Incident Report Analysis Using NIST CSF Framework

# Summary

This analysis applies the NIST Cybersecurity Framework (CSF) to a Distributed Denial of Service (DDoS) attack that occurred on a multimedia company's network. The attack compromised the network for two hours and was resolved by blocking incoming ICMP packets and restoring critical services. This document outlines the steps taken to identify, protect, detect, respond to, and recover from the incident, and provides recommendations for improving overall security.

# 1. Identify

- Conduct regular audits of network infrastructure and firewall configurations.  
- Create an inventory of hardware and software used, including firewalls.  
- Perform vulnerability scans to detect misconfigured firewalls and security gaps.

# 2. Protect

- Ensure firewalls are configured to limit incoming ICMP traffic and verify source IP addresses.  
- Develop policies on firewall and network traffic management and train IT staff.  
- Review access privileges to critical systems like firewalls.  
- Implement safeguards like IDS/IPS to prevent malicious traffic.

# 3. Detect

- Implement network monitoring software to detect anomalies in real-time.  
- Set up a Security Information and Event Management (SIEM) tool to send real-time alerts.  
- Use IDS/IPS systems to detect and filter malicious ICMP traffic.

# 4. Respond

- Update the incident response plan with lessons learned from this DDoS attack.  
- Ensure that containment and neutralization procedures are in place.  
- Establish communication protocols for notifying internal and external stakeholders.  
- Conduct forensic analysis to identify the source and method of attack.

# 5. Recover

- Develop recovery procedures to restore normal operations and make permanent firewall changes.  
- Perform a post-incident review to evaluate response effectiveness.  
- Implement improvements to firewall configurations and incident response strategies.

# Reflections/Notes

This incident highlighted the importance of proper firewall configuration and real-time monitoring in preventing DDoS attacks. By following the NIST CSF framework, the organization can enhance its cybersecurity posture and be better prepared for future incidents. Ongoing training, continuous monitoring, and regular updates to incident response plans are essential for maintaining security.