

**SY0-601.premium.154q - DEMO**

Number: SY0-601  
Passing Score: 800  
Time Limit: 120 min



**SY0-601**

**CompTIA Security+ Certification Exam**



**Exam A****QUESTION 1**  
SIMULATION

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

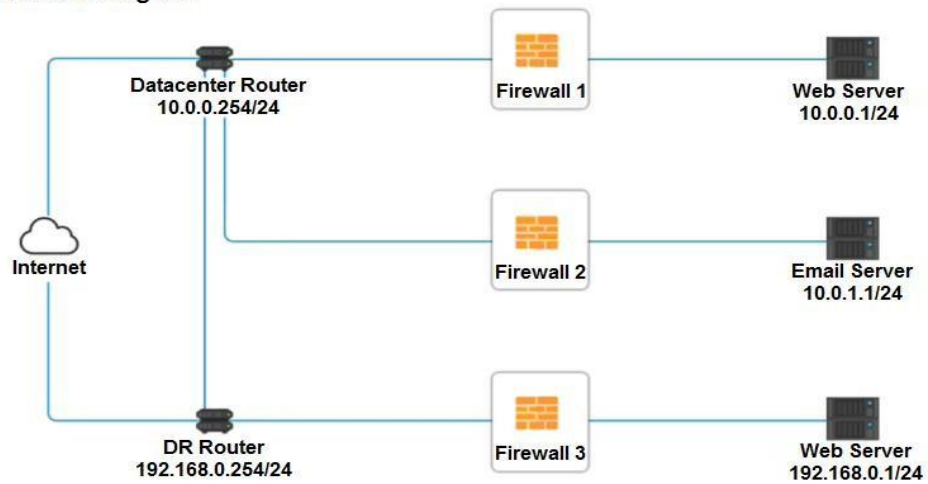
**INSTRUCTIONS**

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

**Network Diagram**

VCEUp

Firewall 1

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

Firewall 2

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

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

**Correct Answer:** See explanation below.

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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

**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

**QUESTION 2**

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.*

**Select and Place:**

Commands	SSH Client
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	

**Correct Answer:**

Commands	SSH Client
chmod 644 ~/.ssh/id_rsa	ssh-keygen -t rsa
chmod 777 ~/.ssh/authorized_keys	ssh-copy-id -i ~/.ssh/id_rsa.pub user@server
ssh-keygen -t rsa	chmod 644 ~/.ssh/id_rsa
scp ~/.ssh/id_rsa user@server:~/.ssh/authorized_keys	ssh root@server
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server	
ssh -i ~/.ssh/id_rsa user@server	
ssh root@server	

**Section: (none)**

**Explanation**  
**Explanation/Reference:**

### QUESTION 3 HOTSPOT

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.*

**Hot Area:**



Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	<div>▼</div> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	<div>▼</div> 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	<div>▼</div> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	<div>▼</div> 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	<div>▼</div> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	<div>▼</div> 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	<div>▼</div> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	<div>▼</div> 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	<div>▼</div> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	<div>▼</div> 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

Correct Answer:



Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	<div>▼</div> <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>	<div>▼</div> <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	<div>▼</div> <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>	<div>▼</div> <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	<div>▼</div> <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>	<div>▼</div> <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	<div>▼</div> <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>	<div>▼</div> <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	<div>▼</div> <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>	<div>▼</div> <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>

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 4**

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

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

**Correct Answer: DF**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 5**

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 6**

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.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 7**

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
- F. Install a captive portal

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 8

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

VCEup

#### QUESTION 9

Which of the following 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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 10** 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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 11** 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

**Correct Answer:** EF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 12**

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 13**

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 14** 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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 15**

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

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:****QUESTION 16**

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

VCEUp

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

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:****QUESTION 17**

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

- A. SaaS
- B. PaaS



- C. IaaS
- D. DaaS

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 18** A network administrator needs to build out a new datacenter, with a focus on resiliency and uptime. Which of the following would BEST meet this objective? (Choose two.)

