

CompTIA

Exam Questions SY0-601

CompTIA Security+ Exam



NEW QUESTION 1

Which of the following ISO standards is certified for privacy?

- A. ISO 9001
- B. ISO 27002
- C. ISO 27701
- D. ISO 31000

Answer: C

NEW QUESTION 2

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

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

Answer: D

NEW QUESTION 3

An organization has decided to host its web application and database in the cloud Which of the following BEST describes the security concerns for this decision?

- A. Access to the organization's servers could be exposed to other cloud-provider clients
- B. The cloud vendor is a new attack vector within the supply chain
- C. Outsourcing the code development adds risk to the cloud provider
- D. Vendor support will cease when the hosting platforms reach EOL.

Answer: B

NEW QUESTION 4

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

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

Answer: C

NEW QUESTION 5

A security analyst is looking for a solution to help communicate to the leadership team the seventy levels of the organization's vulnerabilities. Which of the following would BEST meet this need?

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

Answer: D

NEW QUESTION 6

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

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

Answer: C

NEW QUESTION 7

An attacker is attempting to exploit users by creating a fake website with the URL users. Which of the following social-engineering attacks does this describe?

- A. Information elicitation
- B. Typo squatting
- C. Impersonation
- D. Watering-hole attack

Answer: D

NEW QUESTION 8

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 9

Which of the following would a European company interested in implementing a technical, hands-on set of security standards MOST likely choose?

- A. GDPR
- B. CIS controls
- C. ISO 27001
- D. ISO 37000

Answer: A

NEW QUESTION 10

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

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

Answer: B

NEW QUESTION 10

A multinational organization that offers web-based services has datacenters that are located only in the United States; however, a large number of its customers are in Australia, Europe, and China. Payments for services are managed by a third party in the United Kingdom that specializes in payment gateways. The management team is concerned the organization is not compliant with privacy laws that cover some of its customers. Which of the following frameworks should the management team follow?

- A. Payment Card Industry Data Security Standard
- B. Cloud Security Alliance Best Practices
- C. ISO/IEC 27032 Cybersecurity Guidelines
- D. General Data Protection Regulation

Answer: A

NEW QUESTION 12

A security analyst is configuring a large number of new company-issued laptops. The analyst received the following requirements:

- The devices will be used internationally by staff who travel extensively.
- Occasional personal use is acceptable due to the travel requirements.
- Users must be able to install and configure sanctioned programs and productivity suites.
- The devices must be encrypted
- The devices must be capable of operating in low-bandwidth environments.

Which of the following would provide the GREATEST benefit to the security posture of the devices?

- A. Configuring an always-on VPN
- B. Implementing application whitelisting
- C. Requiring web traffic to pass through the on-premises content filter
- D. Setting the antivirus DAT update schedule to weekly

Answer: A

NEW QUESTION 14

The website <http://companywebsite.com> requires users to provide personal Information, Including security question responses, for registration. Which of the following would MOST likely cause a data breach?

- A. Lack of input validation
- B. Open permissions
- C. Unsecure protocol
- D. Missing patches

Answer: C

NEW QUESTION 19

Which of the following utilize a subset of real data and are MOST likely to be used to assess the features and functions of a system and how it interacts or performs from an end user's perspective against defined test cases? (Select TWO).

- A. Production

- B. Test
- C. Research and development
- D. PoC
- E. UAT
- F. SDLC

Answer: BE

NEW QUESTION 24

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

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

Answer: B

NEW QUESTION 26

A researcher has been analyzing large data sets for the last ten months. The researcher works with colleagues from other institutions and typically connects via SSH to retrieve additional data. Historically, this setup has worked without issue, but the researcher recently started getting the following message:

Which of the following network attacks is the researcher MOST likely experiencing?

- A. MAC cloning
- B. Evil twin
- C. Man-in-the-middle
- D. ARP poisoning

Answer: C

NEW QUESTION 28

A security administrator currently spends a large amount of time on common security tasks, such as report generation, phishing investigations, and user provisioning and deprovisioning. This prevents the administrator from spending time on other security projects. The business does not have the budget to add more staff members. Which of the following should the administrator implement?

- A. DAC
- B. ABAC
- C. SCAP
- D. SOAR

Answer: D

NEW QUESTION 30

A security operations analyst is using the company's SIEM solution to correlate alerts. Which of the following stages of the incident response process is this an example of?

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

Answer: C

NEW QUESTION 33

A smart retail business has a local store and a newly established and growing online storefront. A recent storm caused a power outage to the business and the local ISP, resulting in several hours of lost sales and delayed order processing. The business owner now needs to ensure two things:

* Protection from power outages

* Always-available connectivity in case of an outage

The owner has decided to implement battery backups for the computer equipment. Which of the following would BEST fulfill the owner's second need?

- A. Lease a point-to-point circuit to provide dedicated access.
- B. Connect the business router to its own dedicated UPS.
- C. Purchase services from a cloud provider for high availability.
- D. Replace the business's wired network with a wireless network.

Answer: C

NEW QUESTION 34

A privileged user at a company stole several proprietary documents from a server. The user also went into the log files and deleted all records of the incident. The systems administrator has just informed investigators that other log files are available for review. Which of the following did the administrator MOST likely configure that will assist the investigators?

- A. Memory dumps
- B. The syslog server
- C. The application logs
- D. The log retention policy

Answer: B

NEW QUESTION 38

A500 is implementing an insider threat detection program. The primary concern is that users may be accessing confidential data without authorization. Which of the following should be deployed to detect a potential insider threat?

- A. A honeypot
- B. A DMZ
- C. ULF
- D. File integrity monitoring

Answer: A

NEW QUESTION 43

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

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

Answer: A

NEW QUESTION 46

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 50

An organization wants to implement a third factor to an existing multifactor authentication. The organization already uses a smart card and password. Which of the following would meet the organization's needs for a third factor?

- A. Date of birth
- B. Fingerprints
- C. PIN
- D. TPM

Answer: B

NEW QUESTION 51

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

- A. An SLA
- B. An NDA
- C. ABPA
- D. An MOU

Answer: D

NEW QUESTION 52

Which of the following often operates in a client-server architecture to act as a service repository, providing enterprise consumers access to structured threat intelligence data?

- A. STIX
- B. CIRT
- C. OSINT
- D. TAXII

Answer:

B

NEW QUESTION 55

Which of the following technical controls is BEST suited for the detection and prevention of buffer overflows on hosts?

- A. DLP
- B. HIDS
- C. EDR
- D. NIPS

Answer: C

NEW QUESTION 59

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 64

While reviewing the wireless router, the systems administrator of a small business determines someone is spoofing the MAC address of an authorized device. Given the table below:

Which of the following should be the administrator's NEXT step to detect if there is a rogue system without impacting availability?

- A. Conduct a ping sweep.
- B. Physically check each system,
- C. Deny Internet access to the "UNKNOWN" hostname.
- D. Apply MAC filtering,

Answer: D

NEW QUESTION 69

A company is concerned about its security after a red-team exercise. The report shows the team was able to reach the critical servers due to the SMB being exposed to the Internet and running NTLMV1. Which of the following BEST explains the findings?

- A. Default settings on the servers
- B. Unsecured administrator accounts
- C. Open ports and services
- D. Weak Data encryption

Answer: C

NEW QUESTION 73

A security analyst is investigating an incident to determine what an attacker was able to do on a compromised laptop. The analyst reviews the following SIEM log:

Which of the following describes the method that was used to compromise the laptop?

- A. An attacker was able to move laterally from PC1 to PC2 using a pass-the-hash attack
- B. An attacker was able to bypass application whitelisting by emailing a spreadsheet attachment with an embedded PowerShell in the file
- C. An attacker was able to install malware to the CAasdf234 folder and use it to gain administrator rights and launch Outlook
- D. An attacker was able to phish user credentials successfully from an Outlook user profile

Answer: A

NEW QUESTION 77

A cybersecurity manager has scheduled biannual meetings with the IT team and department leaders to discuss how they would respond to hypothetical cyberattacks. During these meetings, the manager presents a scenario and injects additional information throughout the session to replicate what might occur in a dynamic cybersecurity event involving the company, its facilities, its data, and its staff. Which of the following describes what the manager is doing?

- A. Developing an incident response plan
- B. Building a disaster recovery plan
- C. Conducting a tabletop exercise
- D. Running a simulation exercise

Answer: C

NEW QUESTION 78

In which of the following situations would it be BEST to use a detective control type for mitigation?

- A. A company implemented a network load balancer to ensure 99.999% availability of its web application.
- B. A company designed a backup solution to increase the chances of restoring services in case of a natural disaster.
- C. A company purchased an application-level firewall to isolate traffic between the accounting department and the information technology department.
- D. A company purchased an IPS system, but after reviewing the requirements, the appliance was supposed to monitor, not block, any traffic.
- E. A company purchased liability insurance for flood protection on all capital assets.

Answer: D

NEW QUESTION 80

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 81

An incident, which is affecting dozens of systems, involves malware that reaches out to an Internet service for rules and updates. The IP addresses for the Internet host appear to be different in each case. The organization would like to determine a common IoC to support response and recovery actions. Which of the following sources of information would BEST support this solution?

- A. Web log files
- B. Browser cache
- C. DNS query logs
- D. Antivirus

Answer: C

NEW QUESTION 83

A financial analyst has been accused of violating the company's AUP and there is forensic evidence to substantiate the allegation. Which of the following would dispute the analyst's claim of innocence?

- A. Legal hold
- B. Order of volatility
- C. Non-repudiation
- D. Chain of custody

Answer: D

NEW QUESTION 87

A cloud administrator is configuring five compute instances under the same subnet in a VPC. Three instances are required to communicate with one another, and the other two must be logically isolated from all other instances in the VPC. Which of the following must the administrator configure to meet this requirement?

- A. One security group
- B. Two security groups
- C. Three security groups
- D. Five security groups

Answer: B

NEW QUESTION 92

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

- A. The order of volatility
- B. A checksum
- C. The location of the artifacts
- D. The vendor's name
- E. The date and time
- F. A warning banner

Answer: AE

NEW QUESTION 96

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 97

A new vulnerability in the SMB protocol on the Windows systems was recently discovered, but no patches are currently available to resolve the issue. The security administrator is concerned if servers in the company's DMZ will be vulnerable to external attack; however, the administrator cannot disable the service on the servers, as SMB is used by a number of internal systems and applications on the LAN. Which of the following TCP ports should be blocked for all external inbound connections to the DMZ as a workaround to protect the servers? (Select TWO).

- A. 135
- B. 139
- C. 143
- D. 161
- E. 443
- F. 445

Answer: BF

NEW QUESTION 102

An organization has implemented a two-step verification process to protect user access to data that is stored in the cloud. Each employee now uses an email address of mobile number a code to access the data. Which of the following authentication methods did the organization implement?

- A. Token key
- B. Static code
- C. Push notification
- D. HOTP

Answer: A

NEW QUESTION 106

During an incident response, a security analyst observes the following log entry on the web server. Which of the following BEST describes the type of attack the analyst is experiencing?

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

Answer: B

NEW QUESTION 109

An organization's Chief Security Officer (CSO) wants to validate the business's involvement in the incident response plan to ensure its validity and thoroughness. Which of the following will the CSO MOST likely use?

- A. An external security assessment
- B. A bug bounty program
- C. A tabletop exercise
- D. A red-team engagement

Answer: C

NEW QUESTION 112

The spread of misinformation surrounding the outbreak of a novel virus on election day led to eligible voters choosing not to take the risk of going to the polls. This is an example of:

- A. prebending.
- B. an influence campaign
- C. a watering-hole attack
- D. intimidation
- E. information elicitation

Answer: D

NEW QUESTION 114

Joe, a security analyst, recently performed a network discovery to fully understand his organization's electronic footprint from a "public" perspective. Joe ran a set of commands and received the following output:

Which of the following can be determined about the organization's public presence and security posture? (Select TWO).

- A. Joe used Whois to produce this output.
- B. Joe used cURL to produce this output.
- C. Joe used Wireshark to produce this output.
- D. The organization has adequate information available in public registration.
- E. The organization has too much information available in public registration.
- F. The organization has too little information available in public registration.

Answer: AD

NEW QUESTION 115

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 116

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

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

Answer: A

NEW QUESTION 118

To mitigate the impact of a single VM being compromised by another VM on the same hypervisor, an administrator would like to utilize a technical control to further segregate the traffic. Which of the following solutions would BEST accomplish this objective?

- A. Install a hypervisor firewall to filter east-west traffic.
- B. Add more VLANs to the hypervisor network switches.
- C. Move exposed or vulnerable VMs to the DMZ.
- D. Implement a zero-trust policy and physically segregate the hypervisor servers.

Answer: B

NEW QUESTION 123

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 126

A security engineer is reviewing log files after a third discovered usernames and passwords for the organization's accounts. The engineer sees there was a change in the IP address for a vendor website one earlier. This change lasted eight hours. Which of the following attacks was MOST likely used?

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

Answer: D

NEW QUESTION 127

A major political party experienced a server breach. The hacker then publicly posted stolen internal communications concerning campaign strategies to give the opposition party an advantage. Which of the following BEST describes these threat actors?

- A. Semi-authorized hackers
- B. State actors
- C. Script kiddies
- D. Advanced persistent threats

Answer: B

NEW QUESTION 128

A smart switch has the ability to monitor electrical levels and shut off power to a building in the event of power surge or other fault situation. The switch was installed on a wired network in a hospital and is monitored by the facilities department via a cloud application. The security administrator isolated the switch on a separate VLAN and set up a patch routine. Which of the following steps should also be taken to harden the smart switch?

- A. Set up an air gap for the switch.
- B. Change the default password for the switch.
- C. Place the switch In a Faraday cage.
- D. Install a cable lock on the switch

Answer:

B

NEW QUESTION 132

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

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

Answer: C

NEW QUESTION 136

An organization relies on third-party video conferencing to conduct daily business. Recent security changes now require all remote workers to utilize a VPN to corporate resources. Which of the following would BEST maintain high-quality video conferencing while minimizing latency when connected to the VPN?

- A. Using geographic diversity to have VPN terminators closer to end users
- B. Utilizing split tunneling so only traffic for corporate resources is encrypted
- C. Purchasing higher-bandwidth connections to meet the increased demand
- D. Configuring QoS properly on the VPN accelerators

Answer: D

NEW QUESTION 140

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 honeypot 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 142

A small business office is setting up a wireless infrastructure with primary requirements centered around protecting customer information and preventing unauthorized access to the business network. Which of the following would BEST support the office's business needs? (Select TWO)

- A. Installing WAPs with strategic placement
- B. Configuring access using WPA3
- C. Installing a WIDS
- D. Enabling MAC filtering
- E. Changing the WiFi password every 30 days
- F. Reducing WiFi transmit power throughout the office

Answer: BD

NEW QUESTION 147

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

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

Answer: A

NEW QUESTION 151

A security assessment determines DES and 3DES are still being used on recently deployed production servers. Which of the following did the assessment identify?

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

Answer: D

NEW QUESTION 156

Which of the following should a data owner require all personnel to sign to legally protect intellectual property?

- A. An NDA
- B. An AUP
- C. An ISA

D. An MOU

Answer: D

NEW QUESTION 161

A security analyst is reviewing the following attack log output:
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 163

A well-known organization has been experiencing attacks from APIs. The organization is concerned that custom malware is being created and emailed into the company or installed on USB sticks that are dropped in parking lots. Which of the following is the BEST defense against this scenario?

- A. Configuring signature-based antivirus to update every 30 minutes
- B. Enforcing S/MIME for email and automatically encrypting USB drives upon insertion.
- C. Implementing application execution in a sandbox for unknown software.
- D. Fuzzing new files for vulnerabilities if they are not digitally signed

Answer: C

NEW QUESTION 164

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

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

Answer: B

NEW QUESTION 167

A company processes highly sensitive data and senior management wants to protect the sensitive data by utilizing classification labels. Which of the following access control schemes would be BEST for the company to implement?

- A. Discretionary
- B. Rule-based
- C. Role-based
- D. Mandatory

Answer: D

NEW QUESTION 168

A security incident may have occurred on the desktop PC of an organization's Chief Executive Officer (CEO). A duplicate copy of the CEO's hard drive must be stored securely to ensure appropriate forensic processes and the chain of custody are followed. Which of the following should be performed to accomplish this task?

- A. Install a new hard drive in the CEO's PC, and then remove the old hard drive and place it in a tamper-evident bag
- B. Connect a write blocker to the hard drive. Then, leveraging a forensic workstation, utilize the dd command in a live Linux environment to create a duplicate copy.
- C. Remove the CEO's hard drive from the PC, connect to the forensic workstation, and copy all the contents onto a remote fileshare while the CEO watches.
- D. Refrain from completing a forensic analysis of the CEO's hard drive until after the incident is confirmed, duplicating the hard drive at this stage could destroy evidence.

Answer: D

NEW QUESTION 173

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. dntenum
- D. logger

Answer: A

NEW QUESTION 176

A company has been experiencing very brief power outages from its utility company over the last few months. These outages only last for one second each time. The utility company is aware of the issue and is working to replace a faulty transformer. Which of the following BEST describes what the company should purchase to ensure its critical servers and network devices stay online?

- A. Dual power supplies
- B. A UPS
- C. A generator
- D. APDU

Answer: B

NEW QUESTION 180

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 181

An enterprise needs to keep cryptographic keys in a safe manner. Which of the following network appliances can achieve this goal?

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

Answer: A

NEW QUESTION 182

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

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

- A. Create firewall rules to restrict traffic to other cloud service providers.
- B. Install a DLP solution to monitor data in transit.
- C. Implement a CASB solution.
- D. Configure a web-based content filter.

Answer: B

NEW QUESTION 185

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 188

A company is setting up a web server on the Internet that will utilize both encrypted and unencrypted web-browsing protocols. A security engineer runs a port scan against the server from the Internet and sees the following output: Which of the following steps would be best for the security engineer to take NEXT?

- A. Allow DNS access from the internet.
- B. Block SMTP access from the Internet
- C. Block HTTPS access from the Internet
- D. Block SSH access from the Internet.

Answer: D

NEW QUESTION 190

A new vulnerability in the SMB protocol on the Windows systems was recently discovered, but no patches are currently available to resolve the issue. The security administrator is concerned that servers in the company's DMZ will be vulnerable to external attack; however, the administrator cannot disable the service on the servers, as SMB is used by a number of internal systems and applications on the LAN Which of the following TCP ports should be blocked for all external inbound connections to the DMZ as a workaround to protect the servers? (Select TWO).

- A. 135
- B. 139
- C. 143

- D. 161
- E. 443
- F. 445

Answer: AE

NEW QUESTION 192

Phishing and spear-phishing attacks have been occurring more frequently against a company's staff. Which of the following would MOST likely help mitigate this issue?

- A. DNSSEC and DMARC
- B. DNS query logging
- C. Exact mail exchanger records in the DNS
- D. The addition of DNS conditional forwarders

Answer: C

NEW QUESTION 194

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 196

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 197

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

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

Answer: B

NEW QUESTION 198

After installing a Windows server, a cybersecurity administrator needs to harden it, following security best practices. Which of the following will achieve the administrator's goal? (Select TWO).

- A. Disabling guest accounts
- B. Disabling service accounts
- C. Enabling network sharing
- D. Disabling NetBIOS over TCP/IP
- E. Storing LAN manager hash values
- F. Enabling NTLM

Answer: AD

NEW QUESTION 202

A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?

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

Answer: A

NEW QUESTION 207

A company has decided to move its operations to the cloud. It wants to utilize technology that will prevent users from downloading company applications for personal use, restrict data that is uploaded, and have visibility into which applications are being used across the company. Which of the following solutions will BEST meet these requirements?

- A. An NGFW
- B. A CASB
- C. Application whitelisting
- D. An NG-SWG

Answer: B

NEW QUESTION 209

A security analyst is reviewing logs on a server and observes the following output:

Which of the following is the security analyst observing?

- A. A rainbow table attack
- B. A password-spraying attack
- C. A dictionary attack
- D. A keylogger attack

Answer: C

NEW QUESTION 214

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

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

Answer: D

NEW QUESTION 219

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

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

Answer: A

NEW QUESTION 223

A security analyst needs to generate a server certificate to be used for 802.1X and secure RDP connections. The analyst is unsure what is required to perform the task and solicits help from a senior colleague. Which of the following is the FIRST step the senior colleague will most likely tell the analyst to perform to accomplish this task?

- A. Create an OCSP
- B. Generate a CSR
- C. Create a CRL
- D. Generate a .pfx file

Answer: B

NEW QUESTION 227

An attacker is attempting to exploit users by creating a fake website with the URL www.validwebsite.com. The attacker's intent is to imitate the look and feel of a legitimate website to obtain personal information from unsuspecting users. Which of the following social-engineering attacks does this describe?

- A. Information elicitation
- B. Typo squatting
- C. Impersonation
- D. Watering-hole attack

Answer: D

NEW QUESTION 229

A Chief Security Office's (CSO's) key priorities are to improve preparation, response, and recovery practices to minimize system downtime and enhance organizational resilience to ransomware attacks. Which of the following would BEST meet the CSO's objectives?

- A. Use email-filtering software and centralized account management, patch high-risk systems, and restrict administration privileges on fileshares.
- B. Purchase cyber insurance from a reputable provider to reduce expenses during an incident.
- C. Invest in end-user awareness training to change the long-term culture and behavior of staff and executives, reducing the organization's susceptibility to phishing attacks.
- D. Implement application whitelisting and centralized event-log management, and perform regular testing and validation of full backups.

Answer: D

NEW QUESTION 231

A network administrator at a large organization is reviewing methods to improve the security of the wired LAN. Any security improvement must be centrally managed and allow corporate-owned devices to have access to the intranet but limit others to Internet access only. Which of the following should the administrator recommend?

- A. 802.1X utilizing the current PKI infrastructure
- B. SSO to authenticate corporate users
- C. MAC address filtering with ACLs on the router
- D. PAM for user account management

Answer: A

NEW QUESTION 236

A company is upgrading its wireless infrastructure to WPA2-Enterprise using EAP-TLS. Which of the following must be part of the security architecture to achieve AAA? (Select TWO)

- A. DNSSEC
- B. Reverse proxy
- C. VPN concentrator
- D. PKI
- E. Active Directory
- F. RADIUS

Answer: EF

NEW QUESTION 240

An end user reports a computer has been acting slower than normal for a few weeks. During an investigation, an analyst determines the system is sending the user's email address and a ten-digit number to an IP address once a day. The only recent log entry regarding the user's computer is the following:

Which of the following is the MOST likely cause of the issue?

- A. The end user purchased and installed a PUP from a web browser
- B. A bot on the computer is brute forcing passwords against a website
- C. A hacker is attempting to exfiltrate sensitive data
- D. Ransomware is communicating with a command-and-control server.

Answer: A

NEW QUESTION 244

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

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

Answer: D

NEW QUESTION 247

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 251

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 255

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

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

Answer: D

NEW QUESTION 257

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 260

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:

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 265

The process of passively gathering information prior to launching a cyberattack is called:

- A. tailgating
- B. reconnaissance
- C. pharming
- D. prepending

Answer: B

NEW QUESTION 266

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

- A. Create a new acceptable use policy.
- B. Segment the network into trusted and untrusted zones.
- C. Enforce application whitelisting.
- D. Implement DLP at the network boundary.

Answer: C

NEW QUESTION 268

An attacker is attempting to harvest user credentials on a client's website. A security analyst notices multiple attempts of random usernames and passwords. When the analyst types in a random username and password, the logon screen displays the following message:

Which of the following should the analyst recommend be enabled?

- A. Input validation
- B. Obfuscation
- C. Error handling
- D. Username lockout

Answer: B

NEW QUESTION 271

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 272

After a phishing scam for a user's credentials, the red team was able to craft a payload to deploy on a server. The attack allowed the installation of malicious software that initiates a new remote session. Which of the following types of attacks has occurred?

- A. Privilege escalation
- B. Session replay
- C. Application programming interface
- D. Directory traversal

Answer: A

NEW QUESTION 276

Which of the following represents a biometric FRR?

- A. Authorized users being denied access
- B. Users failing to enter the correct PIN
- C. The denied and authorized numbers being equal
- D. The number of unauthorized users being granted access

Answer: A

NEW QUESTION 280

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 284

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 286

An attacker is trying to gain access by installing malware on a website that is known to be visited by the target victims. Which of the following is the attacker MOST likely attempting?

- A. A spear-phishing attack
- B. A watering-hole attack
- C. Typo squatting
- D. A phishing attack

Answer: B

NEW QUESTION 290

A company provides mobile devices to its users to permit access to email and enterprise applications. The company recently started allowing users to select from several different vendors and device models. When configuring the MDM, which of the following is a key security implication of this heterogeneous device approach?

- A. The most common set of MDM configurations will become the effective set of enterprise mobile security controls.
- B. All devices will need to support SCEP-based enrollment; therefore, the heterogeneity of the chosen architecture may unnecessarily expose private keys to adversaries.
- C. Certain devices are inherently less secure than others, so compensatory controls will be needed to address the delta between device vendors.
- D. MDMs typically will not support heterogeneous deployment environments, so multiple MDMs will need to be installed and configured.

Answer: C

NEW QUESTION 294

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

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

Answer: D

NEW QUESTION 297

An analyst is trying to identify insecure services that are running on the internal network After performing a port scan the analyst identifies that a server has some insecure services enabled on default ports Which of the following BEST describes the services that are currently running and the secure alternatives for replacing them' (Select THREE)

- A. SFTP FTPS
- B. SNMPv2 SNMPv3
- C. HTTP, HTTPS
- D. TFTP FTP
- E. SNMPv1, SNMPv2
- F. Telnet SSH
- G. TLS, SSL
- H. POP, IMAP
- I. Login, rlogin

Answer: BCF

NEW QUESTION 299

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

www.company.com (main website)

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

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

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

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

Answer: B

NEW QUESTION 303

Which of the following cryptographic concepts would a security engineer utilize while implementing non-repudiation? (Select TWO)

- A. Block cipher
- B. Hashing
- C. Private key
- D. Perfect forward secrecy
- E. Salting
- F. Symmetric keys

Answer: BC

NEW QUESTION 305

A security engineer has enabled two-factor authentication on all workstations. Which of the following approaches are the MOST secure? (Select TWO).

- A. Password and security question
- B. Password and CAPTCHA
- C. Password and smart card
- D. Password and fingerprint
- E. Password and one-time token
- F. Password and voice

Answer: CD

NEW QUESTION 308

A user recently entered a username and password into a recruiting application website that had been forged to look like the legitimate site. Upon investigation, a security analyst identifies the following:

- The legitimate website's IP address is 10.1.1.20 and eRecruit local resolves to the IP
- The forged website's IP address appears to be 10.2.12.99, based on NetFlow records
- All three at the organization's DNS servers show the website correctly resolves to the legitimate IP
- DNS query logs show one of the three DNS servers returned a result of 10.2.12.99 (cached) at the approximate time of the suspected compromise.

Which of the following MOST likely occurred?

- A. A reverse proxy was used to redirect network traffic
- B. An SSL strip MITM attack was performed
- C. An attacker temporarily pawned a name server
- D. An ARP poisoning attack was successfully executed

Answer: B

NEW QUESTION 313

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

An incident responder learns the following information:

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

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

Answer: C

NEW QUESTION 316

A consultant is configuring a vulnerability scanner for a large, global organization in multiple countries. The consultant will be using a service account to scan systems with administrative privileges on a weekly basis, but there is a concern that hackers could gain access to the account and pivot through the global network. Which of the following would be BEST to help mitigate this concern?

- A. Create consultant accounts for each region, each configured with push MFA notifications.
- B. Create one global administrator account and enforce Kerberos authentication
- C. Create different accounts for each region
- D. Limit their logon times, and alert on risky logins
- E. Create a guest account for each region
- F. Remember the last ten passwords, and block password reuse

Answer: C

NEW QUESTION 318

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

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

Answer: BC

NEW QUESTION 323

An attacker is exploiting a vulnerability that does not have a patch available. Which of the following is the attacker exploiting?

- A. Zero-day
- B. Default permissions
- C. Weak encryption
- D. Unsecure root accounts

Answer: A

NEW QUESTION 326

A retail executive recently accepted a job with a major competitor. The following week, a security analyst reviews the security logs and identifies successful logon attempts to access the departed executive's accounts. Which of the following security practices would have addressed the issue?

- A. A non-disclosure agreement
- B. Least privilege
- C. An acceptable use policy
- D. Offboarding

Answer: D

NEW QUESTION 330

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 333

A network manager is concerned that business may be negatively impacted if the firewall in its datacenter goes offline. The manager would like to Implement a high availability pair to:

- A. decrease the mean ne between failures
- B. remove the single point of failure
- C. cut down the mean time to repair
- D. reduce the recovery time objective

Answer: B

NEW QUESTION 337

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 340

A Chief Executive Officer's (CEO) personal information was stolen in a social engineering attack. Which of the following sources would reveal if the CEO's personal information is for sale?

- A. Automated information sharing
- B. Open-source intelligence
- C. The dark web
- D. Vulnerability databases

Answer: C

NEW QUESTION 341

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 344

A security researcher is attempting to gather data on the widespread use of a Zero-day exploit. Which of the following will the researcher MOST likely use to capture this data?

- A. A DNS sinkhole

- B. A honeypot
- C. A vulnerability scan
- D. cvss

Answer: B

NEW QUESTION 345

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

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

Answer: C

NEW QUESTION 346

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

Answer: B

NEW QUESTION 348

A recent security assessment revealed that an actor exploited a vulnerable workstation within an organization and has persisted on the network for several months. The organization realizes the need to reassess its security.

Strategy for mitigating risks within the perimeter Which of the following solutions would BEST support the organization's strategy?

- A. FIM
- B. DLP
- C. EDR
- D. UTM

Answer: C

NEW QUESTION 352

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

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

Answer: BD

NEW QUESTION 355

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 359

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

- A. SSO would simplify username and password management, making it easier for hackers to pass guess accounts.
- B. SSO would reduce password fatigue, but staff would still need to remember more complex passwords.
- C. SSO would reduce the password complexity for frontline staff.
- D. SSO would reduce the resilience and availability of system if the provider goes offline.

Answer: D

NEW QUESTION 360

A Chief Security Officer (CSO) was notified that a customer was able to access confidential internal company files on a commonly used file-sharing service. The file-sharing service is the same one used by company staff as one of its approved third-party applications.

After further investigation, the security team determines the sharing of confidential files was accidental and not malicious. However, the CSO wants to implement changes to minimize this type of incident from reoccurring but does not want to impact existing business processes. Which of the following would BEST meet the CSO's objectives?

- A. DLP
- B. SWG
- C. CASB
- D. Virtual network segmentation
- E. Container security

Answer: A

NEW QUESTION 362

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

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

Answer: B

NEW QUESTION 365

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

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

Answer: C

NEW QUESTION 368

Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?

- A. SSAE SOC 2
- B. PCI DSS
- C. GDPR
- D. ISO 31000

Answer: C

NEW QUESTION 373

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 376

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 380

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 383

An organization's finance department is implementing a policy to protect against collusion. Which of the following control types and corresponding procedures should the organization implement to fulfill this policy's requirement? (Select TWO).

- A. Corrective
- B. Deterrent
- C. Preventive
- D. Mandatory vacations
- E. Job rotation
- F. Separation of duties

Answer: DE

NEW QUESTION 385

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 386

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 391

An analyst has determined that a server was not patched and an external actor exfiltrated data on port 139. Which of the following sources should the analyst review to BEST ascertain how the Incident could have been prevented?

- A. The vulnerability scan output
- B. The security logs
- C. The baseline report
- D. The correlation of events

Answer: A

NEW QUESTION 396

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

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

Answer: D

NEW QUESTION 401

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 402

During a routine scan of a wireless segment at a retail company, a security administrator discovers several devices are connected to the network that do not match the company's naming convention and are not in the asset inventory. WiFi access is protected with 256-bit encryption via WPA2. Physical access to the company's facility requires two-factor authentication using a badge and a passcode. Which of the following should the administrator implement to find and remediate the issue? (Select TWO).

- A. Check the SIEM for failed logins to the LDAP directory.
- B. Enable MAC filtering on the switches that support the wireless network.
- C. Run a vulnerability scan on all the devices in the wireless network.
- D. Deploy multifactor authentication for access to the wireless network.
- E. Scan the wireless network for rogue access points.
- F. Deploy a honeypot on the network.

Answer: BE

NEW QUESTION 403

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:

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 404

Users at the organization have been installing programs from the internet on their workstations without first proper authorization. The organization maintains a portal from which users can install standardized programs. However, some users have administrative access on their workstations to enable legacy programs to function properly. Which of the following should the security administrator consider implementing to address this issue?

- A. Application code signing
- B. Application whitelisting
- C. Data loss prevention
- D. Web application firewalls

Answer: B

NEW QUESTION 406

A network administrator would like to configure a site-to-site VPN utilizing IPsec. The administrator wants the tunnel to be established with data integrity, encryption, authentication, and anti-replay functions. Which of the following should the administrator use when configuring the VPN?

- A. AH
- B. EDR
- C. ESP
- D. DNSSEC

Answer: C

NEW QUESTION 409

An organization recently recovered from a data breach. During the root cause analysis, the organization determined the source of the breach to be a personal cell phone that had been reported lost. Which of the following solutions should the organization implement to reduce the likelihood of future data breaches?

- A. MDM
- B. MAM
- C. VDI
- D. DLP

Answer: A

NEW QUESTION 412

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

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

Answer: C

NEW QUESTION 415

A security analyst is logged into a Windows file server and needs to see who is accessing files and from which computers Which of the following tools should the analyst use?

- A. netstat
- B. net share
- C. netcat
- D. nbtstat
- E. net session

Answer: A

NEW QUESTION 418

A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator MOST likely use to confirm the suspicions?

- A. Nmap
- B. Wireshark
- C. Autopsy
- D. DNSEnum

Answer: A

NEW QUESTION 419

A company just implemented a new telework policy that allows employees to use personal devices for official email and file sharing while working from home. Some of the requirements are:

- * Employees must provide an alternate work location (i.e., a home address)
- * Employees must install software on the device that will prevent the loss of proprietary data but will not restrict any other software from being installed.

Which of the following BEST describes the MDM options the company is using?

- A. Geofencing, content management, remote wipe, containerization, and storage segmentation
- B. Content management, remote wipe, geolocation, context-aware authentication, and containerization
- C. Application management, remote wipe, geofencing, context-aware authentication, and containerization
- D. Remote wipe, geolocation, screen locks, storage segmentation, and full-device encryption

Answer: D

NEW QUESTION 422

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

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

Answer: A

NEW QUESTION 425

Which of the following is the BEST reason to maintain a functional and effective asset management policy that aids in ensuring the security of an organization?

- A. To provide data to quantify risk based on the organization's systems.
- B. To keep all software and hardware fully patched for known vulnerabilities
- C. To only allow approved, organization-owned devices onto the business network
- D. To standardize by selecting one laptop model for all users in the organization

Answer: A

NEW QUESTION 429

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 430

An end user reports a computer has been acting slower than normal for a few weeks. During an investigation, an analyst determines the system is sending the user's email address and a ten-digit number to an IP address once a day. The only recent log entry regarding the user's computer is the following:

Which of the following is the MOST likely cause of the issue?

- A. The end user purchased and installed 2 PUP from a web browser.
- B. A bot on the computer is brute forcing passwords against a website.
- C. A hacker is attempting to exfiltrate sensitive data.
- D. Ransomware is communicating with a command-and-control server.

Answer: A

NEW QUESTION 432

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. Basic awareness training

Answer: B

NEW QUESTION 437

Which of the following BEST describes the MFA attribute that requires a callback on a predefined landline?

- A. Something you exhibit
- B. Something you can do
- C. Someone you know
- D. Somewhere you are

Answer: D

NEW QUESTION 438

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 model?

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

Answer: A

NEW QUESTION 441

A worldwide manufacturing company has been experiencing email account compromise. 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 444

A SOC is implementing an insider-threat-detection program. The primary concern is that users may be accessing confidential data without authorization. Which of the following should be deployed to detect a potential insider threat?

- A. A honeyfile
- B. ADMZ
- C. DLP
- D. File integrity monitoring

Answer: A

NEW QUESTION 448

The Chief Financial Officer (CFO) of an insurance company received an email from Ann, the company's Chief Executive Officer (CEO), requesting a transfer of \$10,000 to an account. The email states Ann is on vacation and has lost her purse, containing cash and credit cards. Which of the following social-engineering techniques is the attacker using?

- A. Phishing
- B. Whaling
- C. Typo squatting
- D. Pharming

Answer: B

NEW QUESTION 451

A security administrator is analyzing the corporate wireless network. The network only has two access points running on channels 1 and 11. While using airodump-ng, the administrator notices other access points are running with the same corporate ESSID on all available channels and with the same BSSID of one of the legitimate access points. Which of the following attacks is happening on the corporate network?

- A. Man in the middle
- B. Evil twin
- C. Jamming
- D. Rogue access point
- E. Disassociation

Answer: B

NEW QUESTION 456

After consulting with the Chief Risk Officer (CRO), a manager decides to acquire cybersecurity insurance for the company. Which of the following risk management strategies is the manager adopting?

- A. Risk acceptance
- B. Risk avoidance
- C. Risk transference
- D. Risk mitigation

Answer: C

NEW QUESTION 459

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

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

Answer: DF

NEW QUESTION 462

A security analyst needs to find real-time data on the latest malware and IoCs. Which of the following best describes the solution the analyst should pursue?

- A. Advisories and bulletins
- B. Threat feeds
- C. Security news articles
- D. Peer-reviewed content

Answer: B

NEW QUESTION 466

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:

Which of the following attacks MOST likely occurred?

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

Answer: D

NEW QUESTION 470

An organization blocks user access to command-line interpreters but hackers still managed to invoke the interpreters using native administrative tools Which of the following should the security team do to prevent this from Happening in the future?

- A. Implement HIPS to block Inbound and outbound SMB ports 139 and 445.
- B. Trigger a SIEM alert whenever the native OS tools are executed by the user
- C. Disable the built-in OS utilities as long as they are not needed for functionality.
- D. Configure the AV to quarantine the native OS tools whenever they are executed

Answer: C

NEW QUESTION 472

A security administrator is trying to determine whether a server is vulnerable to a range of attacks. After using a tool, the administrator obtains the following output:

Which of the following attacks was successfully implemented based on the output?

- A. Memory leak
- B. Race conditions
- C. SQL injection
- D. Directory traversal

Answer: D

NEW QUESTION 475

A security analyst is reviewing the following output from a system:

Which of the following is MOST likely being observed?

- A. ARP palsoning
- B. Man in the middle
- C. Denial of service
- D. DNS poisoning

Answer: C

NEW QUESTION 479

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

- A. hping3 -S corsptia.org -p 80
- B. nc —1 —v comptia.org -p 80
- C. nmap comptia.org -p 80 —sV
- D. nslookup -port=80 comptia.org

Answer: C

NEW QUESTION 482

To further secure a company's email system, an administrator is adding public keys to DNS records in the company's domain Which of the following is being used?

- A. PFS
- B. SPF
- C. DMARC
- D. DNSSEC

Answer: D

NEW QUESTION 484

A university is opening a facility in a location where there is an elevated risk of theft The university wants to protect the desktops in its classrooms and labs Which of the following should the university use to BEST protect these assets deployed in the facility?

- A. Visitor logs
- B. Cable locks
- C. Guards
- D. Disk encryption
- E. Motion detection

Answer: B

NEW QUESTION 485

Entering a secure area requires passing through two doors, both of which require someone who is already inside to initiate access. Which of the following types of physical security controls does this describe?

- A. Cameras
- B. Faraday cage
- C. Access control vestibule
- D. Sensors
- E. Guards

Answer: C

NEW QUESTION 487

An engineer is setting up a VDI environment for a factory location, and the business wants to deploy a low-cost solution to enable users on the shop floor to log in to the VDI environment directly. Which of the following should the engineer select to meet these requirements?

- A. Laptops
- B. Containers
- C. Thin clients
- D. Workstations

Answer: C

NEW QUESTION 490

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

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

Answer: A

NEW QUESTION 492

A remote user recently took a two-week vacation abroad and brought along a corporate-owned laptop. Upon returning to work, the user has been unable to connect the laptop to the VPN. Which of the following is the MOST likely reason for the user's inability to connect the laptop to the VPN?

- A. Due to foreign travel, the user's laptop was isolated from the network.
- B. The user's laptop was quarantined because it missed the latest path update.
- C. The VPN client was blacklisted.
- D. The user's account was put on a legal hold.

Answer: A

NEW QUESTION 495

Which of the following BEST describes a social-engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested?

- A. Whaling
- B. Spam
- C. Invoice scam
- D. Pharming

Answer: A

NEW QUESTION 498

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 499

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 503

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 506

A security analyst needs to perform periodic vulnerability scans on production systems. Which of the following scan types would produce the BEST vulnerability scan report?

- A. Port
- B. Intrusive
- C. Host discovery
- D. Credentialed

Answer: D

NEW QUESTION 508

The new Chief Executive Officer (CEO) of a large company has announced a partnership with a vendor that will provide multiple collaboration applications to make remote work easier. The company has a geographically dispersed staff located in numerous remote offices in different countries. The company's IT administrators are concerned about network traffic and load if all users simultaneously download the application. Which of the following would work BEST to allow each geographic region to download the software without negatively impacting the corporate network?

- A. Update the host IDS rules.
- B. Enable application whitelisting.
- C. Modify the corporate firewall rules.
- D. Deploy all applications simultaneously.

Answer: B

NEW QUESTION 512

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

- A. data controller.
- B. data owner

- C. data custodian.
- D. data processor

Answer: D

NEW QUESTION 513

An attacker was easily able to log in to a company's security camera by performing a basic online search for a setup guide for that particular camera brand and model Which of the following BEST describes the configurations the attacker exploited?

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

Answer: C

NEW QUESTION 516

A bank detects fraudulent activity on user's account. The user confirms transactions completed yesterday on the bank's website at <https://www.company.com>. A security analyst then examines the user's

Internet usage logs and observes the following output: date; username; url;destinationport; responsecode

2020-03-01; userann; http: //www.company.org/;80;302; userann: http://www.company.org/secure_login/;80;200 2020-03-01; userann:

<http://www.company.org/dashboard/;80;200>

Which of the following has MOST likely occurred?

- A. Replay attack
- B. SQL injection
- C. SSL stripping
- D. Race conditions

Answer: A

NEW QUESTION 517

A company uses specially configured workstations tor any work that requires administrator privileges to its Tier 0 and Tier 1 systems. The company follows a strict process to harden systems immediately upon delivery. Even with these strict security measures in place, an incident occurred from one of the workstations. The root cause appears to be that the SoC was tampered with or replaced. Which of the following MOST likely occurred?

- A. Fileless malware
- B. A downgrade attack
- C. A supply-chain attack
- D. A logic bomb
- E. Misconfigured BIOS

Answer: C

NEW QUESTION 520

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 525

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

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

Answer: A

NEW QUESTION 526

An organization's corporate offices were destroyed due to a natural disaster, so the organization is now setting up offices in a temporary work space. Which of the following will the organization MOST likely consult?

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

Answer: A

NEW QUESTION 528

A forensics examiner is attempting to dump password cached in the physical memory of a live system but keeps receiving an error message. Which of the following BEST describes the cause of the error?

- A. The examiner does not have administrative privileges to the system
- B. The system must be taken offline before a snapshot can be created
- C. Checksum mismatches are invalidating the disk image
- D. The swap file needs to be unlocked before it can be accessed

Answer: D

NEW QUESTION 530

A security administrator has noticed unusual activity occurring between different global instances and workloads and needs to identify the source of the unusual traffic. Which of the following log sources would be BEST to show the source of the unusual traffic?

- A. HIDS
- B. UEBA
- C. CASB
- D. VPC

Answer: C

NEW QUESTION 534

The following are the logs of a successful attack.

Which of the following controls would be BEST to use to prevent such a breach in the future?

- A. Password history
- B. Account expiration
- C. Password complexity
- D. Account lockout

Answer: D

NEW QUESTION 537

A security analyst receives the configuration of a current VPN profile and notices the authentication is only applied to the IP datagram portion of the packet. Which of the following should the analyst implement to authenticate the entire packet?

- A. AH
- B. ESP
- C. SRTP
- D. LDAP

Answer: B

NEW QUESTION 538

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

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

Answer: D

NEW QUESTION 543

A security analyst is running a vulnerability scan to check for missing patches during a suspected security incident. During which of the following phases of the response process is this activity MOST likely occurring?

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

Answer: D

NEW QUESTION 547

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 550

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SY0-601 Practice Exam Features:

- * SY0-601 Questions and Answers Updated Frequently
- * SY0-601 Practice Questions Verified by Expert Senior Certified Staff
- * SY0-601 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SY0-601 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SY0-601 Practice Test Here](#)