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 organization encountered a security incident marked by the sudden cessation of all network services. Upon investigation, the cybersecurity team identified that the disruption stemmed from a distributed denial of service (DDoS) attack. This attack involved inundating the network with an overwhelming volume of incoming Internet Control Message Protocol (ICMP) packets. In response, the team swiftly took action by thwarting the attack and halting all network services that were deemed non-essential. This strategic move enabled the restoration of critical network services and the resumption of normal operations.
Identify	An individual or a group of malicious actors directed an ICMP flood attack towards the company, resulting in a widespread impact across the internal network. Given the severity of the situation, immediate measures were taken to safeguard and reinstate all essential network assets, ensuring their protection and returning them to a fully operational condition.
Protect	The cybersecurity team took proactive steps to enhance the network's security posture. They introduced a fresh firewall rule designed to restrict the rate at which incoming ICMP packets could enter the network. In addition, they deployed an Intrusion Detection System/Intrusion Prevention System (IDS/IPS)

	to analyze and filter specific ICMP traffic that displayed suspicious attributes. These measures collectively bolstered the organization's defense against potential threats and bolstered the network's resilience.
Detect	The cybersecurity team enacted several measures to fortify the network's security. They initiated the configuration of source IP address verification within the firewall, a step aimed at scrutinizing incoming ICMP packets for potential spoofed IP addresses. Additionally, they introduced network monitoring software to actively identify any deviations from normal traffic patterns, thereby enhancing their capacity to promptly detect and respond to anomalous activities. These efforts collectively contribute to the organization's heightened defense against potential threats.
Respond	In anticipation of future security incidents, the cybersecurity team has formulated a comprehensive strategy. In the event of a breach, they plan to promptly isolate affected systems as a preemptive measure to curtail any further disruption to the network. Subsequently, they will prioritize the restoration of critical systems and services that were impacted by the event. Following system restoration, the team will delve into the analysis of network logs with the aim of identifying any signs of suspicious or abnormal activity. This proactive step facilitates the swift detection and response to potential threats. Furthermore, the cybersecurity team remains committed to ensuring transparency and accountability. They pledge to diligently report all incidents to upper management, keeping them informed about the situation. In cases where applicable, they will also engage appropriate legal authorities to ensure that the necessary actions are taken. This comprehensive approach underscores the team's dedication to maintaining the security and integrity of the organization's digital landscape.

Recover	In the aftermath of a DDoS attack involving ICMP flooding, the primary objective is to restore access to network services and return them to their usual operational state. To better prepare for similar incidents in the future, a comprehensive recovery plan can be employed: External ICMP Flood Attack Blocking: Implement firewall rules to proactively block external ICMP flood attacks at the network perimeter. This preemptive step reduces the entry of malicious traffic. Halting Non-Critical Network Services: Temporarily cease non-essential network services to mitigate internal network congestion caused by the attack. This reduction in activity helps alleviate strain on critical resources. Priority Restoration of Critical Services: Focus on restoring critical network services first. This ensures that essential business functions regain functionality swiftly. Strategic Service Reinstatement: Once critical services are operational, monitor the attack's ICMP packet influx. When the attack's impact subsides due to packet timeouts, initiate the process of gradually bringing back non-critical network systems and services. By systematically following these steps, organizations can navigate the recovery process more effectively and minimize the disruption caused by ICMP flood attacks.

Reflections/Notes: