**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** | La red interna de la compania fue inundad por paquetes ICMP durante dos horas. Dejando inactivo los servicios internos y sin acceso. |
| Identify | El equipo de seguridad encontro por medio de una auditoria que una mala implementacion del firewall fue usada en contra para inundar la red con paquetes ICMP y la exploto por medio de un ataque DDoS. Asi sobrecargo la red interna y dejando sin acceso a los recursos de la red |
| Protect | El equipo implemento nuevas reglas de firewall como la limitacion de paquetes ICMP, verificacion de las IP basados en las nuevas reglas del firewall. Tambien se establecio una linea base de configuracion del sistema operativo para reducir la superficie de ataque de esta manera nos aseguramos que las implementaciones se hagan de acuerdo a los lineamientos. La segmentacion de las redes de acuerdo con los departamentos protegera tambien fue implementado. |
| Detect | Para detectar patrones similares de ataques se implemento un sistema de detecion de intrusos basados en caracteristicas sospechosas ademas software de monitoreo de red que sera un complemento al IDS descrito previamente. |
| Respond | Para responder en un futuro a nuevos eventos similares a este se usara el marco de referencia NIST CSF. Como ultima medida de contencion sera el aislamiento fisico de la red interna con el internet desconectando los cables de red. |
| Recover | El equipo de seguridad regresara los servicios de red deteniendo los servicios internos no indispensables para enfocarse en los de alta prioridad en el menor tiempo posible para continuar con las actividades operaciones. Se informo a los empleados el evento de manera exhaustiva ademas comunicando que los servicios fueron restaurados a su estado normal. |

|  |
| --- |
| Reflections/Notes: |