Incident report analysis

Summary	Today our organization's network services suddenly stopped responding. After investigation by the team, they found that the organization experienced a DDoS attack caused by a malicious actor that had sent a flood of ICMP pings into the company's network. The incident management team managed to restore critical network services after 2 hours by blocking incoming ICMP packets and stopping all non-critical network services.
Identify	The team found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious actor to overwhelm the company's internal network through a DDoS attack called ICMP flood attack.
Protect	To address it, the team implemented: • 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 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	For future incidents, the team will isolate affected systems to prevent further disruption to the network. They will attempt to restore any critical systems and services that were disrupted by the incident. The team will also report all incidents to upper management and appropriate legal authorities, if applicable.
Recover	To recover from 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 at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online.

Reflections/Notes: