# Incident Report Analysis

## Summary

The multimedia company experienced a Distributed Denial of Service (DDoS) attack that disrupted internal network operations for approximately two hours. The attack involved a flood of ICMP packets (ping requests) that overwhelmed the network bandwidth, making internal resources inaccessible. The root cause was an unconfigured firewall, which failed to filter or limit incoming ICMP packets. A malicious actor exploited this vulnerability using a botnet to launch an ICMP flood. The attack resulted in temporary downtime, loss of productivity, and disruption of client-facing services. The incident management team mitigated the issue by blocking ICMP traffic, taking non-critical systems offline, and restoring critical operations once the network stabilized.

## Identify

Type of Attack: Distributed Denial of Service (DDoS) attack using ICMP flood  
Cause: Unconfigured firewall allowed unrestricted inbound ICMP traffic  
Systems Affected:  
- Internal network infrastructure (routers, switches, and servers)  
- Internal and client-facing applications (web, email, and file services)  
- Employee workstations dependent on network connectivity  
  
Impact:  
- Two hours of network downtime  
- Disrupted business operations and communication  
- Temporary unavailability of client-facing systems

## Protect

Objective: Strengthen the network and prevent similar future incidents.  
  
Immediate Action Plan:  
1. Firewall Configuration: Properly configure the firewall to restrict and rate-limit ICMP traffic. Implement source IP address verification to block spoofed packets.  
2. Network Segmentation: Isolate critical systems from public-facing networks to minimize exposure.  
3. Monitoring Enhancements: Deploy advanced monitoring tools and IDS/IPS systems to identify abnormal traffic.  
4. Policy Updates: Update security policies to include routine firewall audits and vulnerability scans.  
5. Training: Conduct regular staff training on firewall management, DDoS mitigation, and security best practices.

## Detect

Objective: Improve monitoring and detection of abnormal network activity.  
  
Detection Methods:  
- Deploy network monitoring tools (e.g., Wireshark, SolarWinds) to detect spikes in ICMP or unusual inbound traffic.  
- Configure an IDS/IPS to automatically detect and block malicious packets.  
- Implement a SIEM system to centralize logs and generate alerts for suspicious activity.  
- Monitor user access logs to identify unauthorized or unusual login attempts.  
- Conduct regular audits and penetration testing to ensure detection systems remain effective.  
  
Outcome: Enhanced visibility and quicker identification of threats, reducing the risk of major disruptions.

## Respond

Objective: Contain, neutralize, and analyze cybersecurity incidents effectively.  
  
Response Plan:  
1. Containment: Isolate affected systems, block malicious traffic, and suspend non-critical services.  
2. Neutralization: Identify the source, implement targeted firewall and IDS/IPS rules, and apply necessary patches.  
3. Analysis: Collect logs and event data to determine root cause and document findings.  
4. Communication: Notify internal leadership, coordinate with ISPs if needed, and maintain transparent updates to stakeholders.  
5. Improvement: Review and update the Incident Response Plan (IRP) based on lessons learned.  
  
Outcome: Rapid containment and mitigation to reduce downtime and improve future response readiness.

## Recover

Objective: Restore normal network operations and ensure long-term resilience.  
  
Recovery Steps:  
1. Restore and Verify: Confirm that critical systems, servers, and routers are operational and free of malicious configurations.  
2. Data Restoration: Validate backups and restore any affected configurations or data from clean sources.  
3. Testing: Perform system integrity checks and confirm secure network functionality.  
4. Post-Recovery Review: Conduct a post-incident assessment and integrate lessons learned into updated recovery plans.  
5. Ongoing Improvements: Implement stronger backup policies, patch management routines, and review business continuity procedures.  
  
Outcome: Network operations restored safely with improved resilience and stronger preventive measures.

## Reflections/Notes

This incident reinforced the importance of proactive network monitoring and regular configuration audits. Applying the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover) provided a clear, structured approach to managing the event. Future focus should include enhanced automation for detection and response, routine employee training, and continuous updates to security policies to ensure the organization stays prepared for evolving threats.