Incident report analysis

Summary	During the attack, your organization's 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. When this incident was investigated we 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 malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.
Identify	The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. The team found that there was an unconfigured firewall on the network and it was exploited to send a flood of ICMP packets.
Protect	The team implemented a new firewall rule to limit the rate of incoming ICMP packets.The firewalls were configured to verify the source IP address for IP address spoofing.
Detect	IDS/IPS were implemented to filter out some ICMP traffic based on suspicious characteristics, and to monitor and detect abnormal traffic patterns.
Respond	To respond to this attack incoming ICMP packets were blocked , stopping all non-critical network services offline, and restoring critical network services.
Recover	Since it was a DDoS attack our organization was not able to identify the correct source IP address of the malicious attacker but to recover from this attack all

	incoming ICMP packets were blocked and an IDS/IPS was installed to filter out the spoofed IP addresses in future and all the network services were then restored.

Reflections/Notes: