Incident Report Analysis

Summary	The incident involved a distributed denial of services (DDoS) attack on the company's network and the attack was conducted via a flood of incoming ICMP packets. This caused a two-hour disruption of network services. The cybersecurity team responded by blocking incoming ICMP packets and taking all non-essential network services offline, and restoring critical services.
Identify	The company was targeted by a malicious actor and subjected to an ICMP flood attack. This attack severely impacted the company's network, which required immediate action to secure and restore the functionality of critical network resources.
Protect	The cybersecurity team has implemented 2 measures to protect its resources: • A new firewall rule to limit the rate of incoming ICMP packets. • An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	The cybersecurity team has implemented 2 measures to detect threats: • Source IP address verification on the firewall to detect spoofed IP addresses on incoming ICMP packets. • Deployed network monitoring software to detect abnormal traffic patterns.
Respond	For security incidents in the future, the cybersecurity team will first isolate impacted systems to minimize network disruption. Then, the team will restore essential systems and services to enable business continuity. Following that, the team will analyze network logs for any signs of further irregular or suspicious behavior. Last but not least, the team will update upper management and legal authorities, if necessary, about all security incidents.

Recover	In the event of a DDoS attack, restoring access to network services to their normal operations should be prioritized. To alleviate network congestion, all non-essential network services should be halted, while critical network services are progressively brought back online. These non-essential network services can be gradually restored once the ICMP flood has subsided. With the implementation of the new firewall rule and an IDS/IPS, future external ICMP flood attacks will be prevented.

Reflections/Notes: NIL