**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 DDoS attack with a flood of incoming ICMP packets which overwhelmed the network, causing service disruptions for two hours and preventing the normal internal network traffic from accessing any network resources. |
| Identify | The attack was a Distributed Denial of Service attack (DDoS) with a flood of ICMP. The systems that were affected were the firewall and the internal network. |
| Protect | Update and configure the firewall rules to prevent unauthorized ICMP traffic. Also, IP address verification to detect and block the spoofed IP addresses. |
| Detect | Implement tools such as SIEM to detect and get alerts in real-time of potential security threats. |
| Respond | Communicate with stakeholders, customers and others to report and manage the incident. Also, create a protocol to quick response to unknown netwrok traffic and analyzing traffic. |
| Recover | Restore operations back to normal and analyzing and assessing any damage to systems or data. As well as creating recovery plans including the lessons learned from the incident and how to tackle it in the future for quicker restoration and minimizing downtime. |

|  |
| --- |
| Reflections/Notes: Continuous IT training for employees and improve and configure the firewall to prevent unknown or unwanted traffic coming in and out of the network. As well as, regular security audits and updates to security protocols to adapt to new threats |