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 afternoon our systems slowed down as we experienced a DDos attack . The system stopped responding as it was flooded with numerous ICMP packets. By doing this the malicious actor overwhelmed the company’s network. It took the security team two hours to resolve the issue.
Identify	The cybersecurity team audited the systems,devices and access policies involved in the attack to identify the gaps in security. The team found that the incident took place due to unconfigured firewall which allowed the flooding of ICMP packets.
Protect	The network security team has implemented a new firewall rule to limit the rate of incoming ICMP packets and network monitoring software to detect abnormal traffic patterns. The team has also set up an IDS/IPS system to filter out some ICMP traffic based on suspicious patterns.
Detect	In future to detect any abnormal ICMP traffic patterns the security team will use configured firewalls along with an IDS system which will help monitor all the incoming traffic.
Respond	The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline and restoring critical network services.
Recover	The team will recover the network services of the company, affected by the DDos attack.

Reflections/Notes: