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 organization noticed a DoS attack on their network, which compromised the network for 2 hours. The network services stopped due to the overload of ICMP packets, and 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 cybersecurity threat found signs of a malicious actor who sent floods of ICMP pings to the company's network due to the unconfigured firewall
Identify	The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. The team found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. Due to the ICMP ping flood, normal internal traffic could not access any network's resources. The cybersecurity team had to block incoming ICMP packets, stop all non-critical network services offline, and restore critical network services.
Protect	The security team implemented: a new firewall rule to limit the rate of incoming ICMP packets, source IP address verification on the firewall to check for

	spoofed IP addresses on incoming ICMP packets, network monitoring software to detect abnormal traffic patterns, and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	To detect new unauthorized access attacks in the future, the team will use firewalls like Next Generation Firewall for deep packet inspection, intrusion protection, and threat intelligence. IDS/IPS systems can be used to identify and stop traffic with suspicious characteristics.
Respond	The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. Following the playbook and the data from the SIEM and network analyzer, the details about the ICMP flood can be identified and noted to use for future attacks. We informed upper management of this event and they will also need to inform law enforcement and other organizations as required by local laws.
Recover	The team will recover the deleted data by restoring the database from last night's full backup. The team restore the normal traffic of the network

Reflections/Notes: