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 faced a security incident where all the network services suddenly stopped responding. The cybersecurity team found the disruption to be caused by a DDoS attack though a flood pf ICPM packets. The team blocked the attack by stoppping all non-critical network services, so that the critical network servies could be restored back.
Identify	An ICMP flood by a threat actor that disrupted the internal network. All the critical network resources needed to be secured
Protect	The network security team responded by implementing a new firewall rule in order to limit the rate of the incoming ICPM packets.In order to check the IP address from being spoofed, it was sourced. They also implemented an IDS/IPS system in order to filter our some ICMP traffic based on suspicious behaviour.
Detect	The team sourced the IP address so that it will not be spoofed in the future. Also implemented an IDS/IPS system for filtering the traffic
Respond	The cybersecurity team will isolate affected systems to prevent further disruptions to the network. They will attempt to restore the effected systems and the services. Then, they will analyze the system logs to be on the look out for any malicious activity that may have happened. The team will then report

	their findings to the management and the respective legal authorities if needed.
Recover	To recover from a DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. In the future, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online.

Reflections/Notes: