**Incident Report Analysis**

**Summary**

Our organization faced a severe network disruption when all services became unresponsive. I led the investigation and confirmed the root cause was a Distributed Denial of Service (DDoS) attack. Specifically, an ICMP flood overwhelmed our network, exhausting its resources. In collaboration with my team, we blocked malicious traffic, prioritized critical services for restoration, and executed long-term mitigation strategies to secure the network.

**Identify**

Upon receiving service disruption alerts, I immediately investigated to identify the root cause. I analyzed network traffic logs, which revealed an unusually high volume of ICMP requests from multiple external sources. These packets were overwhelming our servers, resulting in a complete system crash. My primary focus was determining the attack vector, isolating compromised systems, and ensuring minimal impact on our core infrastructure.

**Actions Taken**

- Conducted traffic analysis using Wireshark and Splunk to identify the IP addresses responsible for the flood.

- Verified system logs and firewall activity to confirm the DDoS nature of the attack.

- Identified entry points through which excessive traffic was routed to internal resources.

**Protect**

I implemented immediate protections to prevent further damage, focusing on fortifying our network perimeter and internal defenses. This included creating

custom firewall rules and rate-limiting ICMP requests to reduce the strain on the network.

**Proactive Measures:**

- Configured firewall rules to block malicious IP addresses and restrict the rate of incoming ICMP traffic.

- Deployed Intrusion Detection and Prevention Systems (IDS/IPS) to monitor and block malicious traffic in real-time actively.

- Implemented network segmentation to isolate critical systems, ensuring that essential services remained operational even during the attack.

**Detect**

I refined our detection mechanisms to improve response times for similar future incidents. This involved enhancing the capabilities of our monitoring tools to detect abnormal traffic patterns earlier and more effectively.

**Detection Strategies:**

- Activated Network Behavior Analysis (NBA) to identify unusual spikes in traffic, particularly ICMP requests.

- Configured Syslog servers to collect detailed logs from all network devices, ensuring early detection of irregular traffic.

- Set up real-time alerts for anomalous activities, including traffic surges and spoofed IP addresses, to enable faster incident response.

**Respond**

I spearheaded the incident response during the attack, coordinating with various teams to execute a structured recovery process. My focus was on prioritizing.

services essential for business continuity while ensuring the attack vector was fully neutralized.

**Incident Response Plan:**

- Temporarily disabled non-critical services to reduce overall traffic load on the network, preventing further resource exhaustion.

- Engaged with our Internet Service Provider (ISP) to implement upstream traffic filtering, mitigating the DDoS attack before it reached our servers.

- Geolocation-based filtering was used to block traffic from specific regions associated with the attack, minimizing external threat vectors.

**Recover**

After neutralizing the attack, I worked with the team to restore all services. Our priority was to ensure that critical services were brought back online with minimal downtime while securing other parts of the infrastructure.

**Recovery Actions:**

- Restored essential services by rerouting traffic through backup servers and using load balancing to distribute the traffic more evenly.

- Conducted a full system audit to verify that no malicious code or configuration changes had been made during the attack.

- Implemented daily incremental backups and full weekly backups to safeguard data in the event of future incidents.

**Future Enhancements and Recommendations**

Moving forward, I recommend implementing several long-term security measures to prevent similar attacks from occurring. These include upgrading our DDoS

mitigation tools and ensuring that all critical systems are equipped to handle unexpected traffic spikes.

**Long-Term Strategies:**

- Implement advanced DDoS mitigation services that can absorb and mitigate large-scale attacks before they reach our network perimeter.

- Continuously train all IT staff on the latest DDoS mitigation techniques and incident response protocols.

- Perform regular penetration testing to assess the strength of our current defenses and uncover any vulnerabilities.

- Establish a more comprehensive Business Continuity Plan (BCP) to ensure the organization can maintain operations even during large-scale disruptions.

**Conclusion**

The DDoS attack exploited our network’s vulnerability to high volumes of ICMP traffic. By promptly identifying and mitigating the attack, I helped restore services and strengthened our defense mechanisms to protect against future threats. This incident emphasized the importance of constant monitoring, real-time response capabilities, and proactive defense strategies. The steps taken in response to this attack have restored normal operations and significantly improved our network’s resilience.