**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** | There was an incident on the network of the Company, where all of the services stopped responding. This was caused by a flooding of incoming ICMP packets caused by a Distributed Denial of Service (DDoS) attack and resulted in the downtime of all non-critical network services for 2 hours. The issue has been resolved by blocking the ICMP requests |
| Identify | Malicious actors targeted the entire internal network causing it to be offline until it was remediated. All of the business and internal processes were effected during this time. |
| Protect | The security team addressed this security incident by implementing the following measures:   * Configuration of the firewall to limit the amount of incoming ICMP packets per time unit. * Setting up IDS/IPS systems using the identifiable source characteristics to filter out suspicious traffic. |
| Detect | The security team addressed this security incident by implementing the following measures:   * Using the firewall to verify the IP addresses sending ICMP packets to identify whether they are spoofed. * Implementing tools which allow for monitoring of network traffic |
| Respond | In the future, the security team can isolate the issues and, thus, not allowing the entire system to be compromised by a similar kind of attack. Mitigating the risk to the business and internal processes |
| Recover | To recover from a DDoS attack the network traffic should be restored to a normal level. This can be done by limiting the amount of incoming ICMP traffic at firewall level and by limiting the internal network traffic. Once all of the ICMP requests have timed out the systems can be put back online |