**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 experienced a DDoS attack, which compromised the internal network for a duration of 2 hours until it was resolved. |
| Identify | Due to a flood of ICMP packets, the network services ceased. |
| Protect | The Incident Management team blocked incoming ICMP packets, stopping all non-critical services, and restoring critical network services. |
| Detect | A malicious actor sent a flood of ICMP pings into the network through an unconfigured firewall. |
| Respond | Suggestion for future events:   * Create a new firewall rule to limit the rate of incoming ICMP packets. * Add a SIEM and IPS or IDS to continuously monitor network traffic. * Source IP verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. |
| Recover | Utilize baseline configuration for improved firewall to determine if there are unverified changes. |

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