**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 | Ataque de denegación de servicio distribuido DDos a traves de paquetes ICMP que hicieron un bloqueo de los servicios. | | |
| Protect | **Para protegener es importante denegar estos tipo de paquetes masivos de ICMP** | | |
| Detect | Para detectar esta vulnerabilidad el equipo de seguridad implementará IDS para detectar este tipo de anomalías en la red y prevenir estos ataques antes de dejar fuera de servicios a las aplicaciones. | | |
| Respond | Se deshabilita la cuenta comprometida pero también se hacen entrenamiento de cómo deben proceder cuando estas solicitudes se envíen, ya que son phising utilizando ingeniería social. | | |
| Recover | Bajar los servicios, después de inhabilitar las cuentas asociadas o comprometidas y configurar el firewall para que filtre este tipo de tráfico. | | |

| Reflections/Notes: |
| --- |