# Incident report analysis

| | |
|---|---|
| **Summary** | A multimedia company experienced a DDoS attack, resulting in a network outage for two hours. The attack involved a flood of ICMP packets overwhelming the network through an unconfigured firewall. The incident was resolved by blocking ICMP packets, taking non-critical services offline, and restoring critical services. The company later implemented new firewall rules, source IP address verification, network monitoring software, and an IDS/IPS system. |
| Identify | **Type of Attack:** DDoS (Distributed Denial of Service) **Systems Impacted:** Internal network, network services |
| Protect | **Immediate Action Plan**:1. Update firewall configurations to limit the rate of incoming ICMP packets.2. Implement source IP address verification to check for spoofed IPs. 3. Enhance training for network security staff on DDoS |

| | |
|---|---|
| | mitigation techniques. 4. Regularly update and patch network devices and software. |
| Detect | **Detection Methods:** 1. Implement continuous network traffic monitoring. 2. Deploy network monitoring software to detect abnormal traffic patterns. 3. Use IDS/IPS systems to filter out suspicious ICMP traffic. 4. Conduct regular network audits to identify vulnerabilities. 5. Implement logging and alerting systems to track unauthorized access attempts. |
| Respond | **Response Plan:** 1. Contain the incident by isolating affected systems. 2. Neutralize the threat by blocking malicious traffic and taking non-critical services offline. 3. Analyze the incident to determine the attack vector and affected systems. 4. Improve the response process by documenting lessons learned and updating incident response plans. 5. Communicate with stakeholders about the incident and mitigation measures taken. |
| Recover | **Recovery Steps:** 1. Restore affected systems to normal operation. 2. Recover and validate system data and assets. 3. Conduct a post-incident review to identify areas for improvement. 4. Update security policies and procedures based on the incident analysis. 5. Enhance disaster recovery plans to ensure quick recovery in future incidents. |

Reflections/Notes:
Continuous improvement in network security practices is essential to mitigate the risk of future attacks.

Regular training and awareness programs for employees can help in early detection and response to cybersecurity incidents.

Collaboration with external cybersecurity experts can provide additional insights and enhance the security posture of the organization.

Keeping stakeholders informed throughout the incident lifecycle helps maintain transparency and trust.