Scenario

You are a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses. Your organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved.
During the attack, your organization's network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.

The company's cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.
To address this security event, the network security team implemented:

- A new firewall rule to limit the rate of incoming ICMP packets
- Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets
- Network monitoring software to detect abnormal traffic patterns
- An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics

As a cybersecurity analyst, you are tasked with using this security event to create a plan to improve your company's network security, following the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). You will use the CSF to help you navigate through the different steps of analyzing this cybersecurity event and integrate your analysis into a general security strategy. We have broken the analysis into different parts in the template below. You can explore them here:

- Identify security risks through regular audits of internal networks, systems, devices, and access privileges to identify potential gaps in security.
- Protect internal assets through the implementation of policies, procedures, training and tools that help mitigate cybersecurity threats.
- Detect potential security incidents and improve monitoring capabilities to increase the speed and efficiency of detections.
- Respond to contain, neutralize, and analyze security incidents; implement improvements to the security process.

Recover affected systems to normal operation and restore systems data and/or assets that have been affected by an incident.

Incident report analysis

Summary	Earlier today, it was reported that the organization's network suddenly stopped responding due to an incoming flood of ICMP packets. Therefore, Normal internal network traffic could not access any network resources for 2 hours until resolved. This was a Distributed Denial of Service (DDoS) attack. The Incident Management team responded by blocking incoming ICMP packets and also found out that a malicious actor sent a flood of ICMP pings into the companies network through an unconfigured firewall and this led to the DDoS attack. The Network Security team did the following: ● Set a new firewall limit rate of incoming ICMP packets ● Source IP verification on the firewall to check for spoofed addresses on the ICMP packets ● Network monitoring software to detect abnormal traffic patterns ● An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Identify	- Conducted an audit to identify the unconfigured firewall that allowed the DDoS attack. - Reviewed access controls and privileges to limit exposure.
Protect	- Implemented a new firewall rule to limit incoming ICMP packets. - Enabled source IP verification to prevent spoofed packets from entering the network. - Developed and enforced stronger password policies and multi-factor authentication (MFA) to secure user access.
Detect	- Deployed network monitoring software to detect unusual traffic patterns. - Utilized IDS/IPS to monitor and filter suspicious ICMP traffic effectively.

Respond	- Activated the incident response plan to contain the DDoS attack. - Blocked incoming ICMP packets to regain network functionality. - Conducted a root cause analysis to determine how the attack occurred and how to prevent future incidents.
Recover	- Restored normal network services after blocking harmful traffic. - Reviewed and updated the incident response plan based on lessons learned from the attack. - Ensured regular backups of critical data to facilitate recovery from future incidents.

Reflections/Notes: