# Incident report analysis

## Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

| | |
|---|---|
| **Summary** | The company's network services stopped responding. This was a result of (DDoS) attack performed through the flooding of ICMP packets. The attack was blocked and all non-critical network services were stopped in order for critical network services to be restored. |
| Identify | A threat actor floods the company's network services with ICMP packets. Almost all of the internal network was affected. The critical network had to be restored and secured. |
| Protect | A new firewall rule was implemented that would limit the rate of the ICMP packets. An IDS/IPS system will be used to filter ICMP traffic that looks suspicious. |
| Detect | Source IP address configuration was added to the firewall that will allow it to search for spoofed IP addresses coming in on ICMP packets. Network monitoring software was added to detect suspicious traffic patterns. |
| Respond | Isolation of affected systems will be used in the future to prevent disruption of other network activities. Restoration of critical systems and services that were disrupted by the event will be performed. Network logs will be analyzed to check for suspicious activity. All incidents will be reported to management and |

| | |
|---|---|
| | legal authorities if needed. |
| Recover | Recovering from a DDoS attack through ICMP packets requires network services to be restored to a normal functioning state. ICMP packets outside of the network will be blocked at the firewall. Non-critical network services should be stopped to reduce internal network traffic. Once the ICMP packets are no longer being flooding into the network all non-critical network systems can be turned online again. |

---

| Reflections/Notes: |
|---|