Use the NIST Cybersecurity Framework to respond to a security incident

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 incident and integrate your analysis into a general security strategy:

Use the NIST Cybersecurity Framework to respond to a security incident

- 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.

Report:

****Cybersecurity Incident Report: DDoS Attack****

1. Identify (NIST CSF - Identify Function):

Incident Overview:
On [Date], our organization experienced a Distributed Denial of Service (DDoS) attack that resulted in a two-hour compromise of our internal network. The attack targeted our network services, particularly flooding ICMP packets, causing a disruption in normal operations.

Security Risk Identification:
- Insufficient Firewall Configuration:
  - Risk Level: High
  - Explanation: Unconfigured firewall allowed the flood of ICMP packets, leading to the DDoS attack.

2. Protect (NIST CSF - Protect Function):

Protective Measures Implemented:
- New Firewall Rule:
  - Purpose: Limit the rate of incoming ICMP packets.
  - Effectiveness: Mitigates the impact of DDoS attacks by controlling the flow of ICMP traffic.

- Source IP Address Verification:
  - Purpose: Check for spoofed IP addresses on incoming ICMP packets.
  - Effectiveness: Prevents the use of spoofed IP addresses in DDoS attacks, enhancing network security.

Use the NIST Cybersecurity Framework to respond to a security incident

3. Detect (NIST CSF - Detect Function):

Detection Measures Implemented:
- Network Monitoring Software:
  - Purpose: Detect abnormal traffic patterns.
  - Effectiveness: Early detection of DDoS attacks and other unusual network behavior.

- IDS/IPS System:
  - Purpose: Filter out suspicious ICMP traffic based on characteristics.
  - Effectiveness: Enhances the ability to identify and respond to malicious ICMP traffic.

4. Respond (NIST CSF - Respond Function):

Response Measures Implemented:
- Blocking Incoming ICMP Packets:
  - Action: Stopped non-critical network services offline during the attack.
  - Effectiveness: Contained the attack and prevented further damage.

- Restoring Critical Network Services:
  - Action: Prioritized the restoration of critical network services.
  - Effectiveness: Minimized downtime and impact on essential operations.

5. Recover (NIST CSF - Recover Function):

Recovery Measures Implemented:
- Post-Incident Analysis:
  - Action: Conducted a thorough analysis of the incident.
  - Effectiveness: Identified weaknesses and areas for improvement in network security.

- Implementing Security Improvements:
  - Action: Implemented new firewall rules, source IP address verification, network monitoring, and IDS/IPS.
  - Effectiveness: Strengthened network security to prevent future DDoS attacks and enhance overall resilience.

General Security Strategy:
- Regular Audits: Conduct periodic audits of internal networks, systems, devices, and access privileges to identify and address security gaps.
- Policies and Procedures: Develop and implement comprehensive policies and procedures to safeguard internal assets.
- Training: Provide ongoing cybersecurity training to staff to enhance their awareness and response capabilities.

Use the NIST Cybersecurity Framework to respond to a security incident

Conclusion:
The incident analysis, following the NIST Cybersecurity Framework, has led to the implementation of targeted measures to address vulnerabilities exposed during the DDoS attack. The organization is now better equipped to identify, protect, detect, respond, and recover from similar incidents in the future, contributing to an overall improvement in network security posture. Regular evaluations and proactive security measures will be crucial for maintaining a resilient cybersecurity framework.