Report on incident response

Incident Response: Compromised Database System (System B)

As part of the Computer Security Incident Response Team (CSIRT), addressing the compromise of System B (a database with several storage disks) involves immediate action to contain the threat, remove the infected system, and ensure that sensitive information is handled appropriately before disposal. Here’s a detailed response plan.

I. Isolation

Objective: To prevent further damage and stop the attacker from gaining more control or exfiltrating data.

1. **Network Segmentation**:
   - **Disconnect System B**: Physically disconnect the compromised system from the network to halt the attack immediately.
   - **Firewall Rules**: Update firewall rules to block all traffic to and from System B’s IP address.
   - **Network Access Control**: Use network access control (NAC) policies to isolate System B from the internal network and any external connections.
2. **Quarantine**:
   - **Quarantine the System**: Move System B into a quarantined network segment where it can be analyzed without risking further contamination of the main network.
   - **Isolation VLAN**: Assign System B to an isolation VLAN to limit its communication capabilities while maintaining the ability to monitor and investigate the incident.
3. **Monitoring**:
   - **Network Traffic Analysis**: Use intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor for any suspicious activity related to the compromised system.
   - **Log Analysis**: Review logs from System B and related network devices to understand the extent of the compromise.

II. Removal of the Infected System B

Objective: To ensure the infected system is safely removed without further risk to the network or data integrity.

1. **Preparation**:
    - **Backup Critical Data**: Before removal, back up any critical data from System B if possible. Ensure this backup is stored securely and not on the same compromised network.
    - **Documentation**: Document the current state of the system, including running processes, network connections, and any signs of the attack for future analysis.
2. **Physical Removal**:
    - **Shutdown**: Perform a controlled shutdown of System B to avoid data corruption and further compromise.
    - **Physical Disconnection**: Physically disconnect all network cables and power down System B.
3. **System Removal**:
    - **Move to Secure Location**: Transport System B to a secure forensic lab for further analysis and investigation.
    - **Secure Storage**: Store System B securely to prevent unauthorized access during the investigation.

Data Sanitization: Purge, Destroy, and Clear

Objective: To remove sensitive information from compromised disks before disposal to ensure data confidentiality.

Purge

- **Definition**: Purging involves rendering data unrecoverable by overwriting it or using other methods that comply with specific standards.
- **Techniques**:
    - **Overwriting**: Use specialized software to overwrite the entire disk multiple times with random data.
    - **Degaussing**: Use a degausser to disrupt the magnetic fields on the disk, making data recovery impossible.
- **Usage**: Suitable when the media will be reused within the organization or for less sensitive data that doesn’t require complete destruction.

Destroy

- **Definition**: Destroying involves physically damaging the disk to the point where data recovery is impossible.
- **Techniques**:

    - **Shredding**: Use a disk shredder to physically break the disk into small pieces.
    - **Incineration**: Burn the disk in a controlled environment to ensure it is completely destroyed.
- **Usage**: Appropriate for highly sensitive data or when the media will be disposed of outside the organization. Ensures total data destruction.

Clear

- **Definition**: Clearing involves using software or hardware to reset storage media to its initial state, effectively removing user data but potentially leaving some data recoverable with advanced methods.
- **Techniques**:
    - **Factory Reset**: Perform a factory reset on the storage device if supported.
    - **Formatting**: Use low-level formatting to clear data from the disk.
- **Usage**: Typically used for less sensitive data or when the risk of data recovery is acceptable. Often used as a preliminary step before more stringent measures like purging or destroying.

Response Plan Implementation

1. **Isolate System B**: Follow the isolation steps to immediately contain the threat and prevent further damage.
2. **Remove System B**: Carefully shut down, disconnect, and transport System B to a secure forensic lab.
3. **Data Sanitization**: Choose the appropriate method (purge, destroy, or clear) based on the sensitivity of the data and the future use or disposal plan for the disks.