**Incident report analysis**

[**Scenario Description**](https://docs.google.com/document/d/1erw8I6qNKCXa98Gt2Gjbm2hnMcj64Mb1bC0kfgf1Y7Y/edit?usp=sharing)

[**NIST CSF Information**](https://docs.google.com/document/d/11lwfcJbbE6hNYe9pgON5hUW62Xzi0fjc3AYyFCkyNCA/edit?usp=sharing)

| **Summary** | It was found that the network services for the organization stopped responding suddenly. This was found to be due to an excessive amount of ICMP packets. Since normal network traffic couldn’t access the network, the incoming ICMP packets were blocked to stop non-vital traffic. | | |
| --- | --- | --- | --- |
| Identify | Investigation of this event occurred in which a malicious attacker was found to have sent the ICMP flood through an unconfigured firewall which allowed for the excess pings to come through. This created a DDoS attack. | | |
| Protect | In order to address this issue, the incident team implemented rules for the firewall allowing for a certain rate of ICMP packets only, IP address verification to check for spoofed IP addresses, network monitoring software, and an IDS/IPS system. | | |
| Detect | In order to detect malicious actors in the future, the organization will primarily use the firewall, an IDS/IPS system, and monitoring to detect and prevent ICMP flooding from happening again. | | |
| Respond | The organization will issue a notice for those clients or users impacted by the network services, namely those impacted by not being able to access the network resources. They may have to apologize for the delay and for any inconvenience this incident may have caused. | | |
| Recover | The incident team will implement all necessary precautions to safeguard this from happening in the future. All normal network activity should be able to resume as usual. A notice should be sent out indicating that normal business operations can continue. | | |

| Reflections/Notes: |
| --- |