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	The company was attacked by DDOS by incoming ICMP packets for 2 hours, compromising the internal network. The tema blocked the attack by stopping the non-critical network services to restore critical network services.
Identify	ICMP packets flooded the network through an unconfigured firewall.
Protect	The team implemented a new firewall rule to limit the rate of incoming ICMP packets, added source IP address verification on the firewall to check for spoofed IPs, network monitoring software to detect abnormal traffic patterns, and an IDS/IPS system to filter suspicious ICMP traffic.
Detect	The attack was detected when all network services stopped responding, and normal internal network traffic couldn’t access any network resources.
Respond	To prevent future issues like this one, the team will isolate the affected systems to prevent any future exploits from shutting down the whole network. Additionally, they will attempt to restore any critical services that were disrupted. Any future incidents will be reported to upper management.
Recover	Once the new firewall rules and rate limiters were installed, the internal network was brought back to full functionality after the ICMP requests timed out..

Reflections/Notes: