Using the NIST Cybersecurity Framework to respond to a security incident

Scenario:
The scenario is a fictional story

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	The organisation's network services stopped responding immediately and the internal network traffic could not access any network resources. The reason for this was a flood of ICMP packets. The incident team management responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Identify	A malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall. This overwhelmed the company’s network through a distributed denial of service (DDoS) attack.

Protect	The network security team implemented a new firewall rule to limit the rate of incoming ICMP packets, an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics
Detect	The team configured the source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets, and implemented network monitoring software to detect abnormal traffic patterns
Respond	For future, the team will isolate the affected computer systems for avoiding further disruption to the network. They will restore the systems and services that were affected by the incident. The team will analyse the log data and find the source IP of the attacker. Then they will report the incident to the senior officers and may complain legally, if applicable
Recover	For recovery, access to network services should be restored. The ICMP flood attack can be blocked at the firewall by immediately disabling ICMP traffic. Once the attack has timed out, the devices and systems should be checked for any damage and vulnerabilities, and should fix it. All networks should be restored after the internal traffic subsides, then re-enable the ICMP traffic with limited rate. Finally, implement IPS(intrusion prevention systems) and strong firewall rules to prevent future attacks.

Reflections/Notes: