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	This morning, the organisation experienced a slow response and the network services eventually stopped working due to normal network traffic analysis that could not access any network resources. This was due to a DDOS attack that compromised the internal network for two hours.
Identify	The cybersecurity team conducted an investigation on the security event and it was found that a malicious attacker had sent a malicious ICMP ping into the company's network through an unconfigured firewall. This made the malicious attacker have access to the network through a distributed denial of service.
Protect	The security team had implemented a new firewall rule to reduce the rate of incoming ICMP packets, network monitoring software to detect abnormal traffic patterns, and 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 logging tool and an intrusion detection system (IDS) to monitor all incoming traffic from the internet.
Respond	The security team contained the attack by blocking incoming ICMP packets, they took non- critical services offline, and restored critical services first. They

	discovered that the firewall was unconfigured and confirmed that ICMP flooding caused the outage.
Recover	After, the non-critical services was brought back online, and the whole network was ensured that it was working again. The team added a firewall rule to rate-limit ICMP, they also implemented networking tools and IDS\IPS to identify suspicious ICMP patterns. Policies were updated

---

Reflections/Notes: