Incident report analysis

Summary	The company experienced a security incident and all the network devices stopped responding. The cybersecurity team the incident was caused by a distributed denial of service (DDoS) attack through a flood of incoming ICMP packets. The team responded by blocking the attack and stopping all non-critical network service, so that critical network services can be restored.
Identify	Malicious actor or actors targeted the company with an ICMP flood attack. The attack compromised the entire internal network. All the critical network resources needed to be secured and restored to a functional state.
Protect	The cybersecurity team implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious activities.
Detect	The cybersecurity team configured the 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	The cybersecurity team will isolate the affected system so that further disruption can be avoided. Critical systems and services will be attempted to be restored. The team will analyze network logs to check for suspicious and abnormal activities. They will also report all incidents to the upper management and appropriate legal authorities for further actions.
Recover	To recover from a DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. In the future, external ICMP

	flood attacks can be blocked by the firewall. Next, all non-critical network services should be stopped to reduce internal network traffic. Then, critical network services should be restored first. Finally, when the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online.

Reflections/Notes: