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 Organisation's network suddenly stopped responding one day due to an incoming flood of ICMP packets.All 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 services.This incident was probably a DDoS (Distributed Denial of Service) attack and it compromised the system for nearly two hours until it was resolved.
Identify	The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security.The found that the malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerable allowed the attackers to overwhelm the company's network through a distributed denial of service attack.
Protect	The team acted by putting a new firewall rule to limit the rate of incoming ICMP packets. They also put a source IP Address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. They implemented the Network Monitoring Software to detect abnormal traffic patterns. An IPS/IDS

	system to filter out some ICMP traffic based on suspicious characteristics.
Detect	To detect new unauthorized access in the future they implemented a firewall which is well configured, Network monitoring software and an IPS/IDS system
Respond	For future incidents, after identifying the incident, the tema will protect the network by shutting down the point of entry to prevent more damage and after that they will detect and respond to the problem and fix the issues and will recover the data lost or damaged by using the last backups they had and the system will come back as normal. They can use logs and Network softwares like packet sniffers to analyse the incident
Recover	Sensitive personal information should be recovered immediately for the company to run smoothly and also the information used to run the daily business.They will use backups which may be on-site or off-site to restore the last clean and uncompromised data for the systems to work again

---

Reflections/Notes: