Incident report analysis

Summary	The company experienced a security event when all network services suddenly stopped responding for two hours. The cybersecurity team found the disruption was caused by a distributed denial of services (DDoS) attack through a flood of incoming ICMP packets. The team also discovered an unconquered firewall in the company's network, allowing the malicious attacker to overwhelm the network via DDoS attack. The team responded by blocking the attack and stopping all non-critical network services, so that critical network services could be restored.
Identify	A distributed denial of service (DDoS) attack occurred and affected the entire internal company's network. Internal network traffic was flooded with ICMP packets. All critical network resources needed to be secured and restored to a functioning state.
Protect	To prevent the same attack from happening again, the company's cybersecurity team implemented and configured a new firewall rule to filter out suspicious ICMP traffic.
Detect	The cybersecurity team had network monitoring software installed in order to inspect unusual traffic activity. The team also configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets.
Respond	For the same future security events, the cybersecurity team will isolate affected systems and devices to prevent further disruption to the network by blocking incoming ICMP packets immediately, stopping all non-critical network services online. The team will then restore critical network services and systems that were affected. Then, the team will analyze network logs to track unusual network traffic patterns.

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: