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	Today, we were victims of a DDoS attack that took our services offline for two hours. The primary cause was a flood of ICMP packets. After an investigation, we discovered that the packets were sent through a misconfigured firewall.
Identify	We identified that the cause of the attack was a large number of ICMP packets sent through a misconfigured firewall, where the attacker was able to overload our systems through this vulnerability.
Protect	To address this vulnerability, our team first blocked the ICMP packets that were disrupting our services and restored critical systems. To prevent future incidents, it is necessary to implement a better firewall and ensure its proper configuration, including a new rule to limit the rate of ICMP packets.
Detect	To detect potential future incidents, our team implemented IP address verification to prevent IP spoofing, a software solution to monitor the network and detect abnormal traffic patterns, and an IPS to filter ICMP packets based on suspicious characteristics.
Respond	In response to the attack, our team blocked ICMP packets, stopped all non-critical services, and restored critical services.
Recover	After two hours of downtime, our services returned to normal operation following the blocking of packets and the restoration of critical network services.

Reflections/Notes: Currently, the NIST framework is one of the most widely used in the world. Therefore, to prevent this type of attack and other similar ones in the future, it is really important to implement and maintain the information and guidelines provided in this document.