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	
Identify	A post-incident audit was conducted on the organization's network infrastructure. The team discovered that the firewall lacked configuration rules to filter ICMP traffic, leaving it vulnerable to abuse. This misconfiguration was exploited by a malicious actor using spoofed IPs to send a flood of ICMP echo requests (pings), overwhelming network resources and preventing legitimate internal traffic from accessing services.
Protect	To strengthen defenses, the security team implemented a new firewall rule to limit the rate of incoming ICMP traffic and added source IP verification to filter spoofed addresses. These steps reduce the likelihood of similar attacks in the future. Additionally, regular firewall reviews and security configuration audits will be scheduled to prevent misconfigurations.
Detect	Network monitoring software was deployed to flag unusual traffic patterns. An Intrusion Detection and Prevention System (IDS/IPS) was also integrated to help detect and block suspicious ICMP packets. These tools will enhance visibility

	across the network and enable the security team to detect anomalies in real time.
Respond	During the attack, the incident response team immediately blocked incoming ICMP traffic and took non-critical systems offline to minimize damage. Critical services were restored to ensure business continuity. Post-incident, the team documented the attack, analyzed network logs, and updated incident response procedures to improve readiness.
Recover	Once the network was stabilized, non-critical services were gradually brought back online. The security team validated network integrity and verified that no data loss or compromise occurred during the attack. Moving forward, a disaster recovery playbook specific to DDoS incidents will be maintained to speed up response and recovery time.

Reflections/Notes: This incident highlighted the critical importance of secure default configurations, proactive monitoring, and layered defenses. Implementing the NIST CSF helped structure an effective response and will guide future improvements in the company's cybersecurity posture. Regular testing of firewall configurations and simulated DDoS scenarios will also be considered as part of ongoing resilience planning.