ARP Spoofing + Wireshark

Introducción del ataque

El ARP Spoofing (también conocido como envenenamiento ARP) es un tipo de ataque Man-in-the-Middle (MITM) que manipula el protocolo ARP (Address Resolution Protocol) en redes locales. Su objetivo es interceptar el tráfico entre dispositivos, haciendo que las víctimas redirijan su comunicación a través del atacante, permitiéndole así interceptar, modificar o reenviar el tráfico.

Funcionamiento del ataque

- **Descubrimiento ARP:** En una red local, los dispositivos utilizan el protocolo ARP para asociar direcciones IP con direcciones MAC. Este proceso se realiza mediante solicitudes ARP que buscan identificar la dirección MAC correspondiente a una IP específica.
- **Fase de envenenamiento:** El atacante envía respuestas ARP falsificadas que vinculan su propia dirección MAC con la IP de la víctima. Esto engaña a los dispositivos objetivo, haciéndoles creer que la MAC del atacante es la correcta para la IP de destino.
- **Redirección del tráfico:** Una vez envenenadas las tablas ARP, todo el tráfico destinado a la IP objetivo se redirige al atacante en lugar del dispositivo legítimo, permitiéndole manipular la comunicación.

Herramientas usadas

- **Ettercap**: Es una herramienta diseñada para realizar ataques en redes locales, especialmente del tipo ***MITM***. Permite interceptar, analizar y manipular tráfico mediante técnicas como ***ARP Spoofing***. Es compatible con múltiples protocolos, lo que la hace útil para explorar vulnerabilidades y realizar pruebas de penetración en redes.
- **Wireshark**: Es una herramienta de análisis de tráfico de red que se utiliza para capturar y examinar paquetes.

Pasos

Ettercap

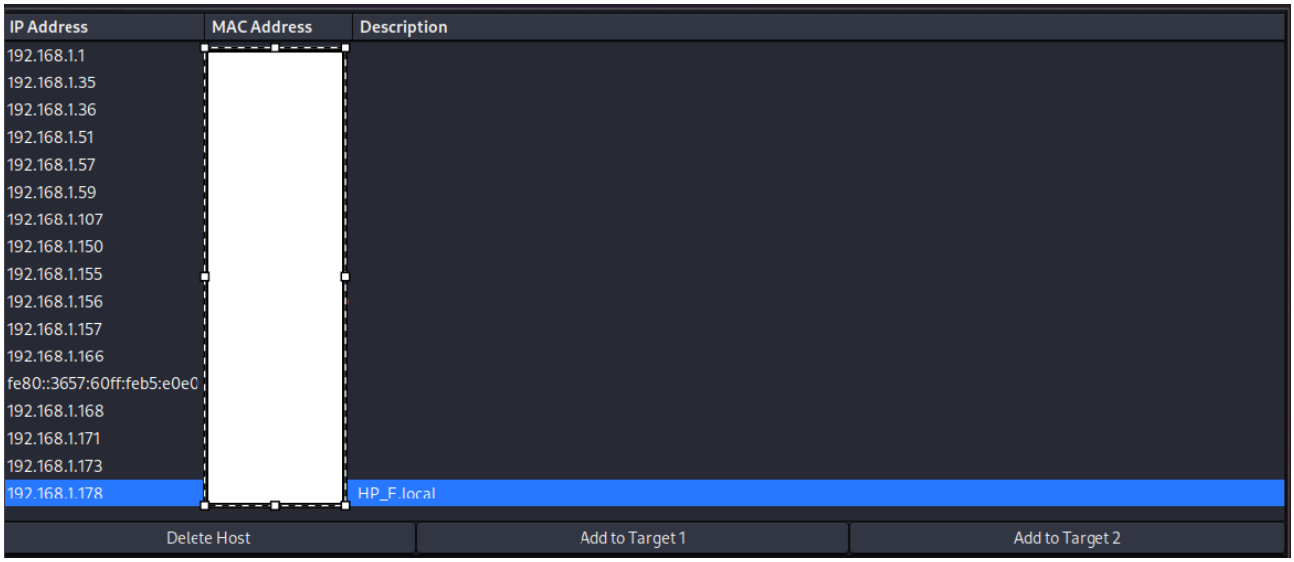
- Abrimos Ettercap, seleccionamos la interfaz de red deseada y pulsamos el botón indicado.

- En la esquina superior izquierda, aparecen los botones:
  - ***Scan for hosts***: Lo pulsamos para escanear la red para identificar las víctimas.
  - ***Hosts list:*** Lo pulsamos para listar los dispositivos encontrados.

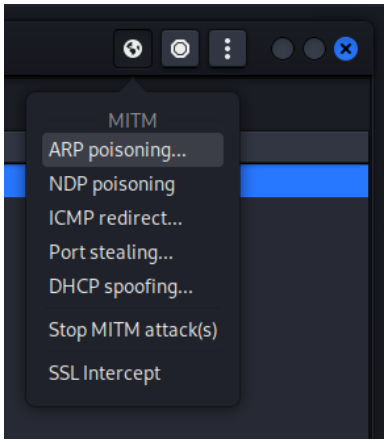
- Con el comando ***route –n***, podemos saber la gateway.

```
└─$ route -n
Kernel IP routing table
Destination     Gateway         Genmask
0.0.0.0         192.168.1.1     0.0.0.0
192.168.1.0     0.0.0.0         255.255.255.0
```

- Añadir Target1 y Target2
  - **Target1**: Especifica la IP del dispositivo víctima.
  - **Target2**: Especifica la IP del gateway o router al que está conectada la víctima. Esto nos permitirá interceptar el tráfico entre la víctima y el router.



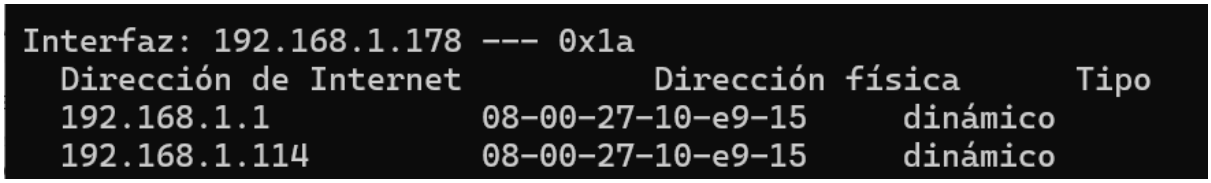
- En la esquina superior derecha, aparece el botón ***MIMT Menu***, y seleccionamos ***ARP poisoning***, que empezará el ataque (marcar la opción de ***Sniff remote connections*** si se desea capturar tráfico HTTPS/HTTP).



- Para comprobar que el ataque ha sido exitoso, podemos verificar la tabla ARP de la máquina afectada ejecutando el comando

arp /a 1

En la salida, observaremos que la IP del router y la del atacante comparten la misma dirección física (MAC). Esto confirma que las tablas ARP han sido envenenadas correctamente.



[1] Muestra la tabla ARP almacena asociaciones actuales entre direcciones IP y direcciones MAC.

Wireshark

Una vez iniciado el ataque, abrimos ***Wireshark*** y seleccionamos la misma interfaz de red activa utilizada en Ettercap.

Empezaremos a capturar tráfico de red, que incluirá paquetes intercambiados entre la víctima, el router y otros dispositivos de la red.

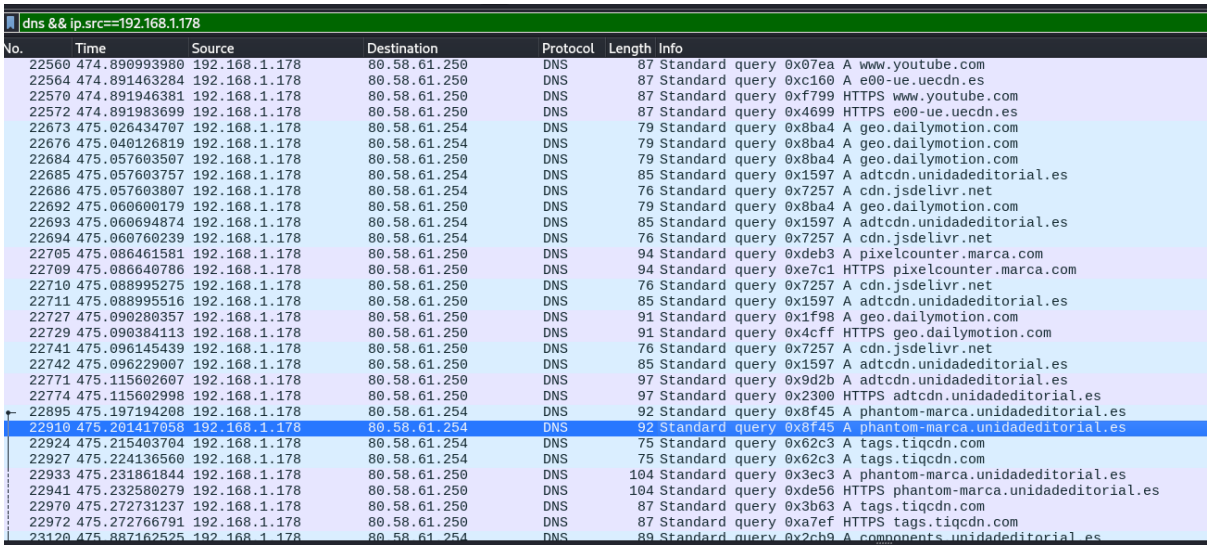
Para filtrar paquetes relevantes, como los que utilizan el ***protocolo DNS*** y provienen de la IP de la víctima, aplicamos el filtro:

dns && ip.src==192.168.1.178

Esto muestra las consultas DNS realizadas por la víctima. Si deseamos incluir también las respuestas del servidor DNS, podemos usar:

dns && (ip.src==192.168.1.178 || ip.dst==192.168.1.178).

Para realizar la prueba, ingresamos en la página marca.es desde la máquina víctima. Esto generara consultas DNS que pueden observarse en Wireshark, incluyendo las direcciones IP asociadas al dominio.



dns && ip.src==192.168.1.178

No.	Time	Source	Destination	Protocol	Length	Info
22560	474.890993980	192.168.1.178	80.58.61.250	DNS	87	Standard query 0x07ea A www.youtube.com
22564	474.891463284	192.168.1.178	80.58.61.250	DNS	87	Standard query 0xc160 A e00-ue.uecdn.es
22570	474.891946381	192.168.1.178	80.58.61.250	DNS	87	Standard query 0xf799 HTTPS www.youtube.com
22572	474.891983699	192.168.1.178	80.58.61.250	DNS	87	Standard query 0x4699 HTTPS e00-ue.uecdn.es
22673	475.026434707	192.168.1.178	80.58.61.254	DNS	79	Standard query 0x8ba4 A geo.dailymotion.com
22676	475.040126819	192.168.1.178	80.58.61.254	DNS	79	Standard query 0x8ba4 A geo.dailymotion.com
22684	475.057603507	192.168.1.178	80.58.61.250	DNS	79	Standard query 0x8ba4 A geo.dailymotion.com
22685	475.057603757	192.168.1.178	80.58.61.254	DNS	85	Standard query 0x1597 A adtcdn.unidadeditorial.es
22686	475.057603807	192.168.1.178	80.58.61.254	DNS	76	Standard query 0x7257 A cdn.jsdelivr.net
22692	475.060600179	192.168.1.178	80.58.61.250	DNS	79	Standard query 0x8ba4 A geo.dailymotion.com
22693	475.060694874	192.168.1.178	80.58.61.254	DNS	85	Standard query 0x1597 A adtcdn.unidadeditorial.es
22694	475.060760239	192.168.1.178	80.58.61.254	DNS	76	Standard query 0x7257 A cdn.jsdelivr.net
22705	475.086461581	192.168.1.178	80.58.61.250	DNS	94	Standard query 0xdeb3 A pixelcounter.marca.com
22709	475.086640786	192.168.1.178	80.58.61.250	DNS	94	Standard query 0xe7c1 HTTPS pixelcounter.marca.com
22710	475.088995275	192.168.1.178	80.58.61.250	DNS	76	Standard query 0x7257 A cdn.jsdelivr.net
22711	475.088995516	192.168.1.178	80.58.61.250	DNS	85	Standard query 0x1597 A adtcdn.unidadeditorial.es
22727	475.090280357	192.168.1.178	80.58.61.250	DNS	91	Standard query 0x1f98 A geo.dailymotion.com
22729	475.090384113	192.168.1.178	80.58.61.250	DNS	91	Standard query 0x4cff HTTPS geo.dailymotion.com
22741	475.096145439	192.168.1.178	80.58.61.250	DNS	76	Standard query 0x7257 A cdn.jsdelivr.net
22742	475.096229007	192.168.1.178	80.58.61.250	DNS	85	Standard query 0x1597 A adtcdn.unidadeditorial.es
22771	475.115602607	192.168.1.178	80.58.61.250	DNS	97	Standard query 0x9d2b A adtcdn.unidadeditorial.es
22774	475.115602998	192.168.1.178	80.58.61.250	DNS	97	Standard query 0x2300 HTTPS adtcdn.unidadeditorial.es
22895	475.197194208	192.168.1.178	80.58.61.254	DNS	92	Standard query 0x8f45 A phantom-marca.unidadeditorial.es
22910	475.201417058	192.168.1.178	80.58.61.254	DNS	92	Standard query 0x8f45 A phantom-marca.unidadeditorial.es
22924	475.215403704	192.168.1.178	80.58.61.254	DNS	75	Standard query 0x62c3 A tags.tiqcdn.com
22927	475.224136560	192.168.1.178	80.58.61.254	DNS	75	Standard query 0x62c3 A tags.tiqcdn.com
22933	475.231861844	192.168.1.178	80.58.61.250	DNS	104	Standard query 0x3ec3 A phantom-marca.unidadeditorial.es
22941	475.232580279	192.168.1.178	80.58.61.250	DNS	104	Standard query 0xde56 HTTPS phantom-marca.unidadeditorial.es
22970	475.272731237	192.168.1.178	80.58.61.250	DNS	87	Standard query 0x3b63 A tags.tiqcdn.com
22972	475.272766791	192.168.1.178	80.58.61.250	DNS	87	Standard query 0xa7ef HTTPS tags.tiqcdn.com
23120	475.887162525	192.168.1.178	80.58.61.254	DNS	89	Standard query 0x2cb9 A components.unidadeditorial.es

¿Por qué funciona el ataque?

- **Funcionamiento Básico de ARP:**
    1. **Solicitud ARP (ARP Request):**
        - Cuando un dispositivo en una red local necesita comunicarse con otro dispositivo, utiliza su dirección IP para identificar al destino. Si el dispositivo no sabe la dirección MAC de la máquina destino, envía una solicitud ARP.
        - Esta solicitud es una transmisión a todos los dispositivos de la red (broadcast). En ella, el dispositivo pide "¿Quién tiene la IP [dirección IP de destino]?".
    2. **Respuesta ARP (ARP Reply):**
        - El dispositivo que tiene la IP solicitada responde con su dirección MAC. La respuesta ARP va dirigida exclusivamente al dispositivo que hizo la solicitud.
        - Una vez que el dispositivo receptor recibe la respuesta, actualiza su tabla ARP (una tabla de asociación entre direcciones IP y direcciones MAC).
    3. **Tabla ARP:**
        - Los dispositivos mantienen una tabla ARP local, que es una lista de asociaciones entre direcciones IP y direcciones MAC.
        - Esta tabla se actualiza con cada respuesta ARP recibida y se utiliza para enviar datos de un dispositivo a otro en la red local.

- **Fase de Envenenamiento ARP:**
    1. **Modificación de las respuestas ARP:**
        - El atacante envía respuestas ARP falsas (spoofed) a los dispositivos de la red. Estas respuestas afirman que la dirección MAC del atacante está asociada con la IP de un dispositivo legítimo (por ejemplo, el router o una víctima específica).
        - Por ejemplo, el atacante podría enviar un mensaje diciendo: "La dirección MAC 00:11:22:33:44:55 es la dirección del router, con la IP 192.168.1.1", cuando en realidad esa dirección MAC pertenece al atacante.
    2. **Actualización de las tablas ARP de las víctimas:**
        - Cuando los dispositivos de la red reciben estas respuestas ARP falsificadas, actualizan sus tablas ARP, creyendo que la dirección MAC del atacante es la dirección legítima del router o de la víctima.
        - Esto provoca que el tráfico destinado al router o a otro dispositivo se envíe en lugar al atacante.
    3. **Redirección del Tráfico:**
        - Ahora, todo el tráfico que debería ir al dispositivo legítimo (como el router) será enviado al atacante.
        - El atacante puede leer, modificar o redirigir ese tráfico, lo que le da la capacidad de llevar a cabo una amplia gama de ataques, incluyendo **interceptación de datos** (como contraseñas y correos electrónicos) y **alteración de los datos** (inyectar malware o modificar mensajes).