Incident report analysis: Applying the NIST CSF

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 week, our organization experienced a Distributed Denial of Service (DDoS) attack that caused a full network outage for approximately two hours. During the incident, none of the internal network services were responsive, severely impacting employee productivity and business operations. After investigation, it was discovered that a flood of ICMP packets was directed at the network from multiple sources, exploiting an unconfigured firewall. This allowed the malicious actor(s) to overwhelm our network infrastructure, effectively making the entire system unavailable. The IT team acted quickly to mitigate the attack by blocking incoming ICMP packets, shutting down non-essential services, and restoring core functions. Post-incident analysis confirmed the attack vector and led to multiple changes in our network defense strategy.
Identify	The cybersecurity team conducted a full audit of the organization's firewall configurations, monitoring rules, and network access logs. The investigation revealed that the company's perimeter firewall lacked restrictions on incoming ICMP traffic, leaving the network exposed to ICMP flood attacks. No IP source verification was enabled, allowing the attacker to spoof IPs and escalate the scale of the attack. It was determined that the lack of rate-limiting rules and monitoring tools also contributed to the delayed detection of the DDoS activity.

	This audit highlighted critical configuration gaps in the firewall and network traffic monitoring policies.
Protect	To better protect internal assets and prevent similar attacks, the team implemented several defensive measures. A new firewall rule was added to limit the rate of incoming ICMP packets, helping to reduce the likelihood of future flood attempts overwhelming the network. Source IP address verification was also enabled to block spoofed traffic. Additionally, the team conducted security training for system administrators focused on secure firewall configuration and traffic filtering. These steps are now part of updated network hardening procedures within the company's security policy.
Detect	To improve detection capabilities, the organization deployed new network monitoring software to continuously analyze traffic and flag abnormal behavior patterns. An Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) were also configured to detect and filter ICMP packets exhibiting suspicious characteristics. These tools will provide real-time alerts and auto-mitigation functions in the event of future DDoS attempts. These upgrades are essential to reducing the response time for similar incidents in the future.
Respond	The incident response team promptly blocked all incoming ICMP traffic during the attack and took non-critical services offline to reduce network load. This helped stabilize the environment so core services could be restored. Communication was issued to stakeholders and internal staff explaining the outage and mitigation steps. The team also conducted a follow-up meeting to review the attack pattern and revise the incident response playbook. Going forward, the team will continue refining response protocols based on lessons learned from this attack.
Recover	Recovery efforts included restoring essential services to full operation and

	verifying the integrity of system and network components affected by the attack. IT verified that no data loss occurred as a result of the incident. Service availability was fully restored within two hours of the attack's onset. The team has scheduled ongoing firewall and IDS/IPS tests as part of routine recovery assurance practices. These measures ensure the systems are resilient and capable of handling similar events in the future.