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	The company faced a security incident when all network services abruptly became unresponsive. Upon investigation, the cybersecurity team determined that the disruption resulted from a DDoS attack, where a flood of incoming ICMP packets overwhelmed the network. To counteract the attack and facilitate the restoration of critical network services, the team swiftly implemented measures to block the malicious traffic and temporarily halted all non-essential network services.
Identify	The company fell victim to an ICMP flood attack initiated by one or more malicious individuals. The attack had a widespread impact on the internal network, necessitating the swift protection and restoration of all critical network resources to ensure their proper functionality.
Protect	In response to the security incident, the cybersecurity team took proactive measures to enhance network protection. They introduced a new firewall rule aimed at restricting the influx of incoming ICMP packets by limiting their rate. Additionally, they deployed an IDS/IPS system that could identify and filter out ICMP traffic exhibiting suspicious characteristics.
Detect	They enabled source IP address verification on the firewall, ensuring that incoming ICMP packets were scrutinized for any spoofed IP addresses. This verification helped identify and prevent the use of falsified source IPs in the

	attack. Additionally, the team deployed network monitoring software that continuously analyzed traffic patterns, enabling the detection of abnormal or suspicious network behavior.
Respond	Firstly, they will promptly isolate affected systems to prevent any further disruptions to the network. Next, their focus will be on restoring any critical systems and services that were impacted by the event. As part of their investigation, the team will meticulously analyze network logs to identify any signs of suspicious or abnormal activity that may have contributed to the incident. Furthermore, all incidents will be reported to upper management, ensuring they are aware of the situation and can provide necessary support.
Recover	To restore network services to their regular functioning state after a DDoS attack involving ICMP flooding, certain steps need to be followed. In future scenarios, external ICMP flood attacks can be prevented by implementing firewall rules to block such traffic. Additionally, to alleviate internal network congestion, it is advisable to temporarily stop all non-critical network services. The focus should then shift to restoring critical network services as a priority. Finally, once the flood of ICMP packets has subsided, non-critical network systems and services can be gradually brought back online.

Reflections/Notes: