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	our organization's network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. The company's cybersecurity team then investigated the security event. We found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.
Identify	The company was targeted by a malicious actor or group using an ICMP flood attack, which disrupted the entire internal network.
protect	the cybersecurity team implemented a new firewall rule to limit the rate of incoming ICMP packets
Detect	The cybersecurity team implemented network monitoring software to detect

	abnormal traffic patterns,source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Respond	The cybersecurity security isolated the affected systems, the team reviewed network logs to identify if any suspicious or abnormal activity and we will report all incidents to upper management as well as the relevant legal authorities.
Recover	The team will recover deleted data by restoring from database, ICMP flood attacks can be mitigated by blocking them at the firewall. Additionally, shutting down all non-essential network services helps reduce internal traffic and limit the impact of the attack.

Reflections/Notes: