



# **Curso de Hacking Ético Escuela de Video Juegos MasterD**

## **Ejercicio 15 - Captura de credenciales con Wireshark**

**Alumno:** Julián Gordon

# Índice

Introducción .....	3
Intercepción de Tráfico FTP .....	4
Conexión desde la máquina de Windows 10 .....	7
Captura y análisis del tráfico .....	9
Conclusiones .....	12

# Introducción

En el ejercicio previo, iniciamos el análisis de red con Wireshark, explorando diversas técnicas y filtros para comprender su funcionalidad y utilidad. Ahora, nuestra tarea se centra en localizar y examinar las capturas resultantes de Wireshark, con el objetivo de identificar los aspectos más relevantes(en este caso credenciales) que nos puedan ayudar a explotar posibles vulnerabilidades o intrusiones en la red.

En este trabajo usaremos nuestra máquina de Kali Linux para captar el tráfico entre la máquina de Windows 10 y la máquina de Metasploitable2. Para ello usaremos FTP (File Transfer Protocol), para conectarnos con Filezilla desde Windows 10 a Metasploitable2 y, con Kali Linux, capturar los paquetes que contengan credenciales.

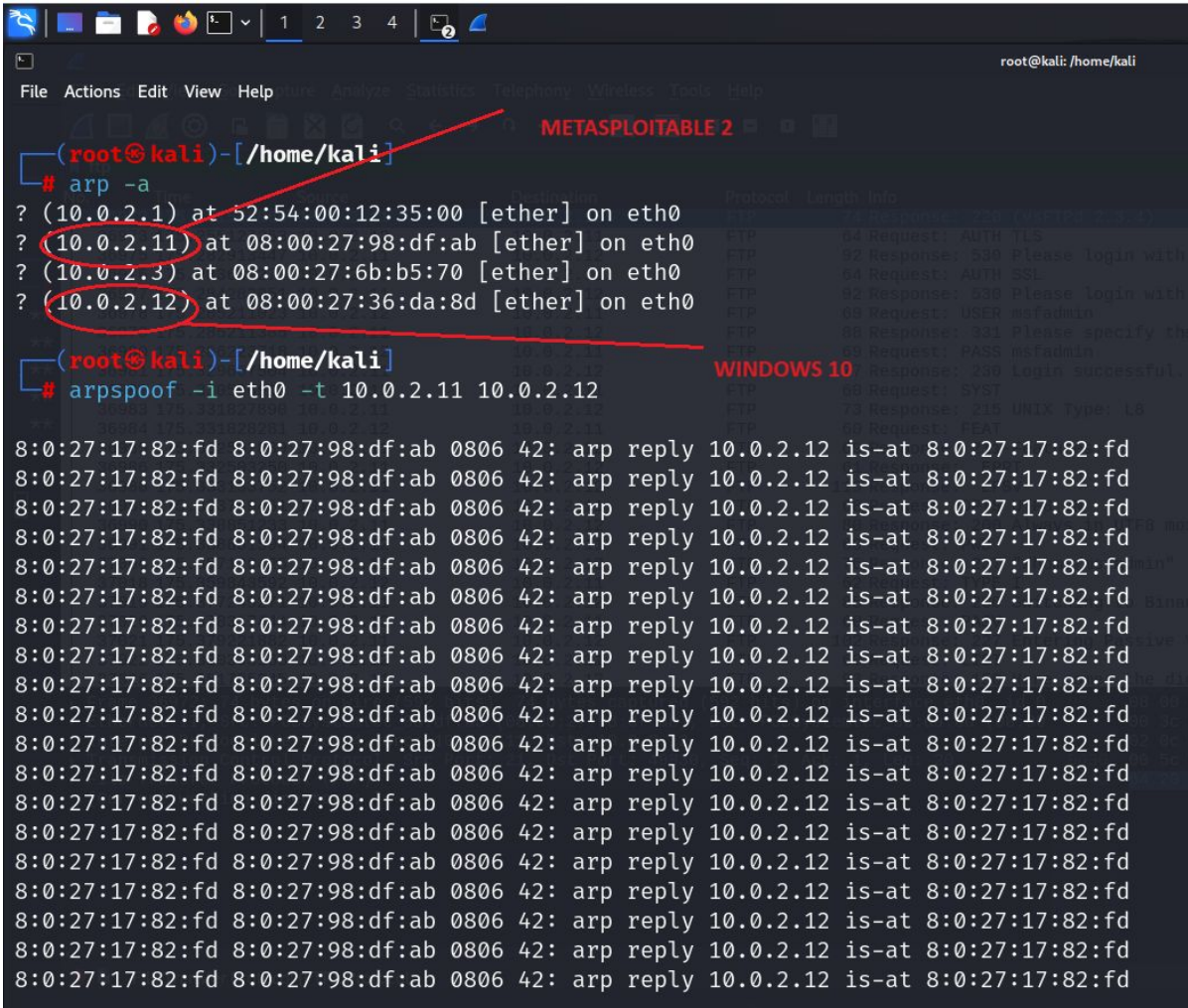
# Intercepción de Tráfico FTP

Para realizar este ejercicio, primero necesitamos identificar las direcciones IP de las máquinas involucradas. Utilizamos el comando 'arp -a', en Kali Linux, para listar las direcciones IP y las direcciones MAC de los dispositivos en nuestra red(haciendo un ping previamente).

El segundo paso será realizar el envenenamiento ARP utilizando la herramienta 'arpspoof' en Kali Linux. Esto nos permite redirigir el tráfico entre la máquina Windows y Metasploitable 2 a través de nuestro sistema Kali Linux.

Para que nuestro sistema Kali Linux pueda actuar como intermediario entre las dos máquinas, habilitamos el reenvío de paquetes IP ejecutando el comando **'echo 1 > /proc/sys/net/ipv4/ip\_forward'** .

A continuación podemos ver imágenes de este primer proceso.



```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# echo 1 > /proc/sys/net/ipv4/ip_forward

? (10.0.2.1) at 52:54:00:12:35:00 [ether] on eth0
? (10.0.2.10) at 08:00:27:08:4b:ab [ether] on eth0
(root@kali)-[/home/kali]
# wireshark
** (wireshark:10678) 23:03:21.666928 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
** (wireshark:10678) 23:03:42.982549 [Capture MESSAGE] -- Capture Start ...
** (wireshark:10678) 23:03:43.115678 [Capture MESSAGE] -- Capture started
** (wireshark:10678) 23:03:43.115734 [Capture MESSAGE] -- File: "/tmp/wireshark_eth01CM6K2.pcapng"
** (wireshark:10678) 23:09:01.052625 [Capture MESSAGE] -- Capture Stop ...
** (wireshark:10678) 23:09:01.107200 [Capture MESSAGE] -- Capture stopped.
** (wireshark:10678) 23:09:01.107249 [Capture WARNING] ./ui/capture.c:722 -- capture_input_closed():
```

Abrimos Wireshark en Kali Linux y seleccionamos la interfaz de red que estamos utilizando para la conexión a Internet o la red local. Esto nos permitirá monitorear y capturar todo el tráfico de red entre las dos máquinas. Con la interfaz de red seleccionada, iniciamos la captura de paquetes en Wireshark para registrar todo el tráfico de red que pasa a través de nuestra máquina. En la imagen anterior podemos observar el proceso.

# Conexión desde la máquina de Windows 10

Desde la máquina Windows, abriremos el cliente FTP FileZilla y nos conectamos al servicio FTP en Metasploitable2. Asignamos el numero de IP de Metasploitable2 (10.0.2.11), luego proporcionamos las credenciales de inicio de sesión y seleccionamos el puerto 21.

A continuación veremos una imagen desde Windows 10, haciendo la conexión ftp a la máquina de Metasploitable2.



Mozilla Firefox payload\_mst\_v...



# Captura y Análisis del Tráfico

Mientras se realiza la conexión FTP desde la máquina Windows a Metasploitable 2, Wireshark captura todo el tráfico de red. Examinamos los paquetes capturados en busca de las credenciales FTP enviadas desde la máquina Windows. Durante el análisis, identificamos con éxito las credenciales de inicio de sesión utilizadas durante la conexión FTP. Podemos verlo en la siguiente imagen.

