



# CompTIA

## Exam Questions SY0-601

CompTIA Security+ Exam

#### NEW QUESTION 1

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 2

An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:

- Check-in/checkout of credentials
- The ability to use but not know the password
- Automated password changes
- Logging of access to credentials

Which of the following solutions would meet the requirements?

- A. OAuth 2.0
- B. Secure Enclave
- C. A privileged access management system
- D. An OpenID Connect authentication system

**Answer:** D

#### NEW QUESTION 3

A cybersecurity department purchased o new PAM solution. The team is planning to randomize the service account credentials of the Windows server first. Which of the following would be the BEST method to increase the security on the Linux server?

- A. Randomize the shared credentials
- B. Use only guest accounts to connect.
- C. Use SSH keys and remove generic passwords
- D. Remove all user accounts.

**Answer:** C

#### NEW QUESTION 4

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 5

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

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

**Answer:** A

#### NEW QUESTION 6

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 7

A security engineer needs to enhance MFA access to sensitive areas in a building. A key card and fingerprint scan are already in use. Which of the following would add another factor of authentication?

- A. Hard token

- B. Retina scan
- C. SMS text
- D. Keypad PIN

**Answer:** B

#### NEW QUESTION 8

A user contacts the help desk to report the following:

- Two days ago, a pop-up browser window prompted the user for a name and password after connecting to the corporate wireless SSID. This had never happened before, but the user entered the information as requested.
- The user was able to access the Internet but had trouble accessing the department share until the next day.
- The user is now getting notifications from the bank about unauthorized transactions. Which of the following attack vectors was MOST likely used in this scenario?

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

**Answer:** A

#### NEW QUESTION 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 company recently experienced a data breach and the source was determined to be an executive who was charging a phone in a public area. Which of the following would MOST likely have prevented this breach?

- A. A firewall
- B. A device pin
- C. A USB data blocker
- D. Biometrics

**Answer:** C

#### NEW QUESTION 12

A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?

- A. Segmentation
- B. Firewall whitelisting
- C. Containment
- D. isolation

**Answer:** A

#### NEW QUESTION 17

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 22

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

- A. Shadow IT
- B. OSINT
- C. Dark web
- D. Insider threats

**Answer: A**

#### NEW QUESTION 23

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 26

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 31

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

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

**Answer: C**

#### NEW QUESTION 33

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 34

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

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

**Answer:** AB

#### NEW QUESTION 35

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 36

A recent audit uncovered a key finding regarding the use of a specific encryption standard in a web application that is used to communicate with business customers. Due to the technical limitations of its customers, the company is unable to upgrade the encryption standard. Which of the following types of controls should be used to reduce the risk created by this scenario?

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

**Answer:** D

#### NEW QUESTION 39

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 40

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

- 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 42

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

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

**Answer: B**

#### NEW QUESTION 47

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\User2 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 Unknown username or bad password.
3/16/20 3:31:22 AM Audit Success: CompanyNetwork\User3 Successful login.
3/16/20 3:31:22 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.
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 Successful login.
3/16/20 3:33:25 AM Audit Success: CompanyNetwork\User4 Successful login.

```

Which of the following attacks MOST likely occurred?

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

**Answer:** D

#### NEW QUESTION 49

A symmetric encryption algorithm is BEST suited for:

- A. key-exchange scalability.
- B. protecting large amounts of data.
- C. providing hashing capabilities,
- D. implementing non-repudiation.

**Answer:** D

#### NEW QUESTION 50

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

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

**Answer:** A

#### NEW QUESTION 52

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 53

A company recently set up an e-commerce portal to sell its product online. The company wants to start accepting credit cards for payment, which requires compliance with a security standard. Which of the following standards must the company comply with before accepting credit cards on its e-commerce platform?

- A. PCI DSS
- B. ISO 22301
- C. ISO 27001
- D. NIST CSF

**Answer:** A

#### NEW QUESTION 57

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 58

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 61

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 63

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 67

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 70

A worldwide manufacturing company has been experiencing email account compromised. In one incident, a user logged in from the corporate office in France, but then seconds later, the same user account attempted a login from Brazil. Which of the following account policies would BEST prevent this type of attack?

- A. Network location
- B. Impossible travel time
- C. Geolocation
- D. Geofencing

**Answer: D**

#### NEW QUESTION 75

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

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

**Answer: C**

#### NEW QUESTION 78

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

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

**Answer: B**

#### NEW QUESTION 79

A security analyst needs to complete an assessment. The analyst is logged into a server and must use native tools to map services running on it to the server's listening ports. Which of the following tools can BEST accomplish this task?

- A. Netcat
- B. Netstat
- C. Nmap
- D. Nessus

Answer: B

#### NEW QUESTION 81

A security analyst has been asked to investigate a situation after the SOC started to receive alerts from the SIEM. The analyst first looks at the domain controller and finds the following events:

Keywords	Date and time	Source	Event ID
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:22 PM	Microsoft Windows security auditing	4771

To better understand what is going on, the analyst runs a command and receives the following output:

<u>name</u>	<u>lastbadpasswordattempt</u>	<u>badpwdcount</u>
John.Smith	12/26/2019 11:37:21 PM	7
Joe.Jones	12/26/2019 11:37:21 PM	13
Michael.Johnson	12/26/2019 11:37:22 PM	8
Mary.Wilson	12/26/2019 11:37:22 PM	8
Jane.Brown	12/26/2019 11:37:23 PM	12

Based on the analyst's findings, which of the following attacks is being executed?

- A. Credential harvesting
- B. Keylogger
- C. Brute-force
- D. Spraying

Answer: D

#### NEW QUESTION 85

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 89

A company uses wireless for all laptops and keeps a very detailed record of its assets, along with a comprehensive list of devices that are authorized to be on the wireless network. The Chief Information Officer (CIO) is concerned about a script kiddie potentially using an unauthorized device to brute force the wireless PSK and obtain access to the internal network. Which of the following should the company implement to BEST prevent this from occurring?

- A. A BPDU guard
- B. WPA-EAP
- C. IP filtering
- D. A WIDS

Answer: B

#### NEW QUESTION 91

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 data? (Select TWO)

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

Answer: BE

#### NEW QUESTION 92

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 94

An auditor is performing an assessment of a security appliance with an embedded OS that was vulnerable during the last two assessments. Which of the following BEST explains the appliance's vulnerable state?

- A. The system was configured with weak default security settings.
- B. The device uses weak encryption ciphers.
- C. The vendor has not supplied a patch for the appliance.
- D. The appliance requires administrative credentials for the assessment.

**Answer:** C

#### NEW QUESTION 97

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

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

**Answer:** B

#### NEW QUESTION 98

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

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

**Answer:** EF

#### NEW QUESTION 102

A security engineer needs to Implement the following requirements:

- All Layer 2 switches should leverage Active Directory for authentication.
- All Layer 2 switches should use local fallback authentication If Active Directory Is offline.
- All Layer 2 switches are not the same and are manufactured by several vendors.

Which of the following actions should the engineer take to meet these requirements? (Select TWO).

- A. Implement RADIUS.
- B. Configure AAA on the switch with local login as secondary.
- C. Configure port security on the switch with the secondary login method.
- D. Implement TACACS+
- E. Enable the local firewall on the Active Directory server.
- F. Implement a DHCP server.

**Answer:** AB

#### NEW QUESTION 107

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 111

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





**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 132**

An employee has been charged with fraud and is suspected of using corporate assets. As authorities collect evidence, and to preserve the admissibility of the evidence, which of the following forensic techniques should be used?

- A. Order of volatility
- B. Data recovery
- C. Chain of custody
- D. Non-repudiation

**Answer: C**

**NEW QUESTION 137**

A company's Chief Information Security Officer (CISO) recently warned the security manager that the company's Chief Executive Officer (CEO) is planning to publish a controversial opinion article in a national newspaper, which may result in new cyberattacks Which of the following would be BEST for the security manager to use in a threat mode?

- A. Hacktivists
- B. White-hat hackers
- C. Script kiddies
- D. Insider threats

**Answer: A**

**NEW QUESTION 142**

A root cause analysis reveals that a web application outage was caused by one of the company's developers uploading a newer version of the third-party libraries that were shared among several applications. Which of the following implementations would be BEST to prevent the issue from reoccurring?

- A. CASB
- B. SWG
- C. Containerization
- D. Automated failover

**Answer: C**

**NEW QUESTION 143**

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 145**

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

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

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

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

**Answer: D**

**NEW QUESTION 150**

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

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

**Answer:** C

#### NEW QUESTION 152

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

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

**Answer:** C

#### NEW QUESTION 153

The IT department at a university is concerned about professors placing servers on the university network in an attempt to bypass security controls. Which of the following BEST represents this type of threat?

- A. A script kiddie
- B. Shadow IT
- C. Hacktivism
- D. White-hat

**Answer:** B

#### NEW QUESTION 156

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

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

**Answer:** D

#### NEW QUESTION 160

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

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

**Answer:** AD

#### NEW QUESTION 163

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 166

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

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

**Answer:** D

**NEW QUESTION 168**

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 173**

A company's Chief Information Office (CIO) is meeting with the Chief Information Security Officer (CISO) to plan some activities to enhance the skill levels of the company's developers. Which of the following would be MOST suitable for training the developers'?

- A. A capture-the-flag competition
- B. A phishing simulation
- C. Physical security training
- D. Baste awareness training

**Answer: B**

**NEW QUESTION 176**

After entering a username and password, and administrator must gesture on a touch screen. Which of the following demonstrates what the administrator is providing?

- A. Multifactor authentication
- B. Something you can do
- C. Biometric
- D. Two-factor authentication

**Answer: D**

**NEW QUESTION 178**

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 183**

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 185**

A security administrator suspects an employee has been emailing proprietary information to a competitor. Company policy requires the administrator to capture an exact copy of the employee's hard disk. Which of the following should the administrator use?

- A. dd
- B. chmod
- C. dnsenum
- D. logger

**Answer: A**

**NEW QUESTION 190**

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

- A. A malicious USB was introduced by an unsuspecting employee.
- B. The ICS firmware was outdated
- C. A local machine has a RAT installed.

D. The HVAC was connected to the maintenance vendor.

**Answer:** A

#### NEW QUESTION 191

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 194

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

A)

```
http://sample.url.com/<script>Please-Visit-Our-Phishing-Site</script>
```

B)

```
http://sample.url.com/someotherpageonsite/../../../../etc/shadow
```

C)

```
http://sample.url.com/select-from-database-where-password-null
```

D)

```
http://redirect.sameple.url.sampleurl.com/malicious-dns-redirect
```

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

**Answer:** B

#### NEW QUESTION 199

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 200

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

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

**Answer:** B

#### NEW QUESTION 203

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 205

A network administrator has been asked to install an IDS to improve the security posture of an organization. Which of the following control types is an IDS?

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

**Answer:** C

#### NEW QUESTION 208

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 213

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 218

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 222

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 227

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

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

**Answer:** E

#### NEW QUESTION 229

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

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

**Answer:** A

#### NEW QUESTION 234

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

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

Which of the following attacks has occurred?

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

**Answer: E**

#### NEW QUESTION 238

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 241

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 242

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

```
Hello everyone,  
I am having the same problem with my server. Can you help me?  
  
<script type="text/javascript" src=http://website.com/user.js>  
Onload=sqlexec();  
</script>  
  
Thank you,  
  
Joe
```

Which of the following BEST describes the attack that was attempted against the forum readers?

- A. SOU attack
- B. DLL attack
- C. XSS attack
- D. API attack

**Answer: C**

#### NEW QUESTION 246

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

- A. Geolocation
- B. Time-of-day restrictions
- C. Certificates
- D. Tokens

- E. Geotagging
- F. Role-based access controls

**Answer:** AE

#### NEW QUESTION 250

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 251

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

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

**Answer:** A

#### NEW QUESTION 252

An organization has implemented a policy requiring the use of conductive metal lockboxes for personal electronic devices outside of a secure research lab. Which of the following did the organization determine to be the GREATEST risk to intellectual property when creating this policy?

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

**Answer:** D

#### NEW QUESTION 256

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 261

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 264

An incident response technician collected a mobile device during an investigation. Which of the following should the technician do to maintain chain of custody?

- A. Document the collection and require a sign-off when possession changes.
- B. Lock the device in a safe or other secure location to prevent theft or alteration.
- C. Place the device in a Faraday cage to prevent corruption of the data.
- D. Record the collection in a blockchain-protected public ledger.

**Answer:** A

#### NEW QUESTION 266

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

- Answer: D**

A security engineer is setting up passwordless authentication for the first time. INSTRUCTIONS

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

A. Mastered  
B. Not Mastered

**Answer: A**

**Explanation:**

NEW QUESTION 275

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 280

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

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

**Answer:** DE

#### NEW QUESTION 285

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 289

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

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

**Answer:** A

#### NEW QUESTION 291

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 296

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 297

A forensics investigator is examining a number of unauthorized payments that were reported on the company's website. Some unusual log entries show users received an email for an unwanted mailing list and clicked on a link to attempt to unsubscribe. One of the users reported the email to the phishing team, and the forwarded email revealed the link to be:



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

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

D. XSRF

**Answer:** B

#### NEW QUESTION 302

An organization routes all of its traffic through a VPN. Most users are remote and connect into a corporate datacenter that houses confidential information. There is a firewall at the Internet border followed by a DLP appliance, the VPN server and the datacenter itself. Which of the following is the WEAKEST design element?

- A. The DLP appliance should be integrated into a NGFW.
- B. Split-tunnel connections can negatively impact the DLP appliance's performance.
- C. Encrypted VPN traffic will not be inspected when entering or leaving the network.
- D. Adding two hops in the VPN tunnel may slow down remote connections.

**Answer:** C

#### NEW QUESTION 306

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

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

**Answer:** C

#### NEW QUESTION 311

The CSIRT is reviewing the lessons learned from a recent incident. A worm was able to spread unhindered throughout the network and infect a large number of computers and servers. Which of the following recommendations would be BEST to mitigate the impacts of a similar incident in the future?

- A. Install a NIDS device at the boundary.
- B. Segment the network with firewalls.
- C. Update all antivirus signatures daily.
- D. Implement application blacklisting.

**Answer:** B

#### NEW QUESTION 312

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 316

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

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

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

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

**Answer:** DE

#### NEW QUESTION 318

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 320

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 324

.....

## 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 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 2

An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:

- Check-in/checkout of credentials
- The ability to use but not know the password
- Automated password changes
- Logging of access to credentials

Which of the following solutions would meet the requirements?

- A. OAuth 2.0
- B. Secure Enclave
- C. A privileged access management system
- D. An OpenID Connect authentication system

**Answer:** D

#### NEW QUESTION 3

A cybersecurity department purchased o new PAM solution. The team is planning to randomize the service account credentials of the Windows server first. Which of the following would be the BEST method to increase the security on the Linux server?

- A. Randomize the shared credentials
- B. Use only guest accounts to connect.
- C. Use SSH keys and remove generic passwords
- D. Remove all user accounts.

**Answer:** C

#### NEW QUESTION 4

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 5

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

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

**Answer:** A

#### NEW QUESTION 6

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 7

A security engineer needs to enhance MFA access to sensitive areas in a building. A key card and fingerprint scan are already in use. Which of the following would add another factor of authentication?

- A. Hard token

- B. Retina scan
- C. SMS text
- D. Keypad PIN

**Answer:** B

#### NEW QUESTION 8

A user contacts the help desk to report the following:

- Two days ago, a pop-up browser window prompted the user for a name and password after connecting to the corporate wireless SSID. This had never happened before, but the user entered the information as requested.
- The user was able to access the Internet but had trouble accessing the department share until the next day.
- The user is now getting notifications from the bank about unauthorized transactions. Which of the following attack vectors was MOST likely used in this scenario?

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

**Answer:** A

#### NEW QUESTION 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 company recently experienced a data breach and the source was determined to be an executive who was charging a phone in a public area. Which of the following would MOST likely have prevented this breach?

- A. A firewall
- B. A device pin
- C. A USB data blocker
- D. Biometrics

**Answer:** C

#### NEW QUESTION 12

A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?

- A. Segmentation
- B. Firewall whitelisting
- C. Containment
- D. isolation

**Answer:** A

#### NEW QUESTION 17

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 22

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

- A. Shadow IT
- B. OSINT
- C. Dark web
- D. Insider threats

**Answer:** A

#### NEW QUESTION 23

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 26

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 31

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

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

**Answer:** C

#### NEW QUESTION 33

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 34

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

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

**Answer:** AB

#### NEW QUESTION 35

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 36

A recent audit uncovered a key finding regarding the use of a specific encryption standard in a web application that is used to communicate with business customers. Due to the technical limitations of its customers, the company is unable to upgrade the encryption standard. Which of the following types of controls should be used to reduce the risk created by this scenario?

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

**Answer:** D

#### NEW QUESTION 39

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 40

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

- 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	<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>

#### NEW QUESTION 42

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

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

**Answer: B**

#### NEW QUESTION 47

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\User2 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 Unknown username or bad password.
3/16/20 3:31:22 AM Audit Success: CompanyNetwork\User3 Successful login.
3/16/20 3:31:22 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.
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 Successful login.
3/16/20 3:33:25 AM Audit Success: CompanyNetwork\User4 Successful login.
  
```

Which of the following attacks MOST likely occurred?

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

**Answer:** D

#### NEW QUESTION 49

A symmetric encryption algorithm is BEST suited for:

- A. key-exchange scalability.
- B. protecting large amounts of data.
- C. providing hashing capabilities,
- D. implementing non-repudiation.

**Answer:** D

#### NEW QUESTION 50

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

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

**Answer:** A

#### NEW QUESTION 52

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 53

A company recently set up an e-commerce portal to sell its product online. The company wants to start accepting credit cards for payment, which requires compliance with a security standard. Which of the following standards must the company comply with before accepting credit cards on its e-commerce platform?

- A. PCI DSS
- B. ISO 22301
- C. ISO 27001
- D. NIST CSF

**Answer:** A

#### NEW QUESTION 57

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 58

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 61

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 63

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 67

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 70

A worldwide manufacturing company has been experiencing email account compromised. In one incident, a user logged in from the corporate office in France, but then seconds later, the same user account attempted a login from Brazil. Which of the following account policies would BEST prevent this type of attack?

- A. Network location
- B. Impossible travel time
- C. Geolocation
- D. Geofencing

**Answer:** D

#### NEW QUESTION 75

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

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

**Answer:** C

#### NEW QUESTION 78

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

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

**Answer:** B

#### NEW QUESTION 79

A security analyst needs to complete an assessment. The analyst is logged into a server and must use native tools to map services running on it to the server's listening ports. Which of the following tools can BEST accomplish this task?

- A. Netcat
- B. Netstat
- C. Nmap
- D. Nessus



Answer: B

#### NEW QUESTION 81

A security analyst has been asked to investigate a situation after the SOC started to receive alerts from the SIEM. The analyst first looks at the domain controller and finds the following events:

Keywords	Date and time	Source	Event ID
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:22 PM	Microsoft Windows security auditing	4771

To better understand what is going on, the analyst runs a command and receives the following output:

name	lastbadpasswordattempt	badpwdcount
John.Smith	12/26/2019 11:37:21 PM	7
Joe.Jones	12/26/2019 11:37:21 PM	13
Michael.Johnson	12/26/2019 11:37:22 PM	8
Mary.Wilson	12/26/2019 11:37:22 PM	8
Jane.Brown	12/26/2019 11:37:23 PM	12

Based on the analyst's findings, which of the following attacks is being executed?

- A. Credential harvesting
- B. Keylogger
- C. Brute-force
- D. Spraying

Answer: D

#### NEW QUESTION 85

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 89

A company uses wireless for all laptops and keeps a very detailed record of its assets, along with a comprehensive list of devices that are authorized to be on the wireless network. The Chief Information Officer (CIO) is concerned about a script kiddie potentially using an unauthorized device to brute force the wireless PSK and obtain access to the internal network. Which of the following should the company implement to BEST prevent this from occurring?

- A. A BPDU guard
- B. WPA-EAP
- C. IP filtering
- D. A WIDS

Answer: B

#### NEW QUESTION 91

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 data? (Select TWO)

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

Answer: BE

#### NEW QUESTION 92

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 94

An auditor is performing an assessment of a security appliance with an embedded OS that was vulnerable during the last two assessments. Which of the following BEST explains the appliance's vulnerable state?

- A. The system was configured with weak default security settings.
- B. The device uses weak encryption ciphers.
- C. The vendor has not supplied a patch for the appliance.
- D. The appliance requires administrative credentials for the assessment.

**Answer:** C

#### NEW QUESTION 97

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

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

**Answer:** B

#### NEW QUESTION 98

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

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

**Answer:** EF

#### NEW QUESTION 102

A security engineer needs to Implement the following requirements:

- All Layer 2 switches should leverage Active Directory for authentication.
- All Layer 2 switches should use local fallback authentication If Active Directory Is offline.
- All Layer 2 switches are not the same and are manufactured by several vendors.

Which of the following actions should the engineer take to meet these requirements? (Select TWO).

- A. Implement RADIUS.
- B. Configure AAA on the switch with local login as secondary.
- C. Configure port security on the switch with the secondary login method.
- D. Implement TACACS+
- E. Enable the local firewall on the Active Directory server.
- F. Implement a DHCP server.

**Answer:** AB

#### NEW QUESTION 107

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 111

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



- Answer: B**

A RAT that was used to compromise an organization's banking credentials was found on a user's computer. The RAT evaded antivirus detection. It was installed by a user who has local administrator rights to the system as part of a remote management tool set. Which of the following recommendations would BEST prevent this from reoccurring?

- Answer: C**

**Answer: B**

**Answer: B**

**Answer: C**

**Answer: B**

#### 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 132

An employee has been charged with fraud and is suspected of using corporate assets. As authorities collect evidence, and to preserve the admissibility of the evidence, which of the following forensic techniques should be used?

- A. Order of volatility
- B. Data recovery
- C. Chain of custody
- D. Non-repudiation

**Answer: C**

#### NEW QUESTION 137

A company's Chief Information Security Officer (CISO) recently warned the security manager that the company's Chief Executive Officer (CEO) is planning to publish a controversial opinion article in a national newspaper, which may result in new cyberattacks Which of the following would be BEST for the security manager to use in a threat mode?

- A. Hacktivists
- B. White-hat hackers
- C. Script kiddies
- D. Insider threats

**Answer: A**

#### NEW QUESTION 142

A root cause analysis reveals that a web application outage was caused by one of the company's developers uploading a newer version of the third-party libraries that were shared among several applications. Which of the following implementations would be BEST to prevent the issue from reoccurring?

- A. CASB
- B. SWG
- C. Containerization
- D. Automated failover

**Answer: C**

#### NEW QUESTION 143

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 145

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

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

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

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

**Answer: D**

#### NEW QUESTION 150

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

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

**Answer:** C

#### NEW QUESTION 152

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

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

**Answer:** C

#### NEW QUESTION 153

The IT department at a university is concerned about professors placing servers on the university network in an attempt to bypass security controls. Which of the following BEST represents this type of threat?

- A. A script kiddie
- B. Shadow IT
- C. Hacktivism
- D. White-hat

**Answer:** B

#### NEW QUESTION 156

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

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

**Answer:** D

#### NEW QUESTION 160

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

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

**Answer:** AD

#### NEW QUESTION 163

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 166

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

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

**Answer:** D

**NEW QUESTION 168**

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 173**

A company's Chief Information Office (CIO) is meeting with the Chief Information Security Officer (CISO) to plan some activities to enhance the skill levels of the company's developers. Which of the following would be MOST suitable for training the developers'?

- A. A capture-the-flag competition
- B. A phishing simulation
- C. Physical security training
- D. Baste awareness training

**Answer: B**

**NEW QUESTION 176**

After entering a username and password, and administrator must gesture on a touch screen. Which of the following demonstrates what the administrator is providing?

- A. Multifactor authentication
- B. Something you can do
- C. Biometric
- D. Two-factor authentication

**Answer: D**

**NEW QUESTION 178**

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 183**

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 185**

A security administrator suspects an employee has been emailing proprietary information to a competitor. Company policy requires the administrator to capture an exact copy of the employee's hard disk. Which of the following should the administrator use?

- A. dd
- B. chmod
- C. dnsenum
- D. logger

**Answer: A**

**NEW QUESTION 190**

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

- A. A malicious USB was introduced by an unsuspecting employee.
- B. The ICS firmware was outdated
- C. A local machine has a RAT installed.

D. The HVAC was connected to the maintenance vendor.

**Answer:** A

#### NEW QUESTION 191

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 194

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

A)

```
http://sample.url.com/<script>Please-Visit-Our-Phishing-Site</script>
```

B)

```
http://sample.url.com/someotherpageonsite/../../../../etc/shadow
```

C)

```
http://sample.url.com/select-from-database-where-password-null
```

D)

```
http://redirect.sameple.url.sampleurl.com/malicious-dns-redirect
```

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

**Answer:** B

#### NEW QUESTION 199

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 200

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

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

**Answer:** B

#### NEW QUESTION 203

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 205

A network administrator has been asked to install an IDS to improve the security posture of an organization. Which of the following control types is an IDS?

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

**Answer:** C

#### NEW QUESTION 208

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 213

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 218

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 222

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 227

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

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

**Answer:** E

#### NEW QUESTION 229

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

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

**Answer:** A

**NEW QUESTION 234**

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

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

Which of the following attacks has occurred?

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

**Answer: E**

**NEW QUESTION 238**

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 241**

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 242**

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

```
Hello everyone,  
I am having the same problem with my server. Can you help me?  
  
<script type="text/javascript" src=http://website.com/user.js>  
Onload=sqlexec();  
</script>  
  
Thank you,  
  
Joe
```

Which of the following BEST describes the attack that was attempted against the forum readers?

- A. SOU attack
- B. DLL attack
- C. XSS attack
- D. API attack

**Answer: C**

**NEW QUESTION 246**

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

- A. Geolocation
- B. Time-of-day restrictions
- C. Certificates
- D. Tokens

- E. Geotagging
- F. Role-based access controls

**Answer:** AE

#### NEW QUESTION 250

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 251

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

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

**Answer:** A

#### NEW QUESTION 252

An organization has implemented a policy requiring the use of conductive metal lockboxes for personal electronic devices outside of a secure research lab. Which of the following did the organization determine to be the GREATEST risk to intellectual property when creating this policy?

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

**Answer:** D

#### NEW QUESTION 256

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 261

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 264

An incident response technician collected a mobile device during an investigation. Which of the following should the technician do to maintain chain of custody?

- A. Document the collection and require a sign-off when possession changes.
- B. Lock the device in a safe or other secure location to prevent theft or alteration.
- C. Place the device in a Faraday cage to prevent corruption of the data.
- D. Record the collection in a blockchain-protected public ledger.

**Answer:** A

#### NEW QUESTION 266

An organization just experienced a major cyberattack modern. 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**

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.

The diagram illustrates the steps to configure SSH keys for secure access to a server. It is divided into two main sections: 'Commands' and 'SSH Client'.

**Commands:** This section lists the terminal commands to be executed on the local machine:

- `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:** This section shows a terminal window with a question mark icon, indicating the next step in the process.

- A. Mastered  
B. Not Mastered

**Answer: A**

**Explanation:**

The diagram illustrates the process of setting up SSH keys. It is divided into two main sections: 'Commands' and 'SSH Client'.

**Commands:** This section lists the commands to be executed on the local machine, each in a yellow box:

- `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:** This section shows the commands executed on the remote server, each in a yellow box. The entire 'SSH Client' section is enclosed in a red dashed border, indicating it is the remote environment:

- `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`

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 280

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

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

**Answer:** DE

#### NEW QUESTION 285

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 289

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

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

**Answer:** A

#### NEW QUESTION 291

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 296

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 297

A forensics investigator is examining a number of unauthorized payments that were reported on the company's website. Some unusual log entries show users received an email for an unwanted mailing list and clicked on a link to attempt to unsubscribe. One of the users reported the email to the phishing team, and the forwarded email revealed the link to be:



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

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



D. XSRF

**Answer: B**

#### NEW QUESTION 302

An organization routes all of its traffic through a VPN. Most users are remote and connect into a corporate datacenter that houses confidential information. There is a firewall at the Internet border followed by a DLP appliance, the VPN server and the datacenter itself. Which of the following is the WEAKEST design element?

- A. The DLP appliance should be integrated into a NGFW.
- B. Split-tunnel connections can negatively impact the DLP appliance's performance.
- C. Encrypted VPN traffic will not be inspected when entering or leaving the network.
- D. Adding two hops in the VPN tunnel may slow down remote connections.

**Answer: C**

#### NEW QUESTION 306

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

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

**Answer: C**

#### NEW QUESTION 311

The CSIRT is reviewing the lessons learned from a recent incident. A worm was able to spread unhindered throughout the network and infect a large number of computers and servers. Which of the following recommendations would be BEST to mitigate the impacts of a similar incident in the future?

- A. Install a NIDS device at the boundary.
- B. Segment the network with firewalls.
- C. Update all antivirus signatures daily.
- D. Implement application blacklisting.

**Answer: B**

#### NEW QUESTION 312

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 316

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

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

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

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

**Answer: DE**

#### NEW QUESTION 318

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 320

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 324

.....

## Relate Links

**100% Pass Your SY0-601 Exam with Exam Bible 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/>