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	The company experienced a DDoS attack where the internal network was flooded with ICMP packets, disrupting services for two hours. The attack exploited an unconfigured firewall, allowing the malicious actor to overwhelm the network. After the incident, new security measures were implemented.
Identify	**Manage security risks through regular audits:** ● Technology/Asset Management: Identify affected hardware, operating systems, and software. Trace the attack path through the internal network. ● Process/Business environment: Determine which business processes were impacted by the attack. ● People: Identify personnel who require access to affected systems for recovery and ongoing security.
Protect	**Develop a strategy to protect internal assets:** ● Access control: Review and restrict access to critical systems and services. Ensure non-trusted sources are blocked. ● Awareness/Training: Educate employees about DDoS attacks, security best practices, and incident response procedures. ● Data security: Enhance security measures for sensitive data affected during the incident. ● Information protection and procedures: Update procedures to protect data assets more effectively. ● Maintenance: Regularly update and patch hardware, operating systems, and software to prevent vulnerabilities. ● Protective technology: Implement and configure firewall rules, intrusion

	prevention systems (IPS), and other protective technologies to mitigate future DDoS attacks.
Detect	**Design and implement a system to detect threats:** ● Anomalies and events: Deploy security information and event management (SIEM) tools to detect abnormal network traffic patterns. ● Security continuous monitoring: Establish continuous monitoring capabilities to promptly identify and respond to security incidents. ● Detection process: Enhance Intrusion Detection Systems (IDS) to detect and alert on suspicious ICMP traffic and other anomalies.
Respond	**Design action plans for responding to threats:** ● Response planning: Develop incident response plans specifically for DDoS attacks, outlining steps to mitigate and recover. ● Communications: Establish clear communication channels to notify internal stakeholders and affected parties during an incident. ● Analysis: Conduct post-incident analysis to understand the attack vectors, weaknesses, and improvements needed. ● Mitigation: Implement strategies to mitigate the impact of future DDoS attacks, such as isolating affected resources or adjusting firewall rules. ● Improvements: Update incident response procedures based on lessons learned from the DDoS attack.
Recover	**Construct a plan to recover affected systems:** ● Recovery planning: Outline procedures to restore network services and data affected by the DDoS attack. ● Improvements: Enhance recovery systems and processes to expedite restoration in future incidents.

	• Communications: Communicate recovery procedures internally and with affected parties to ensure coordinated recovery efforts.

Reflections/Notes:

Ensure that all security measures and procedures are updated regularly to address evolving threats. Continuous training and awareness programs are crucial to maintaining a strong security posture. Incident response plans should be tested periodically through simulations to ensure effectiveness.

By applying the NIST CSF framework, the company can systematically strengthen its cybersecurity defenses, mitigate risks, and enhance its ability to detect, respond to, and recover from future cybersecurity incidents effectively.