# Incident Report Analysis

## Summary

A multimedia company that provides web design, graphic design, and social media marketing services experienced a Distributed Denial of Service (DDoS) attack that disrupted internal network services for approximately two hours. The attack involved a flood of incoming ICMP packets that overwhelmed the network, rendering internal resources inaccessible. The incident response team mitigated the attack by blocking incoming ICMP packets, disabling non-critical services, and restoring critical systems. Further investigation revealed that the attack was possible due to an improperly configured firewall.

## Identify

- The incident response team audited firewall configurations and identified that the firewall was not configured to restrict ICMP traffic, making the network vulnerable to flooding attacks.  
- Critical systems affected: internal communication servers, database access, and client-facing services.  
- Attack origin: Malicious actor sending a high volume of ICMP packets through an unprotected entry point.

## Protect

- Implement strict firewall rules to limit the rate of incoming ICMP packets.  
- Deploy source IP validation at the firewall to block packets from spoofed addresses.  
- Install and configure Intrusion Detection and Prevention Systems (IDS/IPS) to detect and filter malicious ICMP traffic.  
- Provide security awareness training to IT staff about network layer attacks and firewall management best practices.

## Detect

- Continuous network traffic monitoring using advanced monitoring software (such as a SIEM system) to detect traffic anomalies.  
- Implement an IDS to specifically detect and alert on high volumes of ICMP traffic or patterns indicative of DDoS attempts.  
- Regular internal audits to verify firewall rule integrity and ensure all traffic patterns are consistent with normal operational behavior.

## Respond

- Establish an incident response plan specifically for DDoS attacks, including immediate firewall rule adjustment and service isolation procedures.  
- Assign roles to IT staff for rapid threat analysis and mitigation during attack events.  
- Communication protocol for notifying leadership, employees, and possibly affected customers.  
- Analyze the source and characteristics of the attack to better prepare for future incidents.

## Recover

- Restore affected services incrementally after the attack subsides and security measures are confirmed active.  
- Review and update all firewall configurations.  
- Perform a full post-incident analysis to identify any gaps in response and recovery efforts.  
- Update the DDoS response plan and train staff based on lessons learned.

## Reflections/Notes

This incident highlighted the importance of proactive firewall management and continuous monitoring. Future security posture improvements should focus on regular system audits, enhanced network visibility, and stronger incident response coordination.