Manual de usuario rootkit

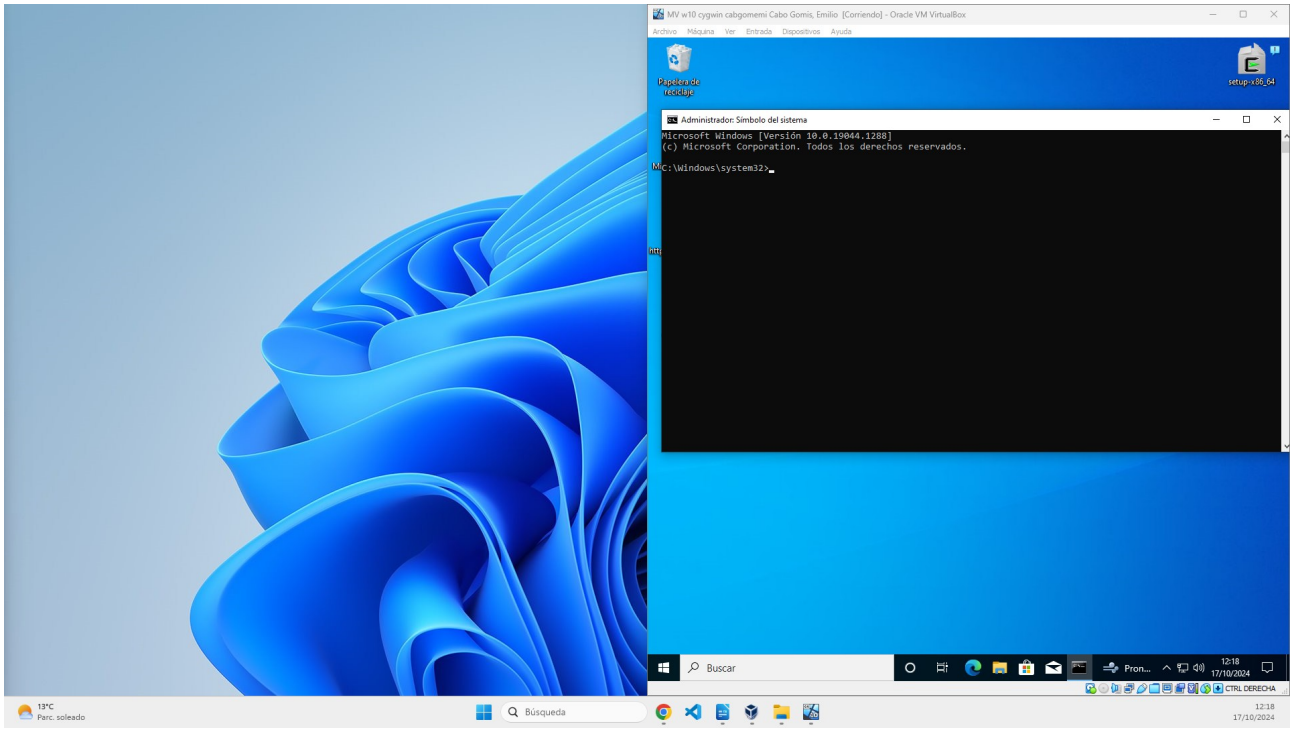
Emilio Cabo Gomis

Indice

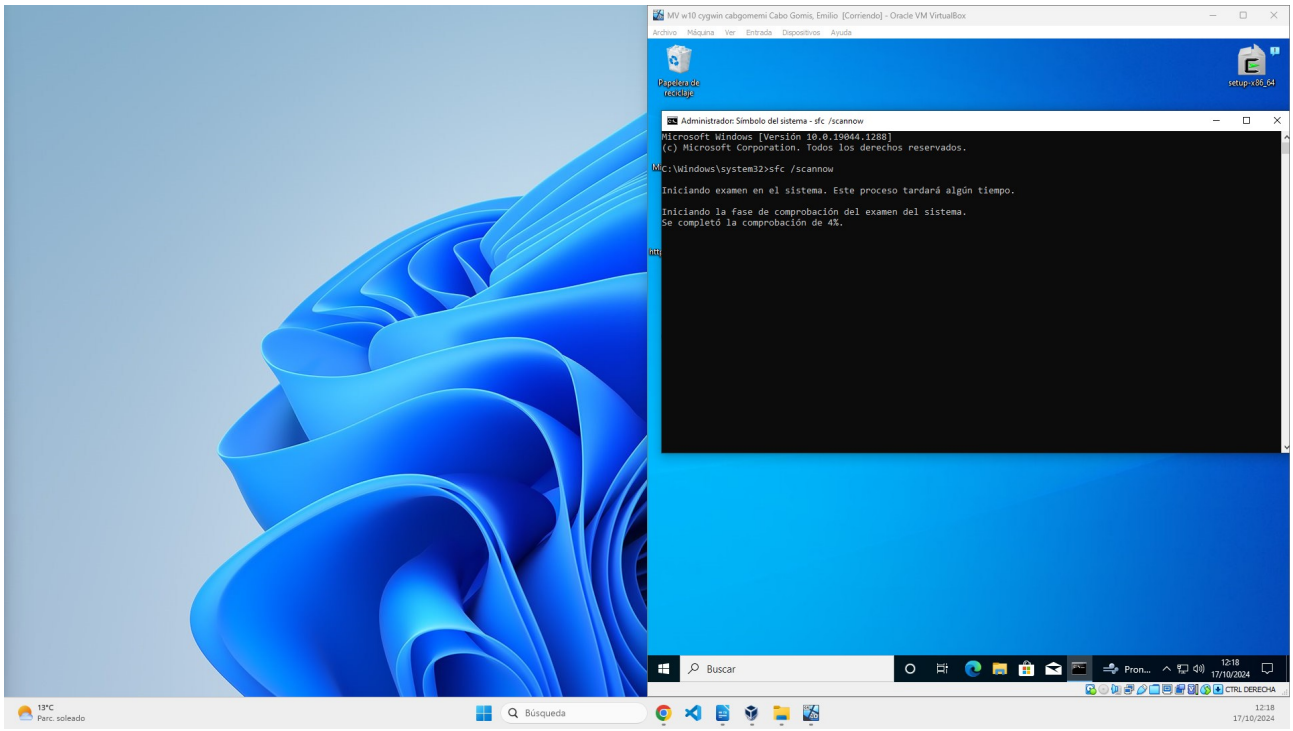
Windows

Abrimos un cmd con permisos de administrador.

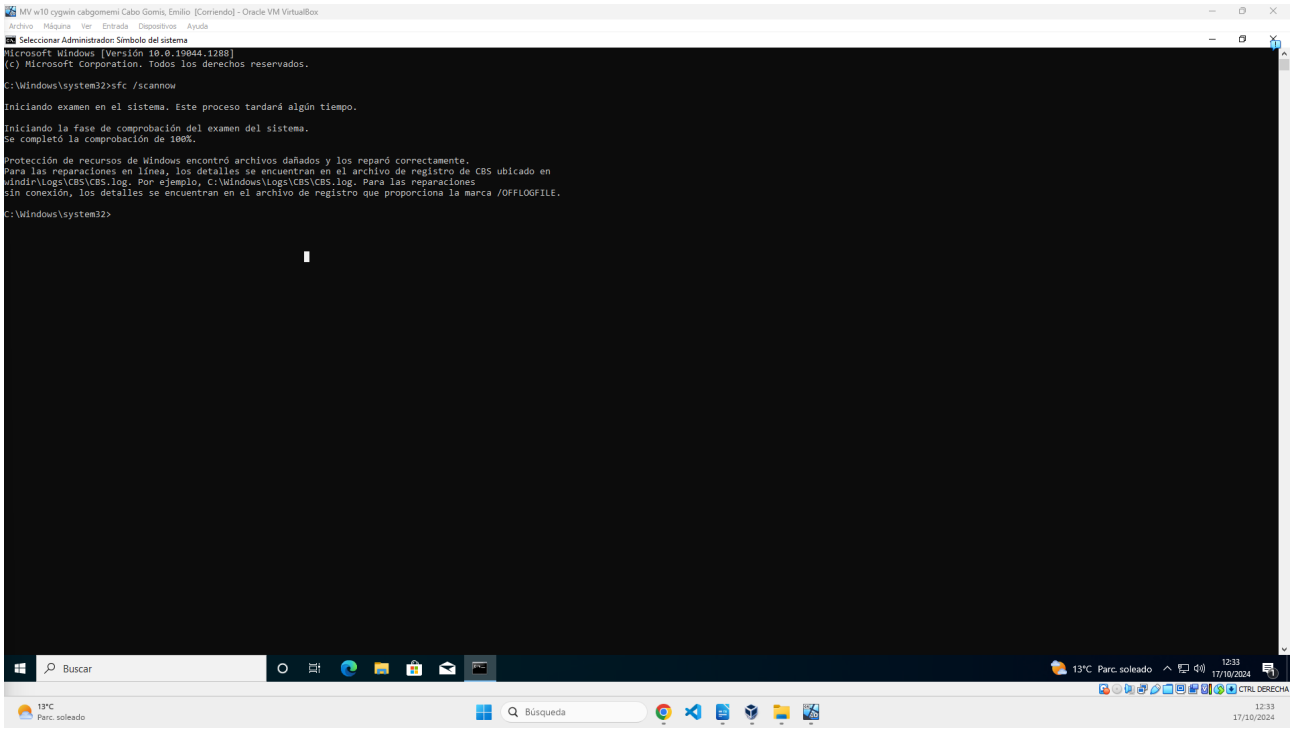
WIN > “cmd” > click derecho > permisos de administrador



Escribimos el comando **sfc /scannow**



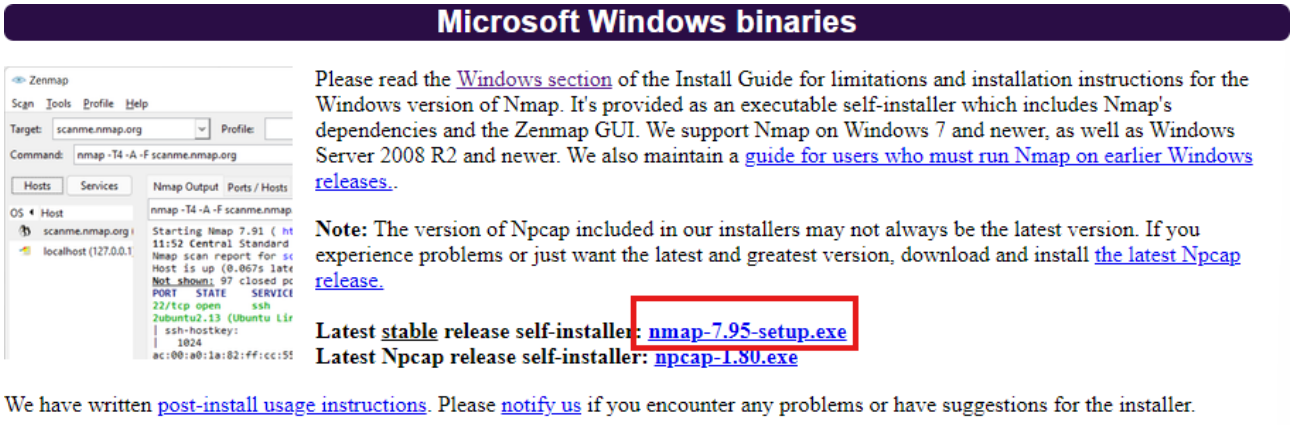
Resultado de la ejecución.



NMAP

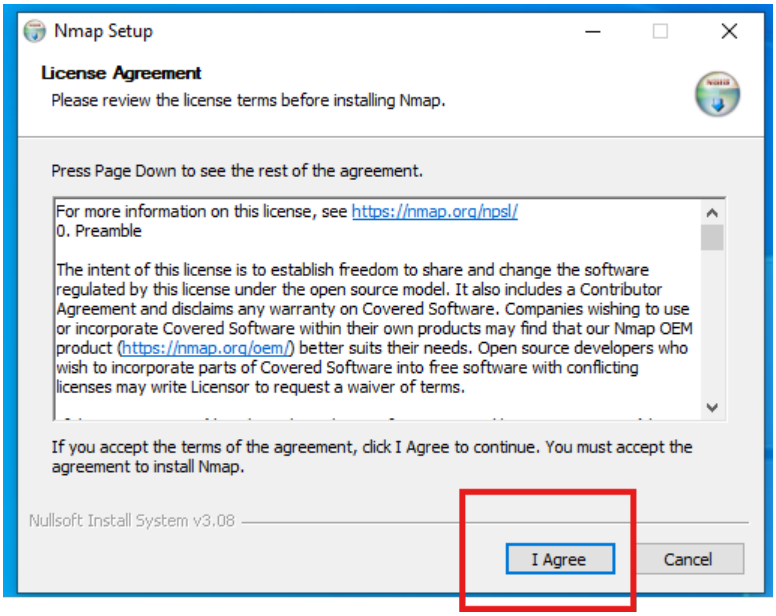
Descargamos el ejecutable de la página web de nmap https://nmap.org/download.html#windows

Descargamos el siguiente paquete.

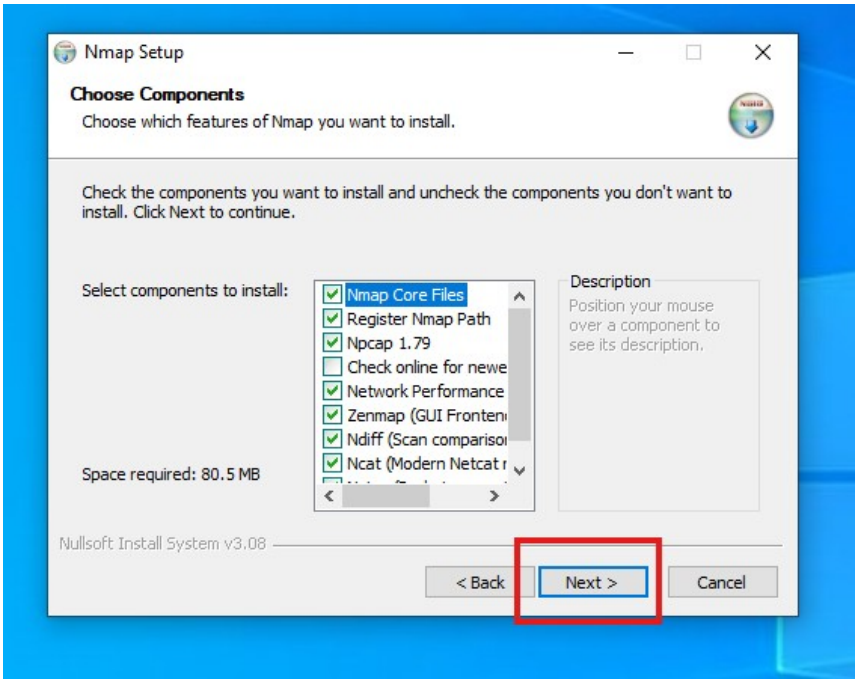


Ejecutamos el instalador.

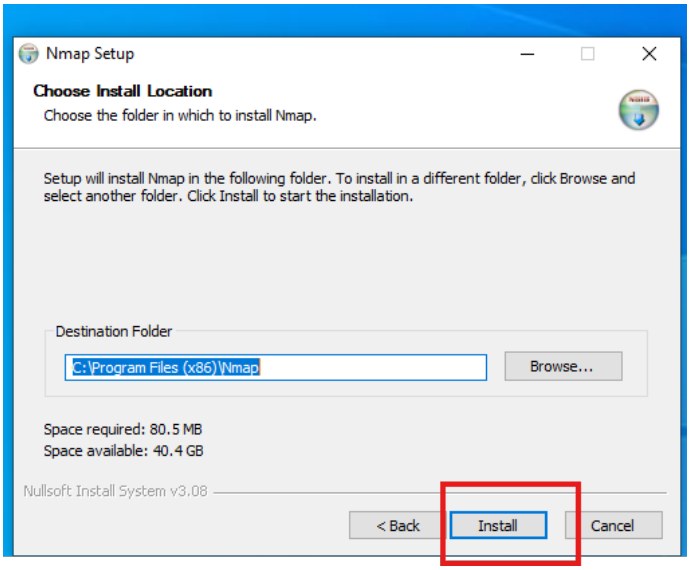
Le damos en “I agree”.



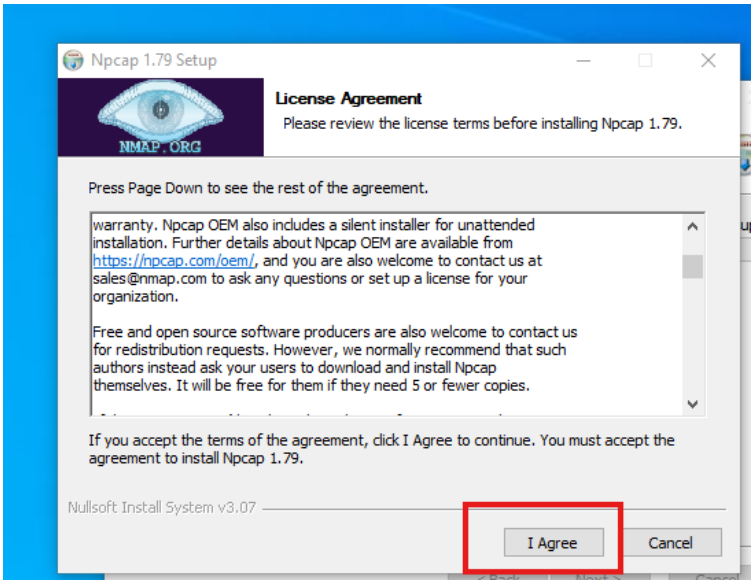
Le damos a next



Le damos a “install”



Aceptamos el acuerdo de licencia.



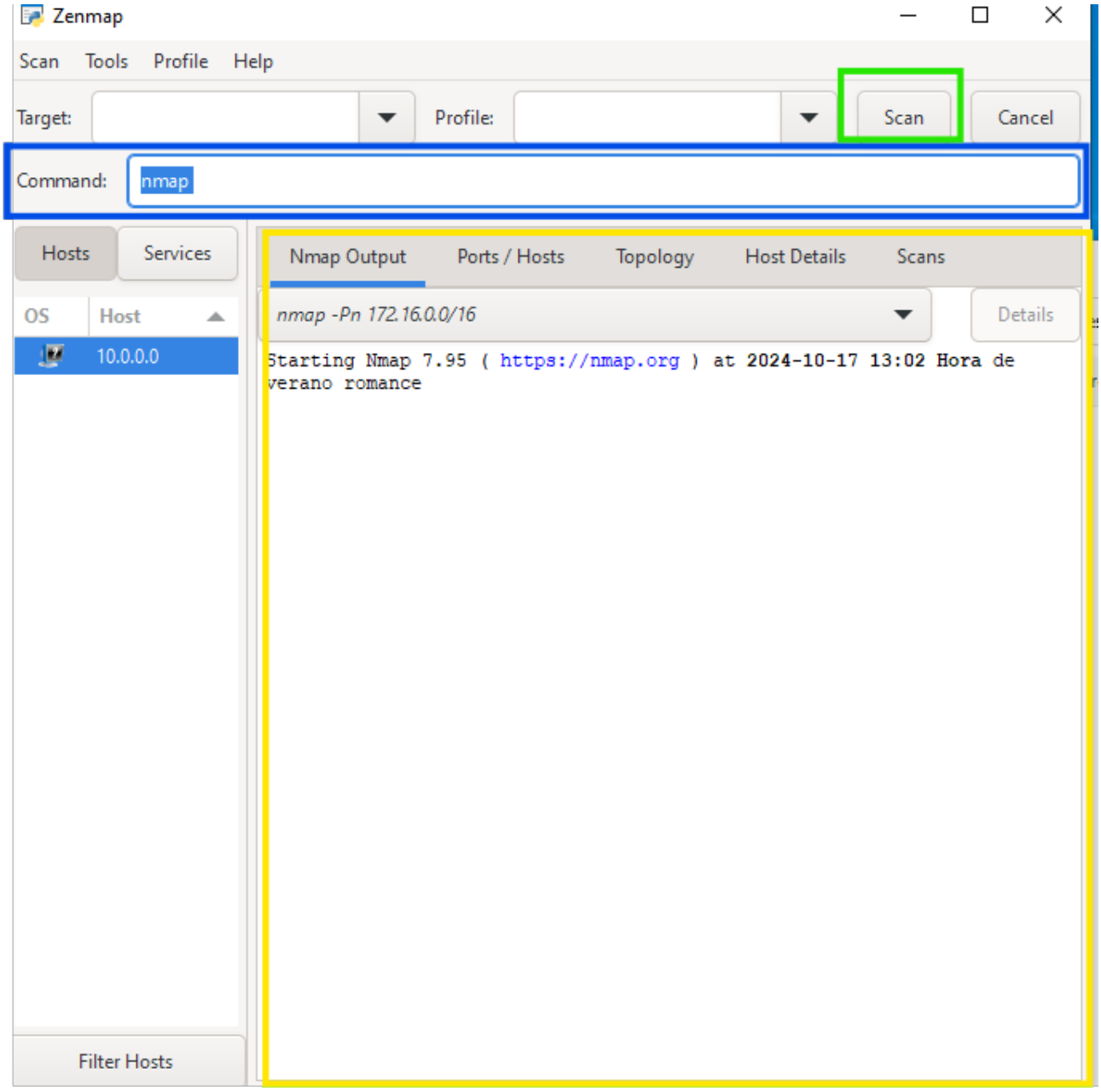
Ejecutamos el programa

Sección: Guía de empleo

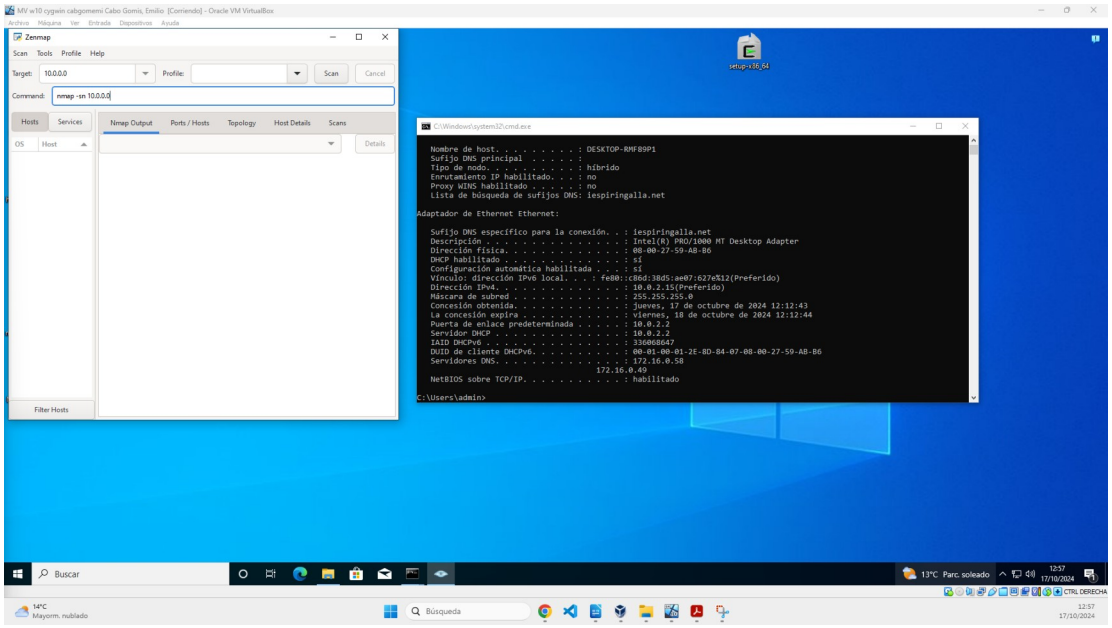
Introducimos el comando en la sección azul

Para escanear le damos al botón verde.

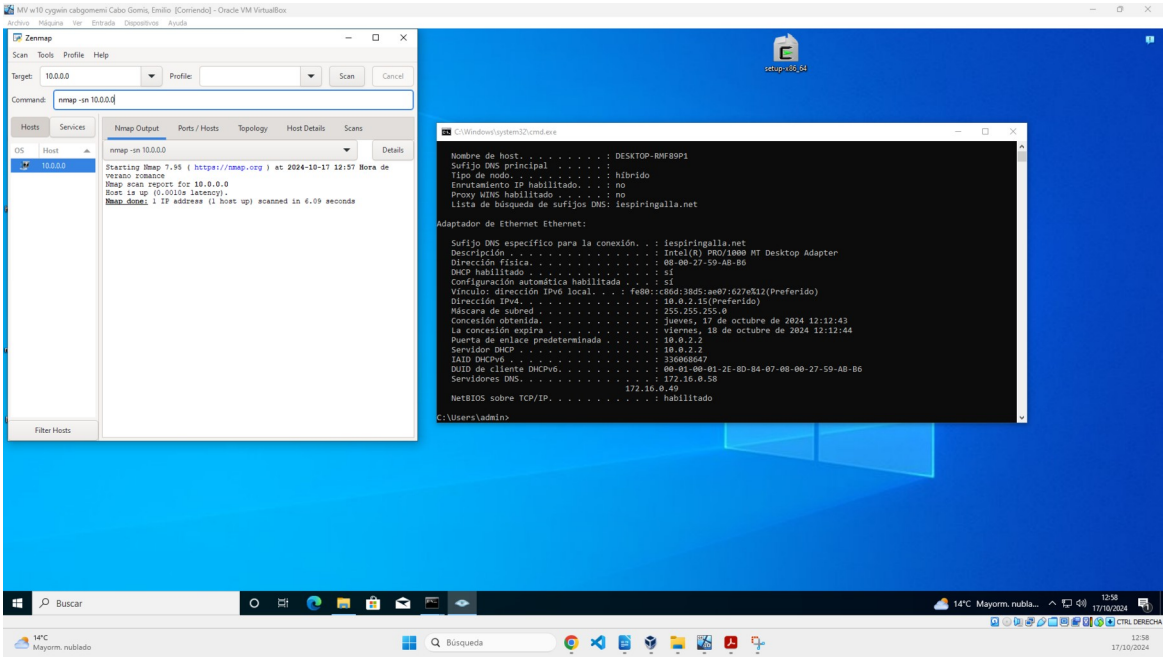
Para ver el resultado del escaneo vemos la sección amarilla.



Ponemos nuestra red como destino de nuestro escaneo.



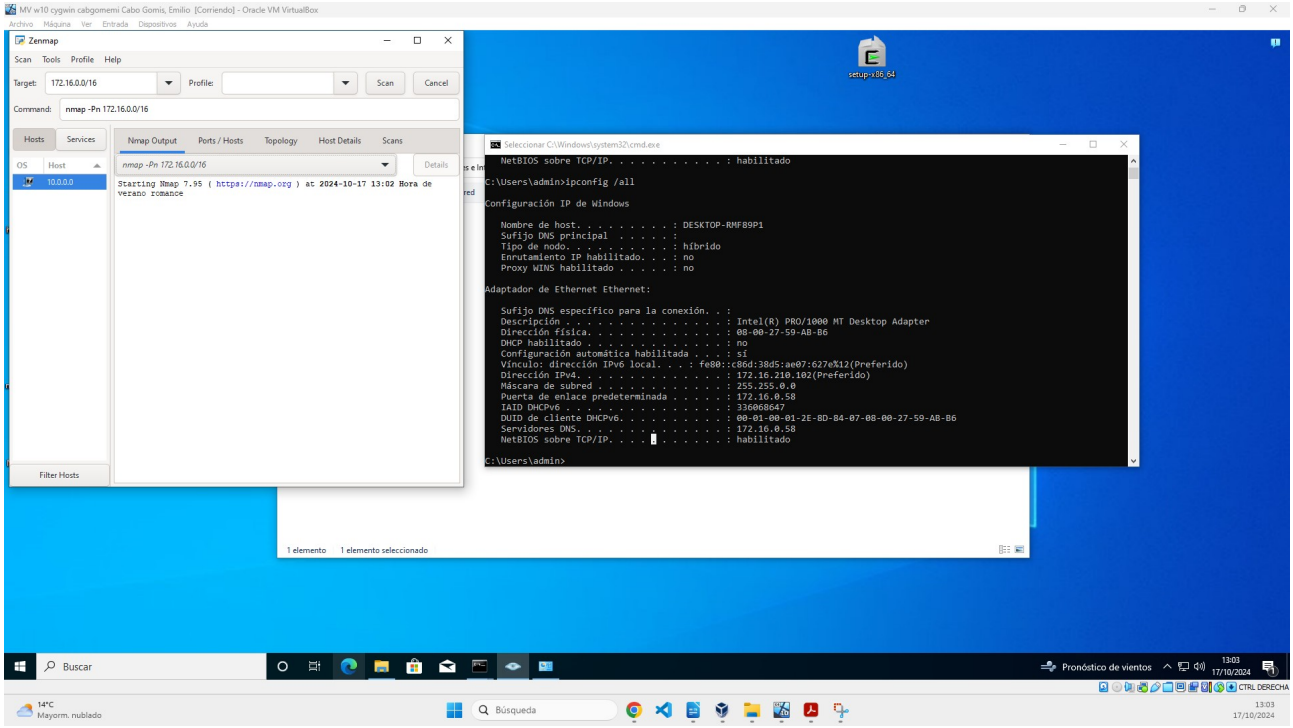
Este es el resultado de nuestro escaneo.



Este será un escaneo para ver que puertos tenemos abiertos.

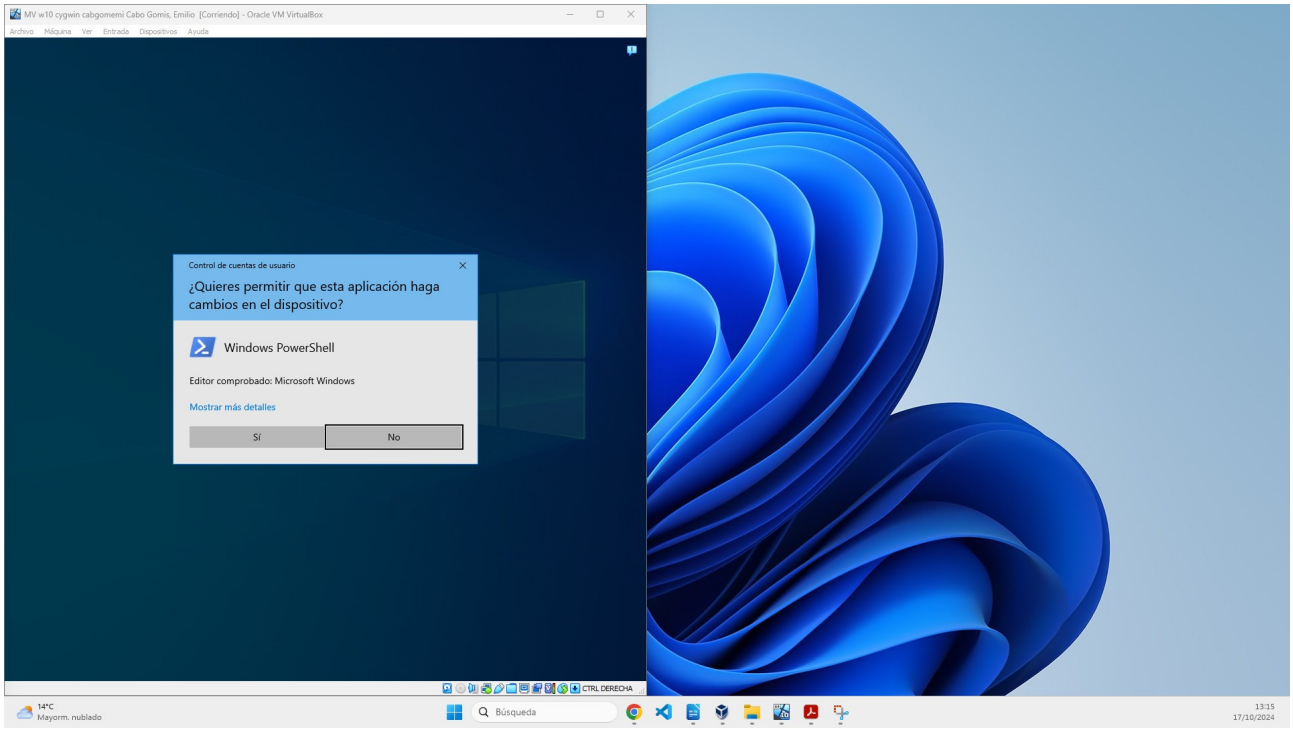
En este caso puse la red en adaptador puente.

Debido a que la res está asegurada no tenemos output.



MBSA

