Incident report analysis

Summary	An incident recently occurred rendering the organization's network unresponsive for a period of two hours. The attack was caused by a sudden 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 and restoring critical network services. On investigation, the security 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 attacker to overwhelm the network through a Distributed Denial of Service (DDoS) attack.
Identify	After auditing the company network and associated devices, the security team found that the attacker had exploited a misconfigured and therefore vulnerable firewall which allowed them to flood the internal network with ICMP pings.
Protect	To protect against this event, the security team have implemented: • A new firewall rule to limit the rate of incoming ICMP packets. • Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets.
Detect	To aid in detection of this type of event, the security team have implemented: • Network monitoring software to detect abnormal traffic patterns. • An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Respond	The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services and restoring critical network services. In the future, consideration should be taken to isolate the affected systems. Once critical

	systems were restored, the incident response team analysed the logs for suspicious activity.
Recover	In the future, external ICMP flood attacks can be blocked at the firewall. To recover, the security team stopped all non-critical network services to reduce internal network traffic. Critical services were then restored first, then once the flood of ICMP packets had been blocked/timed out, non-critical network services were brought back online.

Reflections/Notes: