# 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 2 hours, during which normal internal network traffic could not access any network resources. The cybersecurity team took action by stopping all non-critical network services, in order to restore critical network services. |
| Identify | A threat actor used an ICMP flood attack to overload the organization’s network using a vulnerability in an unconfigured firewall. The resources affected were the entire internal network, which the cybersecurity team had to restore to a working state. |
| Protect | To protect against similar attacks, the cybersecurity team implemented a couple controls: a firewall rule to limit the rate of incoming ICMP attacks and an IDS/IPS system to filter out suspicious ICMP traffic |
| Detect | To assist detection of similar attacks, the cybersecurity team added source IP verification to check for spoofed IP addresses and a network monitoring software to detect abnormal traffic patterns |
| Respond | In response to the attack, the cybersecurity team stopped all non-critical network services, so that critical network services could be restored. For the future, the system could be configured in a way that an attack on the system does not affect the entire internal network to ensure business continuity. The team will report all details of the incident to upper management and legal authorities as applicable. |

| | |
|---|---|
| Recover | After a DDoS attack, critical network services first need to be recovered in order to provide business continuity for internal users. Then, non-critical services can be restored. In the future, using a combination of properly configured firewall rules and an IDS/IPS system will help prevent another system failure due to DDoS attack |

---

| |
|---|
| Reflections/Notes: |