

Manual de usuario rootkit

Emilio Cabo Gomis

Indice

Windows..... 3

 NMAP.....4

 MBSA..... 10

Linux.....12

 rkhunter.....12

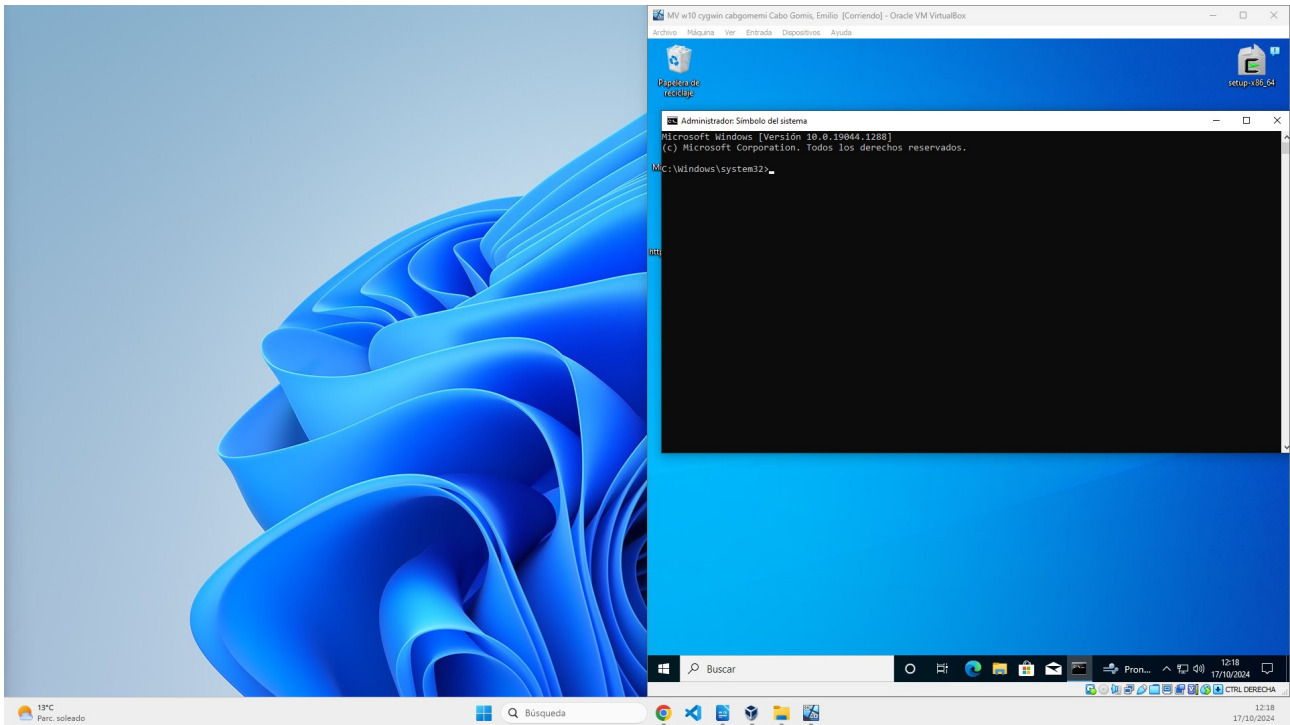
 Nmap.....13

Bibliografía.....15

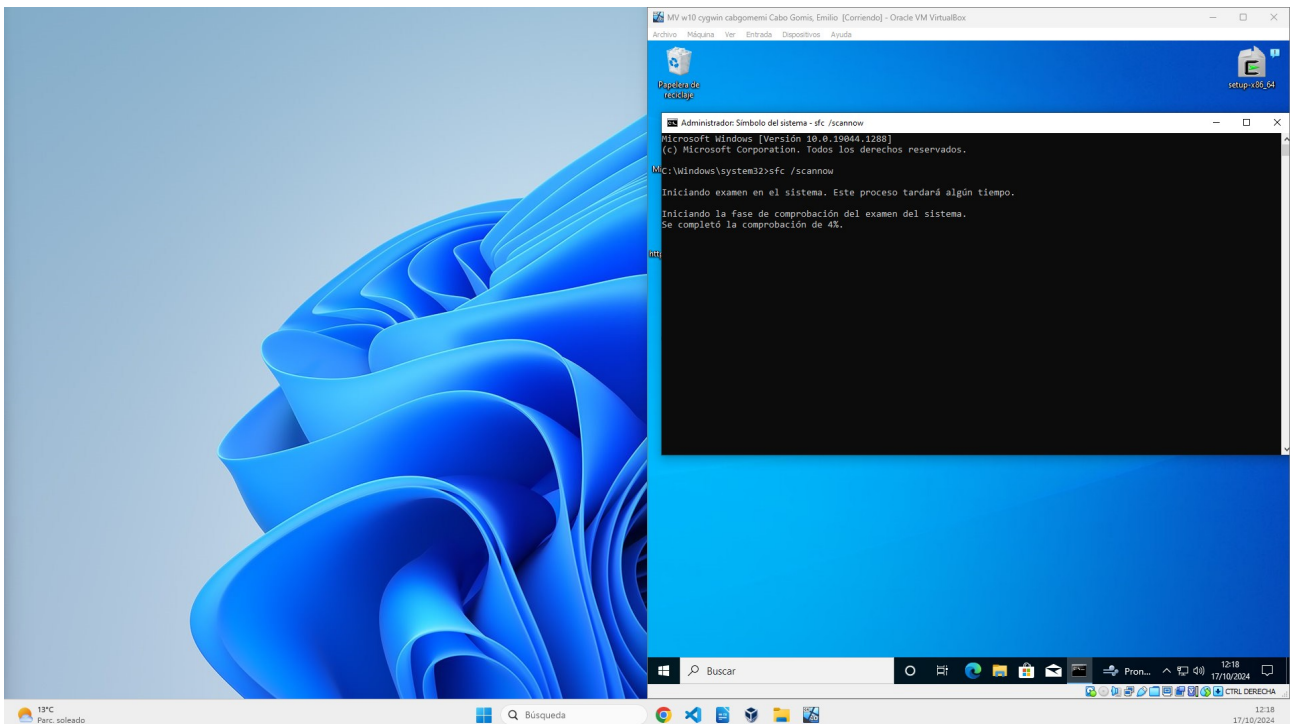
Windows

Abrimos un cmd con permisos de administrador.

WIN > “cmd” > click derecho > permisos de administrador



Escribimos el comando **sfc /scannow**



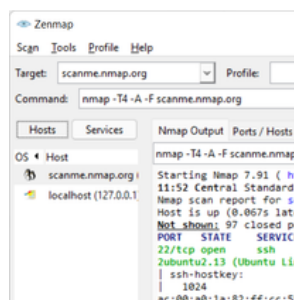
Resultado de la ejecución.

NMAP

Descargamos el ejecutable de la página web de nmap <https://nmap.org/download.html#windows>

Descargamos el siguiente paquete.

Microsoft Windows binaries



Please read the [Windows section](#) of the Install Guide for limitations and installation instructions for the Windows version of Nmap. It's provided as an executable self-installer which includes Nmap's dependencies and the Zenmap GUI. We support Nmap on Windows 7 and newer, as well as Windows Server 2008 R2 and newer. We also maintain a [guide for users who must run Nmap on earlier Windows releases](#).

Note: The version of Npcap included in our installers may not always be the latest version. If you experience problems or just want the latest and greatest version, download and install [the latest Npcap release](#).

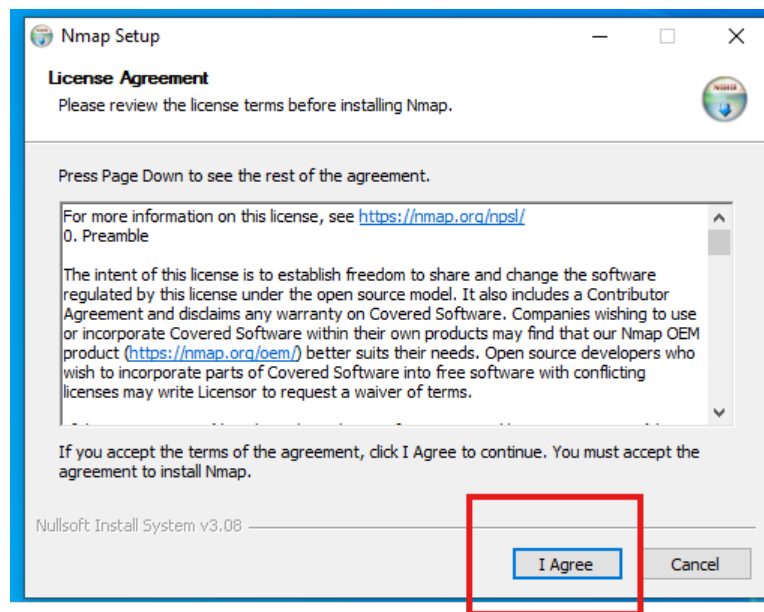
Latest stable release self-installer: [nmap-7.95-setup.exe](#)

Latest Npcap release self-installer: [npcap-1.80.exe](#)

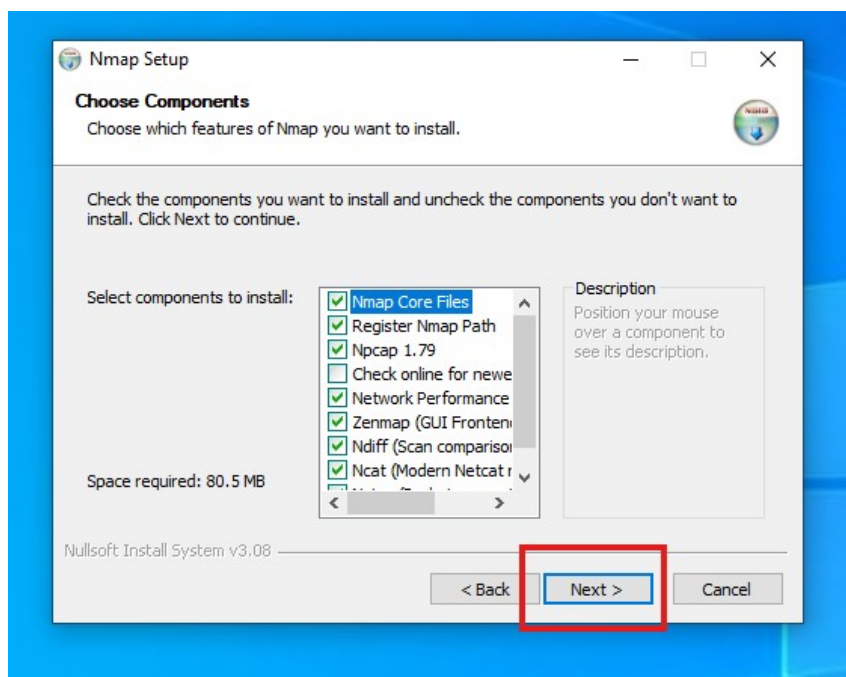
We have written [post-install usage instructions](#). Please [notify us](#) if you encounter any problems or have suggestions for the installer.

Ejecutamos el instalador.

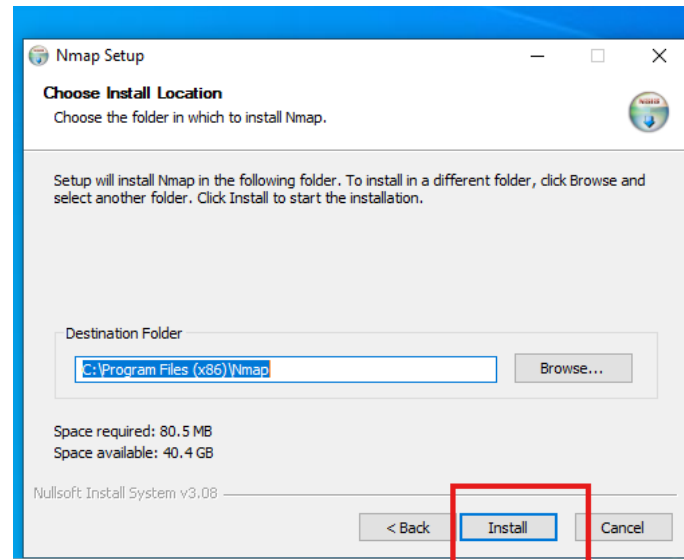
Le damos en "I agree".



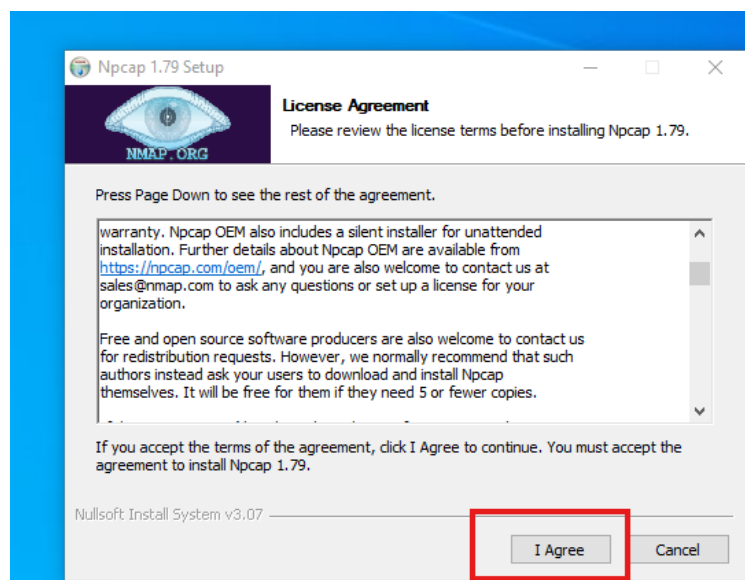
Le damos a next



Le damos a “install”



Aceptamos el acuerdo de licencia.



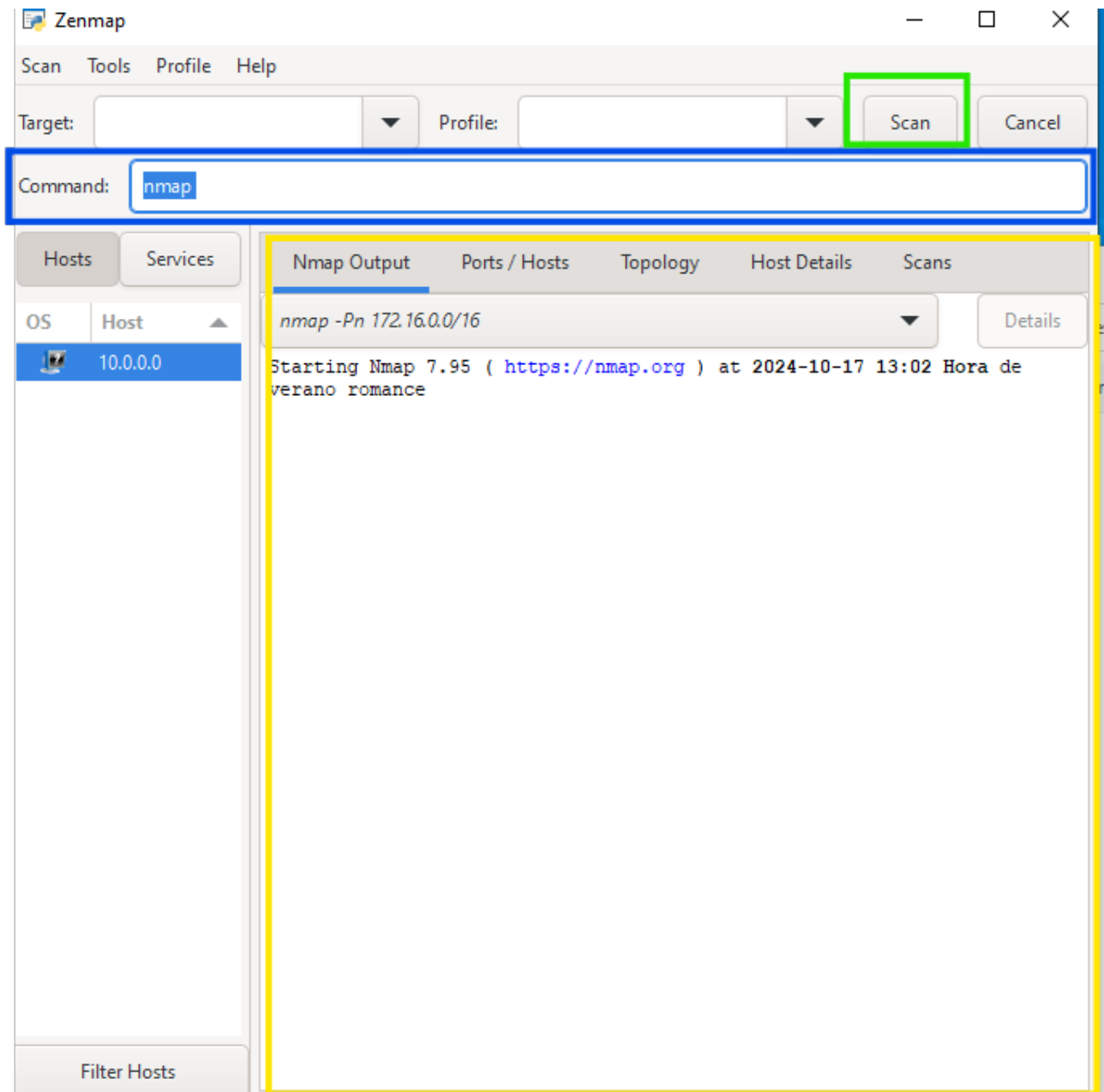
Ejecutamos el programa

Sección: Guía de empleo

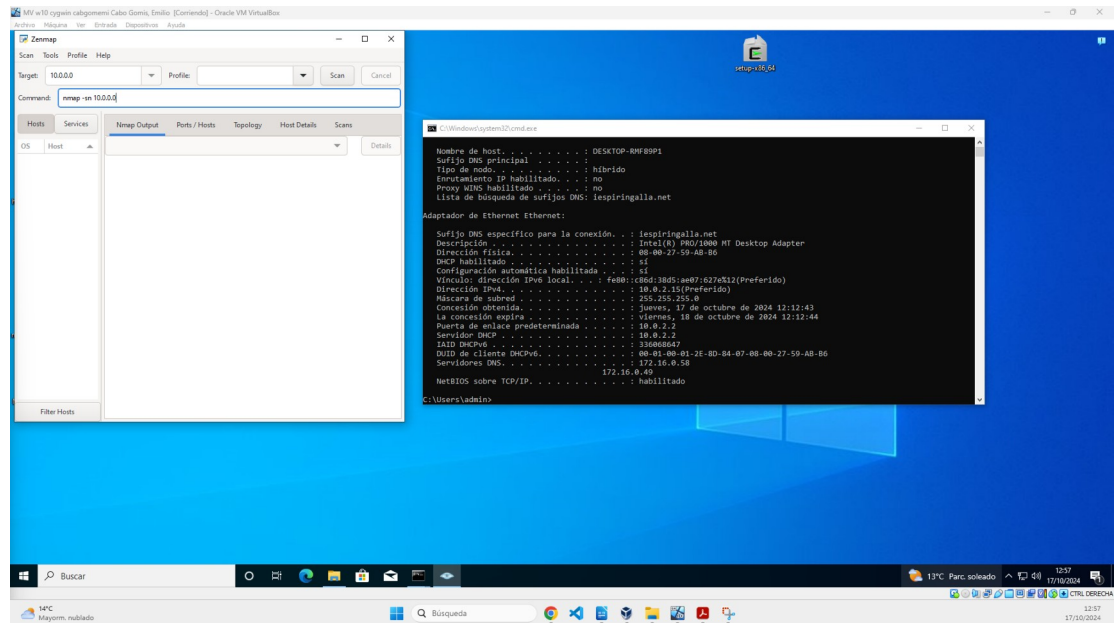
Introducimos el comando en la sección azul

Para escanear le damos al botón verde.

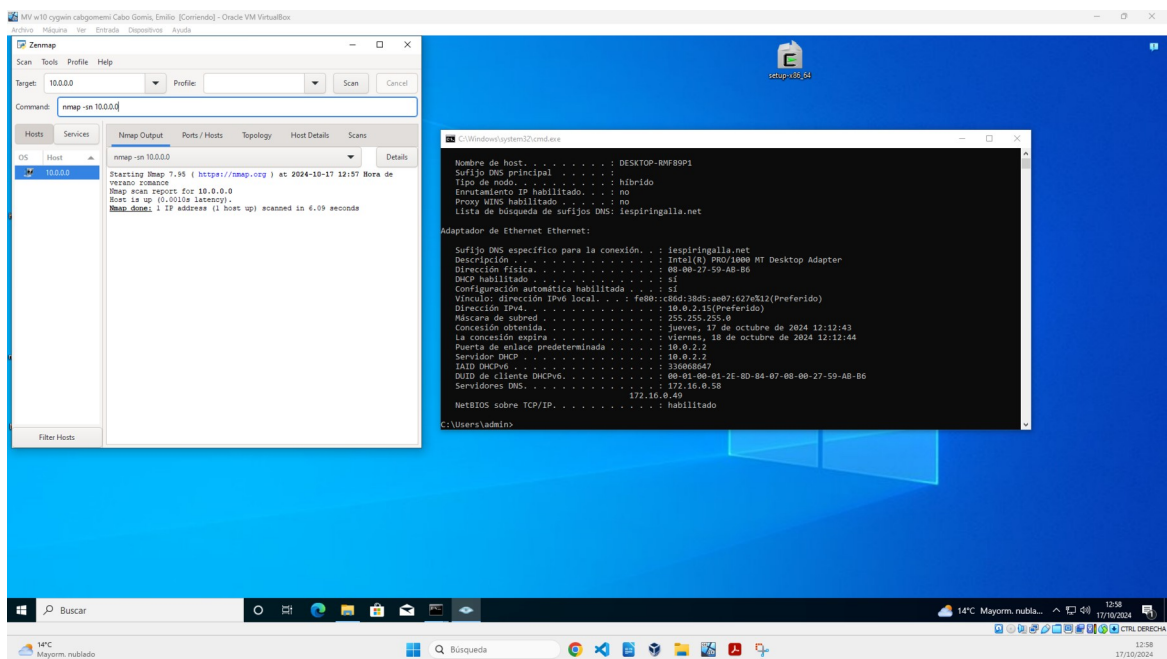
Para ver el resultado del escaneo vemos la sección amarilla.



Ponemos nuestra red como destino de nuestro escaneo.



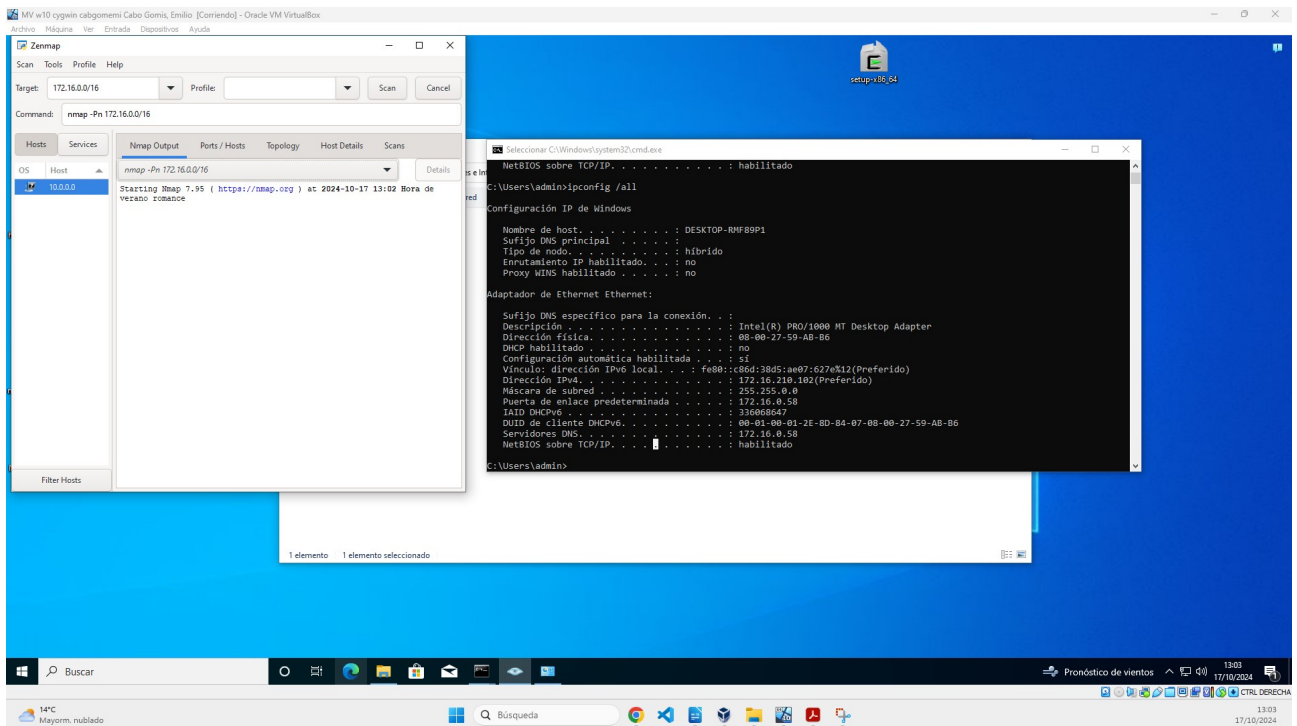
Este es el resultado de nuestro escaneo.



Este será un escaneo para ver que puertos tenemos abiertos.

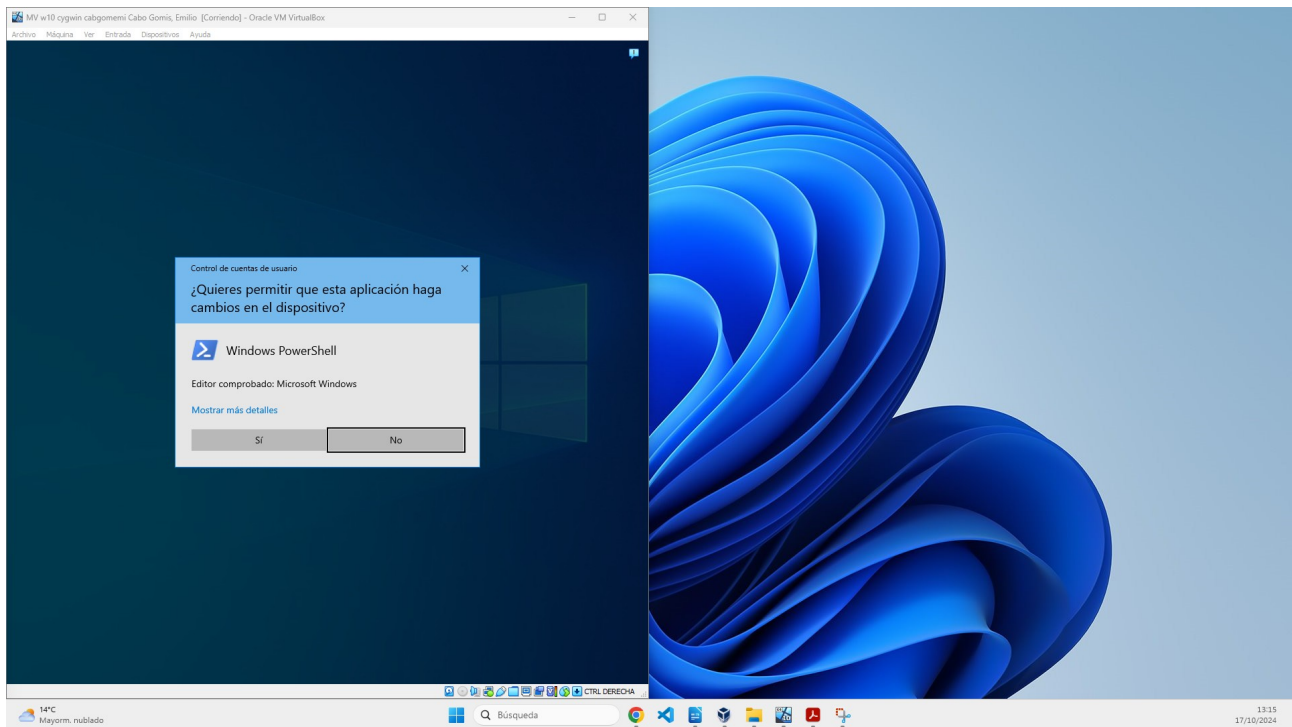
En este caso puse la red en adaptador puente.

Debido a que la red está asegurada no tenemos output.



MBSA

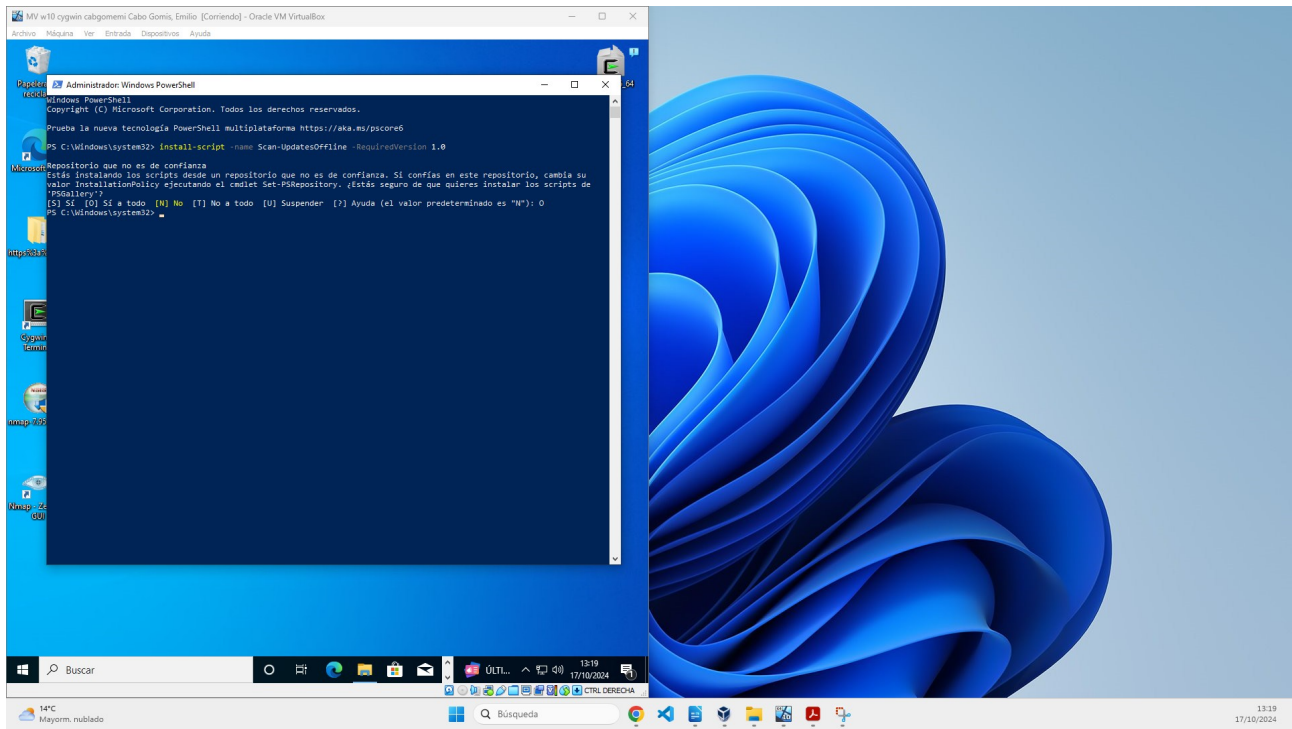
Pulsamos la tecla de Windows > escribimos “Powershell” > click derecho > ejecutar como administrador.



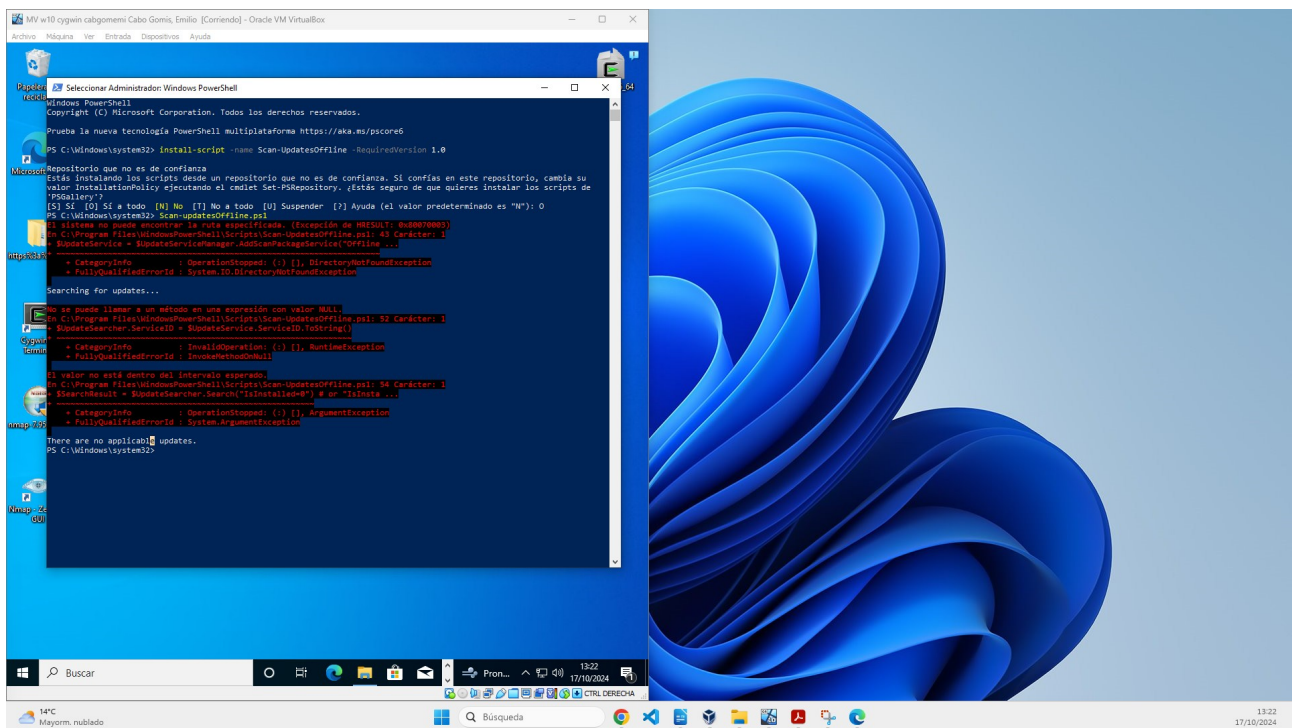
Instalamos el script.

Install-Script -Name Scan-UpdatesOffline -RequiredVersion 1.0

Cuando nos pida si queremos instalar los scripts. Le damos a Sí a todo escribiendo una “O” mayúscula.



Ahora ejecutamos el script.



El resultado es que no tenemos actualizaciones de sistema disponibles.

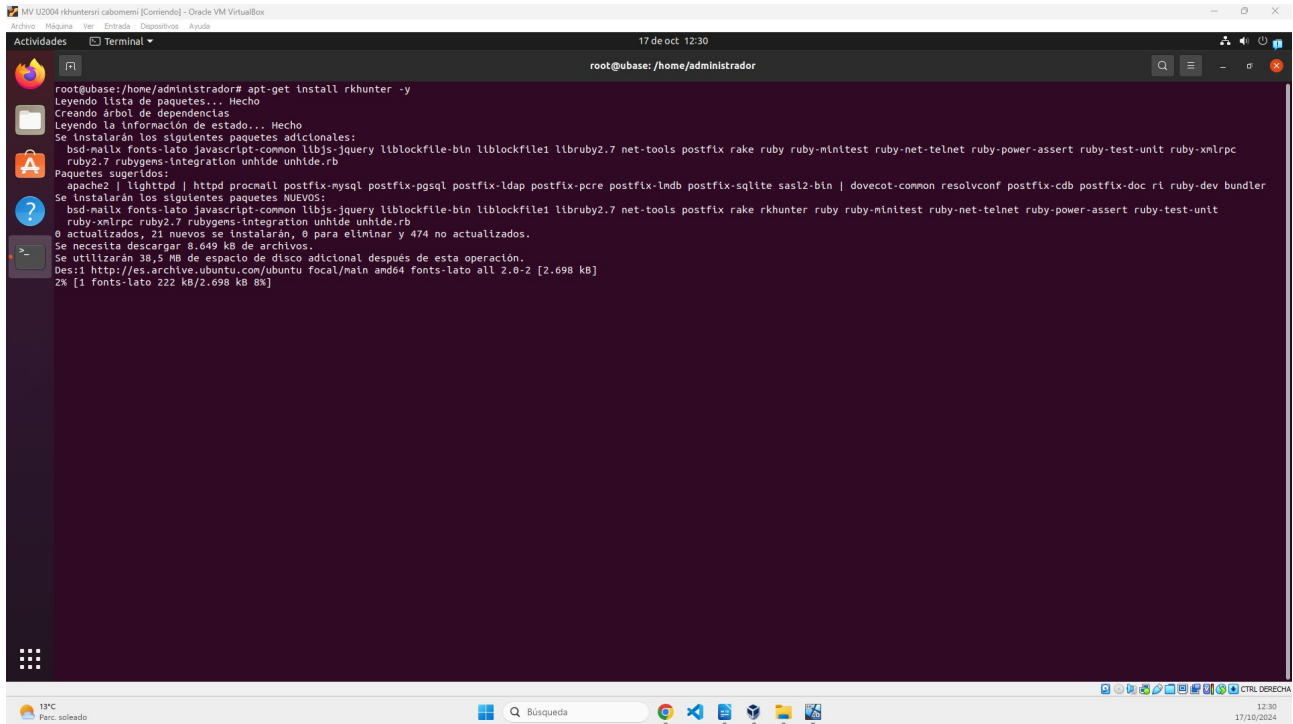
Linux

rkhunter

Abrimos un terminal mediante el shortcut `ctrl + alt + t`

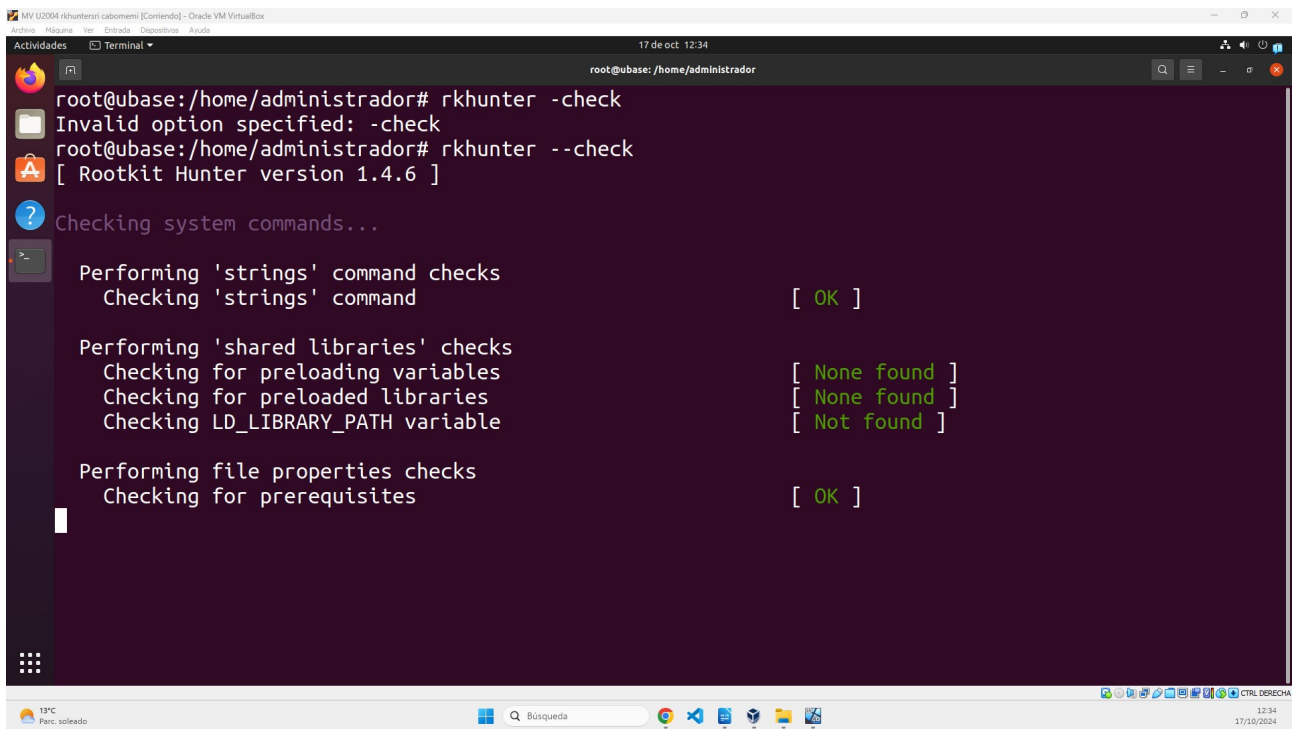
Instalamos el programa necesario escribiendo el comando

`sudo apt-get install rkhunter -y`



```
root@ubase:/home/administrador# apt-get install rkhunter -y
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
bsd-mailx fonts-lato javascript-common libjs-jquery liblockfile-bin liblockfile1 libruby2.7 net-tools postfix rake ruby ruby-minitest ruby-net-telnet ruby-power-assert ruby-test-unit ruby-xmllrpc
Paquetes sugeridos:
apache2 | lighttpd | httpd procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre postfix-lmdb postfix-sqlite sasl2-bin | dovecot-common resolvconf postfix-cdb postfix-doc ri ruby-dev bundler
Se instalarán los siguientes paquetes NUEVOS:
bsd-mailx fonts-lato javascript-common libjs-jquery liblockfile-bin liblockfile1 libruby2.7 net-tools postfix rake rkhunter ruby ruby-minitest ruby-net-telnet ruby-power-assert ruby-test-unit
ruby-xmllrpc ruby2.7 rubygems-integration unhide unhide.rb
0 actualizados, 21 nuevos se instalarán, 0 para eliminar y 474 no actualizados.
Se necesita descargar 8.649 kB de archivos.
Se utilizarán 38,5 MB de espacio de disco adicional después de esta operación.
Des:1 http://es.archive.ubuntu.com/ubuntu focal/main amd64 fonts-lato all 2.0-2 [2.698 kB]
2% [1 fonts-lato 222 kB/2.698 kB 8%]
```

Ejecutamos el comando `rkhunter --check`



```
root@ubase:/home/administrador# rkhunter -check
Invalid option specified: -check
root@ubase:/home/administrador# rkhunter --check
[ Rootkit Hunter version 1.4.6 ]

Checking system commands...

Performing 'strings' command checks
Checking 'strings' command                [ OK ]

Performing 'shared libraries' checks
Checking for preloading variables          [ None found ]
Checking for preloaded libraries           [ None found ]
Checking LD_LIBRARY_PATH variable          [ Not found ]

Performing file properties checks
Checking for prerequisites                 [ OK ]
```

Nmap

Abrimos un terminal mediante el shortcut `ctrl + alt + t`

Instalamos el programa necesario escribiendo el comando

`sudo apt-get install nmap -y`

```
17 de oct. 12:35
root@ubase: /home/administrador

administrador@ubase:~$ sudo su
[sudo] contraseña para administrador:
root@ubase:/home/administrador# sudo apt-get install nmap -y
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
libblas3 liblinear4 liblua5.3-0 lua-lpeg nmap-common
Paquetes sugeridos:
liblinear-tools liblinear-dev ncat ndiff zenmap
Se instalarán los siguientes paquetes NUEVOS:
libblas3 liblinear4 liblua5.3-0 lua-lpeg nmap nmap-common
0 actualizados, 6 nuevos se instalarán, 0 para eliminar y 474 no actualizados.
Se necesita descargar 5.673 kB de archivos.
Se utilizarán 26,8 MB de espacio de disco adicional después de esta operación.
Des:1 http://es.archive.ubuntu.com/ubuntu focal/main amd64 libblas3 amd64 3.9.0-1build1 [142 kB]
Des:2 http://es.archive.ubuntu.com/ubuntu focal/universe amd64 liblinear4 amd64 2.3.0+dfsg-3build1 [41,7 kB]
Des:3 http://es.archive.ubuntu.com/ubuntu focal/main amd64 liblua5.3-0 amd64 5.3.3-1.1ubuntu2 [116 kB]
Des:4 http://es.archive.ubuntu.com/ubuntu focal/universe amd64 lua-lpeg amd64 1.0.2-1 [31,4 kB]
Des:5 http://es.archive.ubuntu.com/ubuntu focal-updates/universe amd64 nmap-common all 7.80+dfsg1-2ubuntu0.1 [3.676 kB]
Des:6 http://es.archive.ubuntu.com/ubuntu focal-updates/universe amd64 nmap amd64 7.80+dfsg1-2ubuntu0.1 [1.666 kB]
Descargados 5.673 kB en 2s (3.620 kB/s)
```

Para escanear los puertos de un dominio. Ejecutamos el comando → `nmap -v www.marca.com`

```
17 de oct. 12:39
root@ubase: /home/administrador

-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@ubase:/home/administrador# nmap -v www.marca.com
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-17 12:38 CEST
Initiating Ping Scan at 12:38
Scanning www.marca.com (151.101.133.50) [4 ports]
Completed Ping Scan at 12:38, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:38
Completed Parallel DNS resolution of 1 host. at 12:38, 0.01s elapsed
Initiating SYN Stealth Scan at 12:38
Scanning www.marca.com (151.101.133.50) [1000 ports]
Discovered open port 80/tcp on 151.101.133.50
Discovered open port 443/tcp on 151.101.133.50
Discovered open port 8008/tcp on 151.101.133.50
Completed SYN Stealth Scan at 12:38, 3.98s elapsed (1000 total ports)
Nmap scan report for www.marca.com (151.101.133.50)
Host is up (0.0055s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8008/tcp   open  http

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.07 seconds
Raw packets sent: 2003 (88.100KB) | Rcvd: 10 (404B)
root@ubase:/home/administrador#
```

Bibliografía

[PowerShell Gallery | Scan-UpdatesOffline 1.0](#)

[Guide to removing Microsoft Baseline Security Analyzer \(MBSA\) | Microsoft Learn](#)

[RKhunter - Community Help Wiki \(ubuntu.com\)](#)

[Windows | Nmap Network Scanning](#)