# Incident report analysis

| | |
|---|---|
| **Summary** | A Distributed Denial of Service (DDoS) attack targeted the internal network of a multimedia company offering web design, graphic design, and social media marketing services. The attack flooded the network with ICMP packets, disrupting services for two hours.<br>The cause was an unconfigured firewall, allowing the attacker to send ICMP pings into the network. The cybersecurity team blocked incoming ICMP traffic, took offline non-critical services, and implemented security measures such as new firewall rules, IP verification, network monitoring, and an IDS/IPS system. |
| Identify | Type of Attack: DDoS using ICMP flood<br>Targeted Systems: Internal network infrastructure (routers, switches, servers)<br>Affected Systems: Network services, down for two hours<br>Attack Source: Malicious external actor exploiting an unconfigured firewall<br>Impact: Business downtime affecting web, graphic design, and social media marketing services |
| Protect | Firewall Configuration: Block unnecessary incoming traffic, especially ICMP from untrusted sources.<br>Access Control: Implement stricter policies for trusted users and devices.<br>Security Training: Educate staff on DDoS risks and firewall best practices.<br>Policy Development: Ensure secure configurations across all network devices.<br>Tool Integration: Deploy IPS and update firewall rules to block known DDoS patterns. |
| Detect | Network Monitoring: Use software to detect unusual traffic patterns indicative of DDoS attacks.<br>IDS/IPS: Monitor abnormal activities, particularly on DDoS-prone ports.<br>Anomaly Detection: Set baselines for normal traffic to spot deviations.<br>Continuous Monitoring: Enable real-time alerts for potential issues. |
| Respond | Containment: Block malicious traffic at the firewall and take non-critical services offline.<br>Neutralization: Collaborate with ISPs or DDoS mitigation services to neutralize the attack.<br>Analysis: Review attack patterns to refine defenses.<br>Communication: Update internal teams, clients, and users on the situation and recovery steps.<br>Process Improvement: Post-incident review to improve detection and mitigation.strategies. |

| | |
|---|---|
| Recover | Recovery Planning: Quickly restore critical systems and ensure data integrity.<br>Backup and Redundancy: Maintain backups and redundant systems for faster recovery.<br>Communication: Notify employees and clients about progress recovery.<br>Post-Incident Review: Conduct a technical review of the attack and response, improving the process for future incidents. |

---

## Reflections/Notes:

This incident highlighted the importance of proactive network security measures, such as regularly configuring firewalls, implementing rate-limiting for incoming traffic, and setting up real-time monitoring tools. Regular audits and testing of internal systems are also essential in identifying and mitigating vulnerabilities before they can be exploited in an attack. Additionally, ensuring all team members are trained in cybersecurity best practices and keeping them informed about emerging threats is vital for maintaining a strong security posture.

The incident also illustrated how critical it is to have an effective and well-documented response plan in place that can be executed quickly in the event of an attack, minimizing downtime and service disruption.