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	A multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses experienced an error in its internal network. We believe this was the work of a threat actor using a DDOS attack due to the incoming flood of Internet Control Message Protocol (ICMP) packets. The Cybersecurity team responded by blocking incoming ICMP packets in order to restore normal network services.
Identify	A threat actor targeted the company with an ICMP flood attack. This caused the internal network to shutdown and is in need to be restored and secured further
Protect	The company blocked all incoming ICMP packets for non critical network services in order to prevent spread and restore critical services. A new firewall rule was implemented to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characters
Detect	Firewalls will not verify the source IP address to check for IP spoofing and installation of Network monitoring software to detect abnormal traffic patterns
Respond	The company will do patch updates to ensure previous attacks will not happen

	again. When another attack were to happen, the company will isolate the problem to prevent spread and attempt to restore critical systems affected. They will also utilize the new Network monitoring software to detect unusual behavior and patterns.
Recover	The company will recover from a DDOS attack by ensuring network services are functioning normally. In the future, ICMP flood attacks can be prevented by rules enforced by a firewall.

Reflections/Notes: