



# CompTIA

## Exam Questions SY0-601

CompTIA Security+ Exam

NEW QUESTION 1

- (Exam Topic 1)

Which of the following is an example of transference of risk?

- A. Purchasing insurance
- B. Patching vulnerable servers
- C. Retiring outdated applications
- D. Application owner risk sign-off

Answer: A

NEW QUESTION 2

- (Exam Topic 1)

Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

INSTRUCTIONS

Not all attacks and remediation actions will be used.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources	Web server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack establishes a connection which allows remote commands to be executed	User	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack is self propagating and compromises a SQL database using well known credentials as it moves through the network	Database server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials	Executive	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login	Application	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Web server Botnet Enable DDoS protection User RAT Implement a host-based IPS Database server Worm Change the default application password Executive Keylogger Disable vulnerable services Application Backdoor Implement 2FA using push notification Graphical user interface, application Description automatically generated

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet ▾	Enable DDoS protection ▾
The attack establishes a connection, which allows remote commands to be executed.	User	RAT ▾	Implement a host-based IPS ▾
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Worm ▾	Change the default application password ▾
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger ▾	Disable vulnerable services ▾
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor ▾	Implement 2FA using push notification ▾

### NEW QUESTION 3

- (Exam Topic 1)

The Chief Information Security Officer (CISO) requested a report on potential areas of improvement following a security incident. Which of the following incident response processes is the CISO requesting?

- A. Lessons learned
- B. Preparation
- C. Detection
- D. Containment
- E. Root cause analysis

**Answer:** A

### NEW QUESTION 4

- (Exam Topic 1)

Certain users are reporting their accounts are being used to send unauthorized emails and conduct suspicious activities After further investigation, a security analyst notices the following

- All users share workstations throughout the day
- Endpoint protection was disabled on several workstations throughout the network.
- Travel times on logins from the affected users are impossible
- Sensitive data is being uploaded to external sites
- All user account passwords were forced to be reset and the issue continued Which of the following attacks is being used to compromise the user accounts?

- A. Brute-force
- B. Keylogger
- C. Dictionary
- D. Rainbow

**Answer:** C

### NEW QUESTION 5

- (Exam Topic 1)

Which of the following would BEST provide a systems administrator with the ability to more efficiently identify systems and manage permissions and policies based on location, role, and service level?

- A. Standard naming conventions
- B. Domain services
- C. Baseline configurations
- D. Diagrams

**Answer:** C

### NEW QUESTION 6

- (Exam Topic 1)

A company is considering transitioning to the cloud. The company employs individuals from various locations around the world The company does not want to increase its on-premises infrastructure blueprint and only wants to pay for additional compute power required. Which of the following solutions would BEST meet the needs of the company?

- A. Private cloud
- B. Hybrid environment
- C. Managed security service provider
- D. Hot backup site

**Answer:** B

#### NEW QUESTION 7

- (Exam Topic 1)

During an incident response, an analyst applied rules to all inbound traffic on the border firewall and implemented ACLs on each critical server. Following an investigation, the company realizes it is still vulnerable because outbound traffic is not restricted and the adversary is able to maintain a presence in the network. In which of the following stages of the Cyber Kill Chain is the adversary currently operating?

- A. Reconnaissance
- B. Command and control
- C. Actions on objective
- D. Exploitation

**Answer: B**

#### NEW QUESTION 8

- (Exam Topic 1)

Security analysts are conducting an investigation of an attack that occurred inside the organization's network. An attacker was able to connect network traffic between workstation throughout the network. The analysts review the following logs:

VLAN	Address
-----	-----
1	0007.1e5d.3213
1	002a.7d.44.8801
1	0011.aab4.344d

The layer 2 address table has hundred of entries similar to the ones above. Which of the following attacks has MOST likely occurred?

- A. SQL injection
- B. DNS spoofing
- C. MAC flooding
- D. ARP poisoning

**Answer: D**

#### NEW QUESTION 9

- (Exam Topic 1)

A business operations manager is concerned that a PC that is critical to business operations will have a costly hardware failure soon. The manager is looking for options to continue business operations without incurring large costs. Which of the following would mitigate the manager's concerns?

- A. Implement a full system upgrade
- B. Perform a physical-to-virtual migration
- C. Install uninterruptible power supplies
- D. Purchase cybersecurity insurance

**Answer: B**

#### NEW QUESTION 10

- (Exam Topic 1)

A security administrator is analyzing the corporate wireless network. The network only has two access points running on channels 1 and 11. While using airodump-ng, the administrator notices other access points are running with the same corporate ESSID on all available channels and with the same BSSID of one of the legitimate access points. Which of the following attacks is happening on the corporate network?

- A. Man in the middle
- B. Evil twin
- C. Jamming
- D. Rogue access point
- E. Disassociation

**Answer: B**

#### NEW QUESTION 10

- (Exam Topic 1)

An organization is migrating several SaaS applications that support SSO. The security manager wants to ensure the migration is completed securely. Which of the following should the organization consider before implementation? (Select TWO).

- A. The back-end directory source
- B. The identity federation protocol
- C. The hashing method
- D. The encryption method
- E. The registration authority
- F. The certificate authority

**Answer: CF**

#### NEW QUESTION 11

- (Exam Topic 1)

An amusement park is implementing a biometric system that validates customers' fingerprints to ensure they are not sharing tickets. The park's owner values customers above all and would prefer customers' convenience over security. For this reason, which of the following features should the security team prioritize FIRST?

- A. Low FAR
- B. Low efficacy
- C. Low FRR
- D. Low CER

**Answer: C**

**Explanation:**

FAR (False Acceptance Rate) FRR (False Rejection Rate)

CER (Crossover Error Rate) AKA ERR (Equal Error Rate)

since he is willing to sacrifice Security for Customer Service, Best way to understand this is. FAR has to go up in order for FRR to go down. typical business practice is in the middle of both which would be near the CER.

**NEW QUESTION 15**

- (Exam Topic 1)

Which of the following tools is effective in preventing a user from accessing unauthorized removable media?

- A. USB data blocker
- B. Faraday cage
- C. Proximity reader
- D. Cable lock

**Answer: B**

**NEW QUESTION 16**

- (Exam Topic 1)

An attack has occurred against a company.

**INSTRUCTIONS**

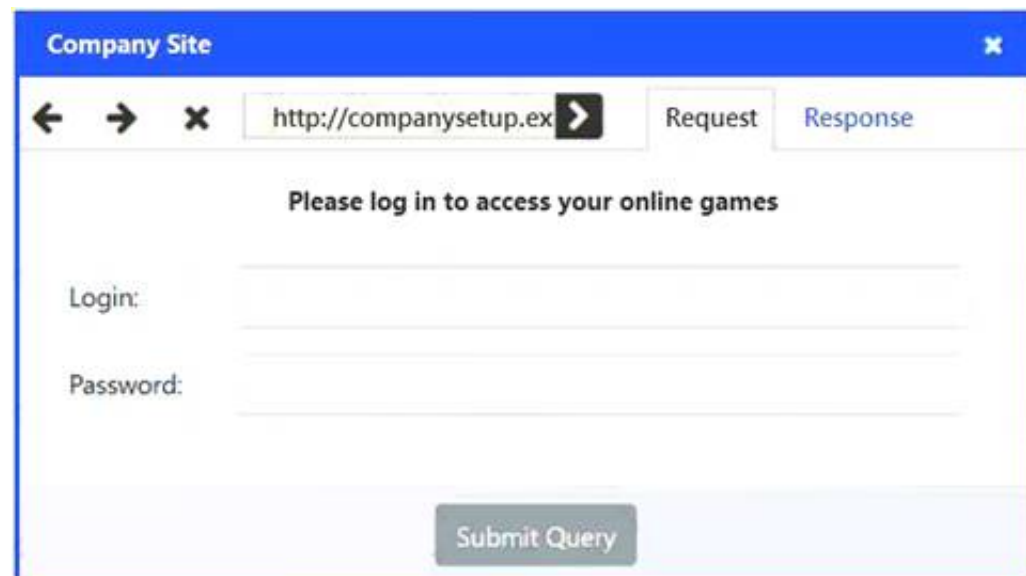
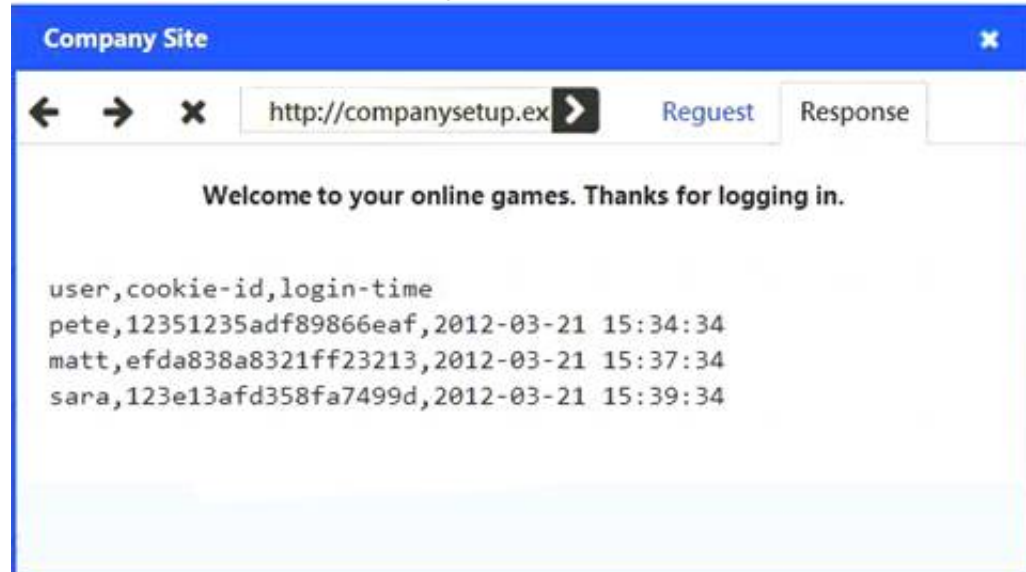
You have been tasked to do the following:

Identify the type of attack that is occurring on the network by clicking on the attacker's tablet and reviewing the output. (Answer Area 1).

Identify which compensating controls should be implemented on the assets, in order to reduce the effectiveness of future attacks by dragging them to the correct server.

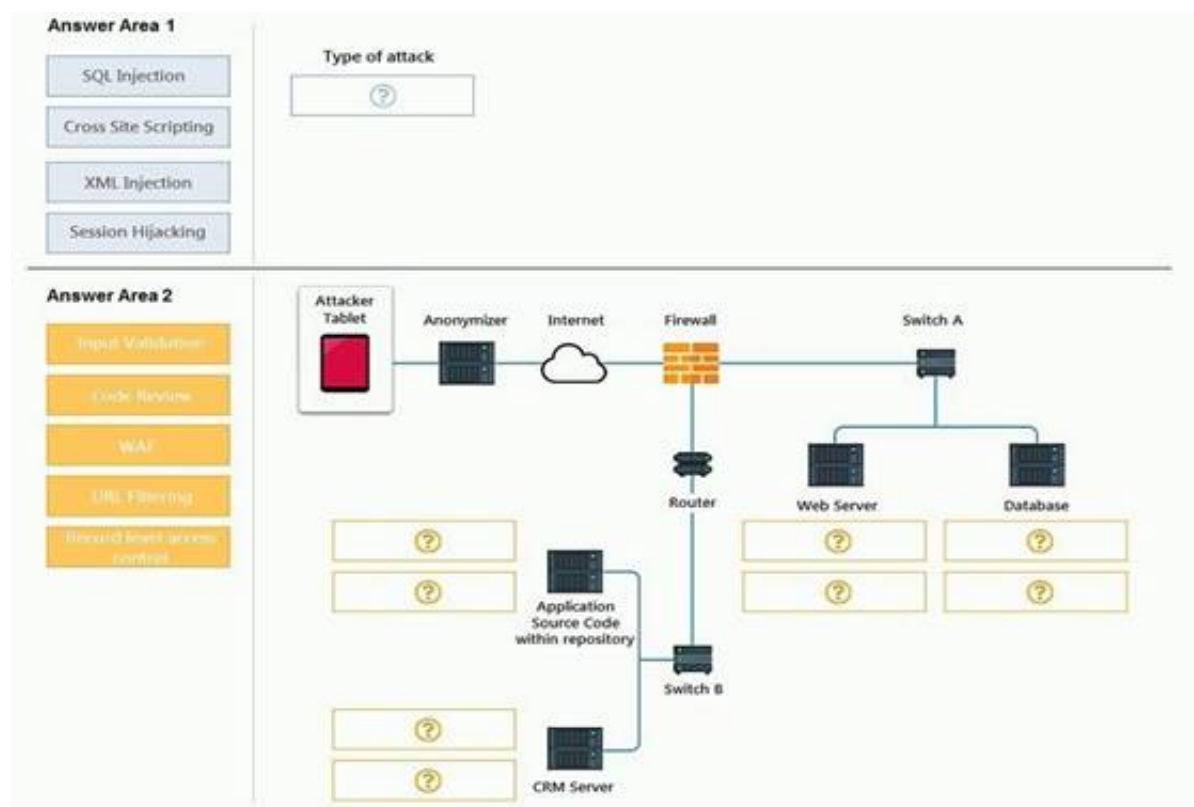
(Answer area 2) All objects will be used, but not all placeholders may be filled. Objects may only be used once.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Select and Place:





- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

Diagram Description automatically generated

**NEW QUESTION 21**

- (Exam Topic 1)

Which of the following would be the BEST way to analyze diskless malware that has infected a VDI?

- A. Shut down the VDI and copy off the event logs.  
 B. Take a memory snapshot of the running system.  
 C. Use NetFlow to identify command-and-control IPs.  
 D. Run a full on-demand scan of the root volume.

**Answer:** B

**NEW QUESTION 22**

- (Exam Topic 1)

Which of the following are common VoIP-associated vulnerabilities? (Select TWO).

- A. SPIM  
 B. vishing  
 C. Hopping  
 D. Phishing  
 E. Credential harvesting  
 F. Tailgating

**Answer:** AB

**NEW QUESTION 27**

- (Exam Topic 1)

A large bank with two geographically dispersed data centers is concerned about major power disruptions at both locations Every day each location experiences very brief outages that last for a few seconds However during the summer a high risk of intentional brownouts that last up to an hour exists particularly at one of the locations near an industrial smelter. Which of the following is the BEST solution to reduce the risk of data loss?

- A. Dual supply  
 B. Generator  
 C. PDU  
 D. Daily backups

**Answer:** B

**NEW QUESTION 30**

- (Exam Topic 1)

An employee received a word processing file that was delivered as an email attachment The subject line and email content enticed the employee to open the attachment. Which of the following attack vectors BEST matches this malware?

- A. Embedded Python code  
 B. Macro-enabled file  
 C. Bash scripting  
 D. Credential-harvesting website

**Answer:** B

**NEW QUESTION 33**

- (Exam Topic 1)

The Chief Compliance Officer from a bank has approved a background check policy for all new hires Which of the following is the policy MOST likely protecting against?

- A. Preventing any current employees' siblings from working at the bank to prevent nepotism
- B. Hiring an employee who has been convicted of theft to adhere to industry compliance
- C. Filternng applicants who have added false information to resumes so they appear better qualified
- D. Ensuring no new hires have worked at other banks that may be trying to steal customer information

**Answer:** B

**NEW QUESTION 37**

- (Exam Topic 1)

An IT manager is estimating the mobile device budget for the upcoming year Over the last five years, the number of devices that were replaced due to loss damage or theft steadily increased by 10%. Which of the following would BEST describe the estimated number of devices to be replaced next year?

- A. ALE
- B. ARO
- C. RPO
- D. SLE

**Answer:** A

**NEW QUESTION 42**

- (Exam Topic 1)

A company labeled some documents with the public sensitivity classification This means the documents can be accessed by:

- A. employees of other companies and the press
- B. all members of the department that created the documents
- C. only the company's employees and those listed in the document
- D. only the individuate listed in the documents

**Answer:** A

**NEW QUESTION 44**

- (Exam Topic 1)

An organization wants to participate in threat intelligence information sharing with peer groups. Which of the following would MOST likely meet the organizations requirement?

- A. Perform OSINT investigations
- B. Subscribe to threat intelligence feeds
- C. Submit RFCs
- D. Implement a TAXII server

**Answer:** B

**NEW QUESTION 46**

- (Exam Topic 1)

Which of the following is a known security nsk associated with data archives that contain financial information?

- A. Data can become a liability if archived longer than required by regulatory guidance
- B. Data must be archived off-site to avoid breaches and meet business requirements
- C. Companies are prohibited from providing archived data to e-discovery requests
- D. Unencrypted archives should be preserved as long as possible and encrypted

**Answer:** A

**NEW QUESTION 48**

- (Exam Topic 1)

A recent audit cited a risk involving numerous low-criticality vulnerabilities created by a web application using a third-party library. The development staff state there are still customers using the application even though it is end of life and it would be a substantial burden to update the application for compatibility with more secure libraries. Which of the following would be the MOST prudent course of action?

- A. Accept the risk if there is a clear road map for timely decommission
- B. Deny the risk due to the end-of-life status of the application.
- C. Use containerization to segment the application from other applications to eliminate the risk
- D. Outsource the application to a third-party developer group

**Answer:** C

**NEW QUESTION 52**

- (Exam Topic 1)

After a recent security incident, a security analyst discovered that unnecessary ports were open on a firewall policy for a web server. Which of the following firewall policies would be MOST secure for a web server?

A)

[Source	Destination	Port	Action]
Any	Any	TCP 53	Allow
Any	Any	TCP 80	Allow
Any	Any	TCP 443	Allow
Any	Any	Any	Any

B)

[Source	Destination	Port	Action]
Any	Any	TCP 53	Deny
Any	Any	TCP 80	Allow
Any	Any	TCP 445	Allow
Any	Any	Any	Allow

C)

[Source	Destination	Port	Action]
Any	Any	TCP 80	Deny
Any	Any	TCP 443	Allow
Any	Any	Any	Allow

D)

[Source	Destination	Port	Action]
Any	Any	TCP 80	Allow
Any	Any	TCP 443	Allow
Any	Any	Any	Deny

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer:** D

#### NEW QUESTION 54

- (Exam Topic 1)

A company is auditing the manner in which its European customers' personal information is handled Which of the following should the company consult?

- A. GDPR
- B. ISO
- C. NIST
- D. PCI DSS

**Answer:** A

#### NEW QUESTION 55

- (Exam Topic 1)

A security analyst has identified malv/are spreading through the corporate network and has activated the CSIRT Which of the following should the analyst do NEXT?

- A. Review how the malware was introduced to the network
- B. Attempt to quarantine all infected hosts to limit further spread
- C. Create help desk tickets to get infected systems reimaged
- D. Update all endpoint antivirus solutions with the latest updates

**Answer:** C

#### NEW QUESTION 60

- (Exam Topic 1)

An organization implemented a process that compares the settings currently configured on systems against secure configuration guidelines in order to identify any gaps Which of the following control types has the organization implemented?

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

**Answer:** C

#### Explanation:

the control acts to eliminate or reduce the likelihood that an attack can succeed. A preventative control operates before an attack can take place. Compensating



means to substitute one control with another (not happened here), Corrective means the attack has already happened (no mentioning), and detective is incorrect because the detective control detects ATTACKS, not vulnerabilities.

#### NEW QUESTION 61

- (Exam Topic 1)

Which of the following is the GREATEST security concern when outsourcing code development to third-party contractors for an internet-facing application?

- A. Intellectual property theft
- B. Elevated privileges
- C. Unknown backdoor
- D. Quality assurance

**Answer: C**

#### NEW QUESTION 66

- (Exam Topic 1)

An organization has decided to purchase an insurance policy because a risk assessment determined that the cost to remediate the risk is greater than the five-year cost of the insurance policy. The organization is enabling risk

- A. avoidance
- B. acceptance
- C. mitigation
- D. transference

**Answer: D**

#### NEW QUESTION 67

- (Exam Topic 1)

A security analyst is working on a project to implement a solution that monitors network communications and provides alerts when abnormal behavior is detected. Which of the following is the security analyst MOST likely implementing?

- A. Vulnerability scans
- B. User behavior analysis
- C. Security orchestration, automation, and response
- D. Threat hunting

**Answer: C**

#### Explanation:

SOAR solutions automatically aggregate and validate data from various sources, including threat intelligence, security information and event management (SIEM), and user and entity behavior analytics (UEBA) tools. It helps make security operations centers (SOCs) intelligence-driven, providing the context needed to make informed decisions and accelerate detection and response.

#### NEW QUESTION 69

- (Exam Topic 1)

A company needs to validate its updated incident response plan using a real-world scenario that will test decision points and relevant incident response actions without interrupting daily operations. Which of the following would BEST meet the company's requirements?

- A. Red-team exercise
- B. Capture-the-flag exercise
- C. Tabletop exercise
- D. Phishing exercise

**Answer: C**

#### NEW QUESTION 70

- (Exam Topic 1)

A company is implementing a DLP solution on the file server. The file server has PII, financial information, and health information stored on it. Depending on what type of data that is hosted on the file server, the company wants different DLP rules assigned to the data. Which of the following should the company do to help accomplish this goal?

- A. Classify the data
- B. Mask the data
- C. Assign an application owner
- D. Perform a risk analysis

**Answer: A**

#### NEW QUESTION 73

- (Exam Topic 1)

A junior security analyst is conducting an analysis after passwords were changed on multiple accounts without users' interaction. The SIEM has multiple log entries with the following text:

```
suspicious event - user: scheduledtasks successfully authenticate on AD on abnormal time  
suspicious event - user: scheduledtasks failed to execute c:\weekly_checkups\amazing-3rdparty-domain-assessment.py  
suspicious event - user: scheduledtasks failed to execute c:\weekly_checkups\secureyourAD-3rdparty-compliance.sh  
suspicious event - user: scheduledtasks successfully executed c:\weekly_checkups\amazing-3rdparty-domain-assessment.py
```

Which of the following is the MOST likely attack conducted on the environment?

- A. Malicious script
- B. Privilege escalation
- C. Domain hijacking
- D. DNS poisoning

**Answer:** A

#### NEW QUESTION 77

- (Exam Topic 1)

During a trial, a judge determined evidence gathered from a hard drive was not admissible. Which of the following BEST explains this reasoning?

- A. The forensic investigator forgot to run a checksum on the disk image after creation
- B. The chain of custody form did not note time zone offsets between transportation regions
- C. The computer was turned off
- D. and a RAM image could not be taken at the same time
- E. The hard drive was not properly kept in an antistatic bag when it was moved

**Answer:** A

#### NEW QUESTION 78

- (Exam Topic 1)

A systems administrator is troubleshooting a server's connection to an internal web server. The administrator needs to determine the correct ports to use. Which of the following tools BEST shows which ports on the web server are in a listening state?

- A. Ipconfig
- B. ssh
- C. Ping
- D. Netstat

**Answer:** D

#### Explanation:

<https://www.sciencedirect.com/topics/computer-science/listening-port>

#### NEW QUESTION 80

- (Exam Topic 1)

Which of the following documents provides expectations at a technical level for quality, availability, and responsibilities?

- A. EOL
- B. SLA
- C. MOU
- D. EOSL

**Answer:** B

#### NEW QUESTION 82

- (Exam Topic 1)

The board of directors at a company contracted with an insurance firm to limit the organization's liability. Which of the following risk management practices does the BEST describe?

- A. Transference
- B. Avoidance
- C. Mitigation
- D. Acknowledgement

**Answer:** A

#### NEW QUESTION 87

- (Exam Topic 1)

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

**Answer:** A

**Explanation:**

Community cloud storage is a variation of the private cloud storage model, which offers cloud solutions for specific businesses or communities. In this model, cloud storage providers offer their cloud architecture, software and other development tools to meet the requirements of the community. A community cloud in computing is a collaborative effort in which infrastructure is shared between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally.

**NEW QUESTION 91**

- (Exam Topic 1)

The Chief Information Security Officer (CISO) has requested that a third-party vendor provide supporting documents that show proper controls are in place to protect customer data. Which of the following would be BEST for the third-party vendor to provide to the CISO?

- A. GDPR compliance attestation
- B. Cloud Security Alliance materials
- C. SOC 2 Type 2 report
- D. NIST RMF workbooks

**Answer:** C

**Explanation:**

<https://www.itgovernance.co.uk/soc-reporting>

**NEW QUESTION 94**

- (Exam Topic 1)

A company wants to improve end users experiences when they log in to a trusted partner website. The company does not want the users to be issued separate credentials for the partner website. Which of the following should be implemented to allow users to authenticate using their own credentials to log in to the trusted partner's website?

- A. Directory service
- B. AAA server
- C. Federation
- D. Multifactor authentication

**Answer:** C

**NEW QUESTION 98**

- (Exam Topic 1)

Which of the following terms describes a broad range of information that is sensitive to a specific organization?

- A. Public
- B. Top secret
- C. Proprietary
- D. Open-source

**Answer:** C

**NEW QUESTION 99**

- (Exam Topic 1)

A security policy states that common words should not be used as passwords. A security auditor was able to perform a dictionary attack against corporate credentials. Which of the following controls was being violated?

- A. Password complexity
- B. Password history
- C. Password reuse
- D. Password length

**Answer:** B

**NEW QUESTION 100**

- (Exam Topic 1)

As part of a security compliance assessment, an auditor performs automated vulnerability scans. In addition, which of the following should the auditor do to complete the assessment?

- A. User behavior analysis
- B. Packet captures
- C. Configuration reviews
- D. Log analysis

**Answer:** D

**Explanation:**

A vulnerability scanner is essentially doing that. It scans every part of your network configuration that it can, and determines if known vulnerabilities are known at any point of that.

**NEW QUESTION 102**

- (Exam Topic 1)

Which of the following should be monitored by threat intelligence researchers who search for leaked credentials?

- A. Common Weakness Enumeration
- B. OSINT
- C. Dark web
- D. Vulnerability databases

**Answer:** C

#### NEW QUESTION 105

- (Exam Topic 1) A

user is attempting to navigate to a website from inside the company network using a desktop. When the user types in the URL. <https://www.site.com>, the user is presented with a certificate mismatch warning from the browser. The user does not receive a warning when visiting <http://www.anothersite.com>. Which of the following describes this attack?

- A. On-path
- B. Domain hijacking
- C. DNS poisoning
- D. Evil twin

**Answer:** C

#### NEW QUESTION 109

- (Exam Topic 1)

Which of the following is the MOST effective control against zero-day vulnerabilities?

- A. Network segmentation
- B. Patch management
- C. Intrusion prevention system
- D. Multiple vulnerability scanners

**Answer:** A

#### NEW QUESTION 113

- (Exam Topic 1)

The SOC for a large MSSP is meeting to discuss the lessons learned from a recent incident that took much too long to resolve This type of incident has become more common in recent weeks and is consuming large amounts of the analysts' time due to manual tasks being performed Which of the following solutions should the SOC consider to BEST improve its response time?

- A. Configure a NIDS appliance using a Switched Port Analyzer
- B. Collect OSINT and catalog the artifacts in a central repository
- C. Implement a SOAR with customizable playbooks
- D. Install a SIEM with community-driven threat intelligence

**Answer:** C

#### Explanation:

SOAR (Security Orchestration, Automation, and Response) Can use either playbook or runbook. It assists in collecting threat related data from a range of sources and automate responses to low level threats. (frees up some of the CSIRT time)

#### NEW QUESTION 117

- (Exam Topic 1)

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.c0mpt1a.com/contact-us/\*3Fname+3D+3Cscript+3Ealert\(document.cookie\)+3C+2Fscript+3E
```

Which of the following was MOST likely observed?

- A. DLL injection
- B. Session replay
- C. SOLI
- D. XSS

**Answer:** B

#### NEW QUESTION 118

- (Exam Topic 1)

An organization would like to give remote workers the ability to use applications hosted inside the corporate network Users will be allowed to use their personal computers or they will be provided organization assets Either way no data or applications will be installed locally on any user systems Which of the following mobile solutions would accomplish these goals?

- A. VDI
- B. MDM
- C. COPE
- D. UTM

**Answer:** A

#### Explanation:

MDM would require something to be installed. VDI, virtual desktop infrastructure, would allow employees to use run apps on the company network without

installing locally.

#### NEW QUESTION 119

- (Exam Topic 1)

A recent security breach exploited software vulnerabilities in the firewall and within the network management solution. Which of the following will MOST likely be used to identify when the breach occurred through each device?

- A. SIEM correlation dashboards
- B. Firewall syslog event logs
- C. Network management solution login audit logs
- D. Bandwidth monitors and interface sensors

**Answer: A**

#### NEW QUESTION 123

- (Exam Topic 1)

A database administrator wants to grant access to an application that will be reading and writing data to a database. The database is shared by other applications also used by the finance department Which of the following account types is MOST appropriate for this purpose?

- A. Service
- B. Shared
- C. eneric
- D. Admin

**Answer: A**

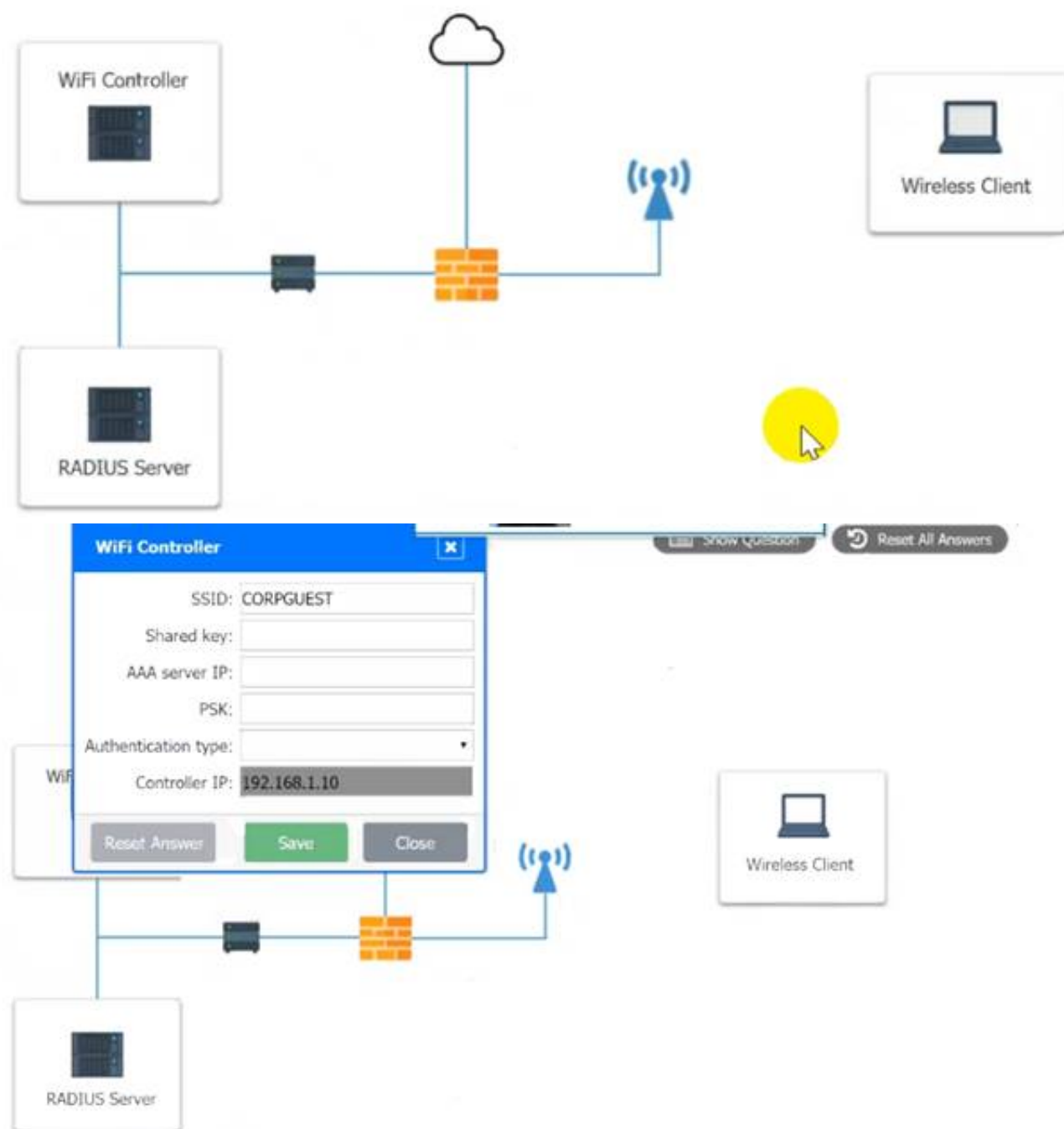
#### NEW QUESTION 126

- (Exam Topic 1)

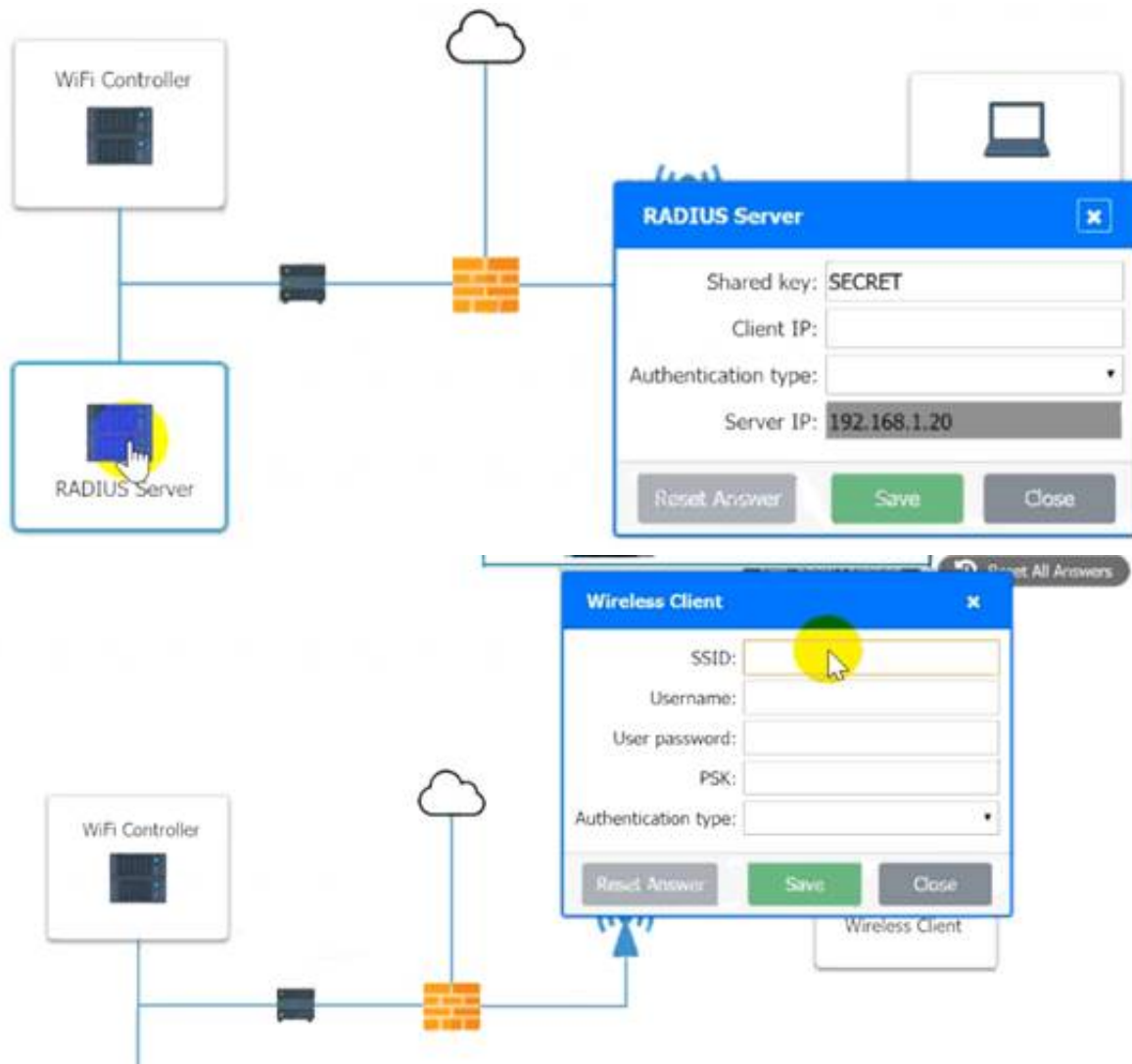
A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802.1X using the most secure encryption and protocol available.

Perform the following steps:

- \* 1. Configure the RADIUS server.
- \* 2. Configure the WiFi controller.
- \* 3. Preconfigure the client for an incoming guest. The guest AD credentials are: User: guest01  
Password: guestpass







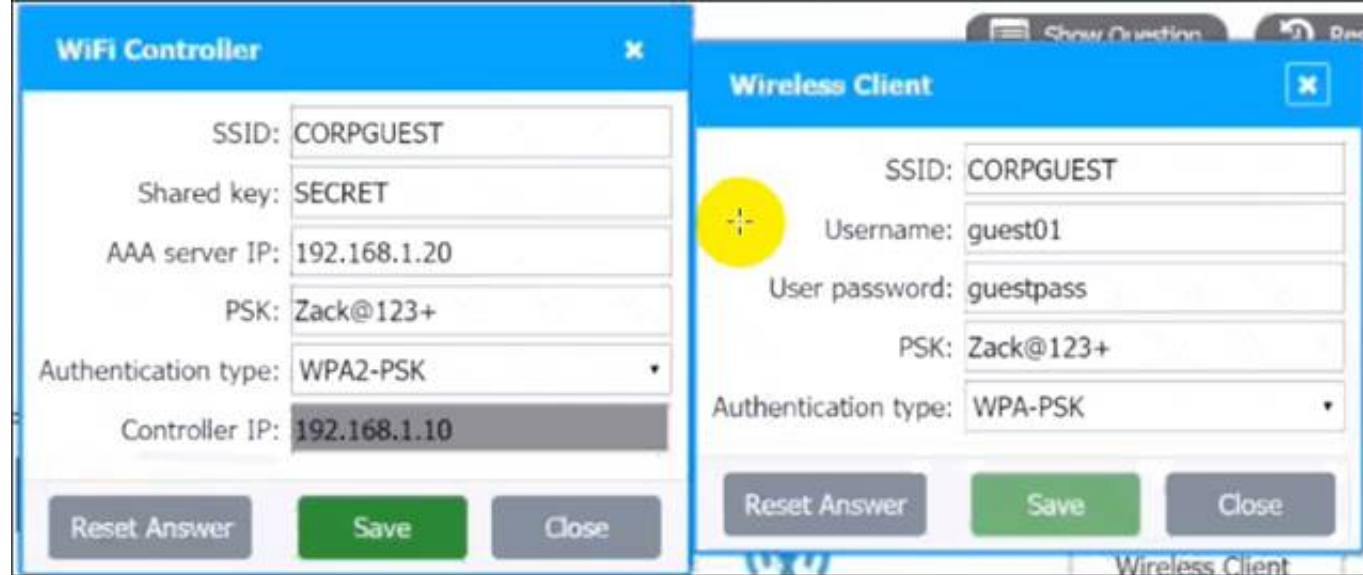
- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Use the same settings as describe in below images.

Graphical user interface, application Description automatically generated



Graphical user interface, text, application Description automatically generated



**NEW QUESTION 127**

- (Exam Topic 1)

A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.

**INSTRUCTIONS**

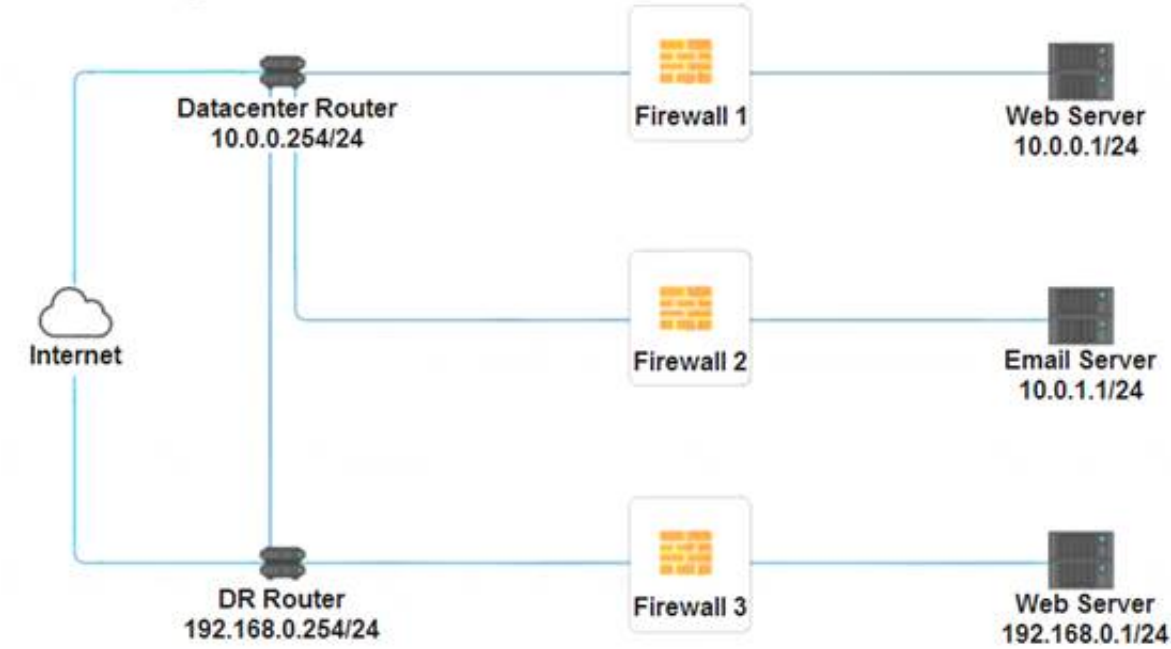
Click on each firewall to do the following:

- > Deny cleartext web traffic.
- > Ensure secure management protocols are used. Please Resolve issues at the DR site.

The ruleset order cannot be modified due to outside constraints.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Network Diagram



Firewall 1				
Rule Name	Source	Destination	Service	Action
DNS Rule	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Outbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
Management	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTP Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY

Firewall 2				
Rule Name	Source	Destination	Service	Action
DNS Rule	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Outbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
Management	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTP Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY

Firewall 3

Rule Name	Source	Destination	Service	Action
DNS Rule	<div>ANY</div> <div>10.0.0.1/24</div> <div>10.0.1.1/24</div> <div>192.168.0.1/24</div>	<div>ANY</div> <div>10.0.0.1/24</div> <div>10.0.1.1/24</div> <div>192.168.0.1/24</div>	<div>ANY</div> <div>DNS</div> <div>HTTP</div> <div>HTTPS</div> <div>TELNET</div> <div>SSH</div>	<div>PERMIT</div> <div>DENY</div>
HTTPS Outbound	<div>ANY</div> <div>10.0.0.1/24</div> <div>10.0.1.1/24</div> <div>192.168.0.1/24</div>	<div>ANY</div> <div>10.0.0.1/24</div> <div>10.0.1.1/24</div> <div>192.168.0.1/24</div>	<div>ANY</div> <div>DNS</div> <div>HTTP</div> <div>HTTPS</div> <div>TELNET</div> <div>SSH</div>	<div>PERMIT</div> <div>DENY</div>
Management	<div>ANY</div> <div>10.0.0.1/24</div> <div>10.0.1.1/24</div> <div>192.168.0.1/24</div>	<div>ANY</div> <div>10.0.0.1/24</div> <div>10.0.1.1/24</div> <div>192.168.0.1/24</div>	<div>ANY</div> <div>DNS</div> <div>HTTP</div> <div>HTTPS</div> <div>TELNET</div> <div>SSH</div>	<div>PERMIT</div> <div>DENY</div>
HTTPS Inbound	<div>ANY</div> <div>10.0.0.1/24</div> <div>10.0.1.1/24</div> <div>192.168.0.1/24</div>	<div>ANY</div> <div>10.0.0.1/24</div> <div>10.0.1.1/24</div> <div>192.168.0.1/24</div>	<div>ANY</div> <div>DNS</div> <div>HTTP</div> <div>HTTPS</div> <div>TELNET</div> <div>SSH</div>	<div>PERMIT</div> <div>DENY</div>
HTTP Inbound	<div>ANY</div> <div>10.0.0.1/24</div> <div>10.0.1.1/24</div> <div>192.168.0.1/24</div>	<div>ANY</div> <div>10.0.0.1/24</div> <div>10.0.1.1/24</div> <div>192.168.0.1/24</div>	<div>ANY</div> <div>DNS</div> <div>HTTP</div> <div>HTTPS</div> <div>TELNET</div> <div>SSH</div>	<div>PERMIT</div> <div>DENY</div>

Reset Answer

Save

Close

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Firewall 1:

Firewall 1

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	• ANY	• DNS	• PERMIT
HTTPS Outbound	10.0.0.1/24	• ANY	• HTTPS	• PERMIT
Management	ANY	• 10.0.0.1/24	• SSH	• PERMIT
HTTPS Inbound	ANY	• 10.0.0.1/24	• HTTPS	• PERMIT
HTTP Inbound	ANY	• 10.0.0.1/24	• HTTP	• DENY

Reset Answer

Save

Close

Firewall 1

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	• ANY	• DNS	• PERMIT
HTTPS Outbound	10.0.0.1/24	• ANY	• HTTPS	• PERMIT
Management	ANY	• 10.0.0.1/24	• SSH	• PERMIT
HTTPS Inbound	ANY	• 10.0.0.1/24	• HTTPS	• PERMIT
HTTP Inbound	ANY	• 10.0.0.1/24	• HTTP	• DENY

Reset Answer

Save

Close

DNS Rule – ANY --> ANY --> DNS --> PERMIT  
HTTPS Outbound – 10.0.0.1/24 --> ANY --> HTTPS --> PERMIT  
Management – ANY --> ANY --> SSH --> PERMIT  
HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT  
HTTP Inbound – ANY --> ANY --> HTTP --> DENY  
Firewall 2: No changes should be made to this firewall  
Graphical user interface, application Description automatically generated



Firewall 2				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	DNS	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY

Firewall 2				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	DNS	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY

Firewall 3:

DNS Rule – ANY --> ANY --> DNS --> PERMIT

HTTPS Outbound – 192.168.0.1/24 --> ANY --> HTTPS --> PERMIT Management – ANY --> ANY --> SSH --> PERMIT

HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT HTTP Inbound – ANY --> ANY --> HTTP --> DENY

Graphical user interface, application Description automatically generated

Firewall 3				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	192.168.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	192.168.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	192.168.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	192.168.0.1/24	HTTP	DENY

Firewall 3				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	192.168.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	192.168.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	192.168.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	192.168.0.1/24	HTTP	DENY

### NEW QUESTION 129

- (Exam Topic 1)

A new company wants to avoid channel interference when building a WLAN. The company needs to know the radio frequency behavior, identify dead zones, and determine the best place for access points. Which of the following should be done FIRST?

- A. Configure heat maps.
- B. Utilize captive portals.
- C. Conduct a site survey.
- D. Install Wi-Fi analyzers.

Answer: A

#### NEW QUESTION 132

- (Exam Topic 1)

Which of the following BEST reduces the security risks introduced when running systems that have expired vendor support and lack an immediate replacement?

- A. Implement proper network access restrictions
- B. Initiate a bug bounty program
- C. Classify the system as shadow IT.
- D. Increase the frequency of vulnerability scans

**Answer:** A

#### NEW QUESTION 137

- (Exam Topic 1)

Multiple business accounts were compromised a few days after a public website had its credentials database leaked on the internet No business emails were Identified in the breach, but the security team thinks that the list of passwords exposed was later used to compromise business accounts Which of the following would mitigate the issue?

- A. Complexity requirements
- B. Password history
- C. Acceptable use policy
- D. Shared accounts

**Answer:** C

#### NEW QUESTION 142

- (Exam Topic 1)

A security analyst is evaluating solutions to deploy an additional layer of protection for a web application The goal is to allow only encrypted communications without relying on network devices Which of the following can be implemented?

- A. HTTP security header
- B. DNSSEC implementation
- C. SRTP
- D. S/MIME

**Answer:** C

#### NEW QUESTION 145

- (Exam Topic 1)

An organization wants to implement a biometric system with the highest likelihood that an unauthorized user will be denied access. Which of the following should the organization use to compare biometric solutions?

- A. FRR
- B. Difficulty of use
- C. Cost
- D. FAR
- E. CER

**Answer:** A

#### NEW QUESTION 148

- (Exam Topic 1)

A report delivered to the Chief Information Security Officer (CISO) shows that some user credentials could be exfiltrated. The report also indicates that users tend to choose the same credentials on different systems and applications. Which of the following policies should the CISO use to prevent someone from using the exfiltrated credentials?

- A. MFA
- B. Lockout
- C. Time-based logins
- D. Password history

**Answer:** B

#### NEW QUESTION 150

- (Exam Topic 1)

A cloud service provider has created an environment where customers can connect existing local networks to the cloud for additional computing resources and block internal HR applications from reaching the cloud. Which of the following cloud models is being used?

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

**Answer:** C

#### Explanation:

Hybrid cloud refers to a mixed computing, storage, and services environment made up of on-premises infrastructure, private cloud services, and a public cloud—such as Amazon Web Services (AWS) or Microsoft Azure—with orchestration among the various platforms



#### NEW QUESTION 151

- (Exam Topic 1)

Which of the following employee roles is responsible for protecting an organization's collected personal information?

- A. CTO
- B. DPO
- C. CEO
- D. DBA

**Answer:** B

#### Explanation:

Many companies also have a data protection officer or DPO. This is a higher-level manager who is responsible for the organization's overall data privacy policies.  
<https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/data-roles-and-responsibilities/#:~:text=>

#### NEW QUESTION 152

- (Exam Topic 1)

A company is providing security awareness training regarding the importance of not forwarding social media messages from unverified sources. Which of the following risks would this training help to prevent?

- A. Hoaxes
- B. SPIMs
- C. Identity fraud
- D. Credential harvesting

**Answer:** A

#### Explanation:

Hoax

A hoax is a falsehood deliberately fabricated to masquerade as the truth. It is distinguishable from errors in observation or judgment, rumors, urban legends, pseudo sciences, and April Fools' Day events that are passed along in good faith by believers or as jokes.

Identity theft

Identity theft occurs when someone uses another person's personal identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes. The term identity theft was coined in 1964. Identity fraud (also known as identity theft or crime) involves someone using another individual's personal information without consent, often to obtain a benefit.

Credential Harvesting

Credential Harvesting (or Account Harvesting) is the use of MITM attacks, DNS poisoning, phishing, and other vectors to amass large numbers of credentials (username / password combinations) for reuse.

#### NEW QUESTION 156

- (Exam Topic 1)

Which of the following components can be used to consolidate and forward inbound Internet traffic to multiple cloud environments through a single firewall?

- A. Transit gateway
- B. Cloud hot site
- C. Edge computing
- D. DNS sinkhole

**Answer:** A

#### NEW QUESTION 159

- (Exam Topic 1)

Which of the following actions would be recommended to improve an incident response process?

- A. Train the team to identify the difference between events and incidents
- B. Modify access so the IT team has full access to the compromised assets
- C. Contact the authorities if a cybercrime is suspected
- D. Restrict communication surrounding the response to the IT team

**Answer:** A

#### NEW QUESTION 163

- (Exam Topic 1)

An organization has activated an incident response plan due to a malware outbreak on its network. The organization has brought in a forensics team that has identified an internet-facing Windows server as the likely point of initial compromise. The malware family that was detected is known to be distributed by manually logging on to servers and running the malicious code. Which of the following actions would be BEST to prevent reinfection from the initial infection vector?

- A. Prevent connections over TFTP from the internal network
- B. Create a firewall rule that blocks port 22 from the internet to the server
- C. Disable file sharing over port 445 to the server
- D. Block port 3389 inbound from untrusted networks

**Answer:** A

#### NEW QUESTION 167

- (Exam Topic 1)

A SOC operator is analyzing a log file that contains the following entries:

```
[06-Apr-2021-18:00:06] GET /index.php/../../../../../../../../etc/passwd
[06-Apr-2021-18:01:07] GET /index.php/../../../../../../../../etc/shadow
[06-Apr-2021-18:01:26] GET /index.php/../../../../../../../../../../../../../../../../etc/passwd
[06-Apr-2021-18:02:16] GET /index.php?var1=cat /etc/passwd;&var2=7865tgydk
[06-Apr-2021-18:02:56] GET /index.php?var1=cat /etc/shadow;&var2=7865tgydk
```

- A. SQL injection and improper input-handling attempts
- B. Cross-site scripting and resource exhaustion attempts
- C. Command injection and directory traversal attempts
- D. Error handling and privilege escalation attempts

**Answer: C**

#### NEW QUESTION 168

- (Exam Topic 1)

A tax organization is working on a solution to validate the online submission of documents. The solution should be earned on a portable USB device that should be inserted on any computer that is transmitting a transaction securely. Which of the following is the BEST certificate for these requirements?

- A. User certificate
- B. Self-signed certificate
- C. Computer certificate
- D. Root certificate

**Answer: D**

#### NEW QUESTION 171

- (Exam Topic 1)

Which of the following is the BEST example of a cost-effective physical control to enforce a USB removable media restriction policy?

- A. Putting security/antitamper tape over USB ports, logging the port numbers and regularly inspecting the ports
- B. Implementing a GPO that will restrict access to authorized USB removable media and regularly verifying that it is enforced
- C. Placing systems into locked key-controlled containers with no access to the USB ports
- D. Installing an endpoint agent to detect connectivity of USB and removable media

**Answer: B**

#### NEW QUESTION 175

- (Exam Topic 1)

A security analyst is concerned about critical vulnerabilities that have been detected on some applications running inside containers. Which of the following is the BEST remediation strategy?

- A. Update the base container image and redeploy the environment
- B. Include the containers in the regular patching schedule for servers
- C. Patch each running container individually and test the application
- D. Update the host in which the containers are running

**Answer: C**

#### NEW QUESTION 180

- (Exam Topic 2)

A recent phishing campaign resulted in several compromised user accounts. The security incident response team has been tasked with reducing the manual labor of filtering through all the phishing emails as they arrive and blocking the sender's email address, along with other time-consuming mitigation actions. Which of the following can be configured to streamline those tasks?

- A. SOAR playbook
- B. MOM policy
- C. Firewall rules
- D. URL filter
- E. SIEM data collection

**Answer: A**

#### NEW QUESTION 183

- (Exam Topic 2)

A security analyst is tasked with defining the "something you are" factor of the company's MFA settings. Which of the following is BEST to use to complete the configuration?

- A. Gait analysis
- B. Vein
- C. Soft token
- D. HMAC-based, one-time password

**Answer: A**

#### NEW QUESTION 187

- (Exam Topic 2)

Which of the following is a targeted attack aimed at compromising users within a specific industry or group?

- A. Watering hole
- B. Typosquatting
- C. Hoax
- D. Impersonation

**Answer: A**

**Explanation:**

A targeted attack refers to a type of threat in which threat actors actively pursue and compromise a target entity's infrastructure while maintaining anonymity. These attackers have a certain level of expertise and have sufficient resources to conduct their schemes over a long-term period. They can adapt, adjust, or improve their attacks to counter their victim's defenses. Background Targeted attacks often employ similar methods found in traditional online threats such as malicious emails, compromised or malicious sites, exploits, and malware. Targeted attacks differ from traditional online threats in many ways:

- Targeted attacks are typically conducted as campaigns. APTs are often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target's network—and are thus not isolated incidents.
- They usually target specific industries such as businesses, government agencies, or political groups. Attackers often have long-term goals in mind, with motives that include, but are not limited to, political gain, monetary profit, or business data theft. Attackers often customize, modify and improve their methods depending on the nature of their target sector and to circumvent any security measures implemented.

Phases of a Targeted Attack

• Intelligence gathering.

Threat actors identify and gather publicly available information about their target to

customize their attacks. This initial phase aims to gain strategic information not only on the intended target's IT environment but also on its organizational structure. The information gathered can range from the business applications and software an enterprise utilizes to the roles and relationships that exist within it.

This phase also utilizes social engineering techniques that leverage recent events, work-related issues or concerns, and other areas of interest for the intended target. Point of entry. Threat actors may use varied methods to infiltrate a target's infrastructure. Common methods include customized spearphishing email, zero-day or software exploits, and watering hole techniques. Attackers also utilize instant-messaging and social networking platforms to entice targets to click a link or download malware. Eventually, establishing a connection with the target is acquired.

- Command-and-control (C&C) communication.

After security has been breached, threat actors constantly communicate to the malware to either execute malicious routines or gather information within the company network. Threat actors use techniques to hide this communication and keep their movements under the radar.

- Lateral movement. Once inside the network, threat actors move laterally throughout the network to seek key information or infect other valuable systems.
- Asset/Data Discovery. Notable assets or data are determined and isolated for future data exfiltration. Threat actors have access to "territories" that contain valuable information and noteworthy assets. These data are then identified and transferred through tools like remote access Trojans (RATs) and customized and legitimate tools. A possible technique used in this stage may be sending back file lists in different directories so attackers can identify what are valuable.
- Data Exfiltration. This is the main goal of targeted attacks. An attack's objective is to gather key information and transfer this to a location that the attackers control. Transferring such data can be conducted quickly or gradually. Targeted attacks strive to remain undetected in the network in order to gain access to the company's crown jewels or valuable data. These valuable data include intellectual property, trade secrets, and customer information. In addition, threat actors may also seek other sensitive data such as top-secret documents from government or military institutions.

Once a targeted attack is successful and has reached as far as the data exfiltration stage, it is not difficult for attackers to draw out the data. Although targeted attacks are not known to specifically target consumers, their data are also at risk once target business sectors have been infiltrated. As a result, such attacks (if successful) may damage a company's reputation.

<https://www.trendmicro.com/vinfo/us/security/definition/targeted-attacks#:~:text=A%20targeted%20attack%20r>

**NEW QUESTION 189**

- (Exam Topic 2)

A security analyst has been tasked with finding the maximum amount of data loss that can occur before ongoing business operations would be impacted. Which of the following terms BEST defines this metric?

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

**Answer: A**

**NEW QUESTION 191**

- (Exam Topic 2)

A security analyst is reviewing application logs to determine the source of a breach and locates the following log:

```
https://www.comptia.com/login.php?id='%20or%20'1'1='1
```

Which Of the following has been observed?

- A. DLL Injection
- B. API attack
- C. SQLI
- D. XSS

**Answer: C**

**NEW QUESTION 194**

- (Exam Topic 2)

A security architect is required to deploy to conference rooms some workstations that will allow sensitive data to be displayed on large screens. Due to the nature of the data, it cannot be stored in the conference rooms. The fileshare is located in a local data center. Which of the following should the security architect recommend to BEST meet the requirement?

- A. Fog computing and KVMs
- B. VDI and thin clients
- C. Private cloud and DLP
- D. Full drive encryption and thick clients

**Answer:** B

**NEW QUESTION 195**

- (Exam Topic 2)

The Chief information Security Officer wants to prevent exfiltration of sensitive information from employee cell phones when using public USB power charging stations. Which of the following would be the Best solution to implement?

- A. DLP
- B. USB data blocker
- C. USB OTG
- D. Disabling USB ports

**Answer:** C

**NEW QUESTION 199**

- (Exam Topic 2)

An organization is planning to roll out a new mobile device policy and issue each employee a new laptop, These laptops would access the users' corporate operating system remotely and allow them to use the laptops for purposes outside of their job roles. Which of the following deployment models is being utilized?

- A. MDM and application management
- B. BYOO and containers
- C. COPE and VDI
- D. CYOD and VMs

**Answer:** C

**NEW QUESTION 203**

- (Exam Topic 2)

A company has a flat network in the cloud. The company needs to implement a solution to segment its production and non-production servers without migrating servers to a new network. Which of the following solutions should the company implement?

- A. internet
- B. Screened Subnet
- C. VLAN segmentation
- D. Zero Trust

**Answer:** C

**NEW QUESTION 207**

- (Exam Topic 2)

A user reports falling for a phishing email to an analyst. Which of the following system logs would the analyst check FIRST?

- A. DNS
- B. Message gateway
- C. Network
- D. Authentication

**Answer:** B

**NEW QUESTION 209**

- (Exam Topic 2)

An analyst is reviewing logs associated with an attack. The logs indicate an attacker downloaded a malicious file that was quarantined by the AV solution. The attacker utilized a local non-administrative account to restore the malicious file to a new location. The file was then used by another process to execute a payload. Which of the following attacks did the analyst observe?

- A. Privilege escalation
- B. Request forgeries
- C. Injection
- D. Replay attack

**Answer:** A

**Explanation:**

Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF

(sometimes pronounced sea-surf[1]) or XSRF, is a type of malicious exploit of a website where unauthenticated commands are submitted from a user that the web application trusts.[2] There are many ways in which a malicious website can transmit such commands; specially-crafted image tags, hidden forms, and JavaScript XMLHttpRequests, for example, can all work without the user's interaction or even knowledge

Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.[3] In a CSRF attack, an innocent end user is tricked by an attacker into submitting a web request that they did not intend. This may cause actions to be performed on the website that can include inadvertent client or server data leakage, change of session state, or manipulation of an end user's account.

**NEW QUESTION 211**

- (Exam Topic 2)

Which of the following is a risk that is specifically associated with hosting applications in the public cloud?

- A. Unsecured root accounts

- B. Zero—day
- C. Shared tenancy
- D. Insider threat

**Answer:** C

#### NEW QUESTION 213

- (Exam Topic 2)

During a recent security assessment, a vulnerability was found in a common OS, The OS vendor was unaware of the issue and promised to release a patch within next quarter, Which of the following BEST describes this type of vulnerability?

- A. Legacy operating system
- B. Weak configuration
- C. Zero day
- D. Supply chain

**Answer:** C

#### NEW QUESTION 218

- (Exam Topic 2)

An attacker has successfully exfiltrated several non-salted password hashes from an online system. Given the logs below:

```
Session           : hashcat
Status            : cracked
Hash.Type         : MD5
Hash.Target       : b3b81d1b7a412bf5aab3a507d0a586a0
Time.Started      : Fri Mar 10 10:18:45 2020
Recovered         : 1/1 (100%) Digests
Progress          : 28756845 / 450365879 (6.38%) hashes
Time.Stopped      : Fri Mar 10 10:20:12 2020
Password found    : Th3B3stP@55w0rd!
```

Which of the following BEST describes the type of password attack the attacker is performing?

- A. Dictionary
- B. Pass-the-hash
- C. Brute-force
- D. Password spraying

**Answer:** A

#### NEW QUESTION 220

- (Exam Topic 2)

While investigating a recent security incident, a security analyst decides to view all network connections on a particular server, Which of the following would provide the desired information?

- A. arp
- B. nslookup
- C. netstat
- D. nmap

**Answer:** C

#### NEW QUESTION 223

- (Exam Topic 2)

During a recent security incident at a multinational corporation a security analyst found the following logs for an account called user:

Account	Login location	Time (UTC)	Message
user	New York	9:00 a.m.	Login: user, successful
user	Los Angeles	9:01 a.m.	Login: user, successful
user	Sao Paolo	9:05 a.m.	Login: user, successful
user	Munich	9:12 a.m.	Login: user, successful

Which Of the following account policies would BEST prevent attackers from logging in as user?

- A. Impossible travel time
- B. Geofencing
- C. Time-based logins
- D. Geolocation

**Answer:** A



#### NEW QUESTION 226

- (Exam Topic 2)

Which of the following is a security best practice that ensures the integrity of aggregated log files within a SIEM?

- A. Set up hashing on the source log file servers that complies with local regulatory requirements,
- B. Back up the aggregated log files at least two times a day or as stated by local regulatory requirements.
- C. Write protect the aggregated log files and move them to an isolated server with limited access.
- D. Back up the source log files and archive them for at least six years or in accordance with local regulatory requirements.

**Answer:** A

#### NEW QUESTION 230

- (Exam Topic 2)

A major political party experienced a server breach. The hacker then publicly posted stolen internal communications concerning campaign strategies to give the opposition party an advantage. Which of the following BEST describes these threat actors?

- A. Semi-authorized hackers
- B. State actors
- C. Script kiddies
- D. Advanced persistent threats

**Answer:** B

#### NEW QUESTION 231

- (Exam Topic 2)

Which of the following uses SAML for authentication?

- A. TOTP
- B. Federation
- C. Kerberos
- D. HOTP

**Answer:** B

#### NEW QUESTION 236

- (Exam Topic 2)

A Chief Security Officer is looking for a solution that can reduce the occurrence of customers receiving errors from back-end infrastructure when systems go offline unexpectedly. The security architect would like the solution to help maintain session persistence. Which of the following would BEST meet the requirements?

- A. Reverse proxy
- B. NIC teaming
- C. Load balancer
- D. Forward proxy

**Answer:** B

#### NEW QUESTION 240

- (Exam Topic 2)

Which of the following supplies non-repudiation during a forensics investigation?

- A. Dumping volatile memory contents first
- B. Duplicating a drive with dd
- C. Using a SHA-2 signature of a drive image
- D. Logging everyone in contact with evidence
- E. Encrypting sensitive data

**Answer:** C

#### NEW QUESTION 241

- (Exam Topic 2)

A security analyst is reviewing web-application logs and finds the following log:



Which of the following attacks is being observed?

- A. Directory traversal
- B. XSS
- C. CSRF
- D. On-path attack

**Answer:** A

#### NEW QUESTION 242

- (Exam Topic 2)

Server administrator want to configure a cloud solution so that computing memory and processor usage is 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 administrator configure to maximize system availability while efficiently utilizing available computing power?

- A. Dynamic resource allocation
- B. High availability
- C. Segmentation
- D. Container security

**Answer:** C

#### NEW QUESTION 246

- (Exam Topic 2)

A cyber-security administrator is using an enterprise firewall. The administrator created some rules, but now Seems to be unresponsive. All connections being dropped by the firewall. Which of the following would be the BEST option to remove the rules?

- A. # iptables -t mangle -x
- B. # iptables -f
- C. # iptables -z
- D. # iptables -p input -j drop

**Answer:** A

#### NEW QUESTION 249

- (Exam Topic 2)

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

**Answer:** C

#### NEW QUESTION 251

- (Exam Topic 2)

Which of the following BEST describes when an organization utilizes a ready-to-use application from a cloud provider?

- A. IaaS
- B. SaaS
- C. PaaS
- D. XaaS

**Answer:** B

#### Explanation:

➤ SaaS, or software as a service, is on-demand access to ready-to-use, cloud-hosted application software. <https://www.ibm.com/cloud/learn/iaas-paas-saas>

#### NEW QUESTION 256

- (Exam Topic 2)

The Chief Information Security Officer (CISO) of a bank recently updated the incident response policy. The CISO is concerned that members of the incident response team do not understand their roles. The bank wants to test the policy but with the least amount of resources or impact. Which of the following BEST meets the requirements?

- A. Warm site failover
- B. Tabletop walk-through
- C. Parallel path testing
- D. Full outage simulation

**Answer:** B

#### NEW QUESTION 261

- (Exam Topic 2)

Which of the following is an effective tool to stop or prevent the exfiltration of data from a network?

- A. DLP
- B. NIDS
- C. TPM
- D. FDE

**Answer:** A

#### Explanation:

Data loss prevention (DLP) makes sure that users do not send sensitive or critical information outside the corporate network

#### NEW QUESTION 263

- (Exam Topic 2)

A company's security team received notice of a critical vulnerability affecting a high-profile device within the web infrastructure. The vendor patch was just made available online but has not yet been regression tested in development environments. In the interim, firewall rules were implemented to reduce the access to the interface affected by the vulnerability. Which of the following controls does this scenario describe?

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

**Answer:** B

#### NEW QUESTION 264

- (Exam Topic 2)

A company is required to continue using legacy software to support a critical service. Which of the following BEST explains a risk of this practice?

- A. Default system configuration
- B. Unsecure protocols
- C. Lack of vendor support
- D. Weak encryption

**Answer:** B

#### NEW QUESTION 269

- (Exam Topic 2)

Which of the following concepts BEST describes tracking and documenting changes to software and managing access to files and systems?

- A. Version control
- B. Continuous monitoring
- C. Stored procedures
- D. Automation

**Answer:** A

#### Explanation:

Version control, also known as source control, is the process of tracking and managing changes to files over time. VCS — version control systems — are software tools designed to help teams work in parallel.

<https://www.perforce.com/blog/vcs/what-is-version-control>

#### NEW QUESTION 274

- (Exam Topic 2)

Which of the following is the BEST action to foster a consistent and auditable incident response process?

- A. Incent new hires to constantly update the document with external knowledge.
- B. Publish the document in a central repository that is easily accessible to the organization.
- C. Restrict eligibility to comment on the process to subject matter experts of each IT silo.
- D. Rotate CIRT members to foster a shared responsibility model in the organization.

**Answer:** B

#### NEW QUESTION 275

- (Exam Topic 2)

Which of the following is a reason to publish files' hashes?

- A. To validate the integrity of the files
- B. To verify if the software was digitally signed
- C. To use the hash as a software activation key
- D. To use the hash as a decryption passphrase

**Answer:** A

#### NEW QUESTION 278

- (Exam Topic 2)

After a recent external audit, the compliance team provided a list of several non-compliant, in-scope hosts that were not encrypting cardholder data at rest, Which of the following compliance frameworks would address the compliance team's GREATEST concern?

- A. PCI DSS
- B. GDPR
- C. ISO 27001
- D. NIST CSF

**Answer:** A

#### NEW QUESTION 280

- (Exam Topic 2)

A Chief Information Security Officer wants to ensure the organization is validating and checking the Integrity of zone transfers. Which of the following solutions should be implemented?

- A. DNSSEC
- B. LOAPS
- C. NGFW
- D. DLP

**Answer:** D

#### NEW QUESTION 282

- (Exam Topic 2)

An organization just implemented a new security system. Local laws state that citizens must be notified prior to encountering the detection mechanism to deter malicious activities. Which of the following is being implemented?

- A. Proximity cards with guards
- B. Fence with electricity
- C. Drones with alarms
- D. Motion sensors with signage

**Answer:** D

#### NEW QUESTION 285

- (Exam Topic 2)

Two hospitals merged into a single organization. The privacy officer requested a review of all records to ensure encryption was used during record storage, in compliance with regulations. During the review, the officer discovered that medical diagnosis codes and patient names were left unsecured. Which of the following types of data does this combination BEST represent?

- A. Personal health information
- B. Personally Identifiable Information
- C. Tokenized data
- D. Proprietary data

**Answer:** A

#### NEW QUESTION 286

- (Exam Topic 2)

A company wants to build a new website to sell products online. The website will host a storefront application that will allow visitors to add products to a shopping cart and pay for the products using a credit card. Which of the following protocols would be the MOST secure to implement?

- A. SSL
- B. FTP
- C. SNMP
- D. TLS

**Answer:** D

#### NEW QUESTION 290

- (Exam Topic 2)

During a security incident investigation, an analyst consults the company's SIEM and sees an event concerning high traffic to a known, malicious command-and-control server. The analyst would like to determine the number of company workstations that may be impacted by this issue. Which of the following can provide the information?

- A. WAF logs
- B. DNS logs
- C. System logs
- D. Application logs

**Answer:** B

#### NEW QUESTION 295

- (Exam Topic 2)

The new Chief Information Security Officer at a company has asked the security team to implement stronger user account policies. The new policies require:

- Users to choose a password unique to their last ten passwords
- Users to not log in from certain high-risk countries

Which of the following should the security team implement? (Select TWO).

- A. Password complexity
- B. Password history
- C. Geolocation
- D. Geofencing
- E. Geotagging
- F. Password reuse

**Answer:** AB

#### NEW QUESTION 298

- (Exam Topic 2)

A security engineer is concerned about using an agent on devices that relies completely on defined known-bad signatures. The security engineer wants to implement a tool with multiple components including the ability to track, analyze, and monitor devices without reliance on definitions alone. Which of the following

solutions BEST fits this use case?

- A. EDR
- B. DLP
- C. NGFW
- D. HIPS

**Answer:** A

**Explanation:**

The acronym EDR stands for Endpoint Detection and Response and is also known as EDTR. It is an endpoint security solution that is responsible for continuous monitoring of endpoints. This permanent monitoring enables the technology to detect and respond to cyber threats such as malware or ransomware at an early stage. The basis for this is always the analysis of context-related information, which can be used to make corrective proposals for recovery.

**NEW QUESTION 299**

- (Exam Topic 2)

Which of the following is the FIRST environment in which proper, secure coding should be practiced?

- A. Stage
- B. Development
- C. Production
- D. Test

**Answer:** B

**Explanation:**

The developer has to start writing secure code from beginning itself. Which will then be tested, staged and finally production

**NEW QUESTION 304**

- (Exam Topic 2)

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

**Answer:** A

**NEW QUESTION 308**

- (Exam Topic 2)

An attacker replaces a digitally signed document with another version that goes unnoticed. Upon reviewing the document's contents, the author notices some additional verbaige that was not originally in the document but can't validate an integrity issue. Which of the following attacks was used?

- A. Cryptomalware
- B. Prepending
- C. Collision
- D. Phising

**Answer:** C

**NEW QUESTION 311**

- (Exam Topic 2)

A penetration tester is fuzzing an application to identify where the EIP of the stack is located on memory. Which of the following attacks is the penetration tester planning to execute?

- A. Race-condition
- B. Pass-the-hash
- C. Buffer overflow
- D. XSS

**Answer:** C

**NEW QUESTION 314**

- (Exam Topic 3)

A company is upgrading its wireless infrastructure to WPA2-Enterprise using EAP-TLS. Which of the following must be part of the security architecture to achieve AAA? (Select TWO)

- A. DNSSEC
- B. Reverse proxy
- C. VPN concentrator
- D. PKI
- E. Active Directory
- F. RADIUS

**Answer:** EF



#### NEW QUESTION 319

- (Exam Topic 3)

Which of the following incident response steps involves actions to protect critical systems while maintaining business operations?

- A. Investigation
- B. Containment
- C. Recovery
- D. Lessons learned

**Answer:** B

#### NEW QUESTION 320

- (Exam Topic 3)

A company has drafted an insider-threat policy that prohibits the use of external storage devices. Which of the following would BEST protect the company from data exfiltration via removable media?

- A. Monitoring large data transfer transactions in the firewall logs
- B. Developing mandatory training to educate employees about the removable media policy
- C. Implementing a group policy to block user access to system files
- D. Blocking removable-media devices and write capabilities using a host-based security tool

**Answer:** D

#### NEW QUESTION 321

- (Exam Topic 3)

A security analyst is using a recently released security advisory to review historical logs, looking for the specific activity that was outlined in the advisory. Which of the following is the analyst doing?

- A. A packet capture
- B. A user behavior analysis
- C. Threat hunting
- D. Credentialed vulnerability scanning

**Answer:** C

#### NEW QUESTION 325

- (Exam Topic 3)

A security administrator checks the table of a network switch, which shows the following output: Which of the following is happening to this switch?

- A. MAC Flooding
- B. DNS poisoning
- C. MAC cloning
- D. ARP poisoning

**Answer:** A

#### NEW QUESTION 328

- (Exam Topic 3)

A network administrator would like to configure a site-to-site VPN utilizing IPsec. The administrator wants the tunnel to be established with data integrity encryption, authentication and anti- replay functions Which of the following should the administrator use when configuring the VPN?

- A. AH
- B. EDR
- C. ESP
- D. DNSSEC

**Answer:** C

#### Explanation:

<https://www.hypr.com/encapsulating-security-payload-esp/>

Encapsulating Security Payload (ESP) is a member of the Internet Protocol Security (IPsec) set of protocols that encrypt and authenticate the packets of data between computers using a Virtual Private Network (VPN). The focus and layer on which ESP operates makes it possible for VPNs to function securely.

#### NEW QUESTION 331

- (Exam Topic 3)

A cybersecurity administrator has a reduced team and needs to operate an on-premises network and security infrastructure efficiently. To help with the situation, the administrator decides to hire a service provider. Which of the following should the administrator use?

- A. SDP
- B. AAA
- C. IaaS
- D. MSSP
- E. Microservices

**Answer:** D

#### Explanation:

<https://www.techtarget.com/searchitchannel/definition/MSSP>

#### NEW QUESTION 336

- (Exam Topic 3)

A security analyst receives a SIEM alert that someone logged in to the appadmin 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.

**Answer: C**

#### NEW QUESTION 338

- (Exam Topic 3)

A security monitoring company offers a service that alerts its customers if their credit cards have been stolen. Which of the following is the MOST likely source of this information?

- A. STIX
- B. The dark web
- C. TAXI
- D. Social media
- E. PCI

**Answer: B**

#### NEW QUESTION 340

- (Exam Topic 3)

Which of the following BEST describes a security exploit for which a vendor patch is not readily available?

- A. Integer overflow
- B. Zero-day
- C. End of life
- D. Race condition

**Answer: B**

#### NEW QUESTION 345

- (Exam Topic 3)

Which of the following is a team of people dedicated testing the effectiveness of organizational security programs by emulating the techniques of potential attackers?

- A. Red team
- B. White team
- C. Blue team
- D. Purple team

**Answer: A**

#### Explanation:

Red team—performs the offensive role to try to infiltrate the target.

#### NEW QUESTION 349

- (Exam Topic 3)

An organization is repairing the damage after an incident, Which of the following controls is being implemented?

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

**Answer: C**

#### NEW QUESTION 354

- (Exam Topic 3)

Which of the following disaster recovery tests is The LEAST time-consuming for the disaster recovery team?

- A. Tabletop
- B. Parallel

- C. Full interruption
- D. Simulation

**Answer:** D

#### NEW QUESTION 358

- (Exam Topic 3)

A system administrator needs to implement an access control scheme that will allow an object's access policy be determined by its owner. Which of the following access control schemes BEST fits the requirements?

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

**Answer:** B

#### Explanation:

Discretionary access control (DAC) is a model of access control based on access being determined "by the owner" of the resource in question. The owner of the resource can decide who does and does not have access, and exactly what access they are allowed to have.

#### NEW QUESTION 360

- (Exam Topic 3)

A company is designing the layout of a new datacenter so it will have an optimal environmental temperature Which of the following must be included? (Select TWO)

- A. An air gap
- B. A cold aisle
- C. Removable doors
- D. A hot aisle
- E. An IoT thermostat
- F. A humidity monitor

**Answer:** EF

#### NEW QUESTION 361

- (Exam Topic 3)

A Chief Security Office's (CSO's) key priorities are to improve preparation, response, and recovery practices to minimize system downtime and enhance organizational resilience to ransomware attacks. Which of the following would BEST meet the CSO's objectives?

- A. Use email-filtering software and centralized account management, patch high-risk systems, and restrict administration privileges on fileshares.
- B. Purchase cyber insurance from a reputable provider to reduce expenses during an incident.
- C. Invest in end-user awareness training to change the long-term culture and behavior of staff and executives, reducing the organization's susceptibility to phishing attacks.
- D. Implement application whitelisting and centralized event-log management, and perform regular testing and validation of full backups.

**Answer:** B

#### NEW QUESTION 362

- (Exam Topic 3)

Which of the following BEST explains the difference between a data owner and a data custodian?

- A. The data owner is responsible for adhering to the rules for using the data, while the data custodian is responsible for determining the corporate governance regarding the data
- B. The data owner is responsible for determining how the data may be used, while the data custodian is responsible for implementing the protection to the data
- C. The data owner is responsible for controlling the data, while the data custodian is responsible for maintaining the chain of custody when handling the data
- D. The data owner grants the technical permissions for data access, while the data custodian maintains the database access controls to the data

**Answer:** B

#### NEW QUESTION 365

- (Exam Topic 3)

A company provides mobile devices to its users to permit access to email and enterprise applications. The company recently started allowing users to select from several different vendors and device models. When configuring the MDM, which of the following is a key security implication of this heterogeneous device approach?

- A. The most common set of MDM configurations will become the effective set of enterprise mobile security controls.
- B. All devices will need to support SCEP-based enrollment; therefore, the heterogeneity of the chosen architecture may unnecessarily expose private keys to adversaries.
- C. Certain devices are inherently less secure than others, so compensatory controls will be needed to address the delta between device vendors.
- D. MDMs typically will not support heterogeneous deployment environments, so multiple MDMs will need to be installed and configured.

**Answer:** C

#### NEW QUESTION 366

- (Exam Topic 3)

A startup company is using multiple SaaS and IaaS platforms to stand up a corporate infrastructure and build out a customer-facing web application. Which of the

