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 company recently experienced a DDoS attack where the organization's internal network was compromised for 2 hours until it was resolved. This was due to the flood of ICMP packets meaning normal internal network traffic could not access any network resources. The cybersecurity team then responded to this by blocking ICMP packets stopping all network services offline, and restoring critical network services.
Identify	Malicious actor targeted the company with an ICMP flood attack. The internal network was affected and critical network resources needed to be secured and restored.
Protect	Since the malicious attacker was able to penetrate through an unconfigured firewall, the cybersecurity team implemented a new firewall rule to limit the rate of incoming ICMP packets.
Detect	The network security team implemented a source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets while also adding a network monitoring system to detect abnormal traffic patterns.
Respond	Security team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.

	They will do this by adding an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. Probelms will be communicated to supervisors and higher ups. Both offlining and isolating affected resources.
Recover	In order to recover, the security team has to plan ahead to ensure everything gets done correctly by restoring it to its original self once all reported problems hav been fixed. To ensure this does not happen again, the security team ensured the flood attacks can be blocked by a firewall, leading to all non-critical network services being able to restored quickly. Leading to network services being fixed on the fly.

Reflections/Notes: NA