# 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. The network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. The cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack. |
| Identify | The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline. The cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack. |

| | |
|---|---|
| Protect | The team has implemented a new firewall rule to limit the rate of incoming ICMP packets.They also added Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets, these tools will help prevent future attacks. |
| Detect | The team implemented network monitoring software to detect abnormal traffic patterns. An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. |
| Respond | Once the network services stopped responding due to the incoming flood of ICMP packets. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline |
| Recover | After blocking incoming ICMP packets and stopping all non critical network services offline. The incident management team restored critical network services. |

---