

CAPTURA DE CREDENCIALES CON *W*IRESHARK

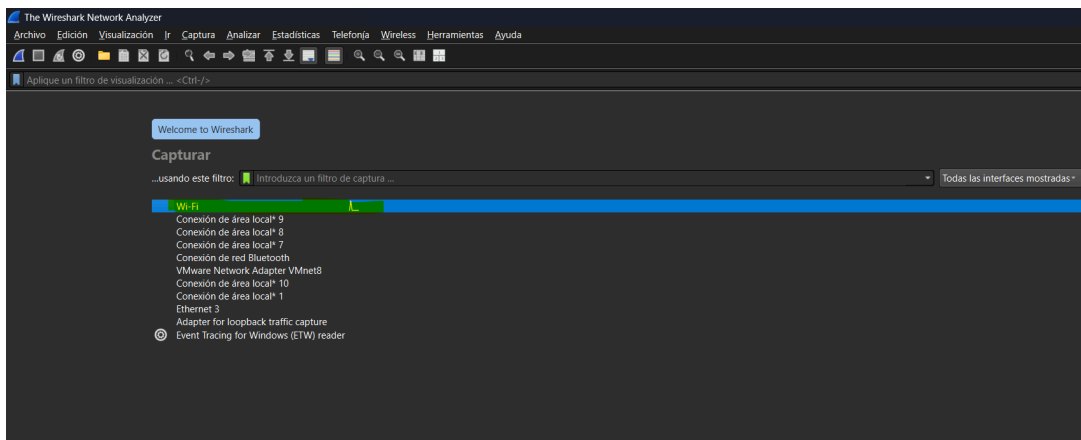
SANTIAGO PEÑARANDA MEJIA

BUENO LO PRIMERO QUE VAMOS HACER ES ABRIR LA HERRAMIENTA **WIRESHARK**, POR SI NO SABES QUE ES **WIRESHARK** ESTA ES UNA HERRAMIENTA QUE SIRVE PARA ESNIFAR O CAPTURAR PAQUETES QUE VIAJAN POR LA RED, EN CUESTIÓN VER EL TRÁFICO DE LA RED.

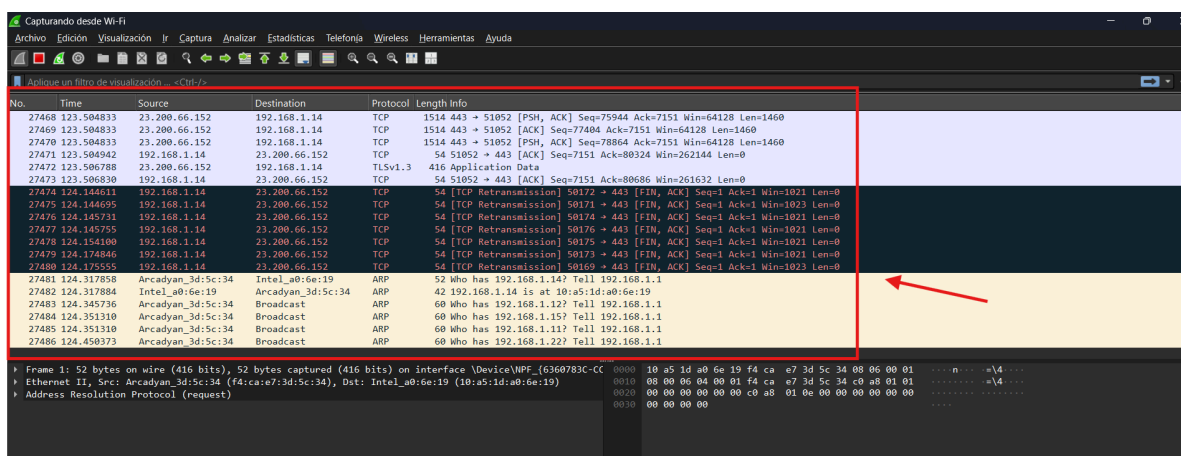
ESTA HERRAMIENTA ES MUY ÚTIL PARA NOSOTROS COMO **PENTESTERS** PORQUE NOS VA A PERMITIR ANALIZAR DATOS Y PROTOCOLOS QUE NOS VIENE MUY ÚTIL PARA LO QUE ESTEMOS HACIENDO SI SE TRATA DEL ÁMBITO DE LA RED, Y ADEMÁS ES UNA HERRAMIENTA MUY COMPLETA.



Una vez ya tengamos abierta la herramienta, es hora de seleccionar la interfaz de red que vamos a usar para hacer el esnifado, en mi caso voy a usar la “**Wifi**”




Al darle click a nuestra interfaz de red seleccionada, el programa automáticamente iniciará con el sniffado de aquella red, capturando así todo los paquetes que viajan por ella.



Mientras por detrás eh prendido la máquina Metasploitable2, que tiene algunos cuantos servicios web para hacer un login a ellos, y así nosotros con Wireshark poder ver las credenciales que pasan por la red



Y como ya tenemos el sniffer activo vamos a escribir las credenciales de este login a ver que pasa.



Username

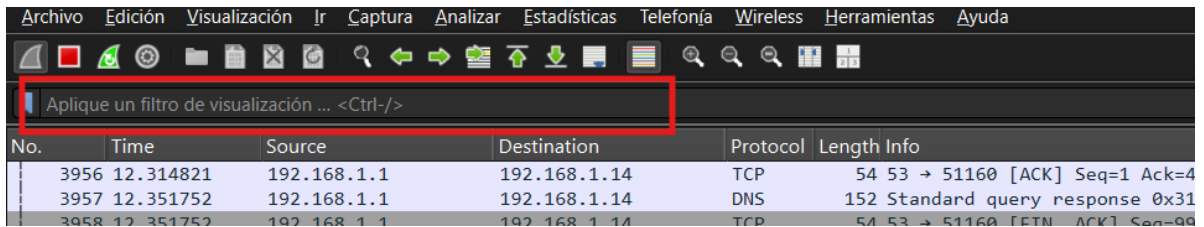
Password

Login

Login failed

Ahora lo que podemos hacer es aplicar una serie de filtros, estos filtros nos sirven para poder buscar y analizar detalladamente la información que necesitamos

Bueno ahora si, una vez ya hecho el escaneo de la red para poder filtrar la información lo que hacemos es darle a el buscador de aqui que dice “***Aplique un filtro de visualización***”



Y ahora la solo queda ir buscando y poner ciertos filtros dependiendo la información y lo que queramos buscas, como por ejemplo:

Este filtro nos sirve para mostrar solo el tráfico TCP que utiliza el puerto 80



Usar este filtro permite ver solicitudes y respuestas HTTP, como:

- Solicitudes GET, POST, PUT, DELETE.
- Respuestas HTTP con códigos de estado (200 OK, 404 Not Found, etc.).

No.	Time	Source	Destination	Protocol	Length	Info
3955	12.281321	192.168.1.14	44.228.249.3	TCP	66	51161 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
3960	12.451032	44.228.249.3	192.168.1.14	TCP	66	80 → 51161 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=1460 SACK_PERM WS=128
3961	12.451203	192.168.1.14	44.228.249.3	TCP	54	51161 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
3962	12.451762	192.168.1.14	44.228.249.3	HTTP	526	GET /userinfo.php HTTP/1.1
3963	12.621211	44.228.249.3	192.168.1.14	TCP	54	80 → 51161 [ACK] Seq=1 Ack=473 Win=62336 Len=0
3964	12.623178	44.228.249.3	192.168.1.14	HTTP	330	HTTP/1.1 302 Found (text/html)
3965	12.627683	192.168.1.14	44.228.249.3	HTTP	523	GET /login.php HTTP/1.1
3966	12.797190	44.228.249.3	192.168.1.14	TCP	56	80 → 51161 [ACK] Seq=277 Ack=942 Win=61952 Len=0
3967	12.797190	44.228.249.3	192.168.1.14	TCP	1514	80 → 51161 [ACK] Seq=277 Ack=942 Win=61952 Len=1460 [TCP PDU reassembled in 3966]
3968	12.797190	44.228.249.3	192.168.1.14	HTTP	1342	HTTP/1.1 200 OK (text/html)
3969	12.797278	192.168.1.14	44.228.249.3	TCP	54	51161 → 80 [ACK] Seq=942 Ack=3025 Win=65280 Len=0
3970	12.812842	192.168.1.14	44.228.249.3	HTTP	397	GET /style.css HTTP/1.1
3971	12.813192	192.168.1.14	44.228.249.3	TCP	66	51162 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
3974	12.975333	44.228.249.3	192.168.1.14	TCP	66	80 → 51162 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=1460 SACK_PERM WS=128
3975	12.975430	192.168.1.14	44.228.249.3	TCP	54	51162 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
3976	12.975955	192.168.1.14	44.228.249.3	HTTP	449	GET /images/logo.gif HTTP/1.1
3977	12.983373	44.228.249.3	192.168.1.14	TCP	56	80 → 51161 [ACK] Seq=3025 Ack=1285 Win=61696 Len=0
3978	12.983373	44.228.249.3	192.168.1.14	TCP	293	80 → 51161 [PSH, ACK] Seq=3025 Ack=1285 Win=61696 Len=239 [TCP PDU reassembled in 3982]
3979	12.983373	44.228.249.3	192.168.1.14	TCP	1514	80 → 51161 [ACK] Seq=3264 Ack=1285 Win=61696 Len=1460 [TCP PDU reassembled in 3982]
3980	12.983373	44.228.249.3	192.168.1.14	TCP	1514	80 → 51161 [PSH, ACK] Seq=4724 Ack=1285 Win=61696 Len=1460 [TCP PDU reassembled in 3982]

Como vemos en la imagen anterior hemos encontrado un **login** que probablemente sea un login con sus credenciales

Info
766 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

Y aquí como podemos ver encontramos las credenciales de la víctima las cuales son **"test"**

```

HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "uname" = "test"
  Form item: "pass" = "test"

```

Y así es como capturamos las credenciales de un login con Wireshark

"NOTA: Profe al final lo iba hacer con el servicio de web de metasploitable2 pero como no me funciona no se porque, pues entonces lo cambie y la hice con este servicio web vulnerable que encontré en internet"

<http://testphp.vulnweb.com/userinfo.php>