Incident report analysis

Summary	Recently, our organization's network services suddenly stopped responding due to a flood of ICMP packets that overwhelmed the network. This prevented normal internal network traffic from accessing network resources. The incident affected our network for two hours until it was resolved by the incident management team. The team blocked all ICMP packets, stopping all non-critical network services offline, and restoring critical services. After an investigation by the cybersecurity team, it was found that a malicious actor had perpetrated a distributed denial of service attack (DDoS), flooding ICMP pings into the company's network.
Identify	The cybersecurity team's investigation found that a malicious actor or actors flooded the network with ICMP pings through an unconfigured firewall. This vulnerability allowed the attacker to overwhelm the network through a DDoS, affecting the entire internal network.
Protect	To protect against similar attacks, the security team has implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. The team recommends performing routine penetration testing to suss out vulnerabilities in the network.
Detect	To detect future attacks, the team has modified the firewall to include source IP address verification to check for spoofed IP addresses on incoming ICMP packets and implemented network monitoring software to detect abnormal traffic patterns. The team recommends using SIEMs

	tools to facilitate the efficiency of detections.
Respond	The cybersecurity team will enact network segmentation to limit and isolate the impact of future attacks. The team will analyze network logs to identify abnormalities in traffic. All incidents will be reported to leadership and legal authorities, when applicable. Procedures will be set to ensure all cybersecurity teams are trained on a playbook that walks them through each step of managing a DDoS attack, as well as other common attack vectors.
Recover	To enable fast recovery, the cybersecurity team will define baseline configurations to reference and implement backups of all systems to use in the event of a compromise network system. In the event of future attacks, the team will cease all non-critical network services. All critical services will then be restored. After this, non-critical systems will be addressed and brought online.

Reflections/Notes: