Note: This is a **simulated cybersecurity incident report** based on real-world attack patterns and mitigation strategies. The analysis follows the **NIST Cybersecurity Framework (CSF)** to demonstrate how a security personnel/team would respond to a DDoS attack in a professional setting.

NIST Cybersecurity Framework to respond to a security incident

Summary of the Security Event

On March 9, 2025, I conducted a simulated Distributed Denial of Service **(DDoS)** attack analysis to understand how an organization's network could be affected by a large-scale **ICMP flood attack**. This attack led to a two-hour network outage, making internal resources inaccessible.

During the simulation, I found that an unconfigured firewall allowed unrestricted ICMP traffic, making it easy for an attacker to flood the network. To mitigate this, I recommended firewall rules to block incoming ICMP packets, disabled non-essential services, and restored critical network functions.

1. Identify (Risk & Vulnerability Assessment)

📌This attack simulation is based on a **fictional DDoS attack scenario**, where an attacker exploited an **unconfigured firewall** to send a flood of **ICMP packets**, causing a network outage.

While this is a simulated case, it mirrors real-world **DDoS attack techniques** seen in the **Mirai Botnet Attack**, where thousands of IoT devices were hijacked to flood networks with ICMP requests. Similarly, the **GitHub DDoS Attack (2018)** used reflection techniques to generate a massive traffic surge. This analysis follows the **NIST Cybersecurity Framework (CSF)** to model how organizations handle such incidents.

Security Gaps Identified:

- The firewall was not properly configured, allowing unrestricted ICMP requests.
- No rate limiting was in place to handle excessive traffic.
- Monitoring tools were not set up to detect high-volume ICMP traffic.

Systems Affected:

- Internal servers supporting design projects and client communications.
- Web-based services related to graphic design, web development, and social media marketing.
- Employee workstations that relied on internal resources.

Business Impact:

- Financial loss estimated at $**15,000** due to downtime and loss of productivity.
- Delayed client projects due to service unavailability.
- Potential damage to company reputation if the issue had been real.

2. Protect (Preventive Measures & Solutions)

To strengthen network security, I recommend (based on my research) the following measures:

- **Firewall Rule Updates**: Set up rate-limiting rules to control incoming ICMP packets.
- **Source IP Verification**: Configured firewall settings to block spoofed IP addresses.
- **Access Control**: Limited network access to verified users and trusted devices.
- **Security Policies**: Developed internal policies for firewall management and traffic filtering.

3. Detect (Threat Monitoring & Anomaly Detection)

To improve **early detection of potential DDoS attacks**, I recommend the following tools:

- **Intrusion Detection and Prevention Systems (IDS/IPS)**: Configured rules to identify and block high-volume ICMP traffic.
- **SIEM (Security Information and Event Management) Tools**: Used for traffic monitoring and log analysis.
- **Automated Alerts**: Set up real-time notifications for abnormal spikes in network traffic.
- **Firewall & Server Log Audits**: Implemented regular log reviews to detect patterns of unauthorized activity.

4. Respond (Incident Handling & Mitigation)

During the attack simulation, I researched and outlined a structured **DDoS response plan** based on industry best practices:

- **Researched firewall rule modifications** that could help block incoming ICMP traffic and mitigate network flooding.
- **Reviewed methods to disable non-critical services** during an attack to preserve bandwidth for essential operations.
- **Studied how spoofed IP addresses** can be identified and analyzed to track the attack source.
- **Outlined a hypothetical stakeholder communication plan** for incident response.
- **Drafted a DDoS response playbook** to document best practices and future mitigation strategies.

5. Recover (Restoration & Future Resilience)

Recovering from a DDoS attack involves multiple steps to restore services and ensure similar incidents do not happen in the future. Based on the analysis, I outlined a structured approach for recovery and long-term security improvements.

Immediate Recovery Needs:

- **System and network logs** to assess the full extent of the attack.
- **Access to network backups** to verify integrity and restore configurations if necessary.
- **Incident response reports** to document lessons learned and inform future security strategies.

Processes in Place for Recovery:

- **Gradual re-enabling of network services** to prevent further disruptions.
- **Firewall rule validation** to ensure security patches and traffic filtering measures are properly implemented.
- **Backup restoration testing** to confirm critical data and system settings remain intact.
- **Coordination with IT security teams** to monitor network activity for any signs of residual attack attempts.

Long-Term Improvements for Resilience:

- **Develop a comprehensive disaster recovery plan** that includes detailed procedures for DDoS mitigation.
- **Implement real-time network traffic monitoring** to identify and respond to threats proactively.
- **Conduct regular penetration testing and simulated DDoS drills** to assess response efficiency.
- **Improve firewall policies** to block potential attack actors before they can impact network resources.

Reflections/Notes

While working on this analysis, I identified several security concepts that I plan to explore further, including **firewall rule configuration, source IP filtering, and advanced access control mechanisms**. My next steps include hands-on labs with **Wireshark, IDS/IPS systems, and firewall security settings** to deepen my understanding.