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 experienced a DDoS attack that disrupted its internal network for two hours, caused by an overwhelming flood of ICMP packets. The incident management team responded by blocking incoming ICMP traffic, shutting down non-essential services, and restoring critical services. This incident revealed an unconfigured firewall as the vulnerability that permitted the attack.
Identify	A security issue was identified as an ICMP Flood DDoS Attack. In this attack, attackers inundate the network with a large volume of ICMP echo requests, leading to a temporary shutdown of services. The primary cause of this incident was an unconfigured firewall that failed to block the incoming requests, which originated from numerous fake IP addresses.
Protect	The organization has implemented several protective measures to enhance security and prevent future attacks. Key strategies include updating firewall settings to manage ICMP requests, introducing Access Control Lists (ACLs) to block unauthorized traffic, enforcing mandatory multi-layered authentication for accessing network systems, providing employee training on cybersecurity

	best practices, and conducting regular security audits to identify and address potential weaknesses.
Detect	The cybersecurity team has improved threat detection using advanced network monitoring tools to analyze unusual ICMP traffic patterns. An Intrusion Detection and Prevention System (IDS/IPS) automatically filters out malicious traffic. Regular reviews of firewall and network logs help identify unauthorized access attempts. Automated alerts notify administrators of any unusual traffic, while anomaly detection algorithms assist in recognizing potential Distributed Denial of Service (DDoS) attacks.
Respond	In response to a cybersecurity incident, our strategy will prioritize immediate containment and mitigation to minimize downtime and damage. Key steps include isolating compromised systems, blocking malicious IP addresses, and suspending non-critical services while ensuring critical resources remain operational. The cybersecurity team will collaborate with internet service providers (ISPs) to implement DDoS mitigation strategies. After containment measures are in place, we will conduct detailed log reviews and forensic analysis to determine the attack's origin, scope, and impact. The findings will be communicated to stakeholders and upper management.
Recover	The recovery process will focus on restoring affected network services while applying security patches to prevent future incidents. Based on insights from the attack, firewall and IDS/IPS configurations will be updated. Redundant failover systems will be implemented to maintain critical services, and a detailed incident response playbook will be developed for future cybersecurity threats. A post-mortem analysis will identify lessons learned and enhance security policies, employee training, and technical defenses.

Reflections/Notes: