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 experienced a Distributed Denial of Service (DDoS) attack, causing a two-hour disruption of internal network services. The attack flooded the network with ICMP pings through an unconfigured firewall. This analysis aims to identify, protect, detect, respond, and recover from the incident, aligning with the NIST Cybersecurity Framework.
Identify	Type of Attack: DDoS attack utilizing ICMP packet flood. Systems Affected: Internal network compromised, disrupting normal network services for two hours.
Protect	Firewall Configuration: • Review and update firewall settings. • Implement a new rule to limit incoming ICMP packets. Employee Training: • Conduct cybersecurity training for employees to enhance their awareness of potential threats and reinforce the importance of following security protocols Policy Review:

	• Update policies and procedures, focusing on DDoS mitigation.
Detect	Monitoring Tools: • Deploy network monitoring software to detect abnormal traffic patterns. Real-time Alerts: • Establish real-time alert system for prompt notification.
Respond	Containment Procedures: • Isolate affected systems and blocking malicious traffic. Neutralization Strategies: • Reroute and filter malicious traffic. Data for Analysis: • Identify the types of data and information that can be used for post-incident analysis, including network logs, IDS/IPS alerts, and firewall logs.
Recover	Immediate Recovery Needs: • Identify critical systems and data that need immediate recovery to minimize downtime. Recovery Processes: • Review and update recovery processes, ensuring they are aligned with the incident specifics and improvements identified during the analysis.

Reflections/Notes: Continuous monitoring and timely response are critical. Regular training to enhance employee awareness should be employed.