

Mario Mendoza

Instalamos wireshark

The image shows two terminal windows side-by-side. Both windows have a dark theme with light-colored text. The top window shows the command `sudo apt install -y wireshark` being typed. The bottom window shows the output of the command, which includes a password prompt, a message indicating Wireshark is already the newest version, and a summary line.

```
kali㉿kali: ~
Session Actions Edit View Help
[(kali㉿kali)-[~]]$ sudo apt install -y wireshark

kali㉿kali: ~
Session Actions Edit View Help
[(kali㉿kali)-[~]]$ sudo apt install -y wireshark
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
wireshark is already the newest version (4.4.9-1).
wireshark set to manually installed.
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 993

[(kali㉿kali)-[~]]$
```

Ejecutamos wireshark

The image shows a single terminal window with a dark theme. It displays the command `wireshark` being typed.

```
[(kali㉿kali)-[~]]$ wireshark
```

En el filtro añadimos: tcp port 80

The screenshot shows the Wireshark Network Analyzer interface. At the top, the menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. A search bar at the top right contains the placeholder "Apply a display filter ... <Ctrl-/>". The main window has a "Welcome to Wireshark" message. Under the "Capture" section, there is a dropdown menu set to "All interfaces shown" and a list of interfaces including eth0, any, Loopback: lo, bluetooth-monitor, nflog, nfqueue, dbus-system, and dbus-session. Below the capture section is a "Learn" section with links to User's Guide, Wiki, Questions and Answers, Mailing Lists, SharkFest, Wireshark Discord, and a "Donate" button. A status message at the bottom says "You are running Wireshark 4.4.9." The bottom of the window shows a toolbar with "Ready to load or capture", "No Packets", and "Profile: Default".

Ready to load or capture No Packets Profile: Default

The Wireshark Network Analyzer

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Welcome to Wireshark

Capture

...using this filter: All interfaces shown

eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session

Learn

User's Guide Wiki Questions and Answers Mailing Lists SharkFest Wireshark Discord Donate

You are running Wireshark 4.4.9.

Ready to load or capture No Packets Profile: Default

The Wireshark Network Analyzer

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Welcome to Wireshark

Open

/home/kali/Desktop/first-20-packets.pcapng (16 KB)

Capture

...using this filter: All interfaces shown

eth0
any
Loopback: lo

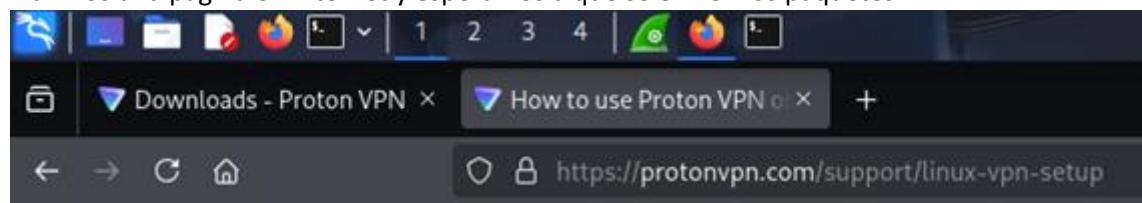
Learn

User's Guide Wiki Questions and Answers Mailing Lists SharkFest Wireshark Discord Donate

You are running Wireshark 4.4.9.

Ready to load or capture No Packets Profile: Default

Abrimos una pagina en internet y esperamos a que se envíen los paquetes



Iniciamos y esperamos a capturar 20 paquetes

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	10.0.2.15	192.124.249.22	TCP	74	347
2	0.000319178	10.0.2.15	192.124.249.22	TCP	74	347
3	0.027634996	192.124.249.22	10.0.2.15	TCP	60	80
4	0.027662753	10.0.2.15	192.124.249.22	TCP	54	347
5	0.028127769	10.0.2.15	192.124.249.22	OCSP	482	Req
6	0.028300798	192.124.249.22	10.0.2.15	TCP	60	80
7	0.250406008	10.0.2.15	192.124.249.22	TCP	74	347
8	0.277930941	192.124.249.22	10.0.2.15	TCP	60	80
9	0.277958282	10.0.2.15	192.124.249.22	TCP	54	347
10	0.278526859	10.0.2.15	192.124.249.22	OCSP	482	Req
11	0.278700820	192.124.249.22	10.0.2.15	TCP	60	80

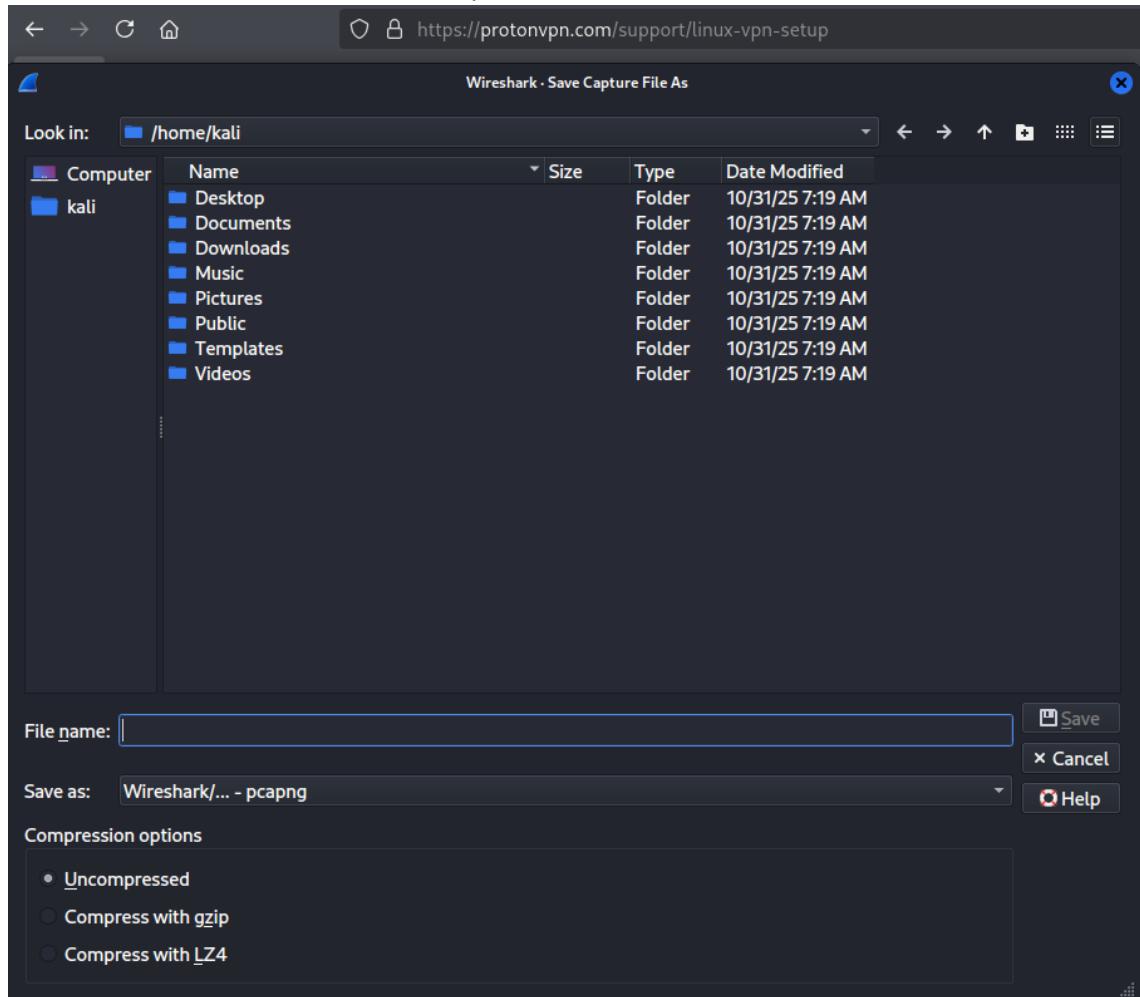
```
Frame 1: 74 bytes on wire (592 bits), 70 bytes captured (560 bits) on interface 1
Ethernet II, Src: PCSSystemtec_1f:b7:23 (08:00:27:1f:b7:23), Dst: 00:0c:ef (00:0c:ef)
Internet Protocol Version 4, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.2 (10.0.0.2)
Transmission Control Protocol, Src Port: 3389 (3389), Dst Port: 445 (445)
```

eth0: <live capture in progress> Packets: 52 Profile: Default

The screenshot shows the Wireshark interface with the following details:

- Interface:** *eth0 (tcp port 80)
- Menu Bar:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help
- Toolbar:** Includes icons for file operations, search, and various analysis tools.
- Search Bar:** Apply a display filter ... <Ctrl-/>
- Table Headers:** No., Time, Source, Destination, Protocol, Length
- Data Rows:** 21 rows of network traffic. Key entries include:
 - Pkt 11: 0.278700820, Source 192.124.249.22, Destination 10.0.2.15, TCP, Length 60
 - Pkt 12: 0.324736666, Source 192.124.249.22, Destination 10.0.2.15, TCP, Length 149
 - Pkt 13: 0.324737297, Source 192.124.249.22, Destination 10.0.2.15, OCSP, Length 133
 - Pkt 14: 0.324761655, Source 10.0.2.15, Destination 192.124.249.22, TCP, Length 54
 - Pkt 15: 0.324807723, Source 10.0.2.15, Destination 192.124.249.22, TCP, Length 54
 - Pkt 16: 0.335157401, Source 192.124.249.22, Destination 10.0.2.15, TCP, Length 149
 - Pkt 17: 0.335157727, Source 192.124.249.22, Destination 10.0.2.15, OCSP, Length 133
 - Pkt 18: 0.335179018, Source 10.0.2.15, Destination 192.124.249.22, TCP, Length 54
 - Pkt 19: 0.335222641, Source 10.0.2.15, Destination 192.124.249.22, TCP, Length 54
 - Pkt 20: 1.023260207, Source 192.124.249.22, Destination 10.0.2.15, TCP, Length 60
 - Pkt 21: 1.023325967, Source 10.0.2.15, Destination 192.124.249.22, TCP, Length 54

Guardamos el documento en el desktop



Listo para analizar luego



Usamos el siguiente comando para analizar los puertos del servidor (Kali)

```
(kali㉿kali)-[~]
$ nmap -sV scanne.nmap.com
```

Resultado del análisis:

```
kali@kali: ~
Session Actions Edit View Help
└─(kali㉿kali)-[~]
$ nmap -sV scanne.nmap.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-14 07:09 EST
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 51.93% done; ETC: 07:09 (0:00:11 remaining)
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.44% done; ETC: 07:09 (0:00:00 remaining)
Stats: 0:00:43 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 87.50% done; ETC: 07:09 (0:00:00 remaining)
Nmap scan report for scanne.nmap.com (50.116.1.184)
Host is up (0.020s latency).
rDNS record for 50.116.1.184: ack.nmap.org
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
25/tcp    open  smtp     Postfix smtpd
80/tcp    open  http     Apache httpd 2.4.6
113/tcp   closed ident
443/tcp   open  ssl/https Apache/2.4.6 (CentOS)
Service Info: Host: ack.nmap.org

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 44.93 seconds
└─(kali㉿kali)-[~]
$
```