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 malicious actor used ICMP flood attack which is a type of DDoS attack, the network was down for two hours, security professionals took down the non-critical functions of the network, added a rule for the firewall to limit ICMP packets and check for IP spoofing.
Identify	The problem was with an unconfigured firewall which caused ICMP flood attack a type of DDoS attack.
Protect	Configure the firewall and perform regular scheduled maintenance for the firewall and the network.
Detect	Add a rule to the firewall to block untrusted IPs or add an IDS/IPS to the network to check for incoming traffic especially known types of DDoS attacks.
Respond	Immediately run tcpdump a packet sniffer tool to detect what is the issue, get the error message, and identify the port causing the error, once identified security professionals should then add a rule to the firewall to block the attack from the malicious actor’s IP to the port. If necessary shut down the network and restore.
Recover	You would need to make sure that the vulnerability or the issue happening has been patched up and that the attacker won’t be able to continue attacking, in addition, make sure to note down all the vulnerabilities found, as some vulnerabilities might not be attacked yet but discovered during the patching

	process.

Reflections/Notes: