Incident report analysis

Summary	The company faced a security incident when all network services abruptly became unresponsive. The cybersecurity team identified the cause as a distributed denial of service (DDoS) attack, which involved a flood of incoming ICMP packets. In response, the team blocked the attack and halted all non-essential network services to prioritize the restoration of critical network services.
Identify	A malicious actor or actors launched an ICMP flood attack on the company, impacting the entire internal network. It was necessary to secure and restore all critical network resources to their functioning state.
Protect	The cybersecurity team established a new firewall rule to limit the rate of incoming ICMP packets and deployed an IDS/IPS system to filter out ICMP traffic with suspicious characteristics.
Detect	The cybersecurity team configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and implemented network monitoring software to detect abnormal traffic patterns.
Respond	In future security events, the cybersecurity team will isolate affected systems to prevent further network disruption. They will focus on restoring any critical systems and services impacted by the event. Subsequently, the team will analyze network logs for suspicious and abnormal activity. All incidents will be reported to upper management and, if applicable, to the appropriate legal authorities.
Recover	To recover from a DDoS attack by ICMP flooding, network services must be

	restored to normal operation. In the future, external ICMP flood attacks can be blocked at the firewall. All non-critical network services should be stopped to reduce internal traffic. Priority should be given to restoring critical network services first. Finally, once the flood of ICMP packets has subsided, all non-critical network systems and services can be brought back online.

Reflections/Notes:

It is clear that the company faced a significant threat from an ICMP flood DDoS attack that disrupted all network services. The cybersecurity team's immediate response was effective in mitigating the damage. Implementing new firewall rules is a crucial step in enhancing future security measures. Additionally, verifying source IP addresses to check for spoofing and employing network monitoring software to detect abnormal patterns further strengthened the defense strategy.

The plan to isolate affected systems during future incidents, prioritize the restoration of critical services, analyze network logs for suspicious activity, and report incidents to management and legal authorities ensures a comprehensive approach to managing and preventing similar threats.

This incident highlights the importance of proactive security measures and a structured response plan to safeguard network integrity.