Incident report analysis

Summary	The organisation recently experienced a DDoS attack, which compromised the internal network. During the attack, network services suddenly stopped 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.
Identify	An ICMP flood attack was used to slow down ordinary business operations. The attack affected the entire network. Critical network resources needed to be secured and restored.
Protect	To address this security event, the network security 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 characteristics.
Detect	The network security team reconfigured the firewall to verify source IP addresses to check for spoofed IP addresses on incoming ICMP packets. Network monitoring software was also implemented to detect abnormal traffic patterns.
Respond	In the future, the cybersecurity team will isolate affected systems to prevent disruption to the network. They will restore critical systems and services affected by the event. The logs will be analysed after the event and suspicious activity will be investigated. The team will report all incidents to upper management and legal authority, if required.
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 at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. 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: