**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** | Basic services were not responding this morning and firewall logs indicate an ICMP flood as a result of DDOS attack. |
| Identify | The organizations services stopped responding and checks by the incident management team revealed a DDOS attack had taken place. A flood of ICMP packets overwhelmed the network. |
| Protect | * A new firewall rule to limit the rate of incoming ICMP packets * Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets * Network monitoring software to detect abnormal traffic patterns * An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics |
| Detect | To detect future occurrences a Network monitoring software to detect and flag abnormal traffic patterns and IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics is implemented. |
| Respond | A rule was created on the firewall to prevent all ICMP traffic, non-critical network services were also stopped. The team will also report all incidents to upper management and appropriate legal authorities, if applicable. |
| Recover | Critical network services were restored from the last full backup performed, upon completion of this restoration and monitoring other non-critical services were also restored. |

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