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	A Distributed Denial of Service (DDoS) attack using ICMP packets disrupted the organization’s network services for two hours. The attack exploited an unconfigured firewall, overwhelming the internal network with traffic.
Identify	Detected unusual network outage impacting internal services. ● Investigation revealed a flood of ICMP packets targeting the network. ● Root cause identified: lack of firewall configuration to limit ICMP traffic.
Protect	**Implemented firewall rules to limit incoming ICMP packet rate.** ● **Enabled source IP verification to prevent spoofed traffic.** ● **Introduced IDS/IPS to filter suspicious ICMP packets.**
Detect	Used network monitoring tools to identify abnormal traffic patterns. ● Recognized spike in ICMP packets from external sources. ● Alert triggered due to degraded network performance.

Respond	Blocked incoming ICMP traffic temporarily to restore services. ● Coordinated with IT and security teams to isolate the traffic source. ● Documented the event and notified leadership.
Recover	Restored critical internal services and resumed business operations. ● Reconfigured firewall permanently with rate-limiting and filtering rules. ● Conducted post-incident review and staff training on incident response.

Reflections/Notes:This incident highlights how overlooked configurations like default firewall settings can become vulnerabilities. Applying the NIST framework ensured a structured approach to identify, mitigate, and prevent future attacks.