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	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. They 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 incident management team audited the systems, devices, and. The team found There were no firewall rules to limit the rate of incoming ICMP packets, no Network monitoring software to detect abnormal traffic patterns and no security measures were taken in the company before the attack.The network was not secured.
Protect	the network security team implemented to prevent future Attacks by: 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 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, A firewall to limit the rate of incoming ICMP packets and an intrusion detection system (IDS) to monitor all incoming traffic from the internet.
Respond	The team is now actively working on firewall, monitoring network 24/7 and preparing to get not attacked again by hackers pentesting their own network We informed upper management of this event and they will contact our customers by mail to inform them about the data breach. Management 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. We have informed staff that any customer information entered or changed this morning would not be recorded on the backup. So, they will need to re-enter that information into the database once it has been restored from last night's backup.

Reflections/Notes: