reflexión 4.3 grafos

Natalia Quiroga Colorado

En esta actividad el uso de listas adyacencias nos permitió modelar las relaciones entre los atacantes y los puertos afectados, lo que facilita la identificación de los ataques cibernéticos.

Los nodos del grafo representan los puertos y mientras que las aristas representan las conexiones , todo es con una condición de un periodo crítico de (00:00 - 05:00) nos ayuda a detectar actividades sospechosas, como el acceso automatizado de bots o posibles ataques.

En la solución identificamos el puerto más atacado , esto sirve para mitigar riesgos y reforzar la seguridad en puertos que sean vulnerables.
La detección de patrones de ataque fue muy importante porque al observar múltiple intentos de la misma ip te puedes dar cuenta que es un acceso malicioso.
Para ubicar al bot master pusimos de condición que la ip intenta acceder como “admin” o con credenciales privilegiadas.

El uso de estructuras nos optimizó el análisis de grandes volúmenes de datos, y también nos abrió la puerta a la automatización de respuestas frente a incidentes para fortalecer la seguridad.