# Incident report analysis

| | |
|---|---|
| **Summary** | Recently, our organisation's network services suddenly stopped responding due to an incoming flood of ICMP packets and would not allow normal internal traffic to access any network resources for 2 hours. |
| Identify | The team found that the attack was orchestrated by a threat actor by sending a flood of ICMP pings into the company's network through a firewall that was unconfigured which allowed the attacker to overwhelm the company's network through a DDoS attack. The internal network was affected by this attack. |
| Protect | To address this security event, the network security team has now implemented the following to prevent future attacks:<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<br>• An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics |
| Detect | To detect future attacks, the network security team have implemented firewall rules, network monitoring software, and an IDS/IPS system to filter out suspicious ICMP traffic. |
| Respond | • Monitoring the network to detect abnormal traffic patterns<br>• Block the suspicious incoming ICMP packets<br>• Stopping all non-critical network services offline<br>• Isolate affected systems from network<br>• Keep monitoring network to ensure attack is contained |

| | |
|---|---|
| Recover | The team will determine if the attack has been completely halted, and then work towards restoring all systems that were affected by the attack and then test and verify that systems are functional, and restore critical network services. |

---

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