Incident report analysis

Summary	The company had been alerted of a potential DDoS attack, which compromised the internal network and caused it to stop responding due to an incoming flood of ICMP packets. 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. The attack took the team 2 hours to resolve.
Identify	The incident management team had audited internal networks, systems, devices, and access privileges to identify potential gaps in security that could lead to the attack. The team found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall, which indicated that this has been an DDoS ICMP flood attack. All critical network resources needed to be secured and restored to a functioning state.
Protect	The team had 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 characteristics.
Detect	The team configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. Additionally, a network monitoring software is used to detect abnormal traffic patterns.
Respond	For future security events, the team will isolate affected resources and contain them from further disrupting the network. The team will aim to restore critical work services and systems as soon as possible to allow work to resume as

	before. Then, the team will analyze network logs to check for suspicious and abnormal activity. The team will also report all incidents to upper management and appropriate legal authorities, if applicable.
Recover	To recover from a DDoS attack caused by ICMP flooding, network services must be restored to normal operation. To prevent future attacks, external ICMP flood traffic should be blocked at the firewall. Non-essential network services should then be temporarily disabled to minimize internal traffic. Priority should be given to restoring critical services first. Once the ICMP packet flood has subsided, all non-essential network systems and services can be brought back online.

Reflections/Notes: