



# CompTIA

## Exam Questions SY0-601

CompTIA Security+ Exam

#### NEW QUESTION 1

A security analyst needs to make a recommendation for restricting access to certain segments of the network using only data-link layer security. Which of the following controls will the analyst MOST likely recommend?

- A. MAC
- B. ACL
- C. BPDU
- D. ARP

**Answer: A**

#### NEW QUESTION 2

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

- A. Watering-hole attack
- B. Credential harvesting
- C. Hybrid warfare
- D. Pharming

**Answer: A**

#### NEW QUESTION 3

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

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

**Answer: D**

#### NEW QUESTION 4

A critical file server is being upgraded and the systems administrator must determine which RAID level the new server will need to achieve parity and handle two simultaneous disk failures. Which of the following RAID levels meets this requirements?

- A. RAID 0+1
- B. RAID 2
- C. RAID 5
- D. RAID 6

**Answer: C**

#### NEW QUESTION 5

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

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

**Answer: C**

#### NEW QUESTION 6

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

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

**Answer: B**

#### NEW QUESTION 7

A global pandemic is forcing a private organization to close some business units and reduce staffing at others. Which of the following would be BEST to help the organization's executives determine the next course of action?

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

**Answer: D**

#### NEW QUESTION 8

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

- A. Hping3 -s comptia.org -p 80
- B. Nc -1 -v comptia.org -p 80
- C. nmap comptia.org -p 80 -aV
- D. nslookup -port=80 comptia.org

**Answer: C**

#### NEW QUESTION 9

A commercial cyber-threat intelligence organization observes IoCs across a variety of unrelated customers. Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely obligated by contracts to:

- A. perform attribution to specific APTs and nation-state actors.
- B. anonymize any PII that is observed within the IoC data.
- C. add metadata to track the utilization of threat intelligence reports.
- D. assist companies with impact assessments based on the observed data.

**Answer: B**

#### NEW QUESTION 10

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

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

**Answer: AD**

#### NEW QUESTION 10

A financial organization has adopted a new secure, encrypted document-sharing application to help with its customer loan process. Some important PII needs to be shared across this new platform, but it is getting blocked by the DLP systems. Which of the following actions will BEST allow the PII to be shared with the secure application without compromising the organization's security posture?

- A. Configure the DLP policies to allow all PII
- B. Configure the firewall to allow all ports that are used by this application
- C. Configure the antivirus software to allow the application
- D. Configure the DLP policies to whitelist this application with the specific PII
- E. Configure the application to encrypt the PII

**Answer: D**

#### NEW QUESTION 15

A security analyst is reviewing the following attack log output:

```
user comptia\john.smith attempted login with the password password123
user comptia\jane.doe attempted login with the password password123
user comptia\user.one attempted login with the password password123
user comptia\user.two attempted login with the password password123
user comptia\user.three attempted login with the password password123

user comptia\john.smith attempted login with the password password234
user comptia\jane.doe attempted login with the password password234
user comptia\user.one attempted login with the password password234
user comptia\user.two attempted login with the password password234
user comptia\user.three attempted login with the password password234
```

Which of the following types of attacks does this MOST likely represent?

- A. Rainbow table
- B. Brute-force
- C. Password-spraying
- D. Dictionary

**Answer: C**

#### NEW QUESTION 18

Which of the following relates to applications and systems that are used within an organization without consent or approval?

- A. Shadow IT

- B. OSINT
- C. Dark web
- D. Insider threats

**Answer:** A

#### NEW QUESTION 22

Which of the following job roles would sponsor data quality and data entry initiatives that ensure business and regulatory requirements are met?

- A. The data owner
- B. The data processor
- C. The data steward
- D. The data privacy officer.

**Answer:** C

#### NEW QUESTION 24

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

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

**Answer:** A

#### NEW QUESTION 28

A malicious actor recently penetration a company's network and moved laterally to the datacenter. Upon investigation, a forensics firm wants to know what was in the memory on the compromised server. Which of the following files should be given to the forensics firm?

- A. Security
- B. Application
- C. Dump
- D. Syslog

**Answer:** C

#### NEW QUESTION 32

A network engineer is troubleshooting wireless network connectivity issues that were reported by users. The issues are occurring only in the section of the building that is closest to the parking lot. Users are intermittently experiencing slow speeds when accessing websites and are unable to connect to network drives. The issues appear to increase when laptop users return desks after using their devices in other areas of the building. There have also been reports of users being required to enter their credentials on web pages in order to gain access to them. Which of the following is the MOST likely cause of this issue?

- A. An external access point is engaging in an evil-twin attack.
- B. The signal on the WAP needs to be increased in that section of the building.
- C. The certificates have expired on the devices and need to be reinstalled.
- D. The users in that section of the building are on a VLAN that is being blocked by the firewall.

**Answer:** A

#### NEW QUESTION 37

Some laptops recently went missing from a locked storage area that is protected by keyless RFID-enabled locks. There is no obvious damage to the physical space. The security manager identifies who unlocked the door, however, human resources confirms the employee was on vacation at the time of the incident. Which of the following describes what MOST likely occurred?

- A. The employee's physical access card was cloned.
- B. The employee is colluding with human resources
- C. The employee's biometrics were harvested
- D. A criminal used lock picking tools to open the door.

**Answer:** A

#### NEW QUESTION 39

A security analyst is performing a packet capture on a series of SOAP HTTP requests for a security assessment. The analyst redirects the output to a file. After the capture is complete, the analyst needs to review the first transactions quickly and then search the entire series of requests for a particular string. Which of the following would be BEST to use to accomplish the task? (Select TWO).

- A. head
- B. Tcpdump
- C. grep
- D. rail
- E. curl
- F. openssl
- G. dd

**Answer:** AB

#### NEW QUESTION 41

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

**Answer:** A

#### NEW QUESTION 43

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

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

**Answer:** B

#### NEW QUESTION 48

When used at the design stage, which of the following improves the efficiency, accuracy, and speed of a database?

- A. Tokenization
- B. Data masking
- C. Normalization
- D. Obfuscation

**Answer:** C

#### NEW QUESTION 50

Which of the following would BEST identify and remediate a data-loss event in an enterprise using third-party, web-based services and file-sharing platforms?

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

**Answer:** D

#### NEW QUESTION 51

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 earlier. This change lasted eight hours. Which of the following attacks was MOST likely used?

- A. Man-in-the-middle
- B. Spear-phishing
- C. Evil twin
- D. DNS poisoning

**Answer:** D

#### NEW QUESTION 52

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

##### INSTRUCTIONS

Not all attacks and remediation actions will be used.

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

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

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

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

**NEW QUESTION 55**

A security analyst needs to determine how an attacker was able to use User3 to gain a foothold within a company's network. The company's lockout policy requires that an account be locked out for a minimum of 15 minutes after three unsuccessful attempts. While reviewing the log files, the analyst discovers the following:

```

3/16/20 3:31:10 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:11 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:12 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:13 AM Audit Failure: CompanyNetwork\User1 Account locked out.
3/16/20 3:31:14 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:15 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:16 AM Audit Failure: CompanyNetwork\User2 Account locked out.
3/16/20 3:31:18 AM Audit Failure: CompanyNetwork\User3 Unknown username or bad password.
3/16/20 3:31:19 AM Audit Failure: CompanyNetwork\User3 Unknown username or bad password.
3/16/20 3:31:20 AM Audit Failure: CompanyNetwork\User3 Successful logon.
3/16/20 3:31:22 AM Audit Success: CompanyNetwork\User3 Successful logon.
3/16/20 3:31:22 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.
3/16/20 3:32:40 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.
3/16/20 3:33:25 AM Audit Success: CompanyNetwork\User4 Successful logon.

```

Which of the following attacks MOST likely occurred?

- A. Dictionary
- B. Credential-stuffing
- C. Password-spraying
- D. Brute-force

**Answer: D**

**NEW QUESTION 60**

A network technician is installing a guest wireless network at a coffee shop. When a customer purchases an item, the password for the wireless network is printed

on the recent so the customer can log in. Which of the following will the technician MOST likely configure to provide the highest level of security with the least amount of overhead?

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

**Answer:** A

#### NEW QUESTION 61

The facilities supervisor for a government agency is concerned about unauthorized access to environmental systems in the event the staff WiFi network is breached. Which of the following would BEST address this security concern?

- A. install a smart meter on the staff WiFi.
- B. Place the environmental systems in the same DHCP scope as the staff WiFi.
- C. Implement Zigbee on the staff WiFi access points.
- D. Segment the staff WiFi network from the environmental systems network.

**Answer:** D

#### NEW QUESTION 62

Joe, a user at a company, clicked an email link led to a website that infected his workstation. Joe, was connected to the network, and the virus spread to the network shares. The protective measures failed to stop this virus, and it has continued to evade detection. Which of the following should administrator implement to protect the environment from this malware?

- A. Install a definition-based antivirus.
- B. Implement an IDS/IPS
- C. Implement a heuristic behavior-detection solution.
- D. Implement CASB to protect the network shares.

**Answer:** C

#### NEW QUESTION 65

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

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

**Answer:** D

#### NEW QUESTION 68

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

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

**Answer:** B

#### NEW QUESTION 72

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

**Answer:** AC

#### NEW QUESTION 74

A Chief Information Security Officer (CISO) is concerned about the organization's ability to continue business operation in the event of a prolonged DDoS attack on its local datacenter that consumes database resources. Which of the following will the CISO MOST likely recommend to mitigate this risk?

- A. Upgrade the bandwidth available into the datacenter
- B. Implement a hot-site failover location
- C. Switch to a complete SaaS offering to customers
- D. Implement a challenge response test on all end-user queries

**Answer:** B

**NEW QUESTION 76**

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

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

**Answer:** D

**NEW QUESTION 81**

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

**Answer:** C

**NEW QUESTION 84**

An analyst needs to set up a method for securely transferring files between systems. One of the requirements is to authenticate the IP header and the payload. Which of the following services would BEST meet the criteria?

- A. TLS
- B. PFS
- C. ESP
- D. AH

**Answer:** A

**NEW QUESTION 86**

A security analyst needs to implement an MDM solution for BYOD users that will allow the company to retain control over company emails residing on the devices and limit data exfiltration that might occur if the devices are lost or stolen. Which of the following would BEST meet these requirements? (Select TWO).

- A. Full-device encryption
- B. Network usage rules
- C. Geofencing
- D. Containerization
- E. Application whitelisting
- F. Remote control

**Answer:** AB

**NEW QUESTION 91**

An organization has hired a security analyst to perform a penetration test. The analyst captures 1Gb worth of inbound network traffic to the server and transfer the pcap back to the machine for analysis. Which of the following tools should the analyst use to further review the pcap?

- A. Nmap
- B. cURL
- C. Netcat
- D. Wireshark

**Answer:** D

**NEW QUESTION 96**

Which of the following organizational policies are MOST likely to detect fraud that is being conducted by existing employees? (Select TWO).

- A. Offboarding
- B. Mandatory vacation
- C. Job rotation
- D. Background checks
- E. Separation of duties
- F. Acceptable use

**Answer:** BC

**NEW QUESTION 98**

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

- A. Dual power supply

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

**Answer:** AB

#### NEW QUESTION 103

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

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

**Answer:** A

#### NEW QUESTION 106

A user is concerned that a web application will not be able to handle unexpected or random input without crashing. Which of the following BEST describes the type of testing the user should perform?

- A. Code signing
- B. Fuzzing
- C. Manual code review
- D. Dynamic code analysis

**Answer:** D

#### NEW QUESTION 108

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

An incident responder learns the following information:

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

Which of the following is the MOST likely root cause?

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

**Answer:** C

#### NEW QUESTION 110

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

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

**Answer:** B

#### NEW QUESTION 112

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

- A. Security awareness training
- B. Frequency of NIDS updates
- C. Change control procedures
- D. EDR reporting cycle

**Answer:** A

#### NEW QUESTION 114

A security manager for a retailer needs to reduce the scope of a project to comply with PCI DSS. The PCI data is located in different offices than where credit cards are accepted. All the offices are connected via MPLS back to the primary datacenter. Which of the following should the security manager implement to achieve the objective?

- A. Segmentation
- B. Containment
- C. Geofencing

D. Isolation

**Answer:** A

#### NEW QUESTION 116

An organization's RPO for a critical system is two hours. The system is used Monday through Friday, from 9:00 am to 5:00 pm. Currently, the organization performs a full backup every Saturday that takes four hours to complete. Which of the following additional backup implementations would be the BEST way for the analyst to meet the business requirements?

- A. Incremental backups Monday through Friday at 6:00 p.m and differential backups hourly
- B. Full backups Monday through Friday at 6:00 p.m and incremental backups hourly.
- C. incremental backups Monday through Friday at 6:00 p.m and full backups hourly.
- D. Full backups Monday through Friday at 6:00 p.m and differential backups hourly.

**Answer:** A

#### NEW QUESTION 117

A security analyst sees the following log output while reviewing web logs:

```
[02/Feb/2019:03:39:21 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?query=%2f..%2f..%2f..%2fetc%2fpasswd HTTP/1.0" 80 200 200  
[02/Feb/2019:03:39:25 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?query=../../../../etc/passwd HTTP/1.0" 80 200 200
```

Which of the following mitigation strategies would be BEST to prevent this attack from being successful?

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

**Answer:** B

#### NEW QUESTION 118

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

- > www.company.com (main website)
- > contactus.company.com (for locating a nearby location)
- > quotes.company.com (for requesting a price quote)

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

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

**Answer:** B

#### NEW QUESTION 123

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

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

**Answer:** C

#### NEW QUESTION 125

Which of the following would be BEST to establish between organizations to define the responsibilities of each party outline the key deliverables and include monetary penalties for breaches to manage third-party risk?

- A. An ARO
- B. An MOU
- C. An SLA
- D. A BPA

**Answer:** B

#### NEW QUESTION 128

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

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

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

**Answer:** AD

#### NEW QUESTION 131

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

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

**Answer:** B

#### NEW QUESTION 135

A vulnerability assessment report will include the CVSS score of the discovered vulnerabilities because the score allows the organization to better.

- A. validate the vulnerability exists in the organization's network through penetration testing
- B. research the appropriate mitigation techniques in a vulnerability database
- C. find the software patches that are required to mitigate a vulnerability
- D. prioritize remediation of vulnerabilities based on the possible impact.

**Answer:** D

#### NEW QUESTION 138

An organization's help desk is flooded with phone calls from users stating they can no longer access certain websites. The help desk escalates the issue to the security team, as these websites were accessible the previous day. The security analysts run the following command: `ipconfig /flushdns`, but the issue persists. Finally, an analyst changes the DNS server for an impacted machine, and the issue goes away. Which of the following attacks MOST likely occurred on the original DNS server?

- A. DNS cache poisoning
- B. Domain hijacking
- C. Distributed denial-of-service
- D. DNS tunneling

**Answer:** B

#### NEW QUESTION 142

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

- A. The DNS logs
- B. The web server logs
- C. The SIP traffic logs
- D. The SNMP logs

**Answer:** A

#### NEW QUESTION 146

A company has limited storage available and online presence that cannot 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, which being mindful of the limited available storage space?

- A. Implement fulltape backup every Sunday at 8:00 p.m and perform nightly tape rotations.
- B. Implement different backups every Sunday at 8:00 and nightly incremental backups at 8:00 p.m
- C. Implement nightly full backups every Sunday at 8:00 p.m
- D. Implement full backups every Sunday at 8:00 p.m and nightly differential backups at 8:00

**Answer:** B

#### NEW QUESTION 147

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

- A. data controller.
- B. data owner
- C. data custodian.
- D. data processor

**Answer:** D

#### NEW QUESTION 149

A recent malware outbreak across a subnet included successful rootkit installations on many PCs, ensuring persistence by rendering remediation efforts ineffective. Which of the following would BEST detect the presence of a rootkit in the future?

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

**Answer: C**

#### NEW QUESTION 152

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 experience?

- A. SQL injection
- B. Cross-site scripting
- C. Pass-the-hash
- D. Directory traversal

**Answer: B**

#### NEW QUESTION 154

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

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

**Answer: C**

#### NEW QUESTION 159

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

- A. The GPS location
- B. When the file was deleted
- C. The total number of print jobs
- D. The number of copies made

**Answer: A**

#### NEW QUESTION 163

An organization suffered an outage and a critical system took 90 minutes to come back online. Though there was no data loss during the outage, the expectation was that the critical system would be available again within 60 minutes Which of the following is the 60-minute expectation an example of:

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

**Answer: D**

#### NEW QUESTION 167

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

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

Which of the following can the security analyst conclude?

- A. A replay attack is being conducted against the application.
- B. An injection attack is being conducted against a user authentication system.
- C. A service account password may have been changed, resulting in continuous failed logins within the application.
- D. A credentialed vulnerability scanner attack is testing several CVEs against the application.

**Answer: C**

#### NEW QUESTION 170

Which of the following policies would help an organization identify and mitigate potential single points of failure in the company's IT/security operations?

- A. Least privilege
- B. Awareness training
- C. Separation of duties
- D. Mandatory vacation

**Answer: C**

#### NEW QUESTION 171

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

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

**Answer: A**

#### NEW QUESTION 174

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

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

**Answer: A**

#### NEW QUESTION 176

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

- A. Tabletop
- B. Parallel
- C. Full interruption
- D. Simulation

**Answer: D**

#### NEW QUESTION 180

A network engineer notices the VPN concentrator overloaded and crashes on days when there are a lot of remote workers. Senior management has placed greater importance on the availability of VPN resources for the remote workers than the security of the end users' traffic. Which of the following would be BEST to solve this issue?

- A. iPSec
- B. Always On
- C. Split tunneling
- D. L2TP

**Answer: B**

#### NEW QUESTION 182

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

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

**Answer: A**

#### NEW QUESTION 184

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

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

**Answer: B**

**NEW QUESTION 188**

A security analyst is reviewing a new website that will soon be made publicly available. The analyst sees the following in the URL:

`http://dev-site.comptia.org/home/show.php?sessionID=77276554&loc=us`

The analyst then sends an internal user a link to the new website for testing purposes, and when the user clicks the link, the analyst is able to browse the website with the following URL:

`http://dev-site.comptia.org/home/show.php?sessionID=98988475&loc=us` Which of the following application attacks is being tested?

- A. Pass-the-hash
- B. Session replay
- C. Object deference
- D. Cross-site request forgery

**Answer: B**

**NEW QUESTION 191**

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

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

**Answer: D**

**NEW QUESTION 193**

Local guidelines require that all information systems meet a minimum-security baseline to be compliant. Which of the following can security administrators use to assess their system configurations against the baseline?

- A. SOAR playbook
- B. Security control matrix
- C. Risk management framework
- D. Benchmarks

**Answer: D**

**NEW QUESTION 196**

A security analyst is investigation an incident that was first reported as an issue connecting to network shares and the internet, While reviewing logs and tool output, the analyst sees the following:

IP address	Physical address
10.0.0.1	00-18-21-ad-24-bc
10.0.0.114	01-31-a3-cd-23-ab
10.0.0.115	00-18-21-ad-24-bc
10.0.0.116	00-19-08-ba-07-da
10.0.0.117	01-12-21-ca-11-ad

Which of the following attacks has occurred?

- A. IP conflict
- B. Pass-the-hash
- C. MAC flooding
- D. Directory traversal
- E. ARP poisoning

**Answer: E**

**NEW QUESTION 199**

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

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

**Answer: A**

**NEW QUESTION 202**

A security analyst is reviewing information regarding recent vulnerabilities. Which of the following will the analyst MOST likely consult to validate which platforms have been affected?

- A. OSINT
- B. SIEM
- C. CVSS

D. CVE

**Answer: D**

#### NEW QUESTION 203

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

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

**Answer: DF**

#### NEW QUESTION 208

Which of the following scenarios would make a DNS sinkhole effective in thwarting an attack?

- A. An attacker is sniffing traffic to port 53, and the server is managed using unencrypted usernames and passwords.
- B. An organization is experiencing excessive traffic on port 53 and suspects an attacker is trying to DoS the domain name server.
- C. Malware trying to resolve an unregistered domain name to determine if it is running in an isolated sandbox
- D. Routing tables have been compromised, and an attacker is rerouting traffic to malicious websites

**Answer: A**

#### NEW QUESTION 209

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

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

**Answer: C**

#### NEW QUESTION 214

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

- A. Limit the use of third-party libraries.
- B. Prevent data exposure queries.
- C. Obfuscate the source code.
- D. Submit the application to QA before releasing it.

**Answer: D**

#### NEW QUESTION 215

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

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

**Answer: B**

#### NEW QUESTION 217

A software developer needs to perform code-execution testing, black-box testing, and non-functional testing on a new product before its general release. Which of the following BEST describes the tasks the developer is conducting?

- A. Verification
- B. Validation
- C. Normalization
- D. Staging

**Answer: A**

#### NEW QUESTION 219

The Chief Security Officer (CSO) at a major hospital wants to implement SSO to help improve in the environment patient data, particularly at shared terminals. The Chief Risk Officer (CRO) is concerned that training and guidance have been provided to frontline staff, and a risk analysis has not been performed. Which of the following is the MOST likely cause of the CRO's concerns?

- A. SSO would simplify username and password management, making it easier for hackers to pass guess accounts.

- B. SSO would reduce password fatigue, but staff would still need to remember more complex passwords.
- C. SSO would reduce the password complexity for frontline staff.
- D. SSO would reduce the resilience and availability of system if the provider goes offline.

**Answer: D**

#### NEW QUESTION 224

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

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

**Answer: A**

#### NEW QUESTION 225

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

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

**Answer: A**

#### NEW QUESTION 229

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. Ofboarding

**Answer: D**

#### NEW QUESTION 230

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. Oder of volatility
- D. A log analysis
- E. A right-to-audit clause

**Answer: D**

#### NEW QUESTION 234

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

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

**Answer: D**

#### NEW QUESTION 239

A startup company is using multiple SaaS and IaaS platforms to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?

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

**Answer: C**

#### NEW QUESTION 242

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.

**Commands**

```

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

**SSH Client**

?

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Commands**

```

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

**SSH Client**

```

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

**NEW QUESTION 243**

Which of the following would be BEST to establish between organizations that have agreed cooperate and are engaged in early discussion to define the responsibilities of each party, but do not want to establish a contractually binding agreement?

- A. An SLA
- B. AnNDA
- C. ABPA
- D. AnMOU

**Answer: D**

#### NEW QUESTION 248

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

**Answer: B**

#### NEW QUESTION 250

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

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

**Answer: C**

#### NEW QUESTION 253

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

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

**Answer: C**

#### NEW QUESTION 255

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 administration use?

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

**Answer: C**

#### NEW QUESTION 260

A database administrator needs to ensure all passwords are stored in a secure manner, so the administrator adds randomly generated data to each password before string. Which of the following techniques BEST explains this action?

- A. Predictability
- B. Key stretching
- C. Salting
- D. Hashing

**Answer: C**

#### NEW QUESTION 263

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

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

**Answer: B**

#### NEW QUESTION 267

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

**Answer: C**

**NEW QUESTION 269**

Which of the following types of controls is a turnstile?

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

**Answer: A**

**NEW QUESTION 272**

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

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

**Answer: C**

**NEW QUESTION 274**

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

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

**Answer: C**

**NEW QUESTION 276**

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

- A. The S/MIME plug-in is not enabled.
- B. The SLL certificate has expired.
- C. Secure IMAP was not implemented
- D. POP3S is not supported.

**Answer: A**

**NEW QUESTION 280**

A user recently attended an exposition and received some digital promotional materials. The user later noticed blue boxes popping up and disappearing on the computer, and reported receiving several spam emails, which the user did not open. Which of the following is MOST likely the cause of the reported issue?

- A. There was a drive-by download of malware
- B. The user installed a cryptominer
- C. The OS was corrupted
- D. There was malicious code on the USB drive

**Answer: D**

**NEW QUESTION 281**

A user reports constant lag and performance issues with the wireless network when working at a local coffee shop. A security analyst walks the user through an installation of Wireshark and gets a five-minute pcap to analyze. The analyst observes the following output:

No.	Time	Source	Destination	Protocol	Length	Info
1234	9.1195665	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=655, FN=0
1235	9.1265649	Sagemcom_87:9f:a3	Broadcast	802.11	39	Deauthentication, SN=655, FN=0
1236	9.2223212	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=657, FN=0

Which of the following attacks does the analyst MOST likely see in this packet capture?

- A. Session replay
- B. Evil twin
- C. Bluejacking
- D. ARP poisoning

**Answer: B**

#### NEW QUESTION 283

An organization hired a consultant to assist with an active attack, and the consultant was able to identify the compromised accounts and computers. Which of the following is the consultant MOST likely to recommend to prepare for eradication?

- A. Quarantining the compromised accounts and computers, only providing them with network access
- B. Segmenting the compromised accounts and computers into a honeynet so as to not alert the attackers.
- C. Isolating the compromised accounts and computers, cutting off all network and internet access.
- D. Logging off and deleting the compromised accounts and computers to eliminate attacker access.

**Answer: B**

#### NEW QUESTION 286

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

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

**Answer: C**

#### NEW QUESTION 288

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

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

**Answer: C**

#### NEW QUESTION 293

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

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

**Answer: A**

#### NEW QUESTION 295

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

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

**Answer: D**

#### NEW QUESTION 297

A security analyst is preparing a threat for an upcoming internal penetration test. The analyst needs to identify a method for determining the tactics, techniques, and procedures of a threat against the organization's network. Which of the following will the analyst MOST likely use to accomplish the objective?

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

**Answer: A**

#### NEW QUESTION 302

A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks. Which of the following methods would BEST prevent the exfiltration of data? (Select TWO).

- A. VPN
- B. Drive encryption
- C. Network firewall
- D. File level encryption
- E. USB blocker
- F. MFA

**Answer:** BE

**NEW QUESTION 306**

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

**Answer:** AB

**NEW QUESTION 308**

An engineer wants to access sensitive data from a corporate-owned mobile device. Personal data is not allowed on the device. Which of the following MDM configurations must be considered when the engineer travels for business?

- A. Screen locks
- B. Application management
- C. Geofencing
- D. Containerization

**Answer:** D

**NEW QUESTION 309**

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

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

**Answer:** A

**NEW QUESTION 312**

.....

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

#### NEW QUESTION 1

A security analyst needs to make a recommendation for restricting access to certain segments of the network using only data-link layer security. Which of the following controls will the analyst MOST likely recommend?

- A. MAC
- B. ACL
- C. BPDU
- D. ARP

**Answer: A**

#### NEW QUESTION 2

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

- A. Watering-hole attack
- B. Credential harvesting
- C. Hybrid warfare
- D. Pharming

**Answer: A**

#### NEW QUESTION 3

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

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

**Answer: D**

#### NEW QUESTION 4

A critical file server is being upgraded and the systems administrator must determine which RAID level the new server will need to achieve parity and handle two simultaneous disk failures. Which of the following RAID levels meets this requirements?

- A. RAID 0+1
- B. RAID 2
- C. RAID 5
- D. RAID 6

**Answer: C**

#### NEW QUESTION 5

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

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

**Answer: C**

#### NEW QUESTION 6

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

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

**Answer: B**

#### NEW QUESTION 7

A global pandemic is forcing a private organization to close some business units and reduce staffing at others. Which of the following would be BEST to help the organization's executives determine the next course of action?

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

**Answer: D**

#### NEW QUESTION 8

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

- A. Hping3 -s comptia.org -p 80
- B. Nc -1 -v comptia.org -p 80
- C. nmap comptia.org -p 80 -aV
- D. nslookup -port=80 comptia.org

**Answer: C**

#### NEW QUESTION 9

A commercial cyber-threat intelligence organization observes IoCs across a variety of unrelated customers. Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely obligated by contracts to:

- A. perform attribution to specific APTs and nation-state actors.
- B. anonymize any PII that is observed within the IoC data.
- C. add metadata to track the utilization of threat intelligence reports.
- D. assist companies with impact assessments based on the observed data.

**Answer: B**

#### NEW QUESTION 10

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

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

**Answer: AD**

#### NEW QUESTION 10

A financial organization has adopted a new secure, encrypted document-sharing application to help with its customer loan process. Some important PII needs to be shared across this new platform, but it is getting blocked by the DLP systems. Which of the following actions will BEST allow the PII to be shared with the secure application without compromising the organization's security posture?

- A. Configure the DLP policies to allow all PII
- B. Configure the firewall to allow all ports that are used by this application
- C. Configure the antivirus software to allow the application
- D. Configure the DLP policies to whitelist this application with the specific PII
- E. Configure the application to encrypt the PII

**Answer: D**

#### NEW QUESTION 15

A security analyst is reviewing the following attack log output:

```
user comptia\john.smith attempted login with the password password123
user comptia\jane.doe attempted login with the password password123
user comptia\user.one attempted login with the password password123
user comptia\user.two attempted login with the password password123
user comptia\user.three attempted login with the password password123

user comptia\john.smith attempted login with the password password234
user comptia\jane.doe attempted login with the password password234
user comptia\user.one attempted login with the password password234
user comptia\user.two attempted login with the password password234
user comptia\user.three attempted login with the password password234
```

Which of the following types of attacks does this MOST likely represent?

- A. Rainbow table
- B. Brute-force
- C. Password-spraying
- D. Dictionary

**Answer: C**

#### NEW QUESTION 18

Which of the following relates to applications and systems that are used within an organization without consent or approval?

- A. Shadow IT

- B. OSINT
- C. Dark web
- D. Insider threats

**Answer:** A

#### NEW QUESTION 22

Which of the following job roles would sponsor data quality and data entry initiatives that ensure business and regulatory requirements are met?

- A. The data owner
- B. The data processor
- C. The data steward
- D. The data privacy officer.

**Answer:** C

#### NEW QUESTION 24

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

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

**Answer:** A

#### NEW QUESTION 28

A malicious actor recently penetration a company's network and moved laterally to the datacenter. Upon investigation, a forensics firm wants to know what was in the memory on the compromised server. Which of the following files should be given to the forensics firm?

- A. Security
- B. Application
- C. Dump
- D. Syslog

**Answer:** C

#### NEW QUESTION 32

A network engineer is troubleshooting wireless network connectivity issues that were reported by users. The issues are occurring only in the section of the building that is closest to the parking lot. Users are intermittently experiencing slow speeds when accessing websites and are unable to connect to network drives. The issues appear to increase when laptop users return desks after using their devices in other areas of the building. There have also been reports of users being required to enter their credentials on web pages in order to gain access to them. Which of the following is the MOST likely cause of this issue?

- A. An external access point is engaging in an evil-twin attack.
- B. The signal on the WAP needs to be increased in that section of the building.
- C. The certificates have expired on the devices and need to be reinstalled.
- D. The users in that section of the building are on a VLAN that is being blocked by the firewall.

**Answer:** A

#### NEW QUESTION 37

Some laptops recently went missing from a locked storage area that is protected by keyless RFID-enabled locks. There is no obvious damage to the physical space. The security manager identifies who unlocked the door, however, human resources confirms the employee was on vacation at the time of the incident. Which of the following describes what MOST likely occurred?

- A. The employee's physical access card was cloned.
- B. The employee is colluding with human resources
- C. The employee's biometrics were harvested
- D. A criminal used lock picking tools to open the door.

**Answer:** A

#### NEW QUESTION 39

A security analyst is performing a packet capture on a series of SOAP HTTP requests for a security assessment. The analyst redirects the output to a file. After the capture is complete, the analyst needs to review the first transactions quickly and then search the entire series of requests for a particular string. Which of the following would be BEST to use to accomplish the task? (Select TWO).

- A. head
- B. Tcpdump
- C. grep
- D. rail
- E. curl
- F. openssl
- G. dd

**Answer:** AB

#### NEW QUESTION 41

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

**Answer:** A

#### NEW QUESTION 43

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

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

**Answer:** B

#### NEW QUESTION 48

When used at the design stage, which of the following improves the efficiency, accuracy, and speed of a database?

- A. Tokenization
- B. Data masking
- C. Normalization
- D. Obfuscation

**Answer:** C

#### NEW QUESTION 50

Which of the following would BEST identify and remediate a data-loss event in an enterprise using third-party, web-based services and file-sharing platforms?

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

**Answer:** D

#### NEW QUESTION 51

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 earlier. This change lasted eight hours. Which of the following attacks was MOST likely used?

- A. Man-in-the-middle
- B. Spear-phishing
- C. Evil twin
- D. DNS poisoning

**Answer:** D

#### NEW QUESTION 52

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

##### INSTRUCTIONS

Not all attacks and remediation actions will be used.

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

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

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

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

**NEW QUESTION 55**

A security analyst needs to determine how an attacker was able to use User3 to gain a foothold within a company's network. The company's lockout policy requires that an account be locked out for a minimum of 15 minutes after three unsuccessful attempts. While reviewing the log files, the analyst discovers the following:

```

3/16/20 3:31:10 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:11 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:12 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:13 AM Audit Failure: CompanyNetwork\User1 Account locked out.
3/16/20 3:31:14 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:15 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:16 AM Audit Failure: CompanyNetwork\User2 Account locked out.
3/16/20 3:31:18 AM Audit Failure: CompanyNetwork\User3 Unknown username or bad password.
3/16/20 3:31:19 AM Audit Failure: CompanyNetwork\User3 Unknown username or bad password.
3/16/20 3:31:20 AM Audit Failure: CompanyNetwork\User3 Successful logon.
3/16/20 3:31:22 AM Audit Success: CompanyNetwork\User3 Successful logon.
3/16/20 3:31:22 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.
3/16/20 3:32:40 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.
3/16/20 3:33:25 AM Audit Success: CompanyNetwork\User4 Successful logon.

```

Which of the following attacks MOST likely occurred?

- A. Dictionary
- B. Credential-stuffing
- C. Password-spraying
- D. Brute-force

**Answer: D**

**NEW QUESTION 60**

A network technician is installing a guest wireless network at a coffee shop. When a customer purchases an item, the password for the wireless network is printed

on the recent so the customer can log in. Which of the following will the technician MOST likely configure to provide the highest level of security with the least amount of overhead?

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

**Answer: A**

#### NEW QUESTION 61

The facilities supervisor for a government agency is concerned about unauthorized access to environmental systems in the event the staff WiFi network is breached. Which of the following would BEST address this security concern?

- A. install a smart meter on the staff WiFi.
- B. Place the environmental systems in the same DHCP scope as the staff WiFi.
- C. Implement Zigbee on the staff WiFi access points.
- D. Segment the staff WiFi network from the environmental systems network.

**Answer: D**

#### NEW QUESTION 62

Joe, a user at a company, clicked an email link led to a website that infected his workstation. Joe, was connected to the network, and the virus spread to the network shares. The protective measures failed to stop this virus, and it has continued to evade detection. Which of the following should administrator implement to protect the environment from this malware?

- A. Install a definition-based antivirus.
- B. Implement an IDS/IPS
- C. Implement a heuristic behavior-detection solution.
- D. Implement CASB to protect the network shares.

**Answer: C**

#### NEW QUESTION 65

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

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

**Answer: D**

#### NEW QUESTION 68

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

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

**Answer: B**

#### NEW QUESTION 72

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

**Answer: AC**

#### NEW QUESTION 74

A Chief Information Security Officer (CISO) is concerned about the organization's ability to continue business operation in the event of a prolonged DDoS attack on its local datacenter that consumes database resources. Which of the following will the CISO MOST likely recommend to mitigate this risk?

- A. Upgrade the bandwidth available into the datacenter
- B. Implement a hot-site failover location
- C. Switch to a complete SaaS offering to customers
- D. Implement a challenge response test on all end-user queries

**Answer:** B

**NEW QUESTION 76**

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

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

**Answer:** D

**NEW QUESTION 81**

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

**Answer:** C

**NEW QUESTION 84**

An analyst needs to set up a method for securely transferring files between systems. One of the requirements is to authenticate the IP header and the payload. Which of the following services would BEST meet the criteria?

- A. TLS
- B. PFS
- C. ESP
- D. AH

**Answer:** A

**NEW QUESTION 86**

A security analyst needs to implement an MDM solution for BYOD users that will allow the company to retain control over company emails residing on the devices and limit data exfiltration that might occur if the devices are lost or stolen. Which of the following would BEST meet these requirements? (Select TWO).

- A. Full-device encryption
- B. Network usage rules
- C. Geofencing
- D. Containerization
- E. Application whitelisting
- F. Remote control

**Answer:** AB

**NEW QUESTION 91**

An organization has hired a security analyst to perform a penetration test. The analyst captures 1Gb worth of inbound network traffic to the server and transfer the pcap back to the machine for analysis. Which of the following tools should the analyst use to further review the pcap?

- A. Nmap
- B. cURL
- C. Netcat
- D. Wireshark

**Answer:** D

**NEW QUESTION 96**

Which of the following organizational policies are MOST likely to detect fraud that is being conducted by existing employees? (Select TWO).

- A. Offboarding
- B. Mandatory vacation
- C. Job rotation
- D. Background checks
- E. Separation of duties
- F. Acceptable use

**Answer:** BC

**NEW QUESTION 98**

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

- A. Dual power supply

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

**Answer:** AB

#### NEW QUESTION 103

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

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

**Answer:** A

#### NEW QUESTION 106

A user is concerned that a web application will not be able to handle unexpected or random input without crashing. Which of the following BEST describes the type of testing the user should perform?

- A. Code signing
- B. Fuzzing
- C. Manual code review
- D. Dynamic code analysis

**Answer:** D

#### NEW QUESTION 108

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

An incident responder learns the following information:

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

Which of the following is the MOST likely root cause?

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

**Answer:** C

#### NEW QUESTION 110

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

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

**Answer:** B

#### NEW QUESTION 112

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

- A. Security awareness training
- B. Frequency of NIDS updates
- C. Change control procedures
- D. EDR reporting cycle

**Answer:** A

#### NEW QUESTION 114

A security manager for a retailer needs to reduce the scope of a project to comply with PCI DSS. The PCI data is located in different offices than where credit cards are accepted. All the offices are connected via MPLS back to the primary datacenter. Which of the following should the security manager implement to achieve the objective?

- A. Segmentation
- B. Containment
- C. Geofencing

D. Isolation

**Answer:** A

#### NEW QUESTION 116

An organization's RPO for a critical system is two hours. The system is used Monday through Friday, from 9:00 am to 5:00 pm. Currently, the organization performs a full backup every Saturday that takes four hours to complete. Which of the following additional backup implementations would be the BEST way for the analyst to meet the business requirements?

- A. Incremental backups Monday through Friday at 6:00 p.m and differential backups hourly
- B. Full backups Monday through Friday at 6:00 p.m and incremental backups hourly.
- C. incremental backups Monday through Friday at 6:00 p.m and full backups hourly.
- D. Full backups Monday through Friday at 6:00 p.m and differential backups hourly.

**Answer:** A

#### NEW QUESTION 117

A security analyst sees the following log output while reviewing web logs:

```
[02/Feb/2019:03:39:21 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?query=%2f..%2f..%2f..%2fetc%2fpasswd HTTP/1.0" 80 200 200  
[02/Feb/2019:03:39:25 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?query=../../../../etc/passwd HTTP/1.0" 80 200 200
```

Which of the following mitigation strategies would be BEST to prevent this attack from being successful?

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

**Answer:** B

#### NEW QUESTION 118

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

- > www.company.com (main website)
- > contactus.company.com (for locating a nearby location)
- > quotes.company.com (for requesting a price quote)

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

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

**Answer:** B

#### NEW QUESTION 123

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

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

**Answer:** C

#### NEW QUESTION 125

Which of the following would be BEST to establish between organizations to define the responsibilities of each party outline the key deliverables and include monetary penalties for breaches to manage third-party risk?

- A. An ARO
- B. An MOU
- C. An SLA
- D. A BPA

**Answer:** B

#### NEW QUESTION 128

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

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

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

**Answer:** AD

#### NEW QUESTION 131

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

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

**Answer:** B

#### NEW QUESTION 135

A vulnerability assessment report will include the CVSS score of the discovered vulnerabilities because the score allows the organization to better.

- A. validate the vulnerability exists in the organization's network through penetration testing
- B. research the appropriate mitigation techniques in a vulnerability database
- C. find the software patches that are required to mitigate a vulnerability
- D. prioritize remediation of vulnerabilities based on the possible impact.

**Answer:** D

#### NEW QUESTION 138

An organization's help desk is flooded with phone calls from users stating they can no longer access certain websites. The help desk escalates the issue to the security team, as these websites were accessible the previous day. The security analysts run the following command: `ipconfig /flushdns`, but the issue persists. Finally, an analyst changes the DNS server for an impacted machine, and the issue goes away. Which of the following attacks MOST likely occurred on the original DNS server?

- A. DNS cache poisoning
- B. Domain hijacking
- C. Distributed denial-of-service
- D. DNS tunneling

**Answer:** B

#### NEW QUESTION 142

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

- A. The DNS logs
- B. The web server logs
- C. The SIP traffic logs
- D. The SNMP logs

**Answer:** A

#### NEW QUESTION 146

A company has limited storage available and online presence that cannot 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, which being mindful of the limited available storage space?

- A. Implement fulltape backup every Sunday at 8:00 p.m and perform nightly tape rotations.
- B. Implement different backups every Sunday at 8:00 and nightly incremental backups at 8:00 p.m
- C. Implement nightly full backups every Sunday at 8:00 p.m
- D. Implement full backups every Sunday at 8:00 p.m and nightly differential backups at 8:00

**Answer:** B

#### NEW QUESTION 147

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

- A. data controller.
- B. data owner
- C. data custodian.
- D. data processor

**Answer:** D

#### NEW QUESTION 149

A recent malware outbreak across a subnet included successful rootkit installations on many PCs, ensuring persistence by rendering remediation efforts ineffective. Which of the following would BEST detect the presence of a rootkit in the future?

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

**Answer: C**

#### NEW QUESTION 152

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 experience?

- A. SQL injection
- B. Cross-site scripting
- C. Pass-the-hash
- D. Directory traversal

**Answer: B**

#### NEW QUESTION 154

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

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

**Answer: C**

#### NEW QUESTION 159

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

- A. The GPS location
- B. When the file was deleted
- C. The total number of print jobs
- D. The number of copies made

**Answer: A**

#### NEW QUESTION 163

An organization suffered an outage and a critical system took 90 minutes to come back online. Though there was no data loss during the outage, the expectation was that the critical system would be available again within 60 minutes Which of the following is the 60-minute expectation an example of:

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

**Answer: D**

#### NEW QUESTION 167

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

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

Which of the following can the security analyst conclude?

- A. A replay attack is being conducted against the application.
- B. An injection attack is being conducted against a user authentication system.
- C. A service account password may have been changed, resulting in continuous failed logins within the application.
- D. A credentialed vulnerability scanner attack is testing several CVEs against the application.

**Answer: C**

#### NEW QUESTION 170

Which of the following policies would help an organization identify and mitigate potential single points of failure in the company's IT/security operations?

- A. Least privilege
- B. Awareness training
- C. Separation of duties
- D. Mandatory vacation

**Answer: C**

#### NEW QUESTION 171

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

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

**Answer: A**

#### NEW QUESTION 174

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

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

**Answer: A**

#### NEW QUESTION 176

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

- A. Tabletop
- B. Parallel
- C. Full interruption
- D. Simulation

**Answer: D**

#### NEW QUESTION 180

A network engineer notices the VPN concentrator overloaded and crashes on days when there are a lot of remote workers. Senior management has placed greater importance on the availability of VPN resources for the remote workers than the security of the end users' traffic. Which of the following would be BEST to solve this issue?

- A. IPSec
- B. Always On
- C. Split tunneling
- D. L2TP

**Answer: B**

#### NEW QUESTION 182

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

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

**Answer: A**

#### NEW QUESTION 184

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

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

**Answer: B**

**NEW QUESTION 188**

A security analyst is reviewing a new website that will soon be made publicly available. The analyst sees the following in the URL:

`http://dev-site.comptia.org/home/show.php?sessionID=77276554&loc=us`

The analyst then sends an internal user a link to the new website for testing purposes, and when the user clicks the link, the analyst is able to browse the website with the following URL:

`http://dev-site.comptia.org/home/show.php?sessionID=98988475&loc=us` Which of the following application attacks is being tested?

- A. Pass-the-hash
- B. Session replay
- C. Object deference
- D. Cross-site request forgery

**Answer: B**

**NEW QUESTION 191**

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

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

**Answer: D**

**NEW QUESTION 193**

Local guidelines require that all information systems meet a minimum-security baseline to be compliant. Which of the following can security administrators use to assess their system configurations against the baseline?

- A. SOAR playbook
- B. Security control matrix
- C. Risk management framework
- D. Benchmarks

**Answer: D**

**NEW QUESTION 196**

A security analyst is investigation an incident that was first reported as an issue connecting to network shares and the internet, While reviewing logs and tool output, the analyst sees the following:

IP address	Physical address
10.0.0.1	00-18-21-ad-24-bc
10.0.0.114	01-31-a3-cd-23-ab
10.0.0.115	00-18-21-ad-24-bc
10.0.0.116	00-19-08-ba-07-da
10.0.0.117	01-12-21-ca-11-ad

Which of the following attacks has occurred?

- A. IP conflict
- B. Pass-the-hash
- C. MAC flooding
- D. Directory traversal
- E. ARP poisoning

**Answer: E**

**NEW QUESTION 199**

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

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

**Answer: A**

**NEW QUESTION 202**

A security analyst is reviewing information regarding recent vulnerabilities. Which of the following will the analyst MOST likely consult to validate which platforms have been affected?

- A. OSINT
- B. SIEM
- C. CVSS

D. CVE

**Answer:** D

**NEW QUESTION 203**

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

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

**Answer:** DF

**NEW QUESTION 208**

Which of the following scenarios would make a DNS sinkhole effective in thwarting an attack?

- A. An attacker is sniffing traffic to port 53, and the server is managed using unencrypted usernames and passwords.
- B. An organization is experiencing excessive traffic on port 53 and suspects an attacker is trying to DoS the domain name server.
- C. Malware trying to resolve an unregistered domain name to determine if it is running in an isolated sandbox
- D. Routing tables have been compromised, and an attacker is rerouting traffic to malicious websites

**Answer:** A

**NEW QUESTION 209**

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

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

**Answer:** C

**NEW QUESTION 214**

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

- A. Limit the use of third-party libraries.
- B. Prevent data exposure queries.
- C. Obfuscate the source code.
- D. Submit the application to QA before releasing it.

**Answer:** D

**NEW QUESTION 215**

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

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

**Answer:** B

**NEW QUESTION 217**

A software developer needs to perform code-execution testing, black-box testing, and non-functional testing on a new product before its general release. Which of the following BEST describes the tasks the developer is conducting?

- A. Verification
- B. Validation
- C. Normalization
- D. Staging

**Answer:** A

**NEW QUESTION 219**

The Chief Security Officer (CSO) at a major hospital wants to implement SSO to help improve in the environment patient data, particularly at shared terminals. The Chief Risk Officer (CRO) is concerned that training and guidance have been provided to frontline staff, and a risk analysis has not been performed. Which of the following is the MOST likely cause of the CRO's concerns?

- A. SSO would simplify username and password management, making it easier for hackers to pass guess accounts.

- B. SSO would reduce password fatigue, but staff would still need to remember more complex passwords.
- C. SSO would reduce the password complexity for frontline staff.
- D. SSO would reduce the resilience and availability of system if the provider goes offline.

**Answer:** D

#### NEW QUESTION 224

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

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

**Answer:** A

#### NEW QUESTION 225

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

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

**Answer:** A

#### NEW QUESTION 229

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. Ofboarding

**Answer:** D

#### NEW QUESTION 230

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. Oder of volatility
- D. A log analysis
- E. A right-to-audit clause

**Answer:** D

#### NEW QUESTION 234

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

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

**Answer:** D

#### NEW QUESTION 239

A startup company is using multiple SaaS and IaaS platforms to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?

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

**Answer:** C

#### NEW QUESTION 242

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.

**Commands**

```

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

**SSH Client**

?

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Commands**

```

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

**SSH Client**

```

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

**NEW QUESTION 243**

Which of the following would be BEST to establish between organizations that have agreed cooperate and are engaged in early discussion to define the responsibilities of each party, but do not want to establish a contractually binding agreement?

- A. An SLA
- B. AnNDA
- C. ABPA
- D. AnMOU

**Answer: D**

#### NEW QUESTION 248

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

**Answer: B**

#### NEW QUESTION 250

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

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

**Answer: C**

#### NEW QUESTION 253

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

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

**Answer: C**

#### NEW QUESTION 255

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 administration use?

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

**Answer: C**

#### NEW QUESTION 260

A database administrator needs to ensure all passwords are stored in a secure manner, so the administrator adds randomly generated data to each password before string. Which of the following techniques BEST explains this action?

- A. Predictability
- B. Key stretching
- C. Salting
- D. Hashing

**Answer: C**

#### NEW QUESTION 263

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

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

**Answer: B**

#### NEW QUESTION 267

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

**Answer: C**

**NEW QUESTION 269**

Which of the following types of controls is a turnstile?

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

**Answer: A**

**NEW QUESTION 272**

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

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

**Answer: C**

**NEW QUESTION 274**

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

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

**Answer: C**

**NEW QUESTION 276**

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

- A. The S/MIME plug-in is not enabled.
- B. The SLL certificate has expired.
- C. Secure IMAP was not implemented
- D. POP3S is not supported.

**Answer: A**

**NEW QUESTION 280**

A user recently attended an exposition and received some digital promotional materials. The user later noticed blue boxes popping up and disappearing on the computer, and reported receiving several spam emails, which the user did not open. Which of the following is MOST likely the cause of the reported issue?

- A. There was a drive-by download of malware
- B. The user installed a cryptominer
- C. The OS was corrupted
- D. There was malicious code on the USB drive

**Answer: D**

**NEW QUESTION 281**

A user reports constant lag and performance issues with the wireless network when working at a local coffee shop. A security analyst walks the user through an installation of Wireshark and gets a five-minute pcap to analyze. The analyst observes the following output:

No.	Time	Source	Destination	Protocol	Length	Info
1234	9.1195665	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=655, FN=0
1235	9.1265649	Sagemcom_87:9f:a3	Broadcast	802.11	39	Deauthentication, SN=655, FN=0
1236	9.2223212	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=657, FN=0

Which of the following attacks does the analyst MOST likely see in this packet capture?

- A. Session replay
- B. Evil twin
- C. Bluejacking
- D. ARP poisoning

**Answer: B**

#### NEW QUESTION 283

An organization hired a consultant to assist with an active attack, and the consultant was able to identify the compromised accounts and computers. Which of the following is the consultant MOST likely to recommend to prepare for eradication?

- A. Quarantining the compromised accounts and computers, only providing them with network access
- B. Segmenting the compromised accounts and computers into a honeynet so as to not alert the attackers.
- C. Isolating the compromised accounts and computers, cutting off all network and internet access.
- D. Logging off and deleting the compromised accounts and computers to eliminate attacker access.

**Answer: B**

#### NEW QUESTION 286

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

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

**Answer: C**

#### NEW QUESTION 288

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

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

**Answer: C**

#### NEW QUESTION 293

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

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

**Answer: A**

#### NEW QUESTION 295

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

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

**Answer: D**

#### NEW QUESTION 297

A security analyst is preparing a threat for an upcoming internal penetration test. The analyst needs to identify a method for determining the tactics, techniques, and procedures of a threat against the organization's network. Which of the following will the analyst MOST likely use to accomplish the objective?

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

**Answer: A**

#### NEW QUESTION 302

A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks. Which of the following methods would BEST prevent the exfiltration of data? (Select TWO).

- A. VPN
- B. Drive encryption
- C. Network firewall
- D. File level encryption
- E. USB blocker
- F. MFA

**Answer:** BE

**NEW QUESTION 306**

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

**Answer:** AB

**NEW QUESTION 308**

An engineer wants to access sensitive data from a corporate-owned mobile device. Personal data is not allowed on the device. Which of the following MDM configurations must be considered when the engineer travels for business?

- A. Screen locks
- B. Application management
- C. Geofencing
- D. Containerization

**Answer:** D

**NEW QUESTION 309**

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

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

**Answer:** A

**NEW QUESTION 312**

.....

## Relate Links

**100% Pass Your SY0-601 Exam with Examible Prep Materials**

<https://www.exambible.com/SY0-601-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>