**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** | This was a DdoS attack which affected the internal network, both critical and non critical network resources were affect. The security team responded by taking non critical network services online and allowing only critical services to operate on the network. |
| Identify | A flood of spoofed ICMP packets targeted the company’s internal network. The company’s critical and non critical network services were affected during the attack. |
| Protect |  |
| Detect |  |
| Respond | Using IDS tools to detect an attack, SEIM tools to identify the assets under attack, and with network segmentation in place the security team can respond to future network attacks by isolating only the affected network while keeping the rest of the system online. |
| Recover | To recover from the incident the organization needs non critical network resources to come back online. However there is need to make sure that all of the organization’s network are safely protected by the firewall before bringing them back online. The organization could keep backup machines that offer redundancy in the case of a future attack, they can redirect network traffic to their backup machines while taking affected network resources offline. The organization can also use cloud hosting platforms that have baseline configurations to reduce misconfiguration vulnerabilities. |

|  |
| --- |
| Reflections/Notes: To protect the system the security team has implemented new firewall rules and is recommneded to start using neXt generation firewalls. The security team is also recommended to implement network segmentation to separate crucial and non crucial network services. The security team will start using IDS/IPS AND SEIM tools to monitor their networks, in the event of future attacks they should be able to easily identify spikes in ICMP packets and isolate affected networks using these tools. To recover from future attacks the team can implement back up network resources so that if any resources are taken offline they can transfer traffic to the back ups. The team should consider using cloud platforms that offer baseline configurations to prevent future mis configurations. |
|  |