# 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 organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. During the attack, the organization’s network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. |
| Identify | The cybersecurity team of the company conducted an investigation and discovered that a malicious actor exploited an unconfigured firewall to launch a flood of ICMP pings into the company's network. This vulnerability enabled the attacker to carry out a distributed denial of service (DDoS) attack, overwhelming the company's network. |
| Protect | The team addressed the security event by implementing:<br>● New firewall rules<br>● An IDS/IPS system |
| Detect | The team has implemented firewall configurations to accomplish two objectives:<br>Limit the rate of incoming ICMP packets and Perform IP address spoofing |

| | |
|---|---|
| | checks on incoming ICMP packets. |
| Respond | To prevent future occurrences of this type of attack, the cybersecurity team will isolate affected systems to prevent any further disruption to the network. the team will also conduct a thorough analysis of network logs to identify any suspicious or abnormal activities that might have occurred. |
| Recover | To recover from a DDoS attack, access to network services need to be restored to a normal functioning state. In the future, external ICMP flood attacks can be blocked at the firewall.<br>Critical network services should be restored first. Then, once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online. |

---

Reflections/Notes: