

Prueba de Scripts en blue team

Scanner.py:

Este escáner, verifica el estado de los puertos de la máquina de blue team para poder hacer ataques a puertos vulnerables desde la máquina del red team, cuenta con niveles de escaneo desde uno rápido hasta uno más completo. Para poder ejecutar el scanner.py sería con el comando “python scanner.py -t 192.168.100.184 -s comprehensive”

Por esta captura, mostramos el resultado obtenido por un escaneo completo a la máquina:

En este caso, se escanearon todos los puertos posibles.

Packet attack.py:

En este script de Python, simulamos ataque de sniffing de tráfico hacia una máquina, pero en este caso, solo serían paquetes simulados sin dañar el dispositivo atacado. Para poder ejecutar el packet_attack.py sería con el comando “python .\packet_attack.py -t 192.168.100.184 -p 22”

Por esta captura, mostramos el resultado obtenido por un ataque simulado a la máquina:

```
P5 D:\UNIVERSIDAD\3 CUATRIMESTRE\PROGRA AVANZADA\proyecto_pruebas> python .\packet_attack.py -t 192.168.100.184 -p 22
=====
Red Team - SYN Attack Tool
=====
Target: 192.168.100.184:22
Packets: 3
Mode: ATTACK
Delay: 1.0s
=====

[ATTACK] Iniciando envío de paquetes SYN...
WARNING: MAC address to reach destination not found. Using broadcast.
.
Sent 1 packets.
[SENT] Paquete #1/3 - SYN enviado a 192.168.100.184:22
WARNING: MAC address to reach destination not found. Using broadcast.
.
Sent 1 packets.
[SENT] Paquete #2/3 - SYN enviado a 192.168.100.184:22
WARNING: MAC address to reach destination not found. Using broadcast.
.
Sent 1 packets.
[SENT] Paquete #3/3 - SYN enviado a 192.168.100.184:22
=====

Ataque completado: 3/3 paquetes
Log guardado en: attack_log.txt
=====

P5 D:\UNIVERSIDAD\3 CUATRIMESTRE\PROGRA AVANZADA\proyecto_pruebas>
```

Sniffer_defense.py:

Este script funciona para monitorear paquetes de red en tiempo real desde la VM, e identificar patrones sospechosos de posibles ataques. Para poder ejecutar el sniffer_defense.py sería con el comando “python sniffer_defense.py”

Por esta captura, mostramos el resultado obtenido por un ataque simulado a la máquina:

```
P5 D:\UNIVERSIDAD\3 CUATRIMESTRE\PROGRAMA AVANZADA\proyecto_pruebas> python sniffer_defense.py
=====
Blue Team - Sniffer de Defensa
=====
Log: log_events.txt
Blocklist: blocked_ips.txt
Umbral de bloqueo: 5 intentos
=====
Presiona Ctrl+C para detener

[2025-12-08 13:12:09] Iniciando sniffer de defensa en interfaz: todas
[2025-12-08 13:12:09] ALERTA: Conexión a puerto inusual 43926 desde 185.162.130.32
[2025-12-08 13:12:09] ALERTA: Conexión a puerto inusual 88 desde 192.168.100.6
[2025-12-08 13:12:10] ALERTA: Conexión a puerto inusual 88 desde 192.168.100.6
[2025-12-08 13:12:10] ALERTA: Conexión a puerto inusual 88 desde 192.168.100.6
[2025-12-08 13:12:10] ALERTA: Conexión a puerto inusual 88 desde 192.168.100.6
[2025-12-08 13:12:10] ALERTA: Conexión a puerto inusual 88 desde 192.168.100.6
[2025-12-08 13:12:10] ALERTA: Conexión a puerto inusual 88 desde 192.168.100.6
[2025-12-08 13:12:10] ALERTA: Conexión a puerto inusual 88 desde 192.168.100.6
[2025-12-08 13:12:10] ALERTA: Conexión a puerto inusual 4529 desde 18.209.201.158
[2025-12-08 13:12:10] ALERTA: Conexión a puerto inusual 4529 desde 18.209.201.158
[2025-12-08 13:12:10] ALERTA: Conexión a puerto inusual 43926 desde 185.162.130.32
[2025-12-08 13:12:10] ALERTA: Conexión a puerto inusual 43926 desde 185.162.130.32
[2025-12-08 13:12:10] ALERTA: Conexión a puerto inusual 43926 desde 185.162.130.32
P5 D:\UNIVERSIDAD\3 CUATRIMESTRE\PROGRAMA AVANZADA\proyecto_pruebas>
```

Recomendaciones de mejora relacionados con hardening y control de intentos

- Configurar políticas que detecten un numero inusual de intentos fallidos, con esto mismo registrar los intentos y la dirección ip a la que proviene.
- Revisar los puertos que deben de estar abiertos y cerrar el resto que no sean necesarios, de igual manera deshabilitar servicios que no se necesiten.
- Añadir reglas básicas al sniffer o al sistema de monitoreo para detectar patrones sospechosos, por ejemplo tráfico repetitivo hacia un puerto, paquetes con tamaños poco comunes, aumentos bruscos de tráfico desde una ip específica.