Incident Report Analysis

Step 1: Summary of the Security Event

- Security Event: The organization experienced a DDoS attack characterized by a flood of ICMP packets, which disrupted network services for two hours.

- Cause: The attack was made possible due to an unconfigured firewall that allowed excessive ICMP traffic into the network.

- Impact: Internal network services became unresponsive, hindering access to network resources for employees and clients.

- Response: The incident management team blocked incoming ICMP packets, stopped non-critical services, and restored critical services. The cybersecurity team implemented new firewall rules, source IP verification, network monitoring software, and an IDS/IPS system.

Identify: Type of Attack and Affected Systems

- Type of Attack: Distributed Denial of Service (DDoS)

- Affected Systems: Internal network services, including web design services and graphic design resources.

- Attack Source: Malicious actor sending ICMP flood through an unconfigured firewall.

Protect: Immediate Action Plan

- Updates Needed:

- Reconfigure the firewall to block unnecessary ICMP packets and verify incoming source IP addresses.

- Develop and implement security policies and procedures for regular firewall audits and updates.

- Provide training for employees on recognizing and responding to potential DDoS attacks.

Detect: Monitoring and Analysis

- Monitoring Strategies:

- Implement network monitoring tools to track traffic patterns and identify anomalies, especially focusing on incoming ICMP packets.

- Regularly analyze user activity logs to differentiate between authorized and unauthorized access.

- Set up alerts for unusual spikes in traffic or abnormal patterns that deviate from standard operating procedures.

Respond: Future Incident Response Plan

- Containment Procedures:

- Isolate affected devices immediately to prevent the spread of the attack.

- Disable non-critical services during an attack to preserve network integrity.

- Neutralization:

- Use firewall rules to block incoming malicious traffic and deploy rate-limiting for ICMP packets.

- Engage in real-time analysis to identify the attack vectors and mitigate them swiftly.

- Data Analysis:

- Maintain logs of incoming traffic during an incident for post-event analysis to understand attack vectors and improve defenses.

- Improving Recovery Process:

- Create a backup strategy for critical services and data to ensure rapid recovery.

- Regularly test recovery procedures to ensure effectiveness and reduce downtime in the event of an incident.

Recover: Restoration Steps

- Immediate Recovery Needs:

- Access to backup systems and data to restore affected services.

- Documentation of the incident to review lessons learned and implement improvements.

- Processes for Recovery:

- Utilize backup systems to restore normal operations.

- Conduct a post-incident review meeting to discuss the response, recovery, and adjustments needed for future incidents.