Incident report analysis

Summary	The organization's network has recently experienced a DDoS attack that involved an incoming flood of ICMP packets to the internal network. This attack prevented business operations and normal internal traffic from accessing the network's resources. This incident was caused due to an unconfigured firewall, this vulnerability allowed the malicious actor to overwhelm the network through the DDoS attack. The cybersecurity team responded to the incident by analyzing the network traffic where they noticed the high volume of ICMP packets. To address the event, the team implemented a new firewall rule to limit the rate of the incoming ICMP packets, source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets, network monitoring software to detect abnormal traffic patterns, and an IDPS to filter out some ICMP traffic based on suspicious characteristics.
Identify	The attack was identified as a DDoS attack, this is known after investigations noted the abnormal flood of ICMP packets on the internal network, which impacted operations and normal traffic for 2 hours. Ultimately, this attack impacted the organization's internal network services due to the oversight of an unconfigured firewall.
Protect	To protect the organization's network from future DDoS incidents, the team has implemented a plan involving configuring and monitoring the firewall to limit the rate of incoming ICMP packets, identify source ip addresses to check for spoofed IP addresses on incoming ICMP packets, along with implementations of systems such as Intrusion Detection Systems (IDS) and Intrusion Protection Systems (IPS) to filter out ICMP packets based on suspicious characteristics.
Detect	With the implementation of network monitoring software and IDS and IPS

	systems, the team will be able to detect and prevent such attacks and incidents ahead of time, this proactive approach will add another layer of security to the organization's internal network and ultimately, reduce the vulnerabilities of the network.
Respond	The team put in place multiple procedures to prevent a future DDoS incident, in the future, detailed documentation will be available to speed up the response of such attacks, management will be notified of the event ASAP and we will include response drills to simulate high traffic DDoS conditions to improve readiness.
Recover	To recover normal operations, the team blocked all incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services, in the case of a future incident, this will be documented and communicated for the team, as a possible step to take so the staff can act quickly and restore normal network services.

Reflections/Notes: