Incident Report Analysis (NIST CSF)

DDoS Attack – Multimedia Company Network Disruption

Summary

The organization experienced a **Distributed Denial-of-Service (DDoS)** attack that flooded the internal network with **ICMP packets**, rendering network services unavailable for two hours.
The attack entered through an **unconfigured firewall**, allowing malicious ICMP traffic to overwhelm internal systems.
The incident management team blocked incoming ICMP packets, shut down non-critical services, and restored critical network functions.
The cybersecurity team later confirmed the attacker exploited missing firewall rules and a lack of rate limiting, allowing the DDoS attack to pass through.

Identify

- **Type of attack:** ICMP-based Distributed Denial of Service (DDoS) attack
- **Affected systems:**
    - Internal network infrastructure
    - Network services (temporarily unavailable)
    - Firewall (unconfigured rule set allowed attack traffic)
- **Attack vector:** Flood of ICMP ping packets from external malicious sources
- **Business impact:**
    - Two hours of downtime
    - Disruption of access to internal systems

    - Degraded service availability for employees and clients

---

Protect

- Configure firewall rules to block or limit unnecessary ICMP traffic.
- Implement ICMP rate limiting to prevent flood conditions.
- Enforce proper firewall hardening and routine configuration reviews.
- Apply source IP verification to prevent spoofed traffic.
- Ensure regular patching and maintenance of network devices.
- Provide staff training on recognizing abnormal network behavior.

Detect

- Use **network monitoring software** to track unusual traffic volumes or spikes.
- Deploy **IDS/IPS** to detect and filter malicious ICMP patterns.
- Set up alerts for abnormal inbound traffic rates, unexpected ICMP traffic, or repeated connection attempts.
- Implement continuous monitoring of firewall logs, router logs, and bandwidth usage.
- Use SIEM tools to correlate network anomalies and generate early warnings.

Respond

- Immediately block malicious traffic by updating firewall rules.
- Isolate or shut down non-critical services to preserve bandwidth.
- Follow the incident response plan to contain and neutralize DDoS traffic.

- Document IP sources, packet patterns, and timeframes for later analysis.
- Communicate status updates to IT teams and leadership.
- Review response actions to identify gaps and improve future procedures.

Recover

- Restore all affected internal network services to normal operation.
- Re-enable services that were taken offline once the network stabilizes.
- Review and update recovery procedures based on lessons learned.
- Implement long-term improvements such as automated firewall updates and enhanced DDoS protection.
- Communicate the completion and post-incident steps to all stakeholders.