Incident report analysis

Summary	Something unusual was sensed when all of a sudden the internal network stopped responding. The cybersecurity team found that the internal network was affected by the attack known as Distributed Denial of Service (DDoS) incident that exploited an unconfigured firewall. A malicious actor flooded the organization’s network with ICMP packets, overwhelming the system and causing network services to stop responding. This affected the organization’s internal traffic, making network resources inaccessible. The cybersecurity team blocked the ICMP packets and stopped all non-critical services and restored critical network service. The attack lasted for two hours before being resolved.
Identify	A company internal network was flooded with the ICMP ping packets which stopped the network from responding and was needed to halt all non-critical services and restore the critical services.
Protect	A new Firewall configuration rule was put in place to filter all incoming traffic and to limit the rate of incoming traffic and an IDS/IPS system to filter out all ICMP traffic based on the suspicious characteristics.
Detect	The cybersecurity team Implemented source IP address verification on the firewall to identify and block spoofed IP addresses in incoming ICMP packets and also implemented network monitoring software to detect abnormal traffic patterns.
Respond	For future cybersecurity teams will isolate the affected system for it to prevent further disruption of the network.They will attempt to restore any critical

	systems and services that were disrupted by the event. Then the team will analyze the network logs to check for suspicious and abnormal activity. The team will also report all incidents to upper management and appropriate legal authorities.
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: