**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** | A DDoS attack hit the network due to poor firewall settings, making key services temporarily unavailable. |
| Identify | The team found the firewall didn’t block ICMP traffic, allowing the attack to disrupt operations. |
| Protect | New firewall rules were added, policies updated, and IDS/IPS systems installed. |
| Detect | Monitoring tools now flag unusual ICMP traffic, and alerts are set up for faster detection. |
| Respond | ICMP traffic was blocked, non-critical services paused, and response plans were updated for quicker action. |
| Recover | Systems were restored step-by-step, firewall settings were improved, and post-incident reviews were done. |

|  |
| --- |
| Reflections/Notes: This incident showed how vital it is to maintain strong and properly configured firewalls. It also demonstrated the value of proactive traffic monitoring and the ability to respond quickly during an attack. Regular security audits and clear communication during incidents play a major role in minimizing damage. The situation also made it clear that having multiple layers of defense and a reliable recovery plan is essential for keeping critical services protected. |