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 encountered a security incident when all network services unexpectedly ceased to function. Upon investigation, the cybersecurity team determined that the disruption resulted from a distributed denial of service (DDoS) attack, involving a flood of incoming ICMP packets. In response, the team promptly took action to block the attack and temporarily suspended all non-critical network services to facilitate the restoration of essential network services.
Identify	The company fell victim to an ICMP flood attack orchestrated by a malicious actor or group. This attack had a widespread impact, causing disruption across the entire internal network. Furthermore, focusing on securing and restoring critical network resources to ensure the network returned to its normal operational state is necessary.
Protect	The cybersecurity team took proactive measures by introducing a new firewall rule to restrict the rate of incoming ICMP packets. Additionally, they deployed an Intrusion Detection System/Intrusion Prevention System (IDS/IPS) to filter out certain ICMP traffic that displayed suspicious attributes. These security enhancements aimed to increase the network's protection against potential threats.

Detect	The cybersecurity team strengthened the firewall's security by setting up source IP address verification, which allowed it to inspect incoming ICMP packets for any signs of spoofed IP addresses. Additionally, they deployed specialized network monitoring software to identify and flag any unusual traffic patterns, enabling them to quickly detect potential anomalies and address security concerns effectively.
Respond	In preparation for future security incidents, the cybersecurity team will take several key actions. Firstly, they will promptly isolate any affected systems to contain the impact and prevent further disruptions to the network. Afterward, their focus will be on restoring critical systems and services that may have been affected during the event. To gain insights into the incident and identify potential security threats, the team will thoroughly analyze network logs, diligently searching for any signs of suspicious or abnormal activity. Furthermore, the team will adopt a transparent approach by reporting all security incidents to upper management. If necessary, they will also collaborate with the appropriate legal authorities to address the situation in compliance with relevant regulations and requirements.
Recover	To mitigate the impact of an ICMP flooding DDoS attack and return network services to their regular operation, the following steps should be taken: 1. Restore Network Services: Initially, the focus should be on restoring access to network services, ensuring they resume functioning as intended. 2. Implement Firewall Rules: In preparation for future external ICMP flood attacks, it is advisable to set up specific firewall rules to block such malicious traffic at the network perimeter.

	3. Suspend Non-Critical Services: To alleviate the strain on the internal network and prioritize critical functions, all non-critical network services should be temporarily halted. 4. Restore Critical Services First: The cybersecurity team should give precedence to the restoration of critical network services, ensuring that essential operations are up and running promptly. 5. Time Out ICMP Flood: Once the surge of ICMP packets has subsided and the threat has diminished, the team can proceed with bringing non-critical network systems and services back online.

Reflections/Notes: