Incident report analysis

Summary	The company faced a security issue when all network services suddenly went offline. The cybersecurity team discovered that this disruption was due to a distributed denial of service (DDoS) attack involving a flood of incoming ICMP packets. To address this, they blocked the attack and temporarily halted non-essential network services to restore the critical ones.
Identify	A malicious actor or actors targeted the company with an ICMP flood attack. The entire internal network was affected. All critical network resources needed to be secured and restored to a functioning state.
Protect	The cybersecurity team 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.
Detect	The cybersecurity team configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and implemented network monitoring software to detect abnormal traffic patterns.
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 To bounce back from an ICMP flood-based DDoS attack, network services must return to their normal state. In the future, the firewall will be equipped to block external ICMP flood attacks. Non-essential network services will be paused to reduce internal network traffic. Critical network services will be prioritized for restoration. Once the flood of ICMP packets has ceased, non-essential network systems and services can be brought back online.

Reflections/Notes: