# Incident report analysis

| | |
|---|---|
| **Summary** | The organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. During the attack, the organization's network services suddenly stopped responding due to an incoming flood of ICMP packets. As a result, normal internal network traffic could not access any network resources. |
| Identify | The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. The company's cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack. |
| Protect | To address this security event, the network security team implemented:<br>● A new firewall rule to limit the rate of incoming ICMP packets<br>● Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets<br>● Network monitoring software to detect abnormal traffic patterns |

| | |
|---|---|
| Detect | To detect new unauthorized access attacks in the future. The team will invest in a IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. |
| Respond | After identifying the attack, the team immediately took action by blocking ICMP packets, restoring critical network services, and isolating non-essential systems to minimize damage. Communication was sent to all affected teams, and security logs were analyzed to determine the scope of the attack |
| Recover | Once the attack was mitigated, the team slowly restored normal network operations while continuously monitoring for further suspicious activity. They conducted a post-incident review to strengthen security measures, updated firewall rules, and provided additional training to IT staff to prevent similar attacks in the future. |