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	Recently, the organization experienced a DDOS attack on our servers, which compromised the internal network for 2 hours. The DDOS method was through an incoming flood of ICMP packets (ping).
Identify	The cybersecurity team successfully identified the attack as a flood of ICMP packets. Upon further investigation, it came to be known that the packet flood managed to get in through an unconfigured firewall.
Protect	The security team has hardened the organizations firewalls by adding a new firewall rule to limit the rate of incoming packets, as well as adding source IP verification on the firewall to check for spoofed IP addresses on incoming ICMP packets.
Detect	The team has also implemented an IDS/IPS system to proactively detect and stop certain ICMP traffic based on suspicious characteristics. They also added network monitoring software to detect abnormal traffic patterns.
Respond	The incident management team responded by blocking the initial incoming ICMP packets, stopping all non-critical network services online, and restoring critical network services.
Recover	Finally, the team fully recovered from the DDOS attack as soon as possible and made sure to harden the firewall and implement additional detection programs to reduce the possibility of it happening again.

Reflections/Notes: