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	I am a security analyst for a multimedia design company that provides its services to different companies. One day, my company experienced a DDoS attack that compromised our internal network for 2 hours. This was caused by a malicious actor who flooded our network with ICMP packets due to an unconfigured firewall. To address this issue, we properly configured our firewall to limit the rate of ICMP packets, verify the source IP address to make sure the IP address isn't spoofed, added network software that monitors abnormal traffic within the network, and added an IDS/IPS to filter out some ICMP traffic based on its suspicious characteristics.
Identify	Misconfigured firewall, no network monitoring software to watch for abnormal traffic within the network, no IDS/IPS to filter out suspicious characteristics.
Protect	Configured firewall properly, added network monitoring software to watch for abnormal traffic within the network, and added IDS/IPS to filter out traffic based on its suspicious characteristics.
Detect	With this incident, if we had an IDS/IPS to filter out traffic based on its suspicious characteristics, it would have been able to detect the abnormal quantity of ICMP packets.

Respond	To respond to this incident, we blocked incoming ICMP packets, stopped all non-critical network services offline, and restored critical network services.
Recover	To recover after this incident, we added solutions to make sure an event like this doesn't happen again, such as a configured firewall, IDS/IPS monitoring, and source IP verification on the firewall to check for potential spoofed IP addresses.