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	Following a DDoS attack that disrupted internal network services, a comprehensive plan has been devised. It identifies the attack type and affected systems, offers prevention measures, outlines detection methods, proposes a response strategy, and highlights recovery procedures. The plan aims to bolster network security, enhance incident detection, ensure efficient response, and facilitate swift recovery. This holistic approach will fortify the organization against future cybersecurity threats and safeguard its digital assets.
Identify	The incident involves a Distributed Denial of Service (DDoS) attack that targeted the internal network and network services of the organization. The attack overwhelmed the network with a flood of ICMP packets, leading to network disruptions and unresponsiveness of services.
Protect	To prevent future DDoS attacks, the organization should: Implement proper firewall rules to limit incoming ICMP packets and verify source IP addresses. Deploy network monitoring software to detect abnormal traffic patterns indicative of DDoS attacks. Utilize an Intrusion Detection/Prevention System (IDS/IPS) to filter out suspicious ICMP traffic.
Detect	Enhance incident detection through: Continuous network monitoring for unusual spikes in network traffic.

	Utilizing IDS/IPS to detect and analyze suspicious patterns. Setting up alerts for abnormal network behavior, especially during peak traffic times.
Respond	In case of a DDoS attack or any cybersecurity incident: Engage the incident management team to assess the situation and initiate a response. Block incoming ICMP packets to mitigate the ongoing attack. Prioritize restoration of critical services while keeping non-critical services offline. Collaborate with network security experts to analyze attack patterns and source IPs. Regularly update incident response plans based on lessons learned from incidents.
Recover	Develop a comprehensive recovery strategy by: Establishing clear roles and responsibilities within the incident response team. Creating a communication plan to inform stakeholders about the incident and recovery progress. Restoring affected systems to normal operation after the attack is mitigated. Conducting a post-incident review to identify areas for improvement and update recovery plans.

Reflections/Notes: By following this incident response and prevention plan, the organization can effectively mitigate the impact of future DDoS attacks and other cybersecurity incidents, minimizing disruptions and ensuring the security of network services and internal systems.