Incident report analysis

Summary	Our organization's network services stopped responding for two hours due to a successful DDoS (Distributed Denial of Service) attack from a malicious actor. The attacker was able to complete this attack by sending a flood of ICMP pings to the company network through an unconfigured firewall. This vulnerability allowed the attacker to overwhelm the company's network. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Identify	The type of attack executed was a DDoS (Distributed Denial of Service) attack. The entry point was through a misconfigured firewall. The company's entire network was affected by the attack as all network services were down for 2 hours.
Protect	In order to protect against the organization the following systems should be put in place immediately. Firewall Configuration ● Firewall rule limiting the rate of incoming ICMP packets. ● Verification of source IP address on firewall to check for spoofed IP addresses on inbound ICMP packets. ● Network monitoring software to detect abnormal traffic patterns. ● Implement IDS/IPS and configure to filter out suspicious ICMP traffic characteristics.
Detect	In order to detect an attack similar to this so that it can be prevented, the following is recommended. ● Monitor network traffic and report suspicious ICMP behavior.

	● Configure IDS/IPS and create custom alerts in SIEM that will notify the security team upon intrusion.
Respond	In future security events, the team will isolate affected systems to prevent network disruption. They will also attempt to restore any systems and services that were disrupted by the event. Lastly, network traffic will be analyzed for suspicious activity and reported accordingly.
Recover	In order to recover from a DDoS attack by ICMP flooding, access to network services must be restored to a normal 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 traffic. Next, critical network services should be restored. Lastly, once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online.

Reflections/Notes: