M2-A5: Detección y evasión

Objetivo: comprender cómo ajustar técnicas para evitar detección por IDS/IPS.

1. Ejecuta un escaneo normal con Nmap (establece la IP de tu objetivo):

   ```
   nmap -sS -p1-1000 192.168.1.50
   ```

2. Ejecuta el mismo escaneo, pero con técnicas de evasión:

   ```
   nmap -sS -p1-1000 -T2 -D RND:10 --data-length 200 192.168.1.50
   ```

3. Documenta la diferencia en:
   - Tiempo de ejecución.
   - Cantidad de tráfico generado
   - Facilidad de detección.

Tiempo de ejecución

Usa el comando `time` delante de Nmap:

```
time nmap -sS -p1-1000 192.168.1.50
time nmap -sS -p1-1000 -T2 -D RND:10 --data-length 200 192.168.1.50
```

- El sistema devolverá `real`, `user`, `sys`.
- El valor `real` (tiempo total) es el que comparas.
- Ejemplo: normal = 8s, evasión = 2m15s.

Cantidad de tráfico generado

Tienes varias opciones:

a) Con tcpdump

Captura paquetes mientras corre Nmap:

```
sudo tcpdump -i eth0 host 192.168.1.50 -w escaneo_normal.pcap
sudo tcpdump -i eth0 host 192.168.1.50 -w escaneo_evasion.pcap
```

Después revisa con Wireshark o `tcpdump -r archivo.pcap | wc -l` para contar paquetes.

b) Con iftop / nload (monitor en tiempo real)

Ejecuta antes del escaneo:

```
sudo iftop -i eth0
```

y observa cuántos KB/MB se transmiten durante cada prueba.

c) Con tshark (línea de comandos de Wireshark)

```
tshark -r escaneo_normal.pcap | wc -l
tshark -r escaneo_evasion.pcap | wc -l
```

Esto te da la cantidad total de paquetes.

Facilidad de detección

Esto no lo "mides" directamente, sino que lo analizas:

- El **escaneo normal** genera un patrón claro: muchos SYN consecutivos a puertos ordenados, trivial para un IDS/IPS.
- El **escaneo de evasión** introduce pausas (`-T2`), señuelos (`-D RND:10`) y paquetes alterados (`--data-length`), lo que **dificulta atribuir la IP real** pero **aumenta el ruido en la red**.
- Puedes comprobarlo en los **logs del IDS** (ej. Snort/Suricata) o en los logs del sistema de destino (`/var/log/syslog`, `/var/log/auth.log`) para ver qué se registró.

Ejemplo de comparación (hipotético)

Escaneo	Tiempo (`time`)	Paquetes (`tcpdump`)	Detección
Normal (`-sS`)	10 segundos	~2000 paquetes	Muy fácil
Evasión (`-T2 ...`)	2 minutos 30 s	~25,000 paquetes	Más difícil atribuir, pero más ruido

Entregar:

- Comparación entre los dos escaneos.
- Explicación en 5–6 frases: ¿qué técnicas son útiles en un pentest real y cuáles son demasiado arriesgadas?