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	An attack was noticed when the network's services stopped responding due to an incoming flood of ICMP packets. During this time, normal internal network traffic could not access any network resources. In response, the incident management team responded by blocking incoming ICMP packets, stopped all non-critical network services, and restored critical network services. An investigation was done by the cybersecurity team, and it was found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall, allowing the DDoS attack. In response, the security team implemented a new firewall rule to limit the rate of incoming ICMP packets, source IP verification to check for spoofed IP addresses, network monitoring to detect abnormal network patterns, and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Identify	The team investigated the devices and systems compromised in the attack. The team found that a malicious actor had sent ICMP pings to the network through an unconfigured firewall.
Protect	The team has implemented new firewall rules against ICMP packets, source IP verification, network monitoring, and an IDS/IPS system.
Detect	To detect future attacks, the team installed an IDS/IPS system to filter out ICMP

	traffic based on suspicious characteristics
Respond	The team blocked all incoming ICMP packets, shut down non-critical systems, and restored critical systems in response to the attack.
Recover	The team will recover what was lost by restoring from backups and by ensuring that a similar attack cannot take place.

Reflections/Notes: In the future, an implementation of a stronger firewall or stronger firewall procedures would help maintain security and ensure protection. By port filtering with a firewall, many attacks like this could be limited in scope.