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 organization experienced a DDos attack that compromised the network for two hours before it was resolved. The network stopped its services because of abnormal number of ICMP flood packets. The internal network also could not access network resources. The incident team responded by blocking all incoming ICMP packets and stopping all non critical network services and restoring critical network services. The security team's investigation reveals the attack was caused by company's unconfigured firewall. The threat actor used this vulnerability to perform a DDoS attack on the organizations network.
Identify	The unconfigured firewall was used by the threat actor to use it as a vulnerability and flood the server with ICMP packets. The organization's services to customers like the web design services, graphic design, and social media marketing solutions were affected. The internal network of the organization was also affected.
Protect	The network security team implemented a new firewall rule to limit the rate of incoming ICMP packets. Also the security team added verification of the Source IP address on the firewall to check for spoofed IP addresses on incoming ICMP packets.Network monitoring software to detect abnormal traffic patterns also implemented. An IDS/IPS system to filter out some ICMP

	traffic based on suspicious characteristics was also implemented.
Detect	The organization could use SIEM tools to log and analyse the network traffic. An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics was also implemented.
Respond	The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. The management will communicate to the customers about the attack and the restoration of services.
Recover	The services for the customer was restored in two hours. The firewall has been reconfigured with new rules. Also IP verification was also added in to the firewall, The staff and the customers were informed by email by the management about the attack and the restoration effort done by the security team.

Reflections/Notes: