



# Curso de Hacking ético Master. D

Ejercicio 14

ENVENENAR Y/O  
SUPLANTAR SERVICIOS

Alumno: Julián Gordon

# Índice

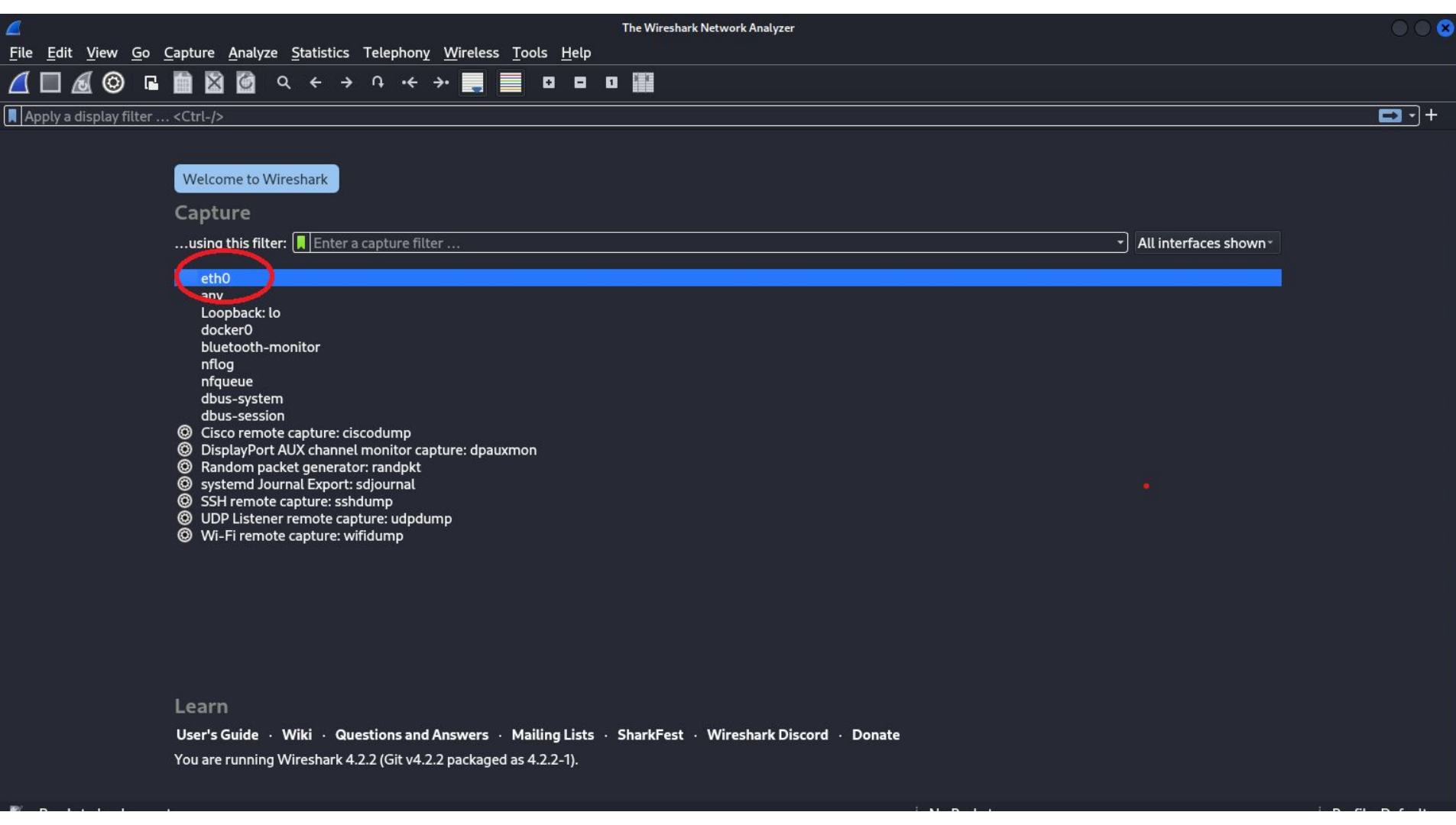
Introducción .....	3
Iniciar esnifado de red con WireShark .....	4
Uso de filtros con WireShark .....	7
Filtro por protocolo .....	8
Filtro por dirección MAC.....	9
Filtro por puerto .....	10
Filtro por dirección IP.....	11
Filtro por dirección y dirección MAC combinado .....	12
Conclusiones .....	113

# Introducción

En este ejercicio, trabajaremos con WireShark. Es una herramienta de análisis de protocolos de red, que nos permite capturar y analizar el tráfico de red en tiempo real. Funciona capturando los paquetes de datos que pasan a través de una red, y luego nos muestra estos datos en un formato comprensible. Podemos filtrar y examinar los paquetes según diversos criterios, como dirección IP, protocolo, tipo de paquete, etc. Esto nos permite diagnosticar problemas de red, detectar actividades sospechosas, y comprender cómo funcionan los diferentes protocolos de red.

# Iniciar esnifado de red con WireShark

Para iniciar Wireshark, lo primero que debemos hacer es elegir la red que vamos a querer capturar el tráfico, en este caso usaremos la eth0. Para empezar a generar tráfico y que lo pueda captar Wireshark, haremos un 'whois google.com' . Podemos observar en las siguientes imágenes este proceso, y como se muestra en la interfaz de Wireshark el envío y recepción de los distintos paquetes.



```

Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface e
Ethernet II, Src: PCSSystemtec_17:82:fd (08:00:27:17:82:fd), Dst: 52:54:00:12:35:
0000 52 54 00 12 35 00 08 00 27 17 82 fd 08 00 45 00 RT-5...E.
0010 00 44 d4 e0 40 00 40 11 b8 ba 0a 00 02 0f 0a fe .D.@.

```

# Uso de filtros con WireShark

Para poder mostrar el uso de los filtros de WireShark, en este ejercicio, generamos distintos tipos de tráfico en nuestra red. Empezamos haciendo un ping desde nuestra máquina de Kali Linux, sobre nuestro objetivo, que será la máquina de Metasploitable2. El comando ping, utiliza el Protocolo de Control de Mensajes de Internet (ICMP) para enviar paquetes de solicitud y recibir respuestas de un dispositivo. Para filtrar este proceso, usaremos el filtro por protocolo 'ICMP'. Luego usamos otro filtro, que será por dirección MAC, para ello se necesita este comando 'eth.addr == {MAC de nuestro objetivo}'. Para saber la MAC de nuestro objetivo, podemos usar el comando 'arp -a' y nos dirá la MAC asociada a la IP. Ahora filtraremos por puerto destino(en este caso telnet que es el 23) con el comando 'tcp.port == 23', para generar este tráfico, solamente con usar el comando 'telnet + ip' con la contraseña que ya obtuvimos en ejercicios anteriores. También podemos filtrar por dirección IP de origen o de destino, con los comandos 'ip.src == x.x.x.x' y 'ip.dst == x.x.x.x'. Además también podemos combinar dichos filtros con 'or' ó 'and' ó negarlo con 'not'.

A continuación se muestran las imágenes de todos los procesos.

# Filtro por protocolo

Wireshark interface showing a packet capture on interface \*eth0. The filter bar is set to 'icmp'. The packet list shows several ICMP Echo (ping) requests and replies between 10.0.2.15 and 10.0.2.11.

No.	Time	Source	Destination	Protocol	Length	Info
13	91.414170027	10.0.2.15	10.0.2.11	ICMP	98	Echo (ping) request id=0x4d75, seq=1/256, ttl=64 (reply in 14)
14	91.414596539	10.0.2.11	10.0.2.15	ICMP	98	Echo (ping) reply id=0x4d75, seq=1/256, ttl=64 (request in 13)
15	92.400575956	10.0.2.15	10.0.2.11	ICMP	98	Echo (ping) request id=0x4d75, seq=2/512, ttl=64 (reply in 16)
16	92.401028344	10.0.2.11	10.0.2.15	ICMP	98	Echo (ping) reply id=0x4d75, seq=2/512, ttl=64 (request in 15)
17	93.414711699	10.0.2.15	10.0.2.11	ICMP	98	Echo (ping) request id=0x4d75, seq=3/768, ttl=64 (reply in 18)
18	93.415171474	10.0.2.11	10.0.2.15	ICMP	98	Echo (ping) reply id=0x4d75, seq=3/768, ttl=64 (request in 17)
19	94.445298607	10.0.2.15	10.0.2.11	ICMP	98	Echo (ping) request id=0x4d75, seq=4/1024, ttl=64 (reply in 20)
20	94.451641217	10.0.2.11	10.0.2.15	ICMP	98	Echo (ping) reply id=0x4d75, seq=4/1024, ttl=64 (request in 19)

Frame 13: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface e  
Ethernet II, Src: PCSSystemtec\_17:82:fd (08:00:27:17:82:fd), Dst: PCSSystemtec\_98:  
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.11  
Internet Control Message Protocol

Hex dump and ASCII representation of the packet data:

```
0000  08 00 27 98 df ab 08 00 27 17 82 fd 08 00 45 00  :.....E.  
0010  00 54 3c 6f 40 00 40 01 e6 20 0a 00 02 0f 0a 00  :T<o@.@..  
0020  02 0b 08 00 7c b5 4d 75 00 01 0b 44 cb 65 00 00  :...|Mu...D.e..  
0030  00 00 97 57 01 00 00 00 00 00 10 11 12 13 14 15  :..W.....!"#$$%  
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  :.....&'()*+,-./012345  
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  :  
0060  36 37 67
```



# Filtro por dirección MAC

\*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.addr == 08:00:27:98:df:ab

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PCSSystemtec_98:df:...	Broadcast	ARP	60	who has 10.0.2.3? Tell 10.0.2.11
6	32.030790521	10.0.2.11	10.0.2.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, ...
12	91.414160303	PCSSystemtec_98:df:...	PCSSystemtec_17:82:...	ARP	60	10.0.2.11 is at 08:00:27:98:df:ab
13	91.414170027	10.0.2.15	10.0.2.11	ICMP	98	Echo (ping) request id=0x4d75, seq=1/256, ttl=64 (reply in 14)
14	91.414596539	10.0.2.11	10.0.2.15	ICMP	98	Echo (ping) reply id=0x4d75, seq=1/256, ttl=64 (request in 13)
15	92.400575956	10.0.2.15	10.0.2.11	ICMP	98	Echo (ping) request id=0x4d75, seq=2/512, ttl=64 (reply in 16)
16	92.401028344	10.0.2.11	10.0.2.15	ICMP	98	Echo (ping) reply id=0x4d75, seq=2/512, ttl=64 (request in 15)
17	93.414711699	10.0.2.15	10.0.2.11	ICMP	98	Echo (ping) request id=0x4d75, seq=3/768, ttl=64 (reply in 18)
18	93.415171474	10.0.2.11	10.0.2.15	ICMP	98	Echo (ping) reply id=0x4d75, seq=3/768, ttl=64 (request in 17)
19	94.445298607	10.0.2.15	10.0.2.11	ICMP	98	Echo (ping) request id=0x4d75, seq=4/1024, ttl=64 (reply in 20)
20	94.451641217	10.0.2.11	10.0.2.15	ICMP	98	Echo (ping) reply id=0x4d75, seq=4/1024, ttl=64 (request in 19)
21	96.561361389	PCSSystemtec_98:df:...	PCSSystemtec_17:82:...	ARP	60	Who has 10.0.2.15? Tell 10.0.2.11
22	96.561378494	PCSSystemtec_17:82:...	PCSSystemtec_98:df:...	ARP	42	10.0.2.15 is at 08:00:27:17:82:fd
23	152.120120306	10.0.2.11	10.0.2.255	NBNS	92	Name query NB WORKGROUP<1d>
24	154.129833635	10.0.2.11	10.0.2.255	NBNS	92	Name query NB WORKGROUP<1d>
25	154.129834105	10.0.2.11	10.0.2.255	NBNS	92	Name query NB WORKGROUP<1d>
26	156.141108764	10.0.2.11	10.0.2.255	NBNS	92	Name query NB WORKGROUP<1d>
27	167.213665362	10.0.2.11	10.0.2.255	BROWSER	239	Browser Election Request
28	169.243155728	10.0.2.11	10.0.2.255	BROWSER	239	Browser Election Request
29	171.341332278	10.0.2.11	10.0.2.255	BROWSER	239	Browser Election Request
30	173.386219635	10.0.2.11	10.0.2.255	BROWSER	239	Browser Election Request
31	175.391881074	10.0.2.11	10.0.2.255	BROWSER	239	Browser Election Request
32	175.461006053	10.0.2.11	10.0.2.255	NBNS	110	Registration NB <01><02>__MSBROWSE__<02><01>
33	177.470413391	10.0.2.11	10.0.2.255	NBNS	110	Registration NB <01><02>__MSBROWSE__<02><01>
34	177.538262329	10.0.2.11	10.0.2.255	NBNS	110	Registration NB <01><02>__MSBROWSE__<02><01>
35	179.571643865	10.0.2.11	10.0.2.255	NBNS	110	Registration NB <01><02>__MSBROWSE__<02><01>
36	179.571644336	10.0.2.11	10.0.2.255	NBNS	110	Registration NB WORKGROUP<1d>
37	181.579153855	10.0.2.11	10.0.2.255	NBNS	110	Registration NB WORKGROUP<1d>
38	181.579154316	10.0.2.11	10.0.2.255	NBNS	110	Registration NB WORKGROUP<1d>
39	183.681426812	10.0.2.11	10.0.2.255	NBNS	110	Registration NB WORKGROUP<1d>
40	183.681427122	10.0.2.11	10.0.2.255	BROWSER	227	Request Announcement
41	183.681847571	10.0.2.11	10.0.2.255	BROWSER	286	Local Master Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix ...
42	183.685990250	10.0.2.11	10.0.2.255	BROWSER	257	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
47	434.461107360	10.0.2.11	10.0.2.255	BROWSER	286	Local Master Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix ...
48	434.461107961	10.0.2.11	10.0.2.255	BROWSER	257	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0  
Ethernet II, Src: PCSSystemtec\_98:df:ab (08:00:27:98:df:ab), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

No.	Time	Source	Destination	Protocol	Length	Info
63	768.741967036	10.0.2.15	10.0.2.11	TCP	74	60918 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4148936791 TSecr=0 WS=128
66	768.843423810	10.0.2.11	10.0.2.15	TCP	74	23 → 60918 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=76717 TSecr=41...
67	768.843491496	10.0.2.15	10.0.2.11	TCP	66	60918 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4148936893 TSecr=76717
68	768.845714793	10.0.2.15	10.0.2.11	TELNET	99	Telnet Data ...
69	768.871030594	10.0.2.11	10.0.2.15	TCP	66	23 → 60918 [ACK] Seq=1 Ack=34 Win=5824 Len=0 TSval=76729 TSecr=4148936895
71	769.044931909	10.0.2.11	10.0.2.15	TELNET	78	Telnet Data ...
72	769.044980327	10.0.2.15	10.0.2.11	TCP	66	60918 → 23 [ACK] Seq=34 Ack=13 Win=64256 Len=0 TSval=4148937094 TSecr=76746
73	769.104788698	10.0.2.11	10.0.2.15	TELNET	111	Telnet Data ...
74	769.104822926	10.0.2.15	10.0.2.11	TCP	66	60918 → 23 [ACK] Seq=34 Ack=58 Win=64256 Len=0 TSval=4148937154 TSecr=76752
75	769.105370108	10.0.2.15	10.0.2.11	TELNET	149	Telnet Data ...
76	769.143434731	10.0.2.11	10.0.2.15	TCP	66	23 → 60918 [ACK] Seq=58 Ack=117 Win=5824 Len=0 TSval=76756 TSecr=4148937155
77	769.143897859	10.0.2.11	10.0.2.15	TELNET	69	Telnet Data ...
78	769.144009356	10.0.2.15	10.0.2.11	TELNET	69	Telnet Data ...
79	769.162077433	10.0.2.11	10.0.2.15	TELNET	69	Telnet Data ...
80	769.162257197	10.0.2.15	10.0.2.11	TELNET	69	Telnet Data ...
81	769.163091039	10.0.2.11	10.0.2.15	TELNET	686	Telnet Data ...
82	769.206676595	10.0.2.15	10.0.2.11	TCP	66	60918 → 23 [ACK] Seq=123 Ack=684 Win=64128 Len=0 TSval=4148937256 TSecr=76758
83	773.213993669	10.0.2.15	10.0.2.11	TELNET	67	Telnet Data ...
84	773.219153084	10.0.2.11	10.0.2.15	TELNET	67	Telnet Data ...
85	773.219177018	10.0.2.15	10.0.2.11	TCP	66	60918 → 23 [ACK] Seq=124 Ack=685 Win=64128 Len=0 TSval=4148941268 TSecr=77164
86	773.356849566	10.0.2.15	10.0.2.11	TELNET	67	Telnet Data ...
87	773.380883397	10.0.2.11	10.0.2.15	TELNET	67	Telnet Data ...
88	773.380922292	10.0.2.15	10.0.2.11	TCP	66	60918 → 23 [ACK] Seq=125 Ack=686 Win=64128 Len=0 TSval=4148941430 TSecr=77180
89	773.621952678	10.0.2.15	10.0.2.11	TELNET	67	Telnet Data ...
90	773.658048236	10.0.2.11	10.0.2.15	TELNET	67	Telnet Data ...
91	773.658084787	10.0.2.15	10.0.2.11	TCP	66	60918 → 23 [ACK] Seq=126 Ack=687 Win=64128 Len=0 TSval=4148941707 TSecr=77208
92	773.912923554	10.0.2.15	10.0.2.11	TELNET	67	Telnet Data ...
93	773.913875512	10.0.2.11	10.0.2.15	TELNET	67	Telnet Data ...
94	773.913898514	10.0.2.15	10.0.2.11	TCP	66	60918 → 23 [ACK] Seq=127 Ack=688 Win=64128 Len=0 TSval=4148941963 TSecr=77234
95	774.064763008	10.0.2.15	10.0.2.11	TELNET	67	Telnet Data ...
96	774.074952839	10.0.2.11	10.0.2.15	TELNET	67	Telnet Data ...
97	774.074981259	10.0.2.15	10.0.2.11	TCP	66	60918 → 23 [ACK] Seq=128 Ack=689 Win=64128 Len=0 TSval=4148942124 TSecr=77250
98	774.199091131	10.0.2.15	10.0.2.11	TELNET	67	Telnet Data ...
99	774.199800570	10.0.2.11	10.0.2.15	TELNET	67	Telnet Data ...
100	774.199823754	10.0.2.15	10.0.2.11	TCP	66	60918 → 23 [ACK] Seq=129 Ack=690 Win=64128 Len=0 TSval=4148942249 TSecr=77262
101	774.418683280	10.0.2.15	10.0.2.11	TELNET	67	Telnet Data ...
102	774.451438248	10.0.2.11	10.0.2.15	TELNET	67	Telnet Data ...

No.	Time	Source	Destination	Protocol	Length	Info
63	768.741967036	10.0.2.15	10.0.2.11	TCP	74	60918 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4148936791 TSecr=0 WS=128
66	768.843423810	10.0.2.11	10.0.2.15	TCP	74	23 → 60918 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=76717 TSecr=41...
67	768.843491496	10.0.2.15	10.0.2.11	TCP	66	60918 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4148936893 TSecr=76717
68	768.845714793	10.0.2.15	10.0.2.11	TELNET	99	Telnet Data ...
69	768.871030594	10.0.2.11	10.0.2.15	TCP	66	23 → 60918 [ACK] Seq=1 Ack=34 Win=5824 Len=0 TSval=76729 TSecr=4148936895
71	769.044931909	10.0.2.11	10.0.2.15	TELNET	78	Telnet Data ...
72	769.044980327	10.0.2.15	10.0.2.11	TCP	66	60918 → 23 [ACK] Seq=34 Ack=13 Win=64256 Len=0 TSval=4148937094 TSecr=76746
73	769.104788698	10.0.2.11	10.0.2.15	TELNET	111	Telnet Data ...
74	769.104822926	10.0.2.15	10.0.2.11	TCP	66	60918 → 23 [ACK] Seq=34 Ack=58 Win=64256 Len=0 TSval=4148937154 TSecr=76752
75	769.105370108	10.0.2.15	10.0.2.11	TELNET	149	Telnet Data ...
76	769.143434731	10.0.2.11	10.0.2.15	TCP	66	23 → 60918 [ACK] Seq=58 Ack=117 Win=5824 Len=0 TSval=76756 TSecr=4148937155
77	769.143897859	10.0.2.11	10.0.2.15	TELNET	69	Telnet Data ...
78	769.144009356	10.0.2.15	10.0.2.11	TELNET	69	Telnet Data ...
79	769.162077433	10.0.2.11	10.0.2.15	TELNET	69	Telnet Data ...
80	769.162257197	10.0.2.15	10.0.2.11	TELNET	69	Telnet Data ...
81	769.163091039	10.0.2.11	10.0.2.15	TELNET	686	Telnet Data ...
82	769.206676595	10.0.2.15	10.0.2.11	TCP	66	60918 → 23 [ACK] Seq=123 Ack=684 Win=64128 Len=0 TSval=4148937256 TSecr=76758
83	773.213993669	10.0.2.15	10.0.2.11	TELNET	67	Telnet Data ...
84	773.219153084	10.0.2.11	10.0.2.15	TELNET	67	Telnet Data ...
85	773.219177018	10.0.2.15	10.0.2.11	TCP	66	60918 → 23 [ACK] Seq=124 Ack=685 Win=64128 Len=0 TSval=4148941268 TSecr=77164
86	773.356849566	10.0.2.15	10.0.2.11	TELNET	67	Telnet Data ...
87	773.380883397	10.0.2.11	10.0.2.15	TELNET	67	Telnet Data ...
88	773.380922292	10.0.2.15	10.0.2.11	TCP	66	60918 → 23 [ACK] Seq=125 Ack=686 Win=64128 Len=0 TSval=4148941430 TSecr=77180
89	773.621952678	10.0.2.15	10.0.2.11	TELNET	67	Telnet Data ...
90	773.658048236	10.0.2.11	10.0.2.15	TELNET	67	Telnet Data ...
91	773.658084787	10.0.2.15	10.0.2.11	TCP	66	60918 → 23 [ACK] Seq=126 Ack=687 Win=64128 Len=0 TSval=4148941707 TSecr=77208
92	773.912923554	10.0.2.15	10.0.2.11	TELNET	67	Telnet Data ...
93	773.913875512	10.0.2.11	10.0.2.15	TELNET	67	Telnet Data ...
94	773.913898514	10.0.2.15	10.0.2.11	TCP	66	60918 → 23 [ACK] Seq=127 Ack=688 Win=64128 Len=0 TSval=4148941963 TSecr=77234
95	774.064763008	10.0.2.15	10.0.2.11	TELNET	67	Telnet Data ...
96	774.074952839	10.0.2.11	10.0.2.15	TELNET	67	Telnet Data ...
97	774.074981259	10.0.2.15	10.0.2.11	TCP	66	60918 → 23 [ACK] Seq=128 Ack=689 Win=64128 Len=0 TSval=4148942124 TSecr=77250
98	774.199091131	10.0.2.15	10.0.2.11	TELNET	67	Telnet Data ...
99	774.199800570	10.0.2.11	10.0.2.15	TELNET	67	Telnet Data ...
100	774.199823754	10.0.2.15	10.0.2.11	TCP	66	60918 → 23 [ACK] Seq=129 Ack=690 Win=64128 Len=0 TSval=4148942249 TSecr=77262
101	774.418683280	10.0.2.15	10.0.2.11	TELNET	67	Telnet Data ...
102	774.451438248	10.0.2.11	10.0.2.15	TELNET	67	Telnet Data ...



# Filtro por dirección IP

*eth0					
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help					
ip.src == 10.0.2.11					
No.	Time	Source	Destination	Protocol	Length Info
4651	1528.0314561...	10.0.2.11	10.0.2.15	FTP	86 Response: 220 (vsFTPd 2.3.4)
4653	1528.0319347...	10.0.2.11	10.0.2.15	FTP	104 Response: 530 Please login with USER and PASS.
4654	1528.0319349...	10.0.2.11	10.0.2.15	FTP	104 Response: 530 Please login with USER and PASS.
4659	1528.0584889...	10.0.2.11	10.0.2.15	TCP	74 5900 → 60582 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=152687 TSecr...
4661	1528.0590732...	10.0.2.11	10.0.2.15	VNC	78 Server protocol version: 003.003
4664	1528.0615974...	10.0.2.11	10.0.2.15	TCP	66 5900 → 60582 [ACK] Seq=13 Ack=13 Win=5824 Len=0 TSval=152687 TSecr=4149696110
4665	1528.0620085...	10.0.2.11	10.0.2.15	VNC	86 Security types supported
4668	1528.1636573...	10.0.2.11	10.0.2.15	TCP	74 5900 → 60596 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=152697 TSecr...
4672	1528.4673469...	10.0.2.11	10.0.2.15	TCP	66 5900 → 60596 [ACK] Seq=1 Ack=518 Win=6912 Len=0 TSval=152728 TSecr=4149696213
4673	1528.4707330...	10.0.2.11	10.0.2.15	VNC	78 Server protocol version: 003.003
4674	1528.4707333...	10.0.2.11	10.0.2.15	TCP	66 5900 → 60582 [FIN, ACK] Seq=33 Ack=14 Win=5824 Len=0 TSval=152728 TSecr=4149696374
4675	1528.4707334...	10.0.2.11	10.0.2.15	TCP	66 5900 → 60596 [RST, ACK] Seq=13 Ack=518 Win=6912 Len=0 TSval=152728 TSecr=4149696213
4679	1528.4769439...	10.0.2.11	10.0.2.15	TCP	60 5900 → 60596 [RST] Seq=13 Win=0 Len=0
4680	1528.4869163...	10.0.2.11	10.0.2.15	TCP	74 5900 → 60606 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=152730 TSecr...
4682	1528.4876319...	10.0.2.11	10.0.2.15	VNC	78 Server protocol version: 003.003
4685	1528.4885275...	10.0.2.11	10.0.2.15	TCP	66 5900 → 60606 [ACK] Seq=13 Ack=93 Win=5824 Len=0 TSval=152730 TSecr=4149696537
4686	1528.4891024...	10.0.2.11	10.0.2.15	TCP	66 5900 → 60606 [RST, ACK] Seq=13 Ack=93 Win=5824 Len=0 TSval=152730 TSecr=4149696537
4688	1528.4911672...	10.0.2.11	10.0.2.15	TCP	74 5432 → 39152 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=152730 TSecr...
4691	1528.4925375...	10.0.2.11	10.0.2.15	TCP	66 5432 → 39152 [ACK] Seq=1 Ack=9 Win=5824 Len=0 TSval=152730 TSecr=4149696541
4692	1528.4927293...	10.0.2.11	10.0.2.15	PGSQL	67 <
4695	1528.5104688...	10.0.2.11	10.0.2.15	TLSv1	1413 Server Hello, Certificate, Server Key Exchange, Server Hello Done
4697	1528.5269402...	10.0.2.11	10.0.2.15	TLSv1	300 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
4700	1528.5293240...	10.0.2.11	10.0.2.15	TLSv1	103 Encrypted Alert
4702	1531.7140723...	10.0.2.11	10.0.2.15	TCP	74 [TCP Retransmission] 42535 → 113 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=153...
4703	1532.6429412...	10.0.2.11	10.0.2.15	TCP	120 2121 → 60760 [PSH, ACK] Seq=1 Ack=519 Win=6912 Len=54 TSval=153146 TSecr=4149691649
4706	1629.2773607...	10.0.2.11	10.0.2.15	TCP	74 21 → 54996 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=162814 TSecr=4...
4708	1629.2793209...	10.0.2.11	10.0.2.15	FTP	86 Response: 220 (vsFTPd 2.3.4)
4711	1633.3301790...	10.0.2.11	10.0.2.15	TCP	66 21 → 54996 [ACK] Seq=21 Ack=16 Win=5824 Len=0 TSval=163219 TSecr=4149801371
4712	1633.3311776...	10.0.2.11	10.0.2.15	FTP	100 Response: 331 Please specify the password.
4715	1636.5604645...	10.0.2.11	10.0.2.15	TCP	66 21 → 54996 [ACK] Seq=55 Ack=31 Win=5824 Len=0 TSval=163543 TSecr=4149804542
4716	1636.5614982...	10.0.2.11	10.0.2.15	FTP	89 Response: 230 Login successful.
4719	1636.5623800...	10.0.2.11	10.0.2.15	TCP	66 21 → 54996 [ACK] Seq=78 Ack=37 Win=5824 Len=0 TSval=163543 TSecr=4149804611
4720	1636.5627502...	10.0.2.11	10.0.2.15	FTP	85 Response: 215 UNIX Type: L8
4722	1636.5637125...	10.0.2.11	10.0.2.15	FTP	81 Response: 211-Features:
4723	1636.5641075...	10.0.2.11	10.0.2.15	FTP	73 Response: EPRT
4725	1636.5644604...	10.0.2.11	10.0.2.15	FTP	73 Response: EPSV
4726	1636.5647176...	10.0.2.11	10.0.2.15	FTP	124 Response: MDTM

Frame 66: 74 bytes on wire (592 bits) 74 bytes captured (592 bits) on interface 00:00:00:00:00:00 08 00 27 17 82 fd 08 00 27 98 df ab 08 00 45 00 .....

# Filtro por dirección IP y dirección MAC combinados

*eth0					
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help					
ip.src == 10.0.2.11 or eth.addr == 08:00:27:98:df:ab					
No.	Time	Source	Destination	Protocol	Length Info
32	175.461006053	10.0.2.11	10.0.2.255	NBNS	110 Registration NB <01><02>__MSBROWSE__<02><01>
33	177.470413391	10.0.2.11	10.0.2.255	NBNS	110 Registration NB <01><02>__MSBROWSE__<02><01>
34	177.538262329	10.0.2.11	10.0.2.255	NBNS	110 Registration NB <01><02>__MSBROWSE__<02><01>
35	179.571643865	10.0.2.11	10.0.2.255	NBNS	110 Registration NB <01><02>__MSBROWSE__<02><01>
36	179.571644336	10.0.2.11	10.0.2.255	NBNS	110 Registration NB WORKGROUP<1d>
37	181.579153855	10.0.2.11	10.0.2.255	NBNS	110 Registration NB WORKGROUP<1d>
38	181.579154316	10.0.2.11	10.0.2.255	NBNS	110 Registration NB WORKGROUP<1d>
39	183.681426812	10.0.2.11	10.0.2.255	NBNS	110 Registration NB WORKGROUP<1d>
40	183.681427122	10.0.2.11	10.0.2.255	BROWSER	227 Request Announcement
41	183.681847571	10.0.2.11	10.0.2.255	BROWSER	286 Local Master Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix...
42	183.685990250	10.0.2.11	10.0.2.255	BROWSER	257 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
47	434.461107360	10.0.2.11	10.0.2.255	BROWSER	286 Local Master Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix...
48	434.461107961	10.0.2.11	10.0.2.255	BROWSER	257 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
61	735.080570957	10.0.2.11	10.0.2.255	BROWSER	286 Local Master Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix...
62	735.080571679	10.0.2.11	10.0.2.255	BROWSER	257 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
63	768.741967036	10.0.2.15	10.0.2.11	TCP	74 60918 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4148936791 TSecr=0 WS=128
64	768.842905764	PCSSystemtec_98:df:...	Broadcast	ARP	60 Who has 10.0.2.15? Tell 10.0.2.11
65	768.842925682	PCSSystemtec_17:82:...	PCSSystemtec_98:df:...	ARP	42 10.0.2.15 is at 08:00:27:17:82:fd
66	768.843423810	10.0.2.11	10.0.2.15	TCP	74 23 → 60918 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=76717 TSecr=41...
67	768.843491496	10.0.2.15	10.0.2.11	TCP	66 60918 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4148936893 TSecr=76717
68	768.845714793	10.0.2.15	10.0.2.11	TELNET	99 Telnet Data ...
69	768.871030594	10.0.2.15	10.0.2.11	TCP	66 23 → 60918 [ACK] Seq=1 Ack=34 Win=5824 Len=0 TSval=76729 TSecr=4148936895
70	768.984551420	PCSSystemtec_98:df:...	Broadcast	ARP	60 Who has 10.0.2.1? Tell 10.0.2.11
71	769.044931909	10.0.2.11	10.0.2.15	TELNET	78 Telnet Data ...
72	769.044980327	10.0.2.15	10.0.2.11	TCP	66 60918 → 23 [ACK] Seq=34 Ack=13 Win=64256 Len=0 TSval=4148937094 TSecr=76746
73	769.104788698	10.0.2.11	10.0.2.15	TELNET	111 Telnet Data ...
74	769.104822926	10.0.2.15	10.0.2.11	TCP	66 60918 → 23 [ACK] Seq=34 Ack=58 Win=64256 Len=0 TSval=4148937154 TSecr=76752
75	769.105370108	10.0.2.15	10.0.2.11	TELNET	149 Telnet Data ...
76	769.143434731	10.0.2.11	10.0.2.15	TCP	66 23 → 60918 [ACK] Seq=58 Ack=117 Win=5824 Len=0 TSval=76756 TSecr=4148937155
77	769.143897859	10.0.2.11	10.0.2.15	TELNET	69 Telnet Data ...
78	769.144009356	10.0.2.15	10.0.2.11	TELNET	69 Telnet Data ...
79	769.162077433	10.0.2.11	10.0.2.15	TELNET	69 Telnet Data ...
80	769.162257197	10.0.2.15	10.0.2.11	TELNET	69 Telnet Data ...
81	769.163091039	10.0.2.11	10.0.2.15	TELNET	686 Telnet Data ...
82	769.206676595	10.0.2.15	10.0.2.11	TCP	66 60918 → 23 [ACK] Seq=123 Ack=684 Win=64128 Len=0 TSval=4148937256 TSecr=76758
83	773.213993669	10.0.2.15	10.0.2.11	TELNET	67 Telnet Data ...
84	773.219153084	10.0.2.11	10.0.2.15	TELNET	67 Telnet Data ...
85	773.219153084	10.0.2.11	10.0.2.15	TCP	66 60918 → 23 [ACK] Seq=123 Ack=684 Win=64128 Len=0 TSval=4148937256 TSecr=76758

# Conclusiones

En este ejercicio, Wireshark demostró ser una herramienta esencial para analizar el tráfico de red en tiempo real, vimos la capacidad que tiene de filtrar paquetes según diversos criterios y obtuvimos una visión profunda de nuestra red. Podríamos detectar actividades sospechosas, al filtrar por dirección MAC y puerto destino, en distintas auditorías que podríamos llegar a realizar en el futuro. Podemos también, identificar rápidamente problemas como latencia y pérdida de paquetes. Wireshark es una herramienta imprescindible para, analizar y diagnosticar problemas, y mejorar la seguridad en redes.