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	Earlier this morning, the company’s network services became unavailable for approximately two hours. The IT team identified that the disruption was caused by a Distributed Denial of Service (DDoS) attack using ICMP packets (ping flood). The incoming traffic overwhelmed the network infrastructure, preventing normal system operations. After investigation, it was discovered that the malicious traffic passed through a misconfigured firewall, allowing the attacker to exploit the vulnerability. There was no evidence of data compromise, but the temporary unavailability directly impacted client-facing services.
Identify	The incident response team audited systems, devices, and access policies to identify security gaps. The analysis revealed that the firewall was not configured to limit or filter ICMP packets, which allowed the ICMP flood attack to reach internal resources. The attack disrupted web hosting, graphic design, and digital marketing services. Access permissions were reviewed to ensure that only authorized personnel have access to critical systems.
Protect	**The team implemented immediate protective measures, including:** ● **Creating a new firewall rule to limit the rate of incoming ICMP**

	packets. ● **Enabling IP source verification to detect spoofing.** ● **Strengthening authentication on security devices.** ● **Training the IT and security staff on DDoS prevention.** ● **Updating firewall configurations and security policies.** ● **Evaluating investment in more robust DDoS mitigation tools.**
Detect	To improve future detection of similar attacks, the team took the following actions: ● Deployed a network monitoring system to identify abnormal traffic patterns. ● Installed an IDS/IPS with the capability to analyze ICMP packet behavior. ● Configured automatic alerts for unusual traffic spikes. ● Adopted SIEM tools to correlate and respond to real-time security events.

Respond	During the incident: ● ICMP traffic was blocked at the firewall level. ● Non-critical services were taken offline to preserve essential resources. ● The cybersecurity team conducted traffic forensics to determine the source and method of attack. ● The incident was formally reported to management. ● Incident response procedures were updated based on lessons learned.
Recover	● Network services were gradually restored after the attack was mitigated. ● No data was lost—only temporary unavailability was reported. ● The recovery plan was reviewed and reinforced to ensure faster future restoration. ● Affected departments were notified and aligned to normalize operations. ● Enhancements to recovery and business continuity plans were documented for implementation.

Reflections/Notes:This incident highlighted the importance of proactive configurations and continuous monitoring. The lack of a basic firewall rule exposed the organization to a preventable attack. The NIST CSF framework effectively guided the response and helped identify critical improvement areas such as early detection, coordinated response, and infrastructure updates. The company emerged stronger and more resilient as a result.