**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 company experienced an event that completely shut down its network services. Through investigation it was found that the cause was a distributed denial of service (DDoS) attack through means of flooding the network with ICMP packets. The team's response was to shut down all networks completely and in turn blocking further damage so they were able to later restore critical networks for the business. | | |
| --- | --- | --- | --- |
| Identify | Malicious threat actors targeted the company through an ICMP packet flood attack (DDoS attack). This stopped all networks from functioning and required the security team to shut everything down in order to restore critical functions. | | |
| Protect | The security team implemented a much needed new firewall and configured it to limit the allowed rate of ICMP packets as well as implementing an IDS/IPS system to filter ICMP traffic based on potential suspicious characteristics. | | |
| Detect | The security team also configured source IP address verification to detect IP spoofing on incoming ICMP traffic as well as implemented network monitoring software to detect suspicious traffic patterns moving to the network. | | |
| Respond | In the future, the security team will isolate any affected systems from malicious threat actors to prevent further damage or disruptions to business continuity. Once isolated, they will restore critical systems that were affected by the event. Further analysis will be conducted in the data logs to check for any more potentially suspicious activity. The team will then report their findings to the appropriate supervisors and/or authorities if applicable. | | |
| Recover | In order to recover from a ICMP flood DDoS attack, access to network resources need to be restored to a functioning state as soon and effectively as possible. From now on, these ICMP flood attacks will be detected by the now configured firewall. Following that, all non-critical network services should be stopped in order to reduce incoming traffic from the attack and to mitigate damage. Then, critical functions should be restored first. After that, once the ICMP flood attack ceases or is contained, non-critical services must be brought back online so the business can continue to function as normal. | | |

| Reflections/Notes: Protocols need to be followed in specific order to mitigate further damage from attacks and so business continuity can be protected in the future. These frameworks give a structure of procedures for all companies to have varied flexibility in responding to these incidents safely and effectively. |
| --- |