**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** |  | | |
| --- | --- | --- | --- |
| Identify | During work hours of a certain day our organization experienced a DDOS attack causing a minimum of 2 hours of down time and risk of having data being leaked during said DDOS attack | | |
| Protect | Immediately we are going to conduct a full scale internal security audit on all of our cyber security measures including firewalls, network rulesets, and so on | | |
| Detect | As we move forward after the audit, we are going to implement specific DDOS attack resistance firewall configuration to any new or existing firewalls | | |
| Respond | We responded by shutting down our internal networks and only opening access to the crippled network be under new encryption keys, thus making the network not respond to requests that do not now carry the new encryption keys, this letting esstial security personal gain access to the system after the DDos attack has been stopped and will result not being able to continue. | | |
| Recover | all old encryption keys are being thrown away and replaced with new keys, we will do this after looking through all logs of outgoing data and confirming that no leaked data came through. | | |

| Reflections/Notes: |
| --- |