**Cybersecurity Incident Report: DDoS Attack Analysis and Mitigation Plan**

**Prepared by: Eshak Basta**

**Date: 3/5/2025**

**Organization: Multimedia Company**

### **Incident Overview**

**On [Date], our organization experienced a Distributed Denial of Service (DDoS) attack that rendered internal network services unavailable for two hours. The attack involved a flood of ICMP packets, overwhelming the network and preventing legitimate traffic from accessing critical resources. The incident management team responded by blocking incoming ICMP packets, shutting down non-critical services, and restoring essential network functions.**

### **NIST Cybersecurity Framework (CSF) Analysis**

**To improve the organization’s cybersecurity posture and prevent future incidents, we applied the NIST Cybersecurity Framework (CSF) in the following ways:**

#### **1. Identify (Risk Assessment & Security Audits)**

* **Conduct regular network audits to detect vulnerabilities in firewall configurations, system security, and access controls.**
* **Implement penetration testing to simulate attacks and identify potential weak points.**
* **Maintain an asset inventory to track all network resources, including devices, applications, and user access levels.**
* **Establish a threat intelligence program to stay informed about emerging cybersecurity threats.**

#### **2. Protect (Preventive Security Measures)**

* **Firewall Hardening: Implemented a firewall rule to limit incoming ICMP packets and prevent future ICMP flood attacks.**
* **Access Control Policies: Enforced network segmentation and role-based access control (RBAC) to restrict access to sensitive data.**
* **Employee Training: Provided cybersecurity awareness training to educate employees on social engineering, phishing, and DDoS attack risks.**
* **Backup and Recovery Plan: Ensured critical business data is backed up and can be restored in case of an attack.**

#### **3. Detect (Monitoring & Threat Identification)**

* **Network Monitoring Software: Deployed tools to monitor and analyze network traffic patterns in real time.**
* **Intrusion Detection and Prevention System (IDS/IPS): Implemented an IDS/IPS to filter out suspicious ICMP traffic and prevent abnormal packet floods.**
* **Log Analysis & Alerting: Configured automated alerts to notify security teams when unusual traffic spikes occur.**
* **Incident Response Drills: Conducted periodic security exercises to test detection and response capabilities.**

#### **4. Respond (Incident Containment & Mitigation)**

* **Incident Response Plan: Defined a structured response plan for DDoS incidents, ensuring quick containment and mitigation.**
* **Source IP Verification: Implemented firewall filtering to check for spoofed IP addresses on incoming ICMP packets.**
* **Security Team Coordination: Strengthened collaboration between IT, cybersecurity, and incident response teams for faster resolution.**
* **Reporting & Documentation: Maintained detailed logs and incident reports for forensic analysis and future reference.**

#### **5. Recover (System Restoration & Future Prevention)**

* **System Restoration: Ensured all affected systems were properly restored and verified for integrity.**
* **Post-Incident Review: Conducted a post-mortem analysis to evaluate response effectiveness and identify areas for improvement.**
* **Continuous Improvement: Integrated lessons learned into security policies and enhanced response strategies.**
* **Redundancy Measures: Developed contingency plans, including secondary network routes and cloud-based DDoS protection services.**

### **Conclusion & Recommendations**

**By applying the NIST Cybersecurity Framework, we have strengthened our network security and reduced the likelihood of future DDoS attacks. Moving forward, we recommend:**

* **Regular penetration testing to identify and address vulnerabilities proactively.**
* **Upgrading firewall capabilities to implement more granular traffic filtering and adaptive security measures.**
* **Increasing investment in cloud-based DDoS protection services to mitigate large-scale attacks.**
* **Conducting regular employee training sessions to reinforce cybersecurity awareness and best practices.**

**With these measures in place, our organization can better protect its digital assets and ensure continued operational stability.**