Incident report analysis

Summary	An incident occurs in which the organization experienced an DdoS attack, compromising the internal network for two hours. The network services suddenly stopped responding due to an incoming flood of ICMP packets so normal internal network traffic could not access any network resources. The cybersecurity team investigated the incident and they found that a malicious actor had sent a flood of ICM pings into the company's network through an unconfigured firewall.
Identify	A malicious actor sent a flood of ICMP pings into the company's network through an unconfigured firewall. The internal network was affected, blocking incoming ICMP packets. The network needed to be stop to be restore.
Protect	To protect, the security team implemented a new firewall rule to help limit the rate of incoming ICMP packets and they implement an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	The implementation of the Source IP address verification helps to detect the incoming ICMP packets to know if (in the firewall) there is check for spoofed IP addresses. This also helps to know the network doing monitoring thanks to a software to detect abnormal traffic patterns
Respond	To respond to this attacks, we need to first shut down the network to stop the ICMP packets to continue to interrupt the network flood. For future incidents is important to know the patterns of this problem, to analyze and restore the network transit filtering the ICMP traffic based on suspicious characteristics. The system need to be online in a few hours thanks to the labor of the firewall rules. The team will also help doing an report to know what happen the next time , and what they do better.
Recover	The first part of the recovery is to understand why the situation happen, the reports help

	to see the vulnerabilities and how to process the incident. The ICMP packets that seam suspicions can be block to prevent an incident and It's important for the recovery to actualized the functions of security (like firewalls). Then, all non-critical network services should be stopped to reduce internal network traffic, if the problem is resolved, its necessary to put online the network (in a sandbox or virtual machine to know if everything is okay).

Reflections/Notes: