Incident report analysis

Summary	Our organization recently experienced a DDoS attack because a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. It compromised the internal network for two hours until it was resolved.
Identify	The company's cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall.
Protect	The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Detect	To address this security event, the network security team 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 • 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 offline, and restoring critical network services.
Recover	

Reflections/Notes: