Incident Response Simulation

Scenario: Malware Attack on Corporate Network

Context: A corporate network has been compromised by a malware attack. The malware, designed to exfiltrate sensitive data, has infiltrated the company's systems through a malicious email attachment. Critical business operations are at risk, and there is potential for significant data loss and financial damage.

Objectives:

- Test the company's ability to detect and respond to malware attacks.
- Evaluate the coordination and efficiency of the incident response team.
- Identify gaps in the current cybersecurity infrastructure and response procedure.

Scope:

- The malware has infected several key servers and workstations.
- Sensitive corporate data, including financial records and intellectual property, is at risk.
- The incident response team must work to detect, contain, and mitigate the malware attack while preserving evidence for forensic analysis.

Incident Detection

Intern Roles:

- Incident Response Coordinator
    - Will oversee the response efforts and ensures communication between team members.
- Network Security Analyst
    - Will monitor network traffic and analyze logs to detect malicious activity.
- System Administrator
    - Will handle the affected systems, applies patches, and restore backups.
- Forensic Analyst
    - Will conduct forensic analysis on compromised systems to determine the attack's origin and method.
- Communication Specialist
    - Will manage internal and external communications.

Incident Detection Simulation:

The Network Security Analyst detects unusual network traffic patterns and multiple alerts from endpoint protection systems. Monitoring tools indicate the presence of known malware signatures and attempts to connect to external command and control servers. Additionally, logs show unauthorized access to sensitive files and data transfers to unknown external IP addresses.

Analysis Tool:

For an effective forensic analysis of the malware attack, Wireshark should be used. Wireshark is a powerful network protocol analyzer that can capture and interactively browse the traffic running on a computer network.

Response Plan Execution

Initiating the Incident Response Plant:

1. Containment
    - Isolate infected systems from the network to prevent further spread of malware.
    - Disable compromised user accounts and change passwords.
2. Mitigation
    - Deploy endpoint protection tools to quarantine and remove infected files.
    - Restore affected systems from the latest clean backups to minimize data loss.
    - Apply security patches to close vulnerabilities exploited by the attackers.

Forensic Analysis

1. Image Affected Systems
    - Create disk images of affected servers and workstations for detailed analysis.
2. Analyze Malware
    - Identify the malware variant and analyze its behavior.
    - Determine the attack vector used to infiltrate the network, for examples:
        - Phishing Email
        - Exploit Kit
3. Gather Evidence
    - Collect relevant logs, network traffic data, and communication records.
    - Document the attack timeline and the actions taken by the attackers.

Post Incident Assessment

Review and Assessment:

1. Effectiveness of Response
   - Evaluate how well the incident response plan was executed.
   - Identify any delays or issues in detecting and responding to the incident.
2. Lessons
   - Highlight successful strategies and areas that need improvements.
   - Recommend enhancements to detections tools, response procedures, and employee training programs.

Improvements for the Company

1. Enhance Detection and Monitoring Tools
   - Upgrade Endpoint Protection
   - Deploy Network Traffic Analysis Tools
   - Integrate Security Information and Event Management Systems
2. Refine Incident Response Protocols
   - Develop Comprehensive Playbooks
   - Conduct Regular Drills and Simulations
   - Implement an Incident Response Platform
3. Strengthen Employee Training Programs
   - Phishing Awareness Training
   - Cybersecurity Best Practices
   - Role-Specific Training