**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** | Network at multimedia company’s network experienced DDOS attack. ICMPS messages flooded the network until it was inoperable.The attack left systems down for 2 hours. |
| Identify | ICMP messages where flooding the network leaving network inoperable. |
| Protect | Firewall was reconfigured to limit incoming ICMP messages and to verify source ip addresses. |
| Detect | IDS and IPS systems were implemented to filter and inform IT of any suspicion ICMP traffic. |
| Respond | IT team took action by blocking incoming ICMP packets, stopping all nonessential network functions, and restoring all network function. |
| Recover | Baseline setting for firewall were changed to monitor and mitigate this kind of attack in the future. All network functions were returned to normal working order. |

|  |
| --- |
| Reflections/Notes: In future if team could use catcpha to verify its a human each time a ICMP message is sent |