**Title** : Cybersecurity Case Study – DDoS Attack & Response in a Multimedia Company according to NIST CSF

**Name & role** : Lyncold Stephensky CHERY – Cybersecurity Analyst

**Date: April 24, 2025**

**This document presents a comprehensive response to a realistic DDoS attack scenario affecting an enterprise. It demonstrates the practical application of the NIST Cybersecurity Framework (CSF) in a business context.**

**Title** : Summary

1. Identify
2. Protect
3. Detect
4. Answer
5. To recover

**Title** : Background to the incident

The company was the victim of a DDoS attack that compromised the internal network for two hours. During this attack, network services were abruptly interrupted due to a massive flood of ICMP packets, rendering internal traffic completely dysfunctional.

**1. Identify**

The cybersecurity team conducted a thorough investigation to identify the origin of the incident. It was discovered that a malicious actor had launched an ICMP ping flood attack, exploiting a misconfigured firewall. This vulnerability allowed the cyberattacker to overwhelm the internal network by sending a large volume of ICMP packets.

Regular future audits of firewalls, network systems, and access privileges are now planned to prevent such vulnerabilities.

**2. Protect**

To strengthen network protection, the team has implemented the following measures:

* **Implementing ICMP rate-limiting rules** on the firewall.
* **Checking source IP addresses** to identify spoofed ICMP packets (IP spoofing).
* **Deployment of a network monitoring tool** to detect abnormal behavior.
* **Implemented an IDS/IPS system** to analyze and filter suspicious ICMP packets.

Strengthened security policies and secure network equipment configuration procedures have also been implemented.

**3. Detect**

To improve its capabilities to detect similar incidents in the future, the company has:

* Enabled **firewall logs** to monitor incoming connections in real time.
* Integrated an **IDS system** to monitor traffic coming from the Internet.
* **SIEM )** solution to correlate events and identify potential threats more quickly.

**4. Reply**

During the incident, the team quickly:

* **Blocked all incoming ICMP packets** through network devices.
* **Stopped non-critical services** to reduce load.
* **Restored critical services** once the threat was contained.

Communication has been initiated with stakeholders to inform them of the incident and the actions taken.

**5. Recover**

Once the attack is neutralized, the team has:

* **Restarted all network services** in a controlled manner.
* **Performed an integrity check** of critical systems.
* **Informed all staff that the network was back up and running and secure.**