Incident report analysis

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or just to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to continue practicing applying the NIST CSF framework to different situations you may encounter.

Summary	The organization experienced a major disruption to its internal network when all network services suddenly stopped responding. Investigation revealed that this outage was caused by a distributed denial-of-service (DDoS) attack that overwhelmed the network with excessive ICMP traffic. The incident response team mitigated the attack by blocking incoming ICMP packets, temporarily shutting down non-essential network services, and restoring access to critical systems.
Identify	A malicious actor launched an ICMP flood attack targeting the company's network through a firewall that had not been properly configured to restrict ICMP traffic. The attack affected the entire internal network and prevented employees from accessing essential network resources. All critical systems, devices, and network services needed to be secured and brought back online to resume normal business operations.
Protect	To reduce exposure to future attacks, the cybersecurity team configured new firewall rules to limit the rate of incoming ICMP packets. Additional layered protections were implemented, including an intrusion detection and prevention system (IDS/IPS) to filter suspicious ICMP traffic before it reached the internal network. These changes help ensure that large volumes of abnormal ICMP

	traffic cannot overwhelm the network again.
Detect	The cybersecurity team improved detection capabilities by enabling source IP address verification on the firewall to identify spoofed IP addresses associated with ICMP packets. Network monitoring software was also deployed to provide early visibility into unusual traffic patterns and detect future abnormal spikes in ICMP activity before they escalate into a network outage.
Respond	In the event of a future DDoS attack, the cybersecurity team will immediately isolate affected systems to prevent network-wide disruption. Response priorities include restoring core services first while limiting or blocking malicious traffic. The team will analyze firewall, IDS/IPS, and system logs to identify the source and characteristics of the attack. All incidents will be documented and escalated to senior leadership and legal authorities if requirements for reporting are met.
Recover	To fully recover from a similar incident, network services must be restored in a controlled and prioritized order. First, ICMP flood traffic will be blocked at the firewall to stabilize the network. Non-critical services will remain offline to reduce internal load while critical systems are fully restored. Once traffic levels return to normal and network performance is stable, non-critical services can be gradually brought back online. Lessons learned will be used to improve business continuity and network resilience.

Reflections/Notes:This incident highlighted how a single misconfiguration, such as an unprotected firewall rule, can have widespread consequences on network availability and business operations. Applying the NIST CSF helped break down the event into clear stages—identifying vulnerabilities, protecting assets, detecting threats, responding quickly, and restoring systems—which made the investigation structured and effective. The experience reinforced the importance of proactive security measures like continuous monitoring, routine configuration audits, and layered defenses to reduce the likelihood of similar attacks. It also emphasized that incident response planning is an ongoing process, and lessons learned from real events should always be used to strengthen future cybersecurity practices.