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 experienced a DDOS attack which compromised the internal network for two hours until it was resolved. During the attack, network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The team responded by blocking incoming ICMP packets, stopping all non-critical network services offline and restoring critical network services.
Identify	A malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. The entire network was affected.
Protect	**The network security team implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system was also implemented to filter out some ICMP traffic based on suspicious characteristics.**
Detect	The team configured source IP address verification on the firewall to check for spoofed IP addresses on incoming packets and implemented network monitoring software to detect abnormal traffic patterns.
Respond	For future security events, the cybersecurity team will isolate affected systems to prevent further disruption to the network. They will attempt to restore any

	critical systems and services that were disrupted by the event. Then the team will analyze network logs to check for suspicious and abnormal activity.
Recover	To recover from DDOS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. Firstly, all non critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored. Finally, once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online.

Reflections/Notes: