyst recommend be enabled?

A. Input validation

B. Obfuscation

C. Error handling

D. Username lockout

Question #:36 - (Exam Topic 4)

Which of the following is an administrative control that would be most effective to reduce the occurrence of malware execution?

A. Security awareness training

B. Frequency of NIDS updates

C. Change control procedures

D. EDR reporting cycle

Question #:37 - (Exam Topic 4)

A security engineer needs to recommend a solution to defend against malicious actors misusing protocols and being allowed through network defenses. Which of the following will the engineer most likely recommended?

A. A content filter

B. AWAF

C. A next-generation firewall

D. An IDS

Question #:38 - (Exam Topic 4)

Which of the following agreements defines response time, escalation points, and performance metrics?

A. BPA

B. MOA

C. NDA

D. SLA

Question #:39 - (Exam Topic 4)

The manager who is responsible for a data set has asked a security engineer to apply encryption to the data on a hard disk. The security engineer is an example of a:

A. data controller

B. data owner.

C. data custodian.

D. data processor

Question #:40 - (Exam Topic 4)

A well-known organization has been experiencing attacks from APTs. The organization is concerned that custom malware is being created and emailed into the company or installed on USB sticks that are dropped in parking lots. Which of the following is the best defense against this scenario?

A. Configuring signature-based antivirus to update every 30 minutes

B. Enforcing S/MIME for email and automatically encrypting USB drives upon insertion

C. Implementing application execution in a sandbox for unknown software

D. Fuzzing new files for vulnerabilities if they are not digitally signed

Question #:41 - (Exam Topic 4)

The concept of connecting a user account across the systems of multiple enterprises is best known as:

A. federation

B. a remote access policy.

C. multifactor authentication

D. single sign-on.

Question #:42 - (Exam Topic 4)

An internet company has created a new collaboration application. To expand the user base, the company wants to implement an option that allows users to log in to the application with the credentials of her popular websites. Which of the following should the company implement?

A. SSO

B. CHAP

C. 802.1X

D. OpenlD

Question #:43 - (Exam Topic 4)

Which of the following security controls is used to isolate a section of the network and its externally available resources from the internal corporate network in order to reduce the number of possible attacks?

A. Faraday cages

B. Air gap

C. Vaulting

D. Proximity readers

Question #:44 - (Exam Topic 4)

A security analyst receives a SIEM alert that someone logged in to the app admin test account, which is only used for the early detection of attacks. The security analyst then reviews the following application log:

```
[03/06/20xx:17:20:18] system 127.0.0.1 FindXPath=//User [Username/text()='foo' or 7=7 or 'o'='o' And Password/text='bar']
[03/06/20xx:17:21:18] appadmin 194.28.114.102 action:login result:success
[03/06/20xx:17:22:18] appadmin 194.28.114.102 action:open.account (12345) result: fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account (23456) result: fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account (23456) result: fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account (45678) result: fail
```

Which of the following can the security analyst conclude?

A. A replay attack is being conducted against the application.

B. An injection attack is being conducted against a user authentication system.

C. A service account password may have been changed, resulting in continuous failed logins within the application.

D. A credentialed vulnerability scanner attack is testing several CVEs against the application.

Question #:45 - (Exam Topic 4)

Which of the following would be most effective to contain a rapidly spreading attack that is affecting a large number of organizations?

A. Machine learning

B. DNS sinkhole

C. Blocklist

D. Honey pot

Question #:46 - (Exam Topic 4)

A threat actor used a sophisticated attack to breach a well-known ride-sharing company. The threat actor posted on social media that this action was in response to the company's treatment of its drivers. Which of the following best describes the type of throat actor?

A. Nation-slate

B. Hacktivist

C. Organized crime

D. Shadow IT

Question #:47 - (Exam Topic 4)

Which of the following is used to validate a certificate when it is presented to a user?

A. OCSP

B. CSR

C. CA

D. CRC

Question #:48 - (Exam Topic 4)

During a recent penetration test, a tester plugged a laptop into an Ethernet port in an unoccupied conference room and obtained a valid IP address. Which of the following would have best prevented this avenue of attack?

A. Enabling MAC address filtering

B. Moving printers inside a firewall

C. Implementing 802.IX

D. Using network port security

Question #:49 - (Exam Topic 4)

The IT department's on-site developer has been with the team for many years. Each time an application is released; the security team is able to identify multiple vulnerabilities. Which of the following would best help the team ensure the application is ready to be released to production?

A. Limit the use of third-party libraries.

B. Prevent data exposure queries.

C. Obfuscate the source code

D. Submit the application to OA before releasing it.

Question #:50 - (Exam Topic 4)

A worldwide manufacturing company has been experiencing email account compromises. In one incident, a user logged in from the corporate office in France, but then seconds later, the same user account attempted a login from Brazil. Which of the following account policies would best prevent this type of attack?

A. Network location

B. Impossible travel time

C. Geolocation

D. Geofencing

Question #:51 - (Exam Topic 4)

A company's legal department drafted sensitive documents in a SaaS application and wants to ensure the documents cannot be accessed by individuals in high-risk countries. Which of the following is the most effective way to limit this access?

A. Data masking

B. Encryption

C. Geolocation policy

D. Data sovereignty regulation

Question #:52 - (Exam Topic 4)

An organization's Chief Security Officer (CSO) wants to validate the business's involvement in the incident response plan to ensure its validity and thoroughness. Which of the following will the CSO most likely use?

A. An external security assessment

B. A bug bounty program

C. A tabletop exercise

D. A red-team engagement

Question #:53 - (Exam Topic 4)

Which of the following holds staff accountable while escorting unauthorized personnel?

A. Locks

B. Badges

C. Cameras

D. Visitor logs

Question #:54 - (Exam Topic 4)

An organization is concerned that its hosted web servers are not running the most updated version of the software. Which of the following would work best to help identify potential vulnerabilities?

A. ping -S comptia.org -p 80

B. nc -1 -v comptia.crg -p 80

C. nmap comptia.org -p 80 -sv

D. nslookup -port 80 comptia.org

Question #:55 - (Exam Topic 4)

A user's login credentials were recently compromised. During the investigation, the security analyst determined the user input credentials into a pop-up window when prompted to confirm the username and password However the trusted website does not use a pop-up for entering user credentials. Which of the following attacks occurred?

A. Cross-site scripting

B. SOL injection

C. DNS poisoning

D. Certificate forgery

Question #:56 - (Exam Topic 4)

A retail executive recently accepted a job with a major competitor. The following week, a security analyst reviews the security logs and identifies successful logon attempts to access the departed executive's accounts. Which of the following security practices would have addressed the issue?

A. A non-disclosure agreement

B. Least privilege

C. An acceptable use policy

D. Off boarding

Question #:57 - (Exam Topic 4)

Which of the following is used to quantitatively measure the criticality of a vulnerability?

A. CVE

B. CVSS

C. CIA

D. CERT

Question #:58 - (Exam Topic 4)

Which of the following is the correct order of volatility from most to least volatile?

A. Memory, temporary filesystems. routing tables, disk, network storage

B. Cache, memory, temporary filesystems. disk, archival media

C. Memory, disk, temporary filesystems. cache, archival media

D. CachSe, disk, temporary filesystems. network storage, archival media

Question #:59 - (Exam Topic 4)

An organization is outlining data stewardship roles and responsibilities. Which of the following employee roles would determine the purpose of data and how to process it?

A. Data custodian

B. Data controller

C. Data protection officer

D. Data processor

Question #:60 - (Exam Topic 4)

A financial analyst is expecting an email containing sensitive information from a client. When the email arrives, the analyst receives an error and is unable to open the encrypted message. Which of the following is the most likely cause of the issue?

A. The S/MIME plug-in is not enabled.

B. The SSL certificate has expired.

C. Secure IMAP was not implemented.

D. P0P3S is not supported.

Question #:61 - (Exam Topic 4)

A help desk technician receives a phone call from someone claiming to be a part of the organization's cybersecurity incident response team. The caller asks the technician to verify the network's internal firewall IP address. Which of the following is the technician's best course of action?

A. Direct the caller to stop by the help desk in person and hang up declining any further requests from the caller.

B. Ask for the caller's name, verify the person's identity in the email directory, and provide the requested information over the phone.

C. Write down the phone number of the caller if possible, the name of the person requesting the information, hang up, and notify the organization's cybersecurity officer.

D. Request the caller send an email for identity verification and provide the requested information via email to the caller.

Question #:62 - (Exam Topic 4)

An engineer is setting up a VDI environment for a factory location, and the business wants to deploy a low-cost solution to enable users on the shop floor to log in to the VDI environment directly. Which of the following should the engineer select to meet these requirements?

A. Laptops

B. Containers

C. Thin clients

D. Workstations

Question #:63 - (Exam Topic 4)

A company recently experienced a data breach and the source was determined to be an executive who was charging a phone in a public area. Which of the following would most likely have prevented this breach?

A. A firewall

B. A device pin

C. A USB data blocker

D. Biometrics

Question #:64 - (Exam Topic 4)

Recent changes to a company's BYOD policy require all personal mobile devices to use a two-factor authentication method that is not something you know or have. Which of the following will meet this requirement?