following solutions would be BEST to provide security, manageability, and visibility into the platforms?

- A. SIEM
- B. DLP
- C. CASB
- D. SWG

**Answer:** C

#### NEW QUESTION 369

- (Exam Topic 3)

An organization has been experiencing outages during holiday sales and needs to ensure availability of its point-of-sale systems. The IT administrator has been asked to improve both server-data fault tolerance and site availability under high consumer load. Which of the following are the BEST options to accomplish this objective? (Select TWO)

- A. Load balancing
- B. Incremental backups
- C. UPS
- D. RAID
- E. Dual power supply
- F. NIC teaming

**Answer:** AD

#### NEW QUESTION 373

- (Exam Topic 3)

A user received an SMS on a mobile phone that asked for bank details. Which of the following social-engineering techniques was used in this case?

- A. SPIM
- B. Vishing
- C. Spear phishing
- D. Smishing

**Answer:** D

#### NEW QUESTION 375

- (Exam Topic 3)

Which of the following is the BEST method for ensuring non-repudiation?

- A. SSO
- B. Digital certificate
- C. Token
- D. SSH key

**Answer:** B

#### NEW QUESTION 379

- (Exam Topic 3)

A security analyst discovers that a company username and password database was posted on an internet forum. The username and passwords are stored in plain text. Which of the following would mitigate the damage done by this type of data exfiltration in the future?

- A. Create DLP controls that prevent documents from leaving the network
- B. Implement salting and hashing
- C. Configure the web content filter to block access to the forum.
- D. Increase password complexity requirements

**Answer:** A

#### NEW QUESTION 380

- (Exam Topic 3)

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

**Answer:** A

#### NEW QUESTION 382

- (Exam Topic 3)

An information security incident recently occurred at an organization, and the organization was required to report the incident to authorities and notify the affected parties. When the organization's customers became aware of the incident, some reduced their orders or stopped placing orders entirely. Which of the following is the organization experiencing?

- A. Reputation damage

- B. Identity theft
- C. Anonymization
- D. Interrupted supply chain

**Answer:** A

#### NEW QUESTION 387

- (Exam Topic 3)

A recently discovered zero-day exploit utilizes an unknown vulnerability in the SMB network protocol to rapidly infect computers. Once infected, computers are encrypted and held for ransom. Which of the following would BEST prevent this attack from reoccurring?

- A. Configure the perimeter firewall to deny inbound external connections to SMB ports.
- B. Ensure endpoint detection and response systems are alerting on suspicious SMB connections.
- C. Deny unauthenticated users access to shared network folders.
- D. Verify computers are set to install monthly operating system, updates automatically.

**Answer:** A

#### NEW QUESTION 388

- (Exam Topic 3)

A company recently transitioned to a strictly BYOD culture due to the cost of replacing lost or damaged corporate-owned mobile devices. Which of the following technologies would be BEST to balance the BYOD culture while also protecting the company's data?

- A. Containerization
- B. Geofencing
- C. Full-disk encryption
- D. Remote wipe

**Answer:** C

#### NEW QUESTION 392

- (Exam Topic 3)

A company's bank has reported that multiple corporate credit cards have been stolen over the past several weeks. The bank has provided the names of the affected cardholders to the company's forensics team to assist in the cyber-incident investigation.

An incident responder learns the following information:

The timeline of stolen card numbers corresponds closely with affected users making Internet-based purchases from diverse websites via enterprise desktop PCs.

All purchase connections were encrypted, and the company uses an SSL inspection proxy for the inspection of encrypted traffic of the hardwired network.

Purchases made with corporate cards over the corporate guest WiFi network, where no SSL inspection occurs, were unaffected.

Which of the following is the MOST likely root cause?

- A. HTTPS sessions are being downgraded to insecure cipher suites
- B. The SSL inspection proxy is feeding events to a compromised SIEM
- C. The payment providers are insecurely processing credit card charges
- D. The adversary has not yet established a presence on the guest WiFi network

**Answer:** C

#### NEW QUESTION 395

- (Exam Topic 3)

Which of the following is a detective and deterrent control against physical intrusions?

- A. A lock
- B. An alarm
- C. A fence
- D. A sign

**Answer:** B

#### NEW QUESTION 398

- (Exam Topic 3)

A company is launching a new internet platform for its clients. The company does not want to implement its own authorization solution but instead wants to rely on the authorization provided by another platform. Which of the following is the BEST approach to implement the desired solution?

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

**Answer:** D

#### NEW QUESTION 400

- (Exam Topic 3)

A network manager is concerned that business may be negatively impacted if the firewall in its datacenter goes offline. The manager would like to implement a high availability pair to:

- A. ensure that business may be negatively impacted if the firewall in its datacenter goes offline.
- B. remove the single point of failure.



- C. cut down the mean time to repair,
- D. reduce the recovery time objective.

**Answer:** B

#### NEW QUESTION 404

- (Exam Topic 3)

Which of the following types of controls is a CCTV camera that is not being monitored?

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

**Answer:** B

#### NEW QUESTION 409

- (Exam Topic 3)

A development team employs a practice of bringing all the code changes from multiple team members into the same development project through automation. A tool is utilized to validate the code and track source code through version control. Which of the following BEST describes this process?

- A. Continuous delivery
- B. Continuous integration
- C. Continuous validation
- D. Continuous monitoring

**Answer:** B

#### NEW QUESTION 410

- (Exam Topic 3)

A remote user recently took a two-week vacation abroad and brought along a corporate-owned laptop. Upon returning to work, the user has been unable to connect the laptop to the VPN. Which of the following is the MOST likely reason for the user's inability to connect the laptop to the VPN?

- A. Due to foreign travel, the user's laptop was isolated from the network.
- B. The user's laptop was quarantined because it missed the latest path update.
- C. The VPN client was blacklisted.
- D. The user's account was put on a legal hold

**Answer:** A

#### NEW QUESTION 413

- (Exam Topic 3)

Which of the following BEST explains the reason why a server administrator would place a document named password.txt on the desktop of an administrator account on a server?

- A. The document is a honeyfile and is meant to attract the attention of a cyberintruder.
- B. The document is a backup file if the system needs to be recovered.
- C. The document is a standard file that the OS needs to verify the login credentials.
- D. The document is a keylogger that stores all keystrokes should the account be compromised.

**Answer:** A

#### NEW QUESTION 416

- (Exam Topic 3)

A company needs to centralize its logs to create a baseline and have visibility on its security events. Which of the following technologies will accomplish this objective?

- A. Security information and event management
- B. A web application firewall
- C. A vulnerability scanner
- D. A next-generation firewall

**Answer:** A

#### NEW QUESTION 420

- (Exam Topic 3)

Which of the following are the MOST likely vectors for the unauthorized inclusion of vulnerable code in a software company's final software releases? (Select TWO.)

- A. Unsecure protocols
- B. Use of penetration-testing utilities
- C. Weak passwords
- D. Included third-party libraries
- E. Vendors/supply chain
- F. Outdated anti-malware software

**Answer:** AD

#### NEW QUESTION 425

- (Exam Topic 3)

On which of the following is the live acquisition of data for forensic analysis MOST dependent? (Choose two.)

- A. Data accessibility
- B. Legal hold
- C. Cryptographic or hash algorithm
- D. Data retention legislation
- E. Value and volatility of data
- F. Right-to-audit clauses

**Answer:** EF

#### NEW QUESTION 427

- (Exam Topic 3)

After a ransomware attack a forensics company needs to review a cryptocurrency transaction between the victim and the attacker. Which of the following will the company MOST likely review to trace this transaction?

- A. The public ledger
- B. The NetFlow data
- C. A checksum
- D. The event log

**Answer:** A

#### Explanation:

<https://www.investopedia.com/tech/what-cryptocurrency-public-ledger/>

#### NEW QUESTION 432

- (Exam Topic 3)

An organization is developing a plan in the event of a complete loss of critical systems and data. Which of the following plans is the organization MOST likely developing?

- A. Incident response
- B. Communications
- C. Disaster recovery
- D. Data retention

**Answer:** C

#### NEW QUESTION 434

- (Exam Topic 3)

A company wants to deploy decoy systems alongside production systems in order to entice threat actors and to learn more about attackers. Which of the following BEST describes these systems?

- A. DNS sinkholes
- B. Hafieypots
- C. Virtual machines
- D. Neural networks

**Answer:** B

#### NEW QUESTION 435

- (Exam Topic 3)

A security assessment determines DES and 3DES are still being used on recently deployed production servers. Which of the following did the assessment identify?

- A. Unsecme protocols
- B. Default settings
- C. Open permissions
- D. Weak encryption

**Answer:** D

#### NEW QUESTION 440

- (Exam Topic 3)

To secure an application after a large data breach, an e-commerce site will be resetting all users' credentials. Which of the following will BEST ensure the site's users are not compromised after the reset?

- A. A password reuse policy
- B. Account lockout after three failed attempts
- C. Encrypted credentials in transit
- D. A geofencing policy based on login history

**Answer:** C

#### NEW QUESTION 445

- (Exam Topic 3)

A security administrator currently spends a large amount of time on common security tasks, such as report generation, phishing investigations, and user provisioning and deprovisioning. This prevents the administrator from spending time on other security projects. The business does not have the budget to add more staff members. Which of the following should the administrator implement?

- A. DAC
- B. ABAC
- C. SCAP
- D. SOAR

**Answer:** D

#### NEW QUESTION 448

- (Exam Topic 3)

An organization Chief Information Security Officer a position that will be responsible for implementing technical controls to protect data, include ensuring backups are properly maintained. Which of the following roles would MOST likely include these responsibilities?

- A. Data protection officer
- B. Data owner
- C. Backup administrator
- D. Data custodian
- E. Internal auditor

**Answer:** A

#### NEW QUESTION 451

- (Exam Topic 3)

A security engineer has enabled two-factor authentication on all workstations. Which of the following approaches are the MOST secure? (Select TWO).

- A. Password and security question
- B. Password and CAPTCHA
- C. Password and smart card
- D. Password and fingerprint
- E. Password and one-time token
- F. Password and voice

**Answer:** CD

#### NEW QUESTION 455

- (Exam Topic 3)

Which of the following is the purpose of a risk register?

- A. To define the level of risk using probability and likelihood
- B. To register the risk with the required regulatory agencies
- C. To identify the risk, the risk owner, and the risk measures
- D. To formally log the type of risk mitigation strategy the organization is using

**Answer:** C

#### NEW QUESTION 458

- (Exam Topic 3)

A website developer is working on a new e-commerce website and has asked an information security expert for the most appropriate way to store credit card numbers to create an easy reordering process. Which of the following methods would BEST accomplish this goal?

- A. Salting the magnetic strip information
- B. Encrypting the credit card information in transit.
- C. Hashing the credit card numbers upon entry.
- D. Tokenizing the credit cards in the database

**Answer:** C

#### NEW QUESTION 461

- (Exam Topic 3)

An enterprise has hired an outside security firm to conduct a penetration test on its network and applications. The enterprise provided the firm with access to a guest account. Which of the following BEST represents the type of testing that is being used?

- A. Black-box
- B. Red-team
- C. Gray-box
- D. Bug bounty
- E. White-box

**Answer:** C

#### NEW QUESTION 464

- (Exam Topic 3)

Developers are writing code and merging it into shared repositories several times a day, where it is tested automatically. Which of the following concepts does

this BEST represent?

- A. Functional testing
- B. Stored procedures
- C. Elasticity
- D. Continuous integration

**Answer:** C

#### NEW QUESTION 468

- (Exam Topic 3)

After reading a security bulletin, a network security manager is concerned that a malicious actor may have breached the network using the same software flaw. The exploit code is publicly available and has been reported as being used against other industries in the same vertical. Which of the following should the network security manager consult FIRST to determine a priority list for forensic review?

- A. The vulnerability scan output
- B. The IDS logs
- C. The full packet capture data
- D. The SIEM alerts

**Answer:** A

#### NEW QUESTION 473

- (Exam Topic 3)

A security engineer needs to implement an MDM solution that complies with the corporate mobile device policy. The policy states that in order for mobile users to access corporate resources on their devices the following requirements must be met:

- Mobile device OSs must be patched up to the latest release
- A screen lock must be enabled (passcode or biometric)
- Corporate data must be removed if the device is reported lost or stolen

Which of the following controls should the security engineer configure? (Select TWO)

- A. Containerization
- B. Storage segmentation
- C. Posturing
- D. Remote wipe
- E. Full-device encryption
- F. Geofencing

**Answer:** DE

#### NEW QUESTION 474

- (Exam Topic 3)

To reduce costs and overhead, an organization wants to move from an on-premises email solution to a cloud-based email solution. At this time, no other services will be moving. Which of the following cloud models would BEST meet the needs of the organization?

- A. MaaS
- B. IaaS
- C. SaaS
- D. PaaS

**Answer:** D

#### NEW QUESTION 476

- (Exam Topic 3)

An organization has a growing workforce that is mostly driven by additions to the sales department. Each newly hired salesperson relies on a mobile device to conduct business. The Chief Information Officer (CIO) is wondering if the organization may need to scale down just as quickly as it scaled up. The CIO is also concerned about the organization's security and customer privacy. Which of the following would be BEST to address the CIO's concerns?

- A. Disallow new hires from using mobile devices for six months
- B. Select four devices for the sales department to use in a CYOD model
- C. Implement BYOD for the sales department while leveraging the MDM
- D. Deploy mobile devices using the COPE methodology

**Answer:** C

#### NEW QUESTION 478

- (Exam Topic 3)

A security analyst needs to be proactive in understanding the types of attacks that could potentially target the company's executive. Which of the following intelligence sources should the security analyst review?

- A. Vulnerability feeds
- B. Trusted automated exchange of indicator information
- C. Structured threat information expression
- D. Industry information-sharing and collaboration groups

**Answer:** D

#### NEW QUESTION 483

- (Exam Topic 3)

A company is adopting a BYOD policy and is looking for a comprehensive solution to protect company. information on user devices. Which of the following solutions would BEST support the policy?

- A. Mobile device management
- B. Full-device encryption
- C. Remote wipe
- D. Biometrics

**Answer:** A

#### NEW QUESTION 484

- (Exam Topic 3)

Which of the following would be the BEST method for creating a detailed diagram of wireless access points and hot-spots?

- A. Footprinting
- B. White-box testing
- C. A drone/UAV
- D. Pivoting

**Answer:** A

#### NEW QUESTION 488

- (Exam Topic 3)

Which of the following should an organization consider implementing in the event executives need to speak to the media after a publicized data breach?

- A. incident response plan
- B. Business continuity plan
- C. Communication plan
- D. Disaster recovery plan

**Answer:** C

#### NEW QUESTION 492

- (Exam Topic 3)

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

**Answer:** D

#### NEW QUESTION 494

- (Exam Topic 3)

An organization that is located in a flood zone is MOST likely to document the concerns associated with the restoration of IT operation in a:

- A. business continuity plan
- B. communications plan.
- C. disaster recovery plan.
- D. continuity of operations plan

**Answer:** C

#### NEW QUESTION 497

- (Exam Topic 3)

An organization is tuning SIEM rules based off of threat intelligence reports. Which of the following phases of the incident response process does this scenario represent?

- A. Lessons learned
- B. Eradication
- C. Recovery
- D. Preparation

**Answer:** A

#### NEW QUESTION 498

- (Exam Topic 3)

A network administrator has been asked to design a solution to improve a company's security posture The administrator is given the following, requirements?

- The solution must be inline in the network
- The solution must be able to block known malicious traffic
- The solution must be able to stop network-based attacks

Which of the following should the network administrator implement to BEST meet these requirements?



- A. HIDS
- B. NIDS
- C. HIPS
- D. NIPS

**Answer:** D

#### NEW QUESTION 503

- (Exam Topic 3)

A cybersecurity administrator is using iptables as an enterprise firewall. The administrator created some rules, but the network now seems to be unresponsive All connections are being dropped by the firewall. Which of the following would be the BEST option to remove the rules?

- A. # iptables -t mangle -X
- B. # iptables -F
- C. # iptables -Z
- D. # iptables -P INPUT -j DROP

**Answer:** D

#### NEW QUESTION 505

- (Exam Topic 3)

A network technician is installing a guest wireless network at a coffee shop. When a customer purchases an Item, the password for the wireless network is printed on the receipt so the customer can log in. Which of the following will the technician MOST likely configure to provide the highest level of security with the least amount of overhead?

- A. WPA-EAP
- B. WEP-TKIP
- C. WPA-PSK
- D. WPS-PIN

**Answer:** A

#### NEW QUESTION 507

- (Exam Topic 3)

Which of the following provides the BEST protection for sensitive information and data stored in cloud-based services but still allows for full functionality and searchability of data within the cloud-based services?

- A. Data encryption
- B. Data masking
- C. Anonymization
- D. Tokenization

**Answer:** A

#### NEW QUESTION 509

- (Exam Topic 3)

Which of the following allows for functional test data to be used in new systems for testing and training purposes to protect the real data?

- A. Data encryption
- B. Data masking
- C. Data deduplication
- D. Data minimization

**Answer:** B

#### NEW QUESTION 510

- (Exam Topic 3)

A company has determined that if its computer-based manufacturing is not functioning for 12 consecutive hours, it will lose more money than it costs to maintain the equipment. Which of the following must be less than 12 hours to maintain a positive total cost of ownership?

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

**Answer:** C

#### NEW QUESTION 511

- (Exam Topic 3)

Which of the following would MOST likely support the integrity of a voting machine?

- A. Asymmetric encryption
- B. Blockchain
- C. Transport Layer Security
- D. Perfect forward secrecy

**Answer:** D

#### NEW QUESTION 514

- (Exam Topic 3)

An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the MOST acceptable?

- A. SED
- B. HSM
- C. DLP
- D. TPM

**Answer:** A

#### NEW QUESTION 518

- (Exam Topic 3)

A systems administrator is looking for a solution that will help prevent OAuth applications from being leveraged by hackers to trick users into authorizing the use of their corporate credentials. Which of the following BEST describes this solution?

- A. CASB
- B. UEM
- C. WAF
- D. VPC

**Answer:** B

#### NEW QUESTION 523

- (Exam Topic 3)

A network engineer needs to create a plan for upgrading the wireless infrastructure in a large office. Priority must be given to areas that are currently experiencing latency and connection issues. Which of the following would be the BEST resource for determining the order of priority?

- A. Nmapn
- B. Heat maps
- C. Network diagrams
- D. Wireshark

**Answer:** C

#### NEW QUESTION 525

- (Exam Topic 3)

The Chief information Security Officer (CISO) has decided to reorganize security staff to concentrate on incident response and to outsource outbound Internet URL categorization and filtering to an outside company. Additionally, the CISO would like this solution to provide the same protections even when a company laptop or mobile device is away from the home office. Which of the following should the CISO choose?

- A. CASB
- B. Next-generation SWG
- C. NGFW
- D. Web-application firewall

**Answer:** A

#### NEW QUESTION 527

- (Exam Topic 3)

Under GDPR, which of the following is MOST responsible for the protection of privacy and website user rights?

- A. The data protection officer
- B. The data processor
- C. The data owner
- D. The data controller

**Answer:** C

#### NEW QUESTION 532

- (Exam Topic 3)

A company processes highly sensitive data and senior management wants to protect the sensitive data by utilizing classification labels. Which of the following access control schemes would be BEST for the company to implement?

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

**Answer:** D

#### NEW QUESTION 535

- (Exam Topic 3)

Two hospitals merged into a single organization. The privacy officer requested a review of audit records to ensure encryption was used during record storage, in compliance with regulations. During the review, the officer discovered that medical diagnosis codes and patient names were left unsecured. Which of the

following types of data does this combination BEST represent?

- A. Personal health information
- B. Personally Identifiable information
- C. Tokenized data
- D. Proprietary data

**Answer:** B

#### NEW QUESTION 536

- (Exam Topic 3)

When selecting a technical solution for identity management, an architect chooses to go from an in-house to a third-party SaaS provider. Which of the following risk management strategies is this an example of?

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

**Answer:** D

#### Explanation:

Risk Transference refers to the shifting of the burden of loss for a risk to another party through legislation, contract, insurance or other means.

[https://www.bcmptedia.org/wiki/Risk\\_Transference](https://www.bcmptedia.org/wiki/Risk_Transference)

#### NEW QUESTION 538

- (Exam Topic 3)

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 whitelisting
- C. Containment
- D. isolation

**Answer:** A

#### NEW QUESTION 542

- (Exam Topic 3)

Law enforcement officials sent a company a notification that states electronically stored information and paper documents cannot be destroyed. Which of the following explains this process?

- A. Data breach notification
- B. Accountability
- C. Legal hold
- D. Chain of custody

**Answer:** C

#### NEW QUESTION 546

- (Exam Topic 3)

A user enters a password to log in to a workstation and is then prompted to enter an authentication code. Which of the following MFA factors or attributes are being utilized in the authentication process? (Select TWO).

- A. Something you know
- B. Something you have
- C. Somewhere you are
- D. Someone you are
- E. Something you are
- F. Something you can do

**Answer:** BE

#### NEW QUESTION 549

- (Exam Topic 3)

A small company that does not have security staff wants to improve its security posture. Which of the following would BEST assist the company?

- A. MSSP
- B. SOAR
- C. IaaS
- D. PaaS

**Answer:** B

#### NEW QUESTION 550

- (Exam Topic 3)

A security analyst is hardening a Linux workstation and must ensure it has public keys forwarded to remote systems for secure login. Which of the following steps should the analyst perform to meet these requirements? (Select TWO).

- A. Forward the keys using ssh-copy-id.
- B. Forward the keys using scp.
- C. Forward the keys using ash -i.
- D. Forward the keys using openssl -s.
- E. Forward the keys using ssh-keygen.

**Answer:** AD

#### NEW QUESTION 554

- (Exam Topic 3)

Which of the following corporate policies is used to help prevent employee fraud and to detect system log modifications or other malicious activity based on tenure?

- A. Background checks
- B. Mandatory vacation
- C. Social media analysis
- D. Separation of duties

**Answer:** B

#### NEW QUESTION 556

- (Exam Topic 3)

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

**Answer:** C

#### NEW QUESTION 560

- (Exam Topic 3)

A security auditor is reviewing vulnerability scan data provided by an internal security team. Which of the following BEST indicates that valid credentials were used?

- A. The scan results show open ports, protocols, and services exposed on the target host
- B. The scan enumerated software versions of installed programs
- C. The scan produced a list of vulnerabilities on the target host
- D. The scan identified expired SSL certificates

**Answer:** B

#### NEW QUESTION 565

- (Exam Topic 3)

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

- A. Fog computing
- B. VM escape
- C. Software-defined networking
- D. Image forgery
- E. Container breakout

**Answer:** B

#### Explanation:

Virtual machine escape is an exploit in which the attacker runs code on a VM that allows an operating system running within it to break out and interact directly with the hypervisor. [https://whatis.techtarget.com/definition/virtual-machine-escape#:~:text=Virtual%20machine%20escape%20is%](https://whatis.techtarget.com/definition/virtual-machine-escape#:~:text=Virtual%20machine%20escape%20is%20)

#### NEW QUESTION 566

- (Exam Topic 3)

Which of the following would be used to find the MOST common web-application vulnerabilities?

- A. OWASP
- B. MITRE ATT&CK
- C. Cyber Kill Chain
- D. SDLC

**Answer:** A

#### NEW QUESTION 571

- (Exam Topic 3)

A nuclear plant was the victim of a recent attack, and all the networks were air gapped. A subsequent investigation revealed a worm as the source of the issue. Which of the following BEST explains what happened?

- A. A malicious USB was introduced by an unsuspecting employee.
- B. The ICS firmware was outdated
- C. A local machine has a RAT installed.
- D. The HVAC was connected to the maintenance vendor.

**Answer:** A

#### NEW QUESTION 574

- (Exam Topic 3)

An attacker is attempting to exploit users by creating a fake website with the URL [www.validwebsite.com](http://www.validwebsite.com). The attacker's intent is to imitate the look and feel of a legitimate website to obtain personal information from unsuspecting users. Which of the following social-engineering attacks does this describe?

- A. Information elicitation
- B. Type squatting
- C. Impersonation
- D. Watering-hole attack

**Answer:** D

#### NEW QUESTION 577

- (Exam Topic 3)

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

- A. Locks
- B. Badges
- C. Cameras
- D. Visitor logs

**Answer:** D

#### NEW QUESTION 578

- (Exam Topic 3)

In which of the following common use cases would steganography be employed?

- A. Obfuscation
- B. Integrity
- C. Non-repudiation
- D. Blockchain

**Answer:** A

#### NEW QUESTION 579

- (Exam Topic 3)

A cybersecurity analyst reviews the log files from a web server and sees a series of files that indicates 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`

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer:** B

#### NEW QUESTION 580

- (Exam Topic 3)

A user contacts the help desk to report the following:

Two days ago, a pop-up browser window prompted the user for a name and password after connecting to the corporate wireless SSID. This had never happened before, but the user entered the information as requested.

The user was able to access the Internet but had trouble accessing the department share until the next day. The user is now getting notifications from the bank about unauthorized transactions.

Which of the following attack vectors was MOST likely used in this scenario?

- A. Rogue access point
- B. Evil twin
- C. DNS poisoning
- D. ARP poisoning



**Answer:** A

#### NEW QUESTION 582

- (Exam Topic 3)

A network administrator needs to build out a new datacenter, with a focus on resiliency and uptime. Which of the following would BEST meet this objective? (Choose two.)

- A. Dual power supply
- B. Off-site backups
- C. Automatic OS upgrades
- D. NIC teaming
- E. Scheduled penetration testing
- F. Network-attached storage

**Answer:** AB

#### Explanation:

<https://searchdatacenter.techtarget.com/definition/resiliency>

#### NEW QUESTION 583

- (Exam Topic 3)

A smart switch has the ability to monitor electrical levels and shut off power to a building in the event of power surge or other fault situation. The switch was installed on a wired network in a hospital and is monitored by the facilities department via a cloud application. The security administrator isolated the switch on a separate VLAN and set up a patch routine. Which of the following steps should also be taken to harden the smart switch?

- A. Set up an air gap for the switch.
- B. Change the default password for the switch.
- C. Place the switch in a Faraday cage.
- D. Install a cable lock on the switch

**Answer:** B

#### NEW QUESTION 585

- (Exam Topic 3)

A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator MOST likely use to confirm the suspicions?

- A. Nmap
- B. Wireshark
- C. Autopsy
- D. DNSEnum

**Answer:** A

#### NEW QUESTION 587

- (Exam Topic 3)

A Chief Security Officer (CSO) has asked a technician to devise a solution that can detect unauthorized execution privileges from the OS in both executable and data files and can work in conjunction with proxies or UTM. Which of the following would BEST meet the CSO's requirements?

- A. Fuzzing
- B. Sandboxing
- C. Static code analysis
- D. Code review

**Answer:** B

#### NEW QUESTION 590

- (Exam Topic 3)

During an investigation, a security manager receives notification from local authorities that company proprietary data was found on a former employee's home computer. The former employee's

corporate workstation has since been repurposed, and the data on the hard drive has been overwritten. Which of the following would BEST provide the security manager with enough details to determine when the data was removed from the company network?

- A. Properly configured hosts with security logging
- B. Properly configured endpoint security tool with alerting
- C. Properly configured SIEM with retention policies
- D. Properly configured USB blocker with encryption

**Answer:** C

#### NEW QUESTION 592

- (Exam Topic 3)

An attacker is exploiting a vulnerability that does not have a patch available. Which of the following is the attacker exploiting?

- A. Zero-day
- B. Default permissions

- C. Weak encryption
- D. Unsecure root accounts

**Answer:** A

#### NEW QUESTION 595

- (Exam Topic 3)

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 QA before releasing it.

**Answer:** D

#### NEW QUESTION 600

- (Exam Topic 3)

Which of the following ISO standards is certified for privacy?

- A. ISO 9001
- B. ISO 27002
- C. ISO 27701
- D. ISO 31000

**Answer:** C

#### Explanation:

ISO 27701 also abbreviated as PIMS (Privacy Information Management System) outlines a framework for Personally Identifiable Information (PII) Controllers and PII Processors to manage data privacy. Privacy information management systems are sometimes referred to as personal information management systems.  
<https://pecb.com/whitepaper/the-future-of-privacy-with-isoiec-27701>

#### NEW QUESTION 602

- (Exam Topic 3)

Which of the following will MOST likely adversely impact the operations of unpatched traditional programmable-logic controllers, running a back-end LAMP server and OT systems with human-management interfaces that are accessible over the Internet via a web interface? (Choose two.)

- A. Cross-site scripting
- B. Data exfiltration
- C. Poor system logging
- D. Weak encryption
- E. SQL injection
- F. Server-side request forgery

**Answer:** DE

#### NEW QUESTION 605

- (Exam Topic 3)

During a routine scan of a wireless segment at a retail company, a security administrator discovers several devices are connected to the network that do not match the company's naming convention and are not in the asset inventory. WiFi access is protected with 255-Wt encryption via WPA2. Physical access to the company's facility requires two-factor authentication using a badge and a passcode. Which of the following should the administrator implement to find and remediate the issue? (Select TWO).

- A. Check the SIEM for failed logins to the LDAP directory.
- B. Enable MAC filtering on the switches that support the wireless network.
- C. Run a vulnerability scan on all the devices in the wireless network.
- D. Deploy multifactor authentication for access to the wireless network.
- E. Scan the wireless network for rogue access points.
- F. Deploy a honeypot on the network.

**Answer:** BE

#### NEW QUESTION 608

- (Exam Topic 3)

An organization has decided to host its web application and database in the cloud. Which of the following BEST describes the security concerns for this decision?

- A. Access to the organization's servers could be exposed to other cloud-provider clients.
- B. The cloud vendor is a new attack vector within the supply chain.
- C. Outsourcing the code development adds risk to the cloud provider.
- D. Vendor support will cease when the hosting platforms reach EOL.

**Answer:** B

#### NEW QUESTION 611

- (Exam Topic 3)

A developer is concerned about people downloading fake malware-infected replicas of a popular game. Which of the following should the developer do to

help verify legitimate versions of the game for users?

- A. Digitally sign the relevant game files.
- B. Embed a watermark using steganography.
- C. Implement TLS on the license activation server.
- D. Fuzz the application for unknown vulnerabilities.

**Answer:** A

#### NEW QUESTION 613

- (Exam Topic 3)

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

- A. Geolocation
- B. Time-of-day restrictions
- C. Certificates
- D. Tokens
- E. Geotagging
- F. Role-based access controls

**Answer:** AE

#### NEW QUESTION 616

- (Exam Topic 3)

Which of the following algorithms has the SMALLEST key size?

- A. DES
- B. Twofish
- C. RSA
- D. AES

**Answer:** B

#### NEW QUESTION 619

- (Exam Topic 3)

A company is setting up a web server on the Internet that will utilize both encrypted and unencrypted web-browsing protocols. A security engineer runs a port scan against the server from the Internet and sees the following output:

Port	Protocol	State	Service
22	tcp	open	ssh
25	tcp	filtered	smtp
53	tcp	filtered	domain
80	tcp	open	http
443	tcp	open	https

Which of the following steps would be best for the security engineer to take NEXT?

- A. Allow DNS access from the internet.
- B. Block SMTP access from the Internet
- C. Block HTTPS access from the Internet
- D. Block SSH access from the Internet.

**Answer:** D

#### NEW QUESTION 620

- (Exam Topic 3)

A university with remote campuses, which all use different service providers, loses Internet connectivity across all locations. After a few minutes, Internet and VoIP services are restored, only to go offline again at random intervals, typically within four minutes of services being restored. Outages continue throughout the day, impacting all inbound and outbound connections and services. Services that are limited to the local LAN or WiFi network are not impacted, but all WAN and VoIP services are affected.

Later that day, the edge-router manufacturer releases a CVE outlining the ability of an attacker to exploit the SIP protocol handling on devices, leading to resource exhaustion and system reloads. Which of the following BEST describe this type of attack? (Choose two.)

- A. DoS
- B. SSL stripping
- C. Memory leak
- D. Race condition
- E. Shimming
- F. Refactoring

**Answer:** AD

#### NEW QUESTION 624

- (Exam Topic 3)

A SOC is currently being outsourced. Which of the following is being used?

- A. Microservice
- B. SaaS
- C. MSSP
- D. PaaS

**Answer:** C

#### NEW QUESTION 628

- (Exam Topic 3)

While checking logs, a security engineer notices a number of end users suddenly downloading files with the .tar.gz extension. Closer examination of the files reveals they are PE32 files. The end users state they did not initiate any of the downloads. Further investigation reveals the end users all clicked on an external email containing an infected MHT file with an href link a week prior. Which of the following is MOST likely occurring?

- A. A RAT was installed and is transferring additional exploit tools.
- B. The workstations are beaconing to a command-and-control server.
- C. A logic bomb was executed and is responsible for the data transfers.
- D. A fireless virus is spreading in the local network environment

**Answer:** A

#### NEW QUESTION 632

- (Exam Topic 3)

An analyst is working on an email incident in which target opened an attachment containing a worm. The analyst wants to implement mitigation techniques to prevent further spread. Which of the following is the BEST course of action for the analyst to take?

- A. Apply a DLP solution
- B. Implement network segmentation.
- C. Utilize email content filtering.
- D. Isolate the infected attachment.

**Answer:** B

#### NEW QUESTION 636

- (Exam Topic 3)

An organization is developing an authentication service for use at the entry and exit ports of country borders. The service will use data feeds obtained from passport systems, passenger manifests, and high-definition video feeds from CCTV systems that are located at the ports. The service will incorporate machine-learning techniques to eliminate biometric enrollment processes while still allowing authorities to identify passengers with increasing accuracy over time. The more frequently passengers travel, the more accurately the service will identify them. Which of the following biometrics will MOST likely be used, without the need for enrollment? (Choose two.)

- A. Voice
- B. Gait
- C. Vein
- D. Facial
- E. Retina
- F. Fingerprint

**Answer:** BD

#### NEW QUESTION 639

- (Exam Topic 3)

An incident response technician collected a mobile device during an investigation. Which of the following should the technician do to maintain 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 blockchain-protected public ledger

**Answer:** A

#### NEW QUESTION 643

- (Exam Topic 3)

Ann, a forensic analyst, needs to prove that the data she originally acquired has remained unchanged while in her custody. Which of the following should Ann use?

- A. Chain of custody
- B. Checksums
- C. Non-repudiation
- D. Legal hold

**Answer:** A

#### NEW QUESTION 647

- (Exam Topic 3)

Which of the following cloud models provides clients with servers, storage, and networks but nothing else?

- A. SaaS

- B. PaaS
- C. IaaS
- D. DaaS

**Answer:** C

#### NEW QUESTION 651

- (Exam Topic 3)

A security analyst is hardening a network infrastructure. The analyst is given the following requirements:

- \* Preserve the use of public IP addresses assigned to equipment on the core router.
- \* Enable "in transport" encryption protection to the web server with the strongest ciphers.

Which of the following should the analyst implement to meet these requirements? (Select TWO).

- A. Configure VLANs on the core router.
- B. Configure NAT on the core router.
- C. Configure BGP on the core router.
- D. Enable AES encryption on the web server.
- E. Enable 3DES encryption on the web server.
- F. Enable TLSv2 encryption on the web server.

**Answer:** AE

#### NEW QUESTION 656

- (Exam Topic 3)

An engineer needs to deploy a security measure to identify and prevent data tampering within the enterprise.

Which of the following will accomplish this goal?

- A. Antivirus
- B. IPS.
- C. FTP
- D. FIM

**Answer:** D

#### NEW QUESTION 658

- (Exam Topic 3)

Employees are having issues accessing the company's website. Some employees report very slow performance, while others cannot the website at all. The web and security administrators search the logs and find millions of half-open connections to port 443 on the web server. Further analysis reveals thousands of different source IPs initiating this traffic. Which of the following attacks is MOST likely occurring?

- A. DDoS
- B. Man-in-the-middle
- C. MAC flooding
- D. Domain hijacking

**Answer:** A

#### NEW QUESTION 663

- (Exam Topic 3)

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. Hping3 -s comptia, org -p 80
- B. Nc -1 -v comptia, org -p 80
- C. nmp comptia, org -p 80 -aV
- D. nslookup -port=80 comtia.org

**Answer:** C

#### Explanation:

Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.

#### NEW QUESTION 665

- (Exam Topic 3)

The SOC is reviewing process and procedures after a recent incident. The review indicates it took more than 30 minutes to determine that quarantining an infected host was the best course of action. The allowed the malware to spread to additional hosts before it was contained. Which of the following would be BEST to improve the incident response process?

- A. Updating the playbooks with better decision points
- B. Dividing the network into trusted and untrusted zones
- C. Providing additional end-user training on acceptable use
- D. Implementing manual quarantining of infected hosts

**Answer:** A

#### NEW QUESTION 667



.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### SY0-601 Practice Exam Features:

- \* SY0-601 Questions and Answers Updated Frequently
- \* SY0-601 Practice Questions Verified by Expert Senior Certified Staff
- \* SY0-601 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* SY0-601 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The SY0-601 Practice Test Here](#)**