# Incident report analysis

| | |
|---|---|
| **Summary** | Recently, our organization experienced a ddos attack that caused network services to stop responding. We were forced to take all non-critical network activities of the organization offline for 2 hours until we could resolve the issue. It was found that the network was flooded with ICMP packets, so we blocked all incoming ICMP packets. The packets came from a malicious actor who found a hole in the firewall due to a misconfiguration and then DDosed the network. Once we removed the threat, we brought all systems back online. |
| Identify | It was found that the attack only affected the network and no other hardware or software was affected. All business processes that required the use of non-critical network functions were interrupted during these 2 hours. Anyone in the organization who uses this network will need access to the network. |
| Protect | The team implemented a new firewall rule to limit the rate of incoming ICMP packets. We also added source IP verification on the firewall to detect any IP spoofing on incoming ICMP packets. |
| Detect | The team implemented network monitoring software to detect abnormal traffic patterns. Also, an IDS and IPS system was implemented to filter ICMP traffic based on suspicious characteristics. |
| Respond | In order to respond to similar events in the future, there should be immediate notification of the security department when an employee is unable to connect to the network to ensure the quickest response time. We will make sure to inform everyone in the organization who uses the network that it will be taken offline to resolve the issue, and we will notify them as soon as the network is back online. We will use the current security management tools as necessary to detect the source of the problem. |

| | |
|---|---|
| Recover | To recover from an ICMP flood DDoS attack, network services must be restored to normal functionality. In the future, external ICMP flood attacks can be blocked at the firewall to prevent recurrence. During recovery, all non-essential network services should be temporarily stopped to reduce internal network traffic. Critical services should be brought back online first. Once the ICMP packet flood subsides, non-essential network systems and services can be gradually restored. |

---

Reflections/Notes: This attack did not affect company or customer data. All that was lost was precious time for our employees to get their work done, but it was only for 2 hours. This can easily be recouped through increased short term effort on behalf of the employees and/or overtime work.