Guía de uso – Sniffer de Defensa

Este script implementa un sistema de detección básica de actividad sospechosa en la red. Su propósito es ayudar a un equipo Blue Team a monitorear tráfico entrante, identificar patrones asociados a reconocimiento (SYN scans) y registrar conexiones hacia puertos inusuales. El sniffer captura paquetes TCP en tiempo real y genera archivos de registro que documentan los eventos detectados.

Características Principales

1. Detecta paquetes TCP con bandera SYN, típicos de escaneos de puertos.
   Cuando una IP supera el umbral de intentos (5 por defecto):
   - Se registra como actividad crítica.
   - Se agrega al archivo *blocked_ips.txt*.
   - Se sugiere un comando iptables para bloquearla.
2. Si un paquete va hacia un puerto que no está en la lista de puertos comunes (22, 80, 443, etc.), se registra como alerta.
3. El script crea dos archivos:
   - **log_events.txt:** registra alertas con timestamp.
   - **blocked_ips.txt:** almacena IPs que deben bloquearse.

Uso del Script

El script está preparado para ejecutarse desde la terminal utilizando argumentos opcionales para personalizar el uso, lo más común es usar los siguientes comandos:

sudo python3 sniffer_defensa.py -i eth0

Opcionalmente se puede limitar cuántos paquetes capturar:

sudo python3 sniffer_defensa.py -i eth0 -c 50

El sniffer permanece activo hasta que el usuario presione Ctrl + C, momento en el cual el programa imprime “Sniffer detenido por el usuario”

Resultados

Durante la ejecución el script muestra:

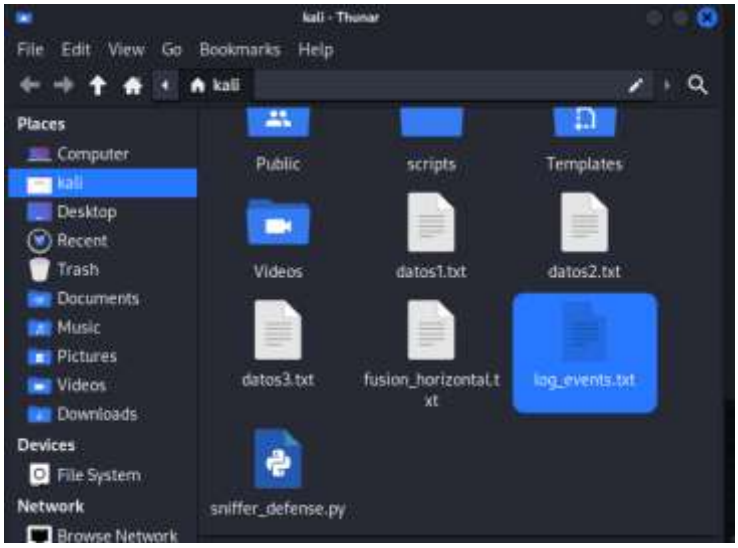
- Alertas de SYN scan.
- Conexiones a puertos inusuales.
- Notificaciones cuando una IP supera el umbral.

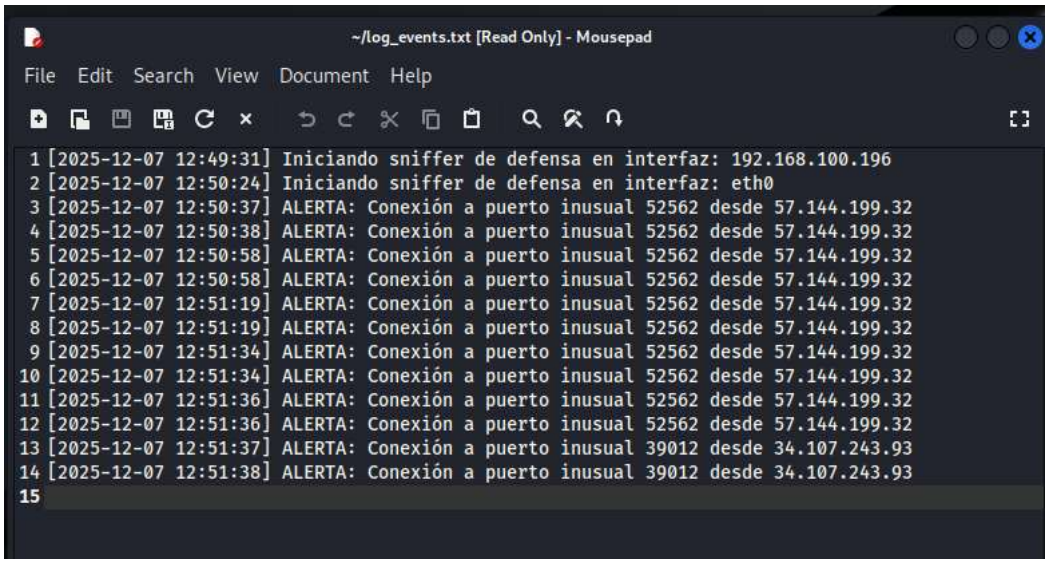
```
┌──(kali㉿kali)-[~]
└─$ sudo python3 sniffer_defense.py -i eth0
═══════════════════════════════════════════════════════
Blue Team - Sniffer de Defensa
═══════════════════════════════════════════════════════
Log: log_events.txt
Blocklist: blocked_ips.txt
Umbral de bloqueo: 5 intentos
═══════════════════════════════════════════════════════
Presiona Ctrl+C para detener

[2025-12-07 12:50:24] Iniciando sniffer de defensa en interfaz: eth0
[2025-12-07 12:50:37] ALERTA: Conexión a puerto inusual 52562 desde 57.144.199.32
[2025-12-07 12:50:38] ALERTA: Conexión a puerto inusual 52562 desde 57.144.199.32
[2025-12-07 12:50:58] ALERTA: Conexión a puerto inusual 52562 desde 57.144.199.32
[2025-12-07 12:50:58] ALERTA: Conexión a puerto inusual 52562 desde 57.144.199.32
[2025-12-07 12:51:19] ALERTA: Conexión a puerto inusual 52562 desde 57.144.199.32
[2025-12-07 12:51:19] ALERTA: Conexión a puerto inusual 52562 desde 57.144.199.32
[2025-12-07 12:51:34] ALERTA: Conexión a puerto inusual 52562 desde 57.144.199.32
[2025-12-07 12:51:34] ALERTA: Conexión a puerto inusual 52562 desde 57.144.199.32
[2025-12-07 12:51:36] ALERTA: Conexión a puerto inusual 52562 desde 57.144.199.32
[2025-12-07 12:51:36] ALERTA: Conexión a puerto inusual 52562 desde 57.144.199.32
[2025-12-07 12:51:37] ALERTA: Conexión a puerto inusual 39012 desde 34.107.243.93
[2025-12-07 12:51:38] ALERTA: Conexión a puerto inusual 39012 desde 34.107.243.93
^C
```

Archivos generados:

- **log_events.txt**: historial de eventos.
- **blocked_ips.txt**: IPs marcadas como hostiles si encuentra.




~/log_events.txt [Read Only] - Mousepad
File Edit Search View Document Help
1 [2025-12-07 12:49:31] Iniciando sniffer de defensa en interfaz: 192.168.100.196
2 [2025-12-07 12:50:24] Iniciando sniffer de defensa en interfaz: eth0
3 [2025-12-07 12:50:37] ALERTA: Conexión a puerto inusual 52562 desde 57.144.199.32
4 [2025-12-07 12:50:38] ALERTA: Conexión a puerto inusual 52562 desde 57.144.199.32
5 [2025-12-07 12:50:58] ALERTA: Conexión a puerto inusual 52562 desde 57.144.199.32
6 [2025-12-07 12:50:58] ALERTA: Conexión a puerto inusual 52562 desde 57.144.199.32
7 [2025-12-07 12:51:19] ALERTA: Conexión a puerto inusual 52562 desde 57.144.199.32
8 [2025-12-07 12:51:19] ALERTA: Conexión a puerto inusual 52562 desde 57.144.199.32
9 [2025-12-07 12:51:34] ALERTA: Conexión a puerto inusual 52562 desde 57.144.199.32
10 [2025-12-07 12:51:34] ALERTA: Conexión a puerto inusual 52562 desde 57.144.199.32
11 [2025-12-07 12:51:36] ALERTA: Conexión a puerto inusual 52562 desde 57.144.199.32
12 [2025-12-07 12:51:36] ALERTA: Conexión a puerto inusual 52562 desde 57.144.199.32
13 [2025-12-07 12:51:37] ALERTA: Conexión a puerto inusual 39012 desde 34.107.243.93
14 [2025-12-07 12:51:38] ALERTA: Conexión a puerto inusual 39012 desde 34.107.243.93
15