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	Our organization recently experienced a DoS attack, which compromised the internal network for about two hours. Our network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal network traffic could not access network resources. We responded by blocking all incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. When we investigated the incident, we found that a malicious actor had sent a flood of ICMP packets through an unconfigured firewall. This allowed the attacker to overwhelm our network through a DoS attack.
Identify	The cybersecurity team investigated the security incident and identified an unconfigured firewall that the attacker used to flood the network with ICMP packets. The internal network was compromised for about 2 hours
Protect	The team has implemented multiple tools and applications to address this incident. A new firewall rule was configured to limit the rate of incoming ICMP packets. Source IP address verification was added to the firewall to check for spoofed IP addresses on incoming ICMP packets. A network monitoring software was installed to detect abnormal traffic patterns, such as an increase in ICMP packets. Additionally, an IDS/IPS system is used to filter out some ICMP

	traffic based on suspicious characteristics.
Detect	To detect attacks like this one in the future, the team implemented a network monitoring software and an IDS/IPS system to detect abnormal traffic and filter out suspicious ICMP traffic.
Respond	The team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. In the future, we will rely on the new IDS/IPS system and network monitoring software to quickly detect if any attacks are about to take place.
Recover	The team will recover by restoring critical network services first, and then restoring non-critical network services. Furthermore, we will allow incoming ICMP packets after configuring the firewall to limit the rate of incoming ICMP traffic.
