**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 DoDDs attack with took the servers down for two hours |
| Identify | It seems like the variability point was at an unconfigured firewall so they could send as many ICMP packets as they wanted. The whole system went down |
| Protect | **They need to check all firewalls and make sure that they are configured to comply with legal and company standards** |
| Detect | The team can use SIEM tools to monitor the network traffic better so that they can react faster to the attack or flag untheorized users that are spamming the server with requests and limit them from sending anything to the server |
| Respond | If another attack occurs, we can use the SIEM tools to identify it and block any network traffic from that IP address. |
| Recover | * An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics |

|  |
| --- |
| Reflections/Notes: seems like there was an attack because there was an unconfigured firewall which led to the attacker sending mass amounts of ICMP packets to take down the network. |