A. Facial recognition

B. Six-digit PIN

C. PKI certificate

D. Smart card

Question #:65 - (Exam Topic 4)

Which of the following describes the ability of code to target a hypervisor from inside a guest OS?

A. Fog computing

B. VM escape

C. Software-defined networking

D. Image forgery

E. Container breakout

Question #:66 - (Exam Topic 4)

A security analyst is reviewing the output of a web server log and notices a particular account is attempting to transfer large amounts of money:

```
GET http://yourbank.com/transfer.do?acctnum=087646959&amount=500000 HTTP/1.1

GET http://yourbank.com/transfer.do?acctnum=087646958&amount=5000000 HTTP/1.1

GET http://yourbank.com/transfer.do?acctnum=087646958&amount=1000000 HTTP/1.1

GET http://yourbank.com/transfer.do?acctnum=087646953 &amount=500 HTTP/1.1
```

Which of the following types of attacks is most likely being conducted?

A. SQLi

B. CSRF

C. Spear phishing

D. API

Question #:67 - (Exam Topic 4)

A security analyst receives alerts about an internal system sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours. Which of the following is most likely occurring?

A. A worm is propagating across the network.

B. Data is being exfiltrated.

C. A logic bomb is deleting data.

D. Ransomware is encrypting files.

Question #:68 - (Exam Topic 4)

A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs, the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be best for the security manager to implement while maintaining alerting capabilities?

A. Segmentation

B. Firewall allow list

C. Containment

D. Isolation

Question #:69 - (Exam Topic 4)

Employees in the research and development business unit receive extensive training to ensure they understand how to best protect company data. Which of the following is the type of data these employees are most likely to use in day-to-day work activities?

A. Encrypted

B. Intellectual property

C. Critical

D. Data in transit

Question #:70 - (Exam Topic 4)

An attacker is trying to gain access by installing malware on a website that is known to be visited by the target victims. Which of the following is the attacker most likely attempting?

A. A spear-phishing attack

B. A watering-hole attack

C. Typosquatting

D. A phishing attack

Question #:71 - (Exam Topic 4)

An organization relies on third-party videoconferencing to conduct daily business. Recent security changes now require all remote workers to utilize a VPN to corporate resources. Which of the following would best maintain high-quality videoconferencing while minimizing latency when connected to the VPN?

A. Using geographic diversity lo have VPN terminators closer to end users

B. Utilizing split tunneling so only traffic for corporate resources is encrypted

C. Purchasing higher bandwidth connections to meet the increased demand

D. Configuring OoS properly on the VPN accelerators

Question #:72 - (Exam Topic 4)

Which of the following teams combines both offensive and defensive testing techniques to protect an organization's critical systems?

A. Red

B. Blue

C. Purple

D. Yellow

Question #:73 - (Exam Topic 4)

A company is adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices. Which of the following vulnerabilities is the organization addressing?

A. Cross-site scripting

B. Buffer overflow

C. Jailbreaking

D. Side loading

Question #:74 - (Exam Topic 4)

Several universities are participating in a collaborative research project and need to share compute and storage resources. Which of the following cloud deployment strategies would best meet this need?

A. Community

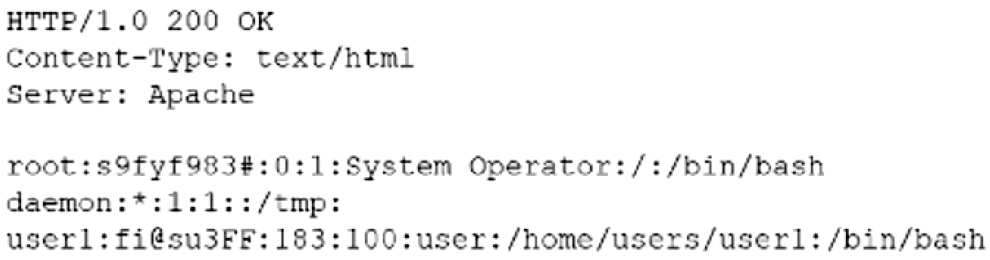
B. Private

C. Public

D. Hybrid

Question #:75 - (Exam Topic 4)

A security administration is trying to determine whether a server is vulnerable to a range of attacks After using a tool, the administrator obtains the following output.



```
HTTP/1.0 200 OK
Content-Type: text/html
Server: Apache

root:s9fyf983#:0:1:System Operator:/:/bin/bash
daemon:*:1:1::/tmp:
user1:fi@su3FF:183:100:user:/home/users/user1:/bin/bash
```

Which of the following attacks was successfully implemented based on the output?

A. Memory leak

B. Race condition

C. SQL injection

D. Directory traversal