# Incident report analysis

| | |
|---|---|
| **Summary** | This incident was discovered because the company's internal network stopped responding. The cybersecurity team's investigation found that it was a DDoS attack through an unconfigured firewall. The incident management team contained the attack by blocking incoming ICMP packets, stopping all non-critical network services offline so that critical network services could be restored.This attack compromised the internal network for two hours. |
| Identify | The cyber security team investigated the network services in the company. It was found that there was an unconfigured firewall. This was entrance point the attacker used to perform a DDoS attack.All critical network resources needed to be secured and restored to a functioning state. . |
| Protect | The network security team added a new firewall rule to limit the rate of incoming ICMP packets. Furthermore, an IDS/IPS system was added to filter out ICMP traffic based on suspicious characteristics. |
| Detect | To detect any future malicious activity, a networking monitoring software was added to detect abnormal traffic patterns on the company system. Furthermore, the security team added a source IP address verification on the firewall to check for any spoofed IP addresses on incoming ICMP packets |
| Respond | For future security events, the cybersecurity team will isolate affected systems to prevent further distruption to the network. They will also attempt to restore any critical systems and services that were disrupted by the event. The team will then analyse network logs for suspicious and abnormal activity. The team will the report all incidents to the upper management and appropriate legal authorities, if applicable |

| | |
|---|---|
| Recover | To recover form a DDoS attack by ICMP flooding, access to the network services need to be restored to normal functioning state. In the future, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Finally once the flood of ICMP packets have been timed out, all non-critical network systems and services can be brought back online. |

---

| |
|---|
| Reflections/Notes: |