Incident report analysis

Summary	A security incident occurred within the company resulting in a sudden halt of all network services. Investigation conducted by the cybersecurity team revealed that the disruption stemmed from a distributed denial of service (DDoS) attack, characterized by an overwhelming influx of ICMP packets. To counteract the attack and facilitate the restoration of critical network services, immediate measures were taken to block the malicious activity and suspend non-essential network services.
Identify	The company fell victim to a deliberate ICMP flood attack, orchestrated by one or multiple malicious actors. As a result, the internal network suffered widespread disruption. As a result, all critical network resources needed to be made secure and restored to full functionality.
Protect	The cybersecurity team took proactive measures in response to this incident. Firstly, a new firewall rule was deployed to restrict the influx of incoming ICMP packets, thereby limiting their rate. Additionally, an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) were implemented to analyze and filter out ICMP traffic exhibiting suspicious attributes.
Detect	The cybersecurity team enhanced network security by implementing source IP address verification on the firewall and deploying network monitoring software. These measures aimed to detect and mitigate spoofed IP addresses on incoming ICMP packets while identifying abnormal traffic patterns.
Respond	In response to future security events, the cybersecurity team will isolate affected systems to contain any potential disruptions to the network. They will prioritize the restoration of critical systems and services impacted by the event. Additionally, the team will conduct a thorough analysis of network logs

	to identify any signs of suspicious or abnormal activity. Finally, they will diligently report all incidents to upper management and, if necessary, involve relevant legal authorities.
Recover	In order to recover from the ICMP flooding DDoS attack, it is crucial to restore network services to their normal functioning state. To prevent future external ICMP flood attacks, implementing firewall rules to block them is recommended. As a proactive measure, suspending non-critical network services helps reduce internal network traffic. Prioritizing the restoration of critical network services is essential. Once the flood of ICMP packets has subsided, non-critical network systems and services can be safely brought back online.

Reflections/Notes: The cybersecurity team showcased expertise in incident response through proactive measures such as firewall configuration and network monitoring. Their swift actions to isolate and restore systems, minimized disruptions. Thorough investigation, compliance, and prioritizing critical services ensured a secure recovery. This incident emphasizes the need for robust security measures, continuous monitoring, and ongoing improvements to safeguard the network and sensitive information.