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

**Correct Answer:** AB  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

#### QUESTION 19

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:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@  WARNING:  REMOTE HOST IDENTIFICATION HAS CHANGED!  @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
The fingerprint for the RSA key sent by the remote host is
SHA256:cBqYjal6ToV3jEIJHUSKtjjVzignVd4Cz+1fhTM6+k4.
Please contact your system administrator.
RSA host key for 18.231.33.78 has changed and you have requested strict checking.
Host key verification failed.
```

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

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

#### QUESTION 20

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

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 21

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 22

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 following is MOST likely causing the malware alerts?

- 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 vCard that is attempting to execute an attack
- 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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 23

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 24

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 25** 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.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 26

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

An incident responder learns the following information:

- The timeline of stolen card numbers corresponds closely with affected users making Internet-based purchases from diverse websites via enterprise desktop PCs.
- All purchase connections were encrypted, and the company uses an SSL inspection proxy for the inspection of encrypted traffic of the hardwired network.
- Purchases made with corporate cards over the corporate guest WiFi network, where no SSL inspection occurs, were unaffected.

Which of the following is the MOST likely root cause?

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 27**

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.)

- A. Trusted Platform Module
- B. A host-based firewall
- C. A DLP solution
- D. Full disk encryption
- E. A VPN
- F. Antivirus software

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 28** 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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 29**

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.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 30** 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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 31**

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 32** 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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 33**

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.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 34**

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

**Correct Answer:** B



**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 35**

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 36**

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 37**

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.
- B. Segment the network into trusted and untrusted zones.
- C. Enforce application whitelisting.
- D. Implement DLP at the network boundary.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 38**

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 39

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 40

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 41

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 42**

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 43** 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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:****QUESTION 44**

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

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:****QUESTION 45**

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 46

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.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 47** An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the MOST acceptable?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 48

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.

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 49**

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.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 50**

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.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 51** 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
- B. SSO
- C. SAML
- D. PAP

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 52** 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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 53**

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.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 54** In which of the following common use cases would steganography be employed?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 55**

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 56** In which of the following risk management strategies would cybersecurity insurance be used?

- A. Transference
- B. Avoidance

- C. Acceptance
- D. Mitigation

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 57**

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 when creating this policy?

- A. The theft of portable electronic devices
- B. Geotagging in the metadata of images
- C. Bluesnarfing of mobile devices
- D. Data exfiltration over a mobile hotspot

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 58** 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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 59**

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 60** 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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 61** 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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 62** 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.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 63**

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.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 64** 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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 65** 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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 66**

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

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 67**

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

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 68**

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

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 69**

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. Typo squatting
- D. Pharming

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 70**

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

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 71** 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



**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 72**

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 73**

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.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 74** 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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 75**

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 76**

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.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 77**

Joe, 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 Joe'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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 78**

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 79**

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 80** 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-basedC. Role-based
- D. Mandatory

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 81**

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 82**

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

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

D. Pivoting

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 83** 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? (Choose two.)

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

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 84** When selecting a technical solution for identity management, an architect chooses to go from an in-house solution to a third-party SaaS provider. Which of the following risk management strategies is this an example of?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 85**

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 86** 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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 87

An analyst visits an Internet forum looking for information about a tool. The analyst finds a thread that appears to contain relevant information. One of the posts says the following:

```
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. SQLi attack
- B. DLL attack
- C. XSS attack
- D. API attack

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 88

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 89

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? (Choose two.)

- A. COPE
- B. VDI
- C. GPS
- D. TOTP
- E. RFID
- F. BYOD

**Correct Answer:** BE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 90

The Chief Security Officer (CSO) at a major hospital wants to implement SSO to help improve security in the environment and protect patient data, particularly at shared terminals. The Chief Risk Officer (CRO) is concerned that training and guidance have not 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 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 systems if the identity provider goes offline.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 91

A smart switch has the ability to monitor electrical levels and shut off power to a building in the event of power surge or 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 patching 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.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 92

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

**Correct Answer:** D

**Section:** (none)

**Explanation**



**Explanation/Reference:****QUESTION 93**

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 94** Which of the following types of controls is a turnstile?

- A. Physical
- B. Detective
- C. Corrective
- D. Technical

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 95** 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.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 96**

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

**Correct Answer:** E

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 97** 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. Biometrics
- D. Two-factor authentication

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 98**

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 99**

Joe, a user at a company, clicked an email links that 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 a security 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.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 100** 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 -l -v comptia.org -p 80`
- C. `nmap comptia.org -p 80 -sV`
- D. `nslookup -port=80 comptia.org`

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 101**

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

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 102**

A security analyst is performing a forensic investigation involving compromised account credentials. Using the Event Viewer, the analyst was able to detect the following message: "Special privileges assigned to new logon." 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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 103** A systems administrator needs to implement an access control scheme that will allow an object's access policy to 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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 104**

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

- A. `http://sample.url.com/<script>Please-Visit-Our-Phishing-Site</script>`
- B. `http://sample.url.com/someotherpageonsite/../../../../etc/shadow`
- C. `http://sample.url.com/select-from-database-where-password-null`
- D. `http://redirect.sameple.url.sampleurl.com/malicious-dns-redirect`

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 105**

A company has limited storage space available and an online presence that cannot be down 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 full tape backups every Sunday at 8:00 p.m. and perform nightly tape rotations.
- B. Implement differential backups every Sunday at 8:00 p.m. 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 p.m.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 106**

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.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 107**

A malicious actor recently penetrated 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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:****QUESTION 108**

A public relations team will be taking a group of guests 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.
- D. credential exposure.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 109** 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.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 110**

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 to their 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.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 111**

A security administrator needs to create a RAID configuration that is focused on high read speeds and fault tolerance. It is unlikely that multiple drives will fail simultaneously. Which of the following RAID configurations should the administrator use?

- A. RAID 0
- B. RAID 1C. RAID 5
- D. RAID 10

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 112**

A company's Chief Information Officer (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. Basic awareness training

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 113**

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 OSCP
- B. Generate a CSR.
- C. Create a CRL.
- D. Generate a .pfx file.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 114**

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 115**

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.

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 116** 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 communications plan
- C. A disaster recovery plan
- D. A business continuity plan

**Correct Answer:** D  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 117** Which of the following describes the ability of code to target a hypervisor from inside a guest OS?

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

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 118** 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

**Correct Answer:** D  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 119**

During an incident response, a security analyst observes the following log entry on the web server:

```
GET http://www.companysite.com/product_info.php?show=../../../../etc/passwd HTTP/1.1
Host: www.companysite.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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 120** Which of the following ISO standards is certified for privacy?

- A. ISO 9001
- B. ISO 27002
- C. ISO 27701D. ISO 31000 **Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 121**

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.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 122** 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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 123** Which of the following is a team of people dedicated to 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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 124

A security analyst discovers that a company's username and password database was posted on an Internet forum. The usernames 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.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 125

Which of the following are requirements that must be configured for PCI DSS compliance? (Choose two.)

- A. Testing security systems and processes regularly
- B. Installing and maintaining a web proxy to protect cardholder data
- C. Assigning a unique ID to each person with computer access
- D. Encrypting transmission of cardholder data across private networks
- E. Benchmarking security awareness training for contractors
- F. Using vendor-supplied default passwords for system passwords

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 126** A security analyst needs to be proactive in understanding the types of attacks that could potentially target the company's executives. Which of the following intelligence sources should the security analyst review?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 127**

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 protected network segment. Which of the following would be MOST effective to implement to further mitigate the reported vulnerability?

- A. DNS sinkholing
- B. DLP rules on the terminal
- C. An IP blacklist
- D. Application whitelisting

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 128**

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 this 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 poisoned a name server.
- D. An ARP poisoning attack was successfully executed.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 129**

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 transfers 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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 130**

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 131

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.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 132

A security engineer is reviewing log files after a third party 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 week 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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 133

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

**Correct Answer:** E

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 134

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 135**

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 136**

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 the account and pivot throughout the global network. Which of the following would be BEST to help mitigate this concern?

- A. Create different 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.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 137** 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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 138**

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 139**

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.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 140**

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 141**

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

- A. SPIM
- B. Vishing

- C. Spear phishing
- D. Smishing

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 142** 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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 143**

Which of the following will provide the BEST physical security countermeasures to stop intruders? (Choose two.)

- A. Alarms
- B. Signage
- C. Lighting
- D. Mantraps
- E. Fencing
- F. Sensors

**Correct Answer:** EF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 144** 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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 145**



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.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 146**

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

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

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 147** In the middle of a cyberattack, a security engineer removes the infected devices from the network and locks down all compromised accounts. In which of the following incident response phases is the security engineer currently operating?

- A. Identification
- B. Preparation
- C. Lessons learned
- D. Eradication
- E. Recovery
- F. Containment

**Correct Answer:** F

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 148**

The SOC is reviewing processes 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. This 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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 149**

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 150** A network administrator is setting up wireless access points in all the conference rooms and wants to authenticate devices using PKI. Which of the following should the administrator configure?

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 151** Which of the following are the MOST likely vectors for the unauthorized or unintentional inclusion of vulnerable code in a software company's final software releases? (Choose 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

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 152**

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 153** An organization just experienced a major cyberattack incident. 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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 154**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**