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 an employee noticed they were unable to access the network services and everything stopped responding. Upon further investigation after several other employees began reporting the same findings, it was determined that the network was under attack using a Distributed Denial of Service attack. (DDoS)
Identify	The network was completely disabled for a period of around 2 hours due to a flood of ICMP packets being sent to over the network. Internal network traffic could not access any network resources during this time.
Protect	The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Detect	New firewall configurations have been put in place alongside settings that limit the amount of incoming ICMP packets into the network. Some filters have also been applied to the IDS/IPS to detect and prevent suspicious ICMP activity.
Respond	Routine maintenance on firewall configuration and monitoring logs of network activity have been implemented to prevent future attacks in the same manner from occurring.

Recover	In future events similar to this attack, we have actions listed to minimize the damage, and restore access to internal network services as fast as possible to prevent disruption in business operations.

Reflections/Notes: