# Incident report analysis

| | |
|---|---|
| **Summary** | Recently, several employees have reported that the organization's network services suddenly stopped responding due to an incoming flood of ICMP packets. Because of this, any network resources in the company cannot be accessed by normal internal network traffic to perform their job. We found out that a malicious actor took advantage of the unconfigured firewall and sent a flood of ICMP pings through the network. This led to overwhelming the company's network through distributed denial of service attacks.<br><br>In response to this attack, we implemented the following: a new firewall rule, source IP address verification, network monitoring software, and IDS/IPS.<br><br>Because of this impact, it was compromised for approximately two hours before it was resolved. |
| Identify | The company's cybersecurity team audits of internal networks, systems, devices, and access privileges to identify potential gaps in security. The team found out that the firewall had been unconfigured which led to the attack in the network. It was confirmed that the malicious attacker used a Distributed Denial of Service (DDoS) attack. As a result, the network infrastructure had been compromised. Employees and customers were affected by this |
| Protect | Upon further investigations, our teams implemented new ways address this security event: A new firewall rule to limit the rate of incoming ICMP packets, Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets,Network monitoring |

| | |
|---|---|
| | software to detect abnormal traffic patterns, and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. |
| Detect | To detect new unauthorized access attacks in the future, the security team will use Intrusion detection system (IDS) and network monitoring software to detect abnormal traffic patterns to the systems from the internet. Also using the SIEM tool can also be effective. |
| Respond | responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. Also needed to communicate with other |
| Recover | • Any internal network systems that have been deleted or altered.<br>• Create backup plans in case that any data has been lost or altered.<br>• Communicate with other IT professionals and establish disaster recovery plans.<br>• Once the flood of ICMP is out, then we can proceed to have network services and systems to be brought back online. |

---

| Reflections/Notes: |
|---|