Incident report analysis

Summary	The company encountered a security event when all network services abruptly ceased functioning. The cybersecurity team identified the disruption as a result of a distributed denial of service (DDoS) attack involving a flood of incoming ICMP packets. In response, the team blocked the attack and halted all non-critical network services to restore the critical network services.
Identify	After investigation, the company's cybersecurity team found that an unknown malicious actor sent a flood of ICMP pings into the company's networks through an unconfigured firewall. This allowed the attacker to overwhelm our servers through a distributed denial of service (DDoS) attack, resulting in an unusable network for two hours until systems could be restored.
Protect	The team has implemented new firewall rules limiting the rate of incoming ICMP packets, as well as verifying the source IP addresses for each packet to ensure they are not spoofed. Network monitoring software was put in place to detect abnormal network traffic patterns, and an IDS/IPS system is now being used to filter out suspicious ICMP traffic automatically.
Detect	Network monitoring software and IDS systems are now in use to detect unusual network traffic and alert the team to possible DDoS attacks immediately.
Respond	The team responded to this incident by blocking all incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Recover	By restoring the affected systems and implementing better network controls such as configured firewalls and IDS/IPS systems, the team has lowered the risk to company assets by reducing the severity and likelihood of similar future attacks.