Incident report analysis

Summary	The organization’s internal network services suddenly stopped responding, internal network traffic could not access any network resources. The cybersecurity team found that the disruption was caused by a distributed denial of service (DDoS) attack and responded by blocking the attack and stopping all non-critical services to restore critical network services.
Identify	The cybersecurity team investigated the security events and found a malicious actor had targeted the organization with an ICMP flood attack through an unconfigured firewall. Since the entire internal network was affected, the team must secure all critical network resources and restore the network to a functional state.
Protect	The network security team implemented new firewall rules to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	To detect abnormal traffic patterns, the team implemented network monitoring software and source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets.
Respond	For future security events, the cybersecurity team will isolate the affected systems to reduce the attack surface and attempt to restore critical systems and services disrupted by the event. Analysis of network logs will then be performed to check for suspicious activity and report all incidents to upper management and appropriate legal authorities.
Recover	To recover from a DDoS attack by ICMP flooding, access to network services needs to be restored to a functioning state. In the future, external ICMP flood attacks can be blocked by 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 has timed out, all non-critical network systems and services can be brought back online.

Reflections/Notes: