Incident Report Analysis

Summary
The company experienced a security incident in which all network services abruptly became unresponsive. The cybersecurity team identified the cause as a distributed denial-of-service (DDoS) attack involving a large volume of incoming ICMP packets. In response, the team blocked the malicious traffic and temporarily shut down non-critical network services to prioritize restoring essential operations.

Identify
An attacker or group of attackers launched an ICMP flood targeting the company. The attack impacted the entire internal network, requiring all critical resources to be secured, stabilized, and returned to normal operation.

Protect
To mitigate future attacks, the cybersecurity team created a firewall rule to throttle incoming ICMP packet rates and deployed an IDS/IPS solution to filter ICMP traffic that exhibited suspicious patterns.

Detect
The team enabled source IP verification on the firewall to identify spoofed ICMP traffic and implemented network monitoring tools to alert on unusual traffic behavior or spikes.

Respond
For similar future events, the cybersecurity team will isolate compromised or affected systems to prevent further disruption. They will focus on restoring critical systems first, then review logs and network activity for indicators of malicious behavior. All incidents will be reported to management and legal authorities as necessary.

Recover
Recovery from an ICMP flood DDoS attack involves restoring access to all network services. Future ICMP flood attempts can be blocked at the firewall. During recovery, non-essential services should be temporarily disabled to reduce strain on the network, while critical services are restored first. Once the excess ICMP traffic subsides, remaining services can be safely brought back online.

Reflections / Notes:

- This incident highlighted the importance of having proactive DDoS mitigation measures already in place rather than reacting after disruption occurs.
- ICMP traffic, while useful for diagnostics, can easily be weaponized, emphasizing the need for stricter rate limiting and monitoring of network utility protocols.
- The team's quick response minimized downtime, but the event revealed gaps in traffic monitoring capabilities that should be addressed with more robust analytics and alerting tools.
- Improved network segmentation could help contain similar attacks and prevent full-network impact in the future.
- The event reinforced the value of regular incident response drills to ensure the team can act quickly and consistently under pressure.
- Documentation and communication were essential during the incident; refining reporting procedures will help streamline coordination with leadership and external authorities.
- Overall, the incident served as a reminder that even basic attack vectors like ICMP flooding can cause major disruption if defenses are not continuously evaluated and updated.