Incident report analysis

Summary	Our organization experienced a DDoS attack, an ICMP flooding attack specifically, which compromised the internal network for two hours until it was resolved. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. They found that the malicious actor exploited the unconfigured firewall, which allowed them to overwhelm the company's network through a DDoS attack.
Identify	A malicious actor or group of actors targeted the company with an ICMP flood attack, resulting in a disruption of the entire internal network. All critical network resources required immediate securing and restoration to operational status.
Protect	In response, the cybersecurity team implemented a new firewall rule to limit the rate of incoming ICMP packets, along with an IDS/IPS system to filter ICMP traffic exhibiting suspicious characteristics. They also enabled source IP address verification on the firewall to detect and block spoofed IP addresses, and deployed network monitoring software to identify abnormal traffic patterns in real time.
Detect	The cybersecurity team implemented a new firewall rule to limit the rate of incoming ICMP packets, along with an IDS/IPS system to filter ICMP traffic exhibiting suspicious characteristics. They also enabled source IP address verification on the firewall to detect and block spoofed IP addresses, and deployed network monitoring software to identify abnormal traffic patterns in real time.

Respond	For future security incidents, the cybersecurity team will isolate affected systems promptly to prevent further network disruption, restore any critical systems and services impacted, and analyze network logs to detect suspicious or anomalous activity. All incidents will be reported to senior management and, where applicable, to the relevant legal authorities.
Recover	To recover from an ICMP flood–based DDoS attack, network service access must be restored to normal operating conditions. Future prevention measures include blocking external ICMP flood traffic at the firewall. During recovery, non-critical network services should be temporarily suspended to reduce internal traffic load, while priority is given to restoring critical services first. Once the ICMP traffic flood subsides, all non-critical systems and services can be safely brought back online.

Reflections/Notes: