Incident Report Analysis – DDoS Attack on Multimedia Company Network

1. Summary of the Security Event

A Distributed Denial of Service (DDoS) attack occurred against the internal network of a multimedia company that provides web and design services. The attack lasted for approximately two hours and rendered internal network services unresponsive. The incident was triggered by an incoming flood of ICMP packets, which overwhelmed the network and prevented legitimate traffic from accessing resources.

Cause: An unconfigured firewall allowed ICMP traffic from external sources to pass unchecked, enabling the attacker to flood the network.
Impact: Internal services (file sharing, web access, and email systems) were unavailable; client communication and operations were interrupted.
Response: The team blocked incoming ICMP packets, took non-critical services offline, restored critical systems, and implemented firewall rules with source IP verification.

2. Identify – Type of Attack and Affected Systems

Attack Type: Distributed Denial of Service (DDoS) using ICMP flood.
Attack Vector: ICMP packets exploiting unfiltered inbound network ports. **Systems Impacted:** Internal web servers, routers, DNS servers, and firewall (misconfigured).

3. Protect – Hardening and Prevention Measures

To prevent future DDoS and ICMP-based attacks, the following protection strategies will be implemented:

- ☐ **Firewall Rule Configuration:** Restrict and rate-limit ICMP traffic; allow only from trusted IPs.
- ☐ **Network Segmentation:** Isolate critical systems with VLANs and ACLs. 3.
- ☐ **Employee Security Training:** Train staff to identify abnormal behavior. 4. **System Configuration Management:** Regularly audit firewall/router settings per NIST SP 800-41.

4. Detect – Monitoring and Early Warning Systems

Enhancing network visibility is critical to detect abnormal behavior before disruption. Key detection tools and practices include:

- ☐ **IDS/IPS Systems:** Use Snort or Suricata to detect and block suspicious ICMP traffic. - **Network Monitoring Tools:** Implement SolarWinds, Wireshark, or Nagios for real-time packet inspection.
- ☐ **Traffic Pattern Analysis:** Establish baselines and flag anomalies.

☐ - **Log Correlation:** Centralize logs in SIEM platforms like Splunk for pattern analysis.

5. Respond – Incident Containment and Analysis

A strong response plan ensures decisive action in future incidents. Procedures include:

☐ **Containment:** Block malicious IPs and isolate affected segments.
☐ **Neutralization:** Apply packet filtering and reroute via load balancers or cloud DDoS mitigation (Cloudflare, AWS Shield).
☐ **Analysis:** Review logs for origins, packet rates, and attack signatures.
☐ **Post-Incident Review:** Document lessons learned and update response playbooks.

6. Recover – System Restoration and Resilience

Recovery actions focus on restoring stability and verifying system integrity:

☐ Restore configurations and restart services in stages.
☐ Verify data integrity and confirm no configuration damage.
☐ Validate firewall and IDS post-restoration.
☐ Implement redundant network topology with failover routers.
☐ Maintain daily backups and conduct quarterly recovery drills.

7. NIST Cybersecurity Framework Mapping

NIST CSF Function	Action Taken / Planned
Identify	Discovered unconfigured firewall vulnerability through incident analysis.
Protect	Configured firewall rules, implemented IP verification, and trained staff.
Detect	Added IDS/IPS and network monitoring to flag unusual ICMP traffic.
Respond	Developed and tested containment and neutralization plan.
Recover	Created restoration and failover strategy to reduce downtime impact.

8. Conclusion

The DDoS incident was caused by an unconfigured firewall allowing unrestricted ICMP traffic. Implementing firewall restrictions, IDS/IPS systems, continuous monitoring, and employee training strengthens the company's resilience. Following NIST CSF functions ensures a structured and proactive approach to cybersecurity risk management and organizational readiness.

Cybersecurity Relevance

This report demonstrates key competencies in DDoS mitigation, incident response, firewall management, and NIST CSF implementation. It showcases applied skills for SOC analysts and cybersecurity professionals in documenting, analyzing, and improving network defense capabilities.