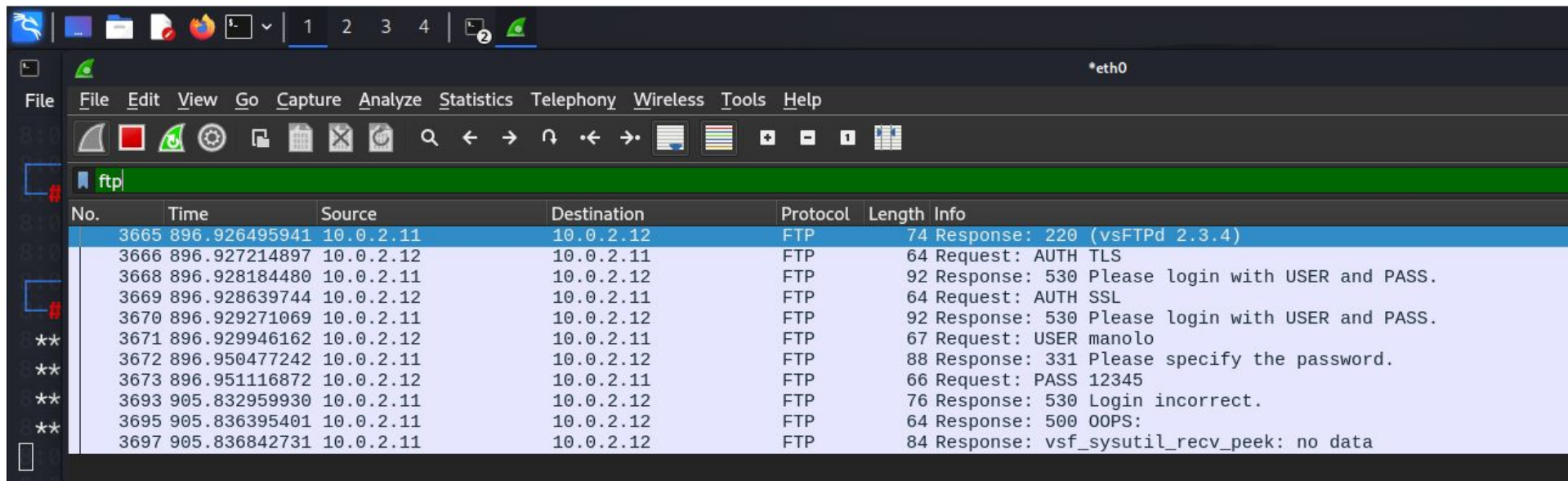
Wireshark interface showing a packet capture on interface eth0. The selected packet is 36978, which is an FTP request for the user 'msfadmin'. The packet details pane shows the structure of the FTP request, including the USER command and the password field.

No.	Time	Source	Destination	Protocol	Length	Info
36972	175.251546068	10.0.2.11	10.0.2.12	FTP	74	Response: 220 (vsFTPD 2.3.4)
36973	175.255127263	10.0.2.12	10.0.2.11	FTP	64	Request: AUTH TLS
36975	175.282913447	10.0.2.11	10.0.2.12	FTP	92	Response: 530 Please login with USER and PASS.
36976	175.283682279	10.0.2.12	10.0.2.11	FTP	64	Request: AUTH SSL
36977	175.284283051	10.0.2.11	10.0.2.12	FTP	92	Response: 530 Please login with USER and PASS.
36978	175.285211023	10.0.2.12	10.0.2.11	FTP	69	Request: USER msfadmin
36979	175.285211385	10.0.2.11	10.0.2.12	FTP	88	Response: 331 Please specify the password.
36980	175.286223718	10.0.2.12	10.0.2.11	FTP	69	Request: PASS msfadmin
36981	175.329667504	10.0.2.11	10.0.2.12	FTP	77	Response: 230 Login successful.
36982	175.330596915	10.0.2.12	10.0.2.11	FTP	60	Request: SYST
36983	175.331827890	10.0.2.11	10.0.2.12	FTP	73	Response: 215 UNIX Type: L8
36984	175.331828281	10.0.2.12	10.0.2.11	FTP	60	Request: FEAT
36985	175.332502889	10.0.2.11	10.0.2.12	FTP	69	Response: 211-Features:
36986	175.332503250	10.0.2.11	10.0.2.12	FTP	61	Response: EPRT
36988	175.333133752	10.0.2.11	10.0.2.12	FTP	119	Response: EPSV
36989	175.333749461	10.0.2.12	10.0.2.11	FTP	68	Request: OPTS UTF8 ON
36990	175.338851233	10.0.2.11	10.0.2.12	FTP	80	Response: 200 Always in UTF8 mode.
36991	175.338851594	10.0.2.12	10.0.2.11	FTP	60	Request: PWD
37006	175.357129425	10.0.2.11	10.0.2.12	FTP	76	Response: 257 "/home/msfadmin"
37018	175.359843592	10.0.2.12	10.0.2.11	FTP	62	Request: TYPE I
37019	175.377249271	10.0.2.11	10.0.2.12	FTP	85	Response: 200 Switching to Binary mode.
37020	175.378317444	10.0.2.12	10.0.2.11	FTP	60	Request: PASV
37021	175.379221882	10.0.2.11	10.0.2.12	FTP	102	Response: 227 Entering Passive Mode (10,0,2,11,153,193).
37022	175.380353560	10.0.2.12	10.0.2.11	FTP	60	Request: LIST
37026	175.381785245	10.0.2.11	10.0.2.12	FTP	93	Response: 150 Here comes the directory listing.

Frame 36972: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0  
Ethernet II, Src: PCSSystemtec\_98:df:ab (08:00:27:98:df:ab), Dst: PCSSystemtec\_36:da:8d (08:00:02:36:da:8d)  
Internet Protocol Version 4, Src: 10.0.2.11, Dst: 10.0.2.12  
Transmission Control Protocol, Src Port: 21, Dst Port: 49830, Seq: 1, Ack: 1, Len: 20  
File Transfer Protocol (FTP)  
[Current working directory: ]

0000 08 00 27 36 da 8d 08 00 27 98 df ab 08 00 45 00 ..'6... '.....E.  
0010 00 3c 08 c8 40 00 40 06 19 de 0a 00 02 0b 0a 00 <..@.@... ..  
0020 02 0c 00 15 c2 a6 38 c7 27 47 c6 49 47 42 50 18 .....8: 'G.IGBP.  
0030 00 5c 09 e1 00 00 32 32 30 20 28 76 73 46 54 50 \.....22 0 (vsFTP  
0040 64 20 32 2e 33 2e 34 29 0d 0a d 2.3.4) ..

Aquí en la siguiente imagen podemos observar el mismo proceso capturado pero con credenciales incorrectas.



The image shows a Wireshark network traffic capture of an FTP session. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar with various icons, and a packet list pane on the left. The main packet details pane shows the selected packet (No. 3665) with its fields: Time (896.926495941), Source (10.0.2.11), Destination (10.0.2.12), Protocol (FTP), Length (74), and Info (Response: 220 (vsFTpd 2.3.4)). The packet list pane displays a list of packets, with the selected packet highlighted in blue. The list includes packets for the FTP session, showing the client's requests and the server's responses, including the final 'no data' response.

No.	Time	Source	Destination	Protocol	Length	Info
3665	896.926495941	10.0.2.11	10.0.2.12	FTP	74	Response: 220 (vsFTpd 2.3.4)
3666	896.927214897	10.0.2.12	10.0.2.11	FTP	64	Request: AUTH TLS
3668	896.928184480	10.0.2.11	10.0.2.12	FTP	92	Response: 530 Please login with USER and PASS.
3669	896.928639744	10.0.2.12	10.0.2.11	FTP	64	Request: AUTH SSL
3670	896.929271069	10.0.2.11	10.0.2.12	FTP	92	Response: 530 Please login with USER and PASS.
3671	896.929946162	10.0.2.12	10.0.2.11	FTP	67	Request: USER manolo
3672	896.950477242	10.0.2.11	10.0.2.12	FTP	88	Response: 331 Please specify the password.
3673	896.951116872	10.0.2.12	10.0.2.11	FTP	66	Request: PASS 12345
3693	905.832959930	10.0.2.11	10.0.2.12	FTP	76	Response: 530 Login incorrect.
3695	905.836395401	10.0.2.11	10.0.2.12	FTP	64	Response: 500 OOPS:
3697	905.836842731	10.0.2.11	10.0.2.12	FTP	84	Response: vsf_sysutil_recv_peek: no data

# Conclusiones

En este ejercicio de interceptación de tráfico FTP, llevamos a cabo una serie de pasos para capturar las credenciales de inicio de sesión utilizadas durante la conexión FTP entre nuestra máquina Windows 10 y Metasploitable2. Empezamos utilizando herramientas de línea de comandos, en Kali Linux, para identificar las direcciones IP de las máquinas involucradas en nuestra red, lo que nos permitió establecer comunicación entre ellas.

Luego mediante el uso de la herramienta 'arp spoof', realizamos un ataque de envenenamiento ARP para redirigir el tráfico entre la máquina Windows y Metasploitable2 a través de nuestro sistema Kali Linux. Utilizamos Wireshark para capturar y analizar todo el tráfico de red, entre las dos máquinas durante la conexión FTP. Esto nos permitió examinar los paquetes capturados en busca de las credenciales, de inicio de sesión, enviadas desde la máquina Windows.

Durante el análisis de los paquetes capturados en Wireshark, identificamos con éxito las credenciales de inicio de sesión utilizadas durante la conexión FTP. Estas credenciales nos proporcionaron acceso al sistema remoto y demostraron la vulnerabilidad del protocolo FTP cuando se transmite en texto plano.

Es importante destacar que el protocolo FTP sigue siendo ampliamente utilizado en muchos entornos de red hoy en día. Sin embargo, una de las principales debilidades del FTP es que transmite las credenciales de inicio de sesión, así como los datos transferidos, en texto plano, lo que las hace susceptibles a la captura por parte de atacantes en la red.