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, there was a disruption in the internal network because of unknown issues. The network services stopped responding for around two hours in this incident. The network and cybersecurity team were investigating it and found out that there were cyber attacks happening within the network. They were working on the resolution and the network services came back active after 2 hours downtime
Identify	The Cybersecurity team identified that there were a large number ICMP packets being sent out to the organization network causing the internal network to stop responding to normal traffic. This method of attack is known as Distributed Denial of Services (DDoS). The packet was sent out by a malicious actor through the unconfigured firewall and overwhelmed the network.
Protect	The network and cyber security team implement following to further prevent the similar attack happened: 1. Properly configure the firewall according to company policies 2. Implement ICMP rate limiting configuration to limit consecutive ICMP request to network 3. Implement IPS system to block the traffic based on malicious patterns
Detect	The network and cybersecurity team also implement IDS as well as network

	monitoring tools to detect malicious pattern in network usage
Respond	The network and cybersecurity team has implemented following configuration to contain the attack: 1. Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and block the traffic
Recover	The team checks all the network services after performing incident response activities as well as implementing protective measures. The team ensure that every network services are back to normal and monitor the situation regularly

---

Reflections/Notes: