

[Download Full Version SY0-601 Exam Dumps \(Updated in Feb/2023\)](#)

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

**Correct Answer: A**

**QUESTION 225**

A large enterprise has moved all its data to the cloud behind strong authentication and encryption. A sales director recently had a laptop stolen and later, enterprise data was found to have been compromised database. Which of the following was the MOST likely cause?

- A. Shadow IT
- B. Credential stuffing
- C. SQL injection
- D. Man-in-the-browser
- E. Bluejacking

**Correct Answer: A**

**QUESTION 226**

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:

Host	Event ID	Event source	Description
PC1	865	Microsoft-Windows-SoftwareRestrictionPolicies	C:\asdf234\asdf234.exe was blocked by Group Policy
PC1	4688	Microsoft-Windows-Security-Auditing	A new process has been created. New Process Name:powershell.exe Creator Process Name:outlook.exe
PC1	4688	Microsoft-Windows-Security-Auditing	A new process has been created. New Process Name:lat.ps1 Creator Process Name:powershell.exe
PC2	4625	Microsoft-Windows-Security-Auditing	An account failed to log on. LogonType:3 SecurityID:Null SID Workstation Name:PC1 Authentication Package Name:NTLM

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 gam administrator nights and launch Outlook
- D. An attacker was able to phish user credentials successfully from an Outlook user profile

**Correct Answer: A**

**QUESTION 227**

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

**Correct Answer: A**

**QUESTION 228**

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

**Correct Answer: D**

**QUESTION 229**

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.

**Correct Answer: D**

**QUESTION 230**

Which of the following would be the BEST resource for a software developer who is looking to improve secure coding practices for web applications?

- A. OWASP
- B. Vulnerability scan results
- C. NIST CSF
- D. Third-party libraries

**Correct Answer: A**

**QUESTION 231**

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

**Correct Answer: A**

**QUESTION 232**

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

**Correct Answer: A**

**QUESTION 233**

Which of the following is MOST likely to contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be managed after mitigating controls have been implemented?

- A. An RTO report
- B. A risk register
- C. A business impact analysis
- D. An asset value register
- E. A disaster recovery plan

**Correct Answer: B**

**QUESTION 234**

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

**Correct Answer: B**

**QUESTION 235**

An information security incident recently occurred at an organization, and the organization was required to report the incident to authorities and notify the affected parties. When the organization's customers became aware of the incident, some reduced their orders or stopped placing orders entirely. Which of the following is the organization experiencing?

- A. Reputation damage
- B. Identity theft
- C. Anonymization
- D. Interrupted supply chain

**Correct Answer: A**

**QUESTION 236**

An attacker is attempting to exploit users by creating a fake website with the URL [www.validwebsite.com](http://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

**Correct Answer: D**

**QUESTION 237**

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

**Correct Answer: D**

**QUESTION 238**

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.

**Correct Answer: C**

**QUESTION 239**

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.

**Correct Answer: A**

**QUESTION 240**

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

**Correct Answer: EF**

**QUESTION 241**

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.

**Correct Answer: BE**

**Explanation:**

Security is pretty good already up to a point, clearly Rogue AP bypass is in the picture. MAC filtering on the switch the AP's hang from will ensure the only AP's allowed to touch the core network are approved known AP's and the "bad guys" will find themselves trapped on an AP island with nowhere to go!