Incident report analysis

Summary	The company encountered a security incident where all network services unexpectedly became unresponsive. The cybersecurity team identified the cause as a Distributed Denial of Service (DDoS) attack, triggered by an overwhelming surge of ICMP packets. In response, the team mitigated the attack by blocking the malicious traffic and temporarily halting all non-essential network services, allowing the restoration of critical services.
Identify	A malicious actor sent a flood of ICMP pings into the company's network through an un-configured firewall. The entire internal network got compromised.
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	In the event of future security incidents, the cybersecurity team will promptly isolate affected systems to prevent additional disruptions across the network. Their priority will be to restore any critical systems and services that were impacted. Following containment, the team will analyze network logs to identify suspicious or abnormal activity. All incidents will be reported to upper management and, if necessary, to the appropriate legal authorities.

Recover	To recover from a DDoS attack caused by ICMP flooding, network services must be restored to normal operation. Future external ICMP flood attacks can be mitigated by blocking them at the firewall. During an attack, non-critical network services should be stopped to reduce internal traffic, allowing critical services to be restored first. Once the ICMP flood subsides, non-critical systems and services can be safely brought back online.

Reflections/Notes: