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 that disrupted internal network operations for approximately two hours. During the attack, the company's network became unresponsive due to a massive flood of incoming ICMP packets. This prevented employees from accessing internal resources or performing routine business tasks. The incident response team restored functionality by blocking incoming ICMP traffic, disabling non-essential services, and bringing core services back online. Further investigation revealed that the attack succeeded because an external actor exploited an unconfigured firewall, allowing the malicious ICMP flood to overwhelm the network.
Identify	A post-incident audit showed that the firewall responsible for filtering external traffic had a misconfiguration that left it unable to properly restrict ICMP packets. This gap allowed an attacker to send a high-volume ICMP ping flood that overloaded the network infrastructure. The review also revealed that real-time monitoring was limited, reducing the organization's ability to detect abnormal traffic early.
Protect	To help prevent similar attacks in the future, the organization implemented several protective measures. These include adding firewall rules to limit the rate

	of incoming ICMP packets, enabling source IP verification to filter out spoofed traffic, and updating internal security policies to include routine firewall configuration reviews. The company also plans to deliver training to IT staff to reinforce proper firewall management and strengthen overall defensive capabilities.
Detect	To improve detection capabilities, the security team deployed new network monitoring tools to identify abnormal traffic patterns more quickly. Additionally, an intrusion detection and prevention system (IDS/IPS) was implemented to analyze incoming packets and flag suspicious ICMP activity. These tools give the team greater visibility into traffic behavior and allow earlier detection of signs of potential DDoS attacks.
Respond	In response to the incident, the cybersecurity team blocked incoming ICMP traffic and temporarily shut down non-critical services to stabilize the network. Critical systems were restored first to ensure business continuity. The security team documented the event, notified leadership, and developed updated response procedures for handling DDoS-related incidents in the future.
Recover	After containment, the team verified that all essential network services were functioning properly and confirmed that no data loss occurred during the attack. Systems were brought back online in phases to ensure stability. The company also reviewed and updated its recovery plans to ensure faster restoration of services if another DDoS attempt occurs.

Reflections/Notes: This incident highlighted the importance of proactive firewall configuration, continuous monitoring, and clearly defined response procedures. Improving visibility into network traffic and regularly auditing system settings will significantly reduce the likelihood and impact of similar attacks moving forward.