Incident report analysis

Summary	The organization experienced a DDoS attack lasting approximately 2 hours before being resolved. The organization's network services were brought to a halt due to an incoming flood of ICMP packets alongside internal network traffic being unable to access any network resources. Steps were taken to block incoming ICMP packets, halting all non-critical network services and restoring critical network services.
Identify	The incident management team audited the assets that were affected by the attack, and found the organization's network services were exploited due to an unconfigured firewall. This allowed the attacker to deploy a DDoS attack to the company's network. This affected the internal network and prevented employees from accessing the internal network.
Protect	The network security team responded by implementing a new firewall rule to limit the rate of incoming ICMP packets, source IP address verification on incoming ICMP packets, and an IPS system to filter any suspicious ICMP traffic.
Detect	In order to prevent incidents like this DDoS attack in the future, further implementation of a network monitoring software, alongside an IDS system have been implemented.
Respond	The incident management team responded by blocking any incoming ICMP packets, stopping non-critical network services, and restoring critical network services. In response to the incident, 2 new firewall rules were created: Limitation of the rate of incoming ICMP packets, source IP address verification to prevent spoofing of incoming ICMP packets.
Recover	All network services were affected by the DDoS attack, after implementation of

	safeguards, steps were taken to restore critical network services first, then non-critical network services second. Implementation of firewall configurations will prevent any attack similar to this one in the future.