Avance 1 del proyecto

Integrantes:

Alexandra Mora Brenes

Isaac David Robles Meza

Jurgen Brenes Arce

Kennan Joved Sánchez Garro

Curso: Programación avanzada

Profesor: Andres Felipe Vargas Rivera

III Cuatrimestre 2025

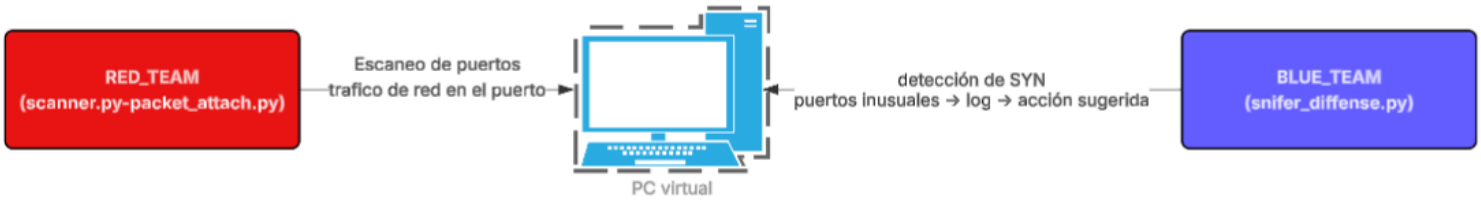
1. Introducción

Objetivo del documento

Este documento corresponde a la versión final del proyecto, en la cual se presenta un flujo completo de ataque, detección y también de respuesta, usando los distintos scripts generados por el Red y el Blue Team.

La finalidad es demostrar la forma en la que un ataque controlado podría ser detectado por distintos mecanismos de defensa básicos y la reacción adecuada ante la mencionada actividad.

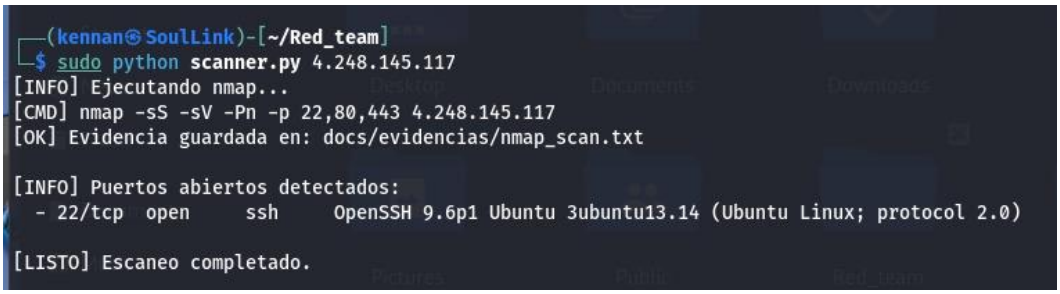
2. Flujo integrado:

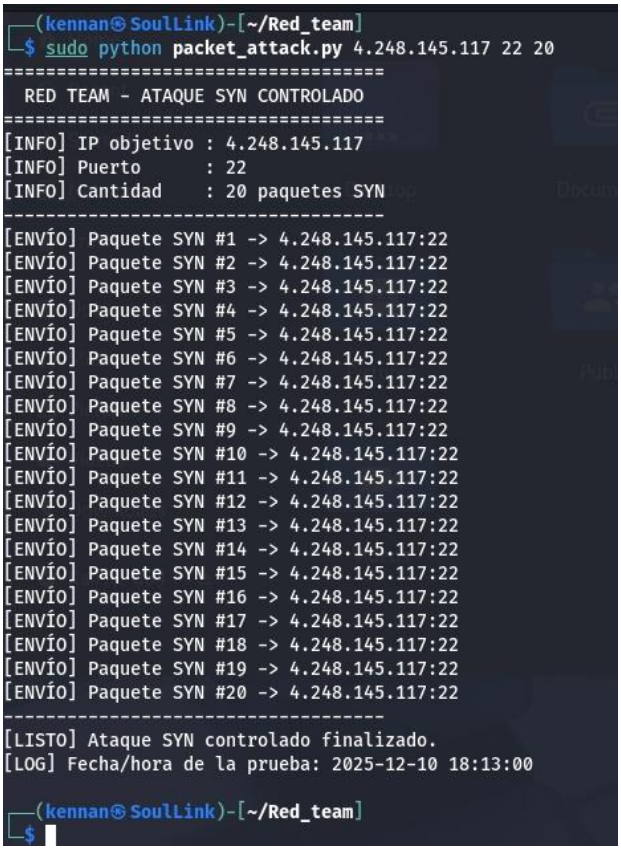


3.

Paso 1 – Ataque / Reconocimiento (Red Team)

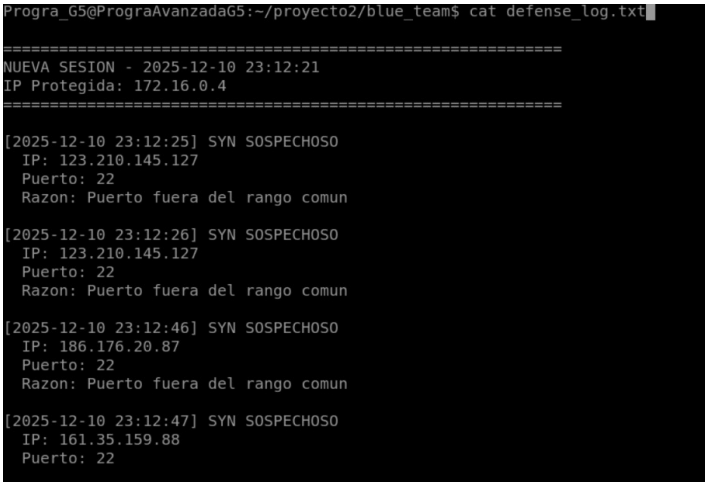
1. Se ejecuta scanner.py para identificar puertos abiertos.
2. Posteriormente se ejecuta packet_attack.py enviando paquetes SYN controlados hacia la VM.





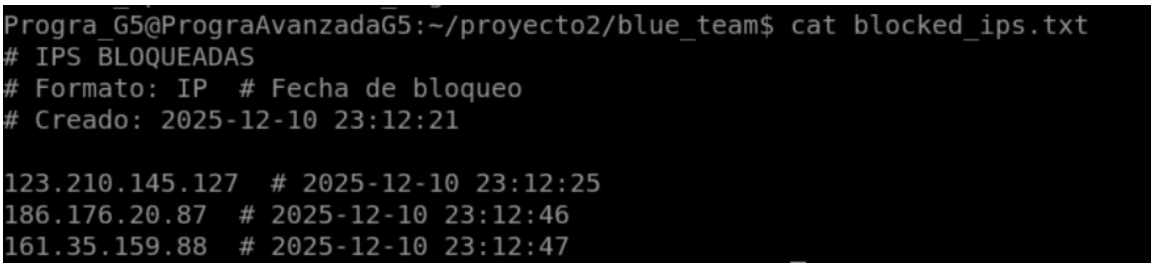
Paso 2 – Detección (Blue Team)

1. El script sniffer_defense.py analiza el tráfico de red.
2. Se detecta tráfico SYN inusual dirigido a un puerto específico.
3. La detección queda registrada en el log.



Paso 3 – Acción / Respuesta

1. Ante la detección, el sistema sugiere una acción defensiva.
   Ejemplo: registrar la IP sospechosa, sugerir bloqueo, o generar alerta.



4. Recomendaciones de mejora:

- Tratar de limitar los intentos (rate limiting).
- Poder implementar distintas reglas de firewall que limiten la cantidad de conexiones SYN por IP para asi lograr reducir ataques de reconocimiento o de flooding.
- Bloquear automáticamente las IPs sospechosas.
- Automatizar el bloqueo de las direcciones IP que generen algún tráfico anómalo detectado por el sniffer.
- Monitoreo y alertas
- Agregar alertas que notifiquen al administrador cuando se detecte algún tráfico inusual en la red.