Incident report analysis

Summary	Our organization recently faced a DDoS attack that disrupted internal network services for two hours. The attack involved a flood of ICMP packets, rendering normal network traffic inaccessible. The incident management team mitigated the attack by blocking incoming ICMP packets, taking non critical services offline temporarily, and restoring critical services. The cybersecurity team discovered that the attack exploited an unconfigured firewall, allowing a malicious actor to conduct a DDoS attack by overwhelming the network with ICMP pings.
Identify	Our 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 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	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
Detect	To detect new attacks in the future, the team implemented source IP address verification on the firewall to check for the spoofed IP addresses, network monitoring softwares to detect abnormal traffic patterns and an IDS/IPS

	system to filter out ICMP traffic based on its characteristics.
Respond	For future security events, the cybersecurity team will isolate affected systems to prevent further disruption to the network. They will attempt to restore any critical systems and services that were disrupted by the event. Then, the team will analyze network logs to check for suspicious and abnormal activity. The team will also report all incidents to upper management and appropriate legal authorities, if applicable.
Recover	To recover from a DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning 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 network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online.

Reflections/Notes: