Incident report analysis

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

Summary	Today the company experienced a distributed denial of service (DDoS) attack that compromised the internal network for two hours. The company's internal network services had stopped responding after receiving a flood of incoming ICMP packets. Normal internal network traffic couldn't access any of the resources it needed.
Identify	Our cybersecurity team investigation found that the ICMP ping flood came through an unconfigured firewall that a malicious actor overwhelmed with a DDoS attack.
Protect	To protect the network from future DDoS attacks the team reconfigured the firewall with a rule to limit incoming ICMP packet rate. They also added source IP address verification to the firewall to check all incoming traffic for spoofed IP addresses.
Detect	To detect similar future attacks, the team installed a network monitoring system to detect abnormal traffic patterns. An IDS/IPS system was also installed behind the firewall to filter out suspicious ICMP packets from incoming traffic.
Respond	The incident management team blocked all incoming ICMP packets and

	stopped all non-critical network services offline.
Recover	After responding to the attack accordingly the cybersecurity restored critical network services that were affected in under two hours.

Reflections/Notes: