# 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 has recently experienced a DDoS attack and the network service stopped due to the flood of ICMP packets. First, the incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. Then, the cybersecurity team investigated the incident and concluded that a malicious actor had set a flood of ICMP pings into the company's network through an unconfigured firewall. At last, the network security team implemented:<br>(1) a new firewall rule to limit rate of incoming ICMP packets;<br>(2) a source IP address verification on the firewall to check for the spoofed IP addresses on incoming ICMP packets;<br>(3) a network monitoring software to detect abnormal traffic patterns;<br>(4) an IDS/IP system to filter out some ICMP traffic. |
| Identify | Due to the DDoS attack, the internal network needed in the day-a-day work stopped for 2 hours and, while it was solved, normal internal network traffic could not access any network resources. |
| Protect | The network security team has implemented:<br>(1) a new firewall rule, to limit the rate of incoming ICMP packets;<br>(2) a source IP address verification on the firewall, to check for spoofed IP |

| | |
|---|---|
| | addresses on incoming ICMP packets;<br>(3) a network monitoring software, to detect abnormal traffic patterns;<br>(4) and an IDS/IP system, to filter out ICMP traffic according to suspicious characteristics.<br>Additionally, in the near future it would be good to also implement an IPS. |
| Detect | Having considered what happened in the security incident, a network monitoring software and an IDS/IP system have been implemented to detect future DDoS attacks. |
| Respond | The team blocked incoming ICMP packets, to mitigate the impact of the attack, and stopped all non-critical network services offline, to contain the incident and affected devices. The improvements done after the security incident are the taken detection and protection measures mentioned above. |
| Recover | The team recovers by restoring the critical network devices, restarting all non-critical network devices offline and allowing ICMP packets to income the network and, of course, implementing all the new security measures. |

---

| Reflections/Notes: |
|---|