



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

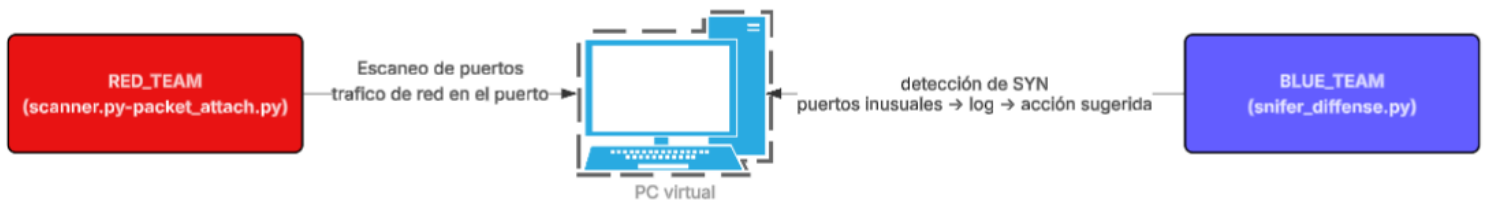
## 1. Introducción

### 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.

```
(kennan@SouLink)-[~/Red_team]
$ sudo python scanner.py 4.248.145.117
[INFO] Ejecutando nmap...
[CMD] nmap -sS -sV -Pn -p 22,80,443 4.248.145.117
[OK] Evidencia guardada en: docs/evidencias/nmap_scan.txt

[INFO] Puertos abiertos detectados:
- 22/tcp open      ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)

[LISTO] Escaneo completado.
```

```
(kennan@SouLink)-[~/Red_team]
$ sudo python packet_attack.py 4.248.145.117 22 20
=====
RED TEAM - ATAQUE SYN CONTROLADO
=====
[INFO] IP objetivo : 4.248.145.117
[INFO] Puerto      : 22
[INFO] Cantidad    : 20 paquetes SYN

-----
[ENVÍO] Paquete SYN #1 -> 4.248.145.117:22
[ENVÍO] Paquete SYN #2 -> 4.248.145.117:22
[ENVÍO] Paquete SYN #3 -> 4.248.145.117:22
[ENVÍO] Paquete SYN #4 -> 4.248.145.117:22
[ENVÍO] Paquete SYN #5 -> 4.248.145.117:22
[ENVÍO] Paquete SYN #6 -> 4.248.145.117:22
[ENVÍO] Paquete SYN #7 -> 4.248.145.117:22
[ENVÍO] Paquete SYN #8 -> 4.248.145.117:22
[ENVÍO] Paquete SYN #9 -> 4.248.145.117:22
[ENVÍO] Paquete SYN #10 -> 4.248.145.117:22
[ENVÍO] Paquete SYN #11 -> 4.248.145.117:22
[ENVÍO] Paquete SYN #12 -> 4.248.145.117:22
[ENVÍO] Paquete SYN #13 -> 4.248.145.117:22
[ENVÍO] Paquete SYN #14 -> 4.248.145.117:22
[ENVÍO] Paquete SYN #15 -> 4.248.145.117:22
[ENVÍO] Paquete SYN #16 -> 4.248.145.117:22
[ENVÍO] Paquete SYN #17 -> 4.248.145.117:22
[ENVÍO] Paquete SYN #18 -> 4.248.145.117:22
[ENVÍO] Paquete SYN #19 -> 4.248.145.117:22
[ENVÍO] Paquete SYN #20 -> 4.248.145.117:22
-----
[LISTO] Ataque SYN controlado finalizado.
[LOG] Fecha/hora de la prueba: 2025-12-10 18:13:00

(kennan@SouLink)-[~/Red_team]
$
```

## 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.

```
Progra_G5@PrograAvanzadaG5:~/proyecto2/blue_team$ cat defense_log.txt
=====
NUEVA SESION - 2025-12-10 23:12:21
IP Protegida: 172.16.0.4
=====
[2025-12-10 23:12:25] SYN SOSPECHOSO
IP: 123.210.145.127
Puerto: 22
Razon: Puerto fuera del rango comun
[2025-12-10 23:12:26] SYN SOSPECHOSO
IP: 123.210.145.127
Puerto: 22
Razon: Puerto fuera del rango comun
[2025-12-10 23:12:46] SYN SOSPECHOSO
IP: 186.176.20.87
Puerto: 22
Razon: Puerto fuera del rango comun
[2025-12-10 23:12:47] SYN SOSPECHOSO
IP: 161.35.159.88
Puerto: 22
```

## Paso 3 – Acción / Respuesta

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

```
Progra_G5@PrograAvanzadaG5:~/proyecto2/blue_team$ cat blocked_ips.txt
# IPS BLOQUEADAS
# Formato: IP # Fecha de bloqueo
# Creado: 2025-12-10 23:12:21

123.210.145.127 # 2025-12-10 23:12:25
186.176.20.87 # 2025-12-10 23:12:46
161.35.159.88 # 2025-12-10 23:12:47
```

#### **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 así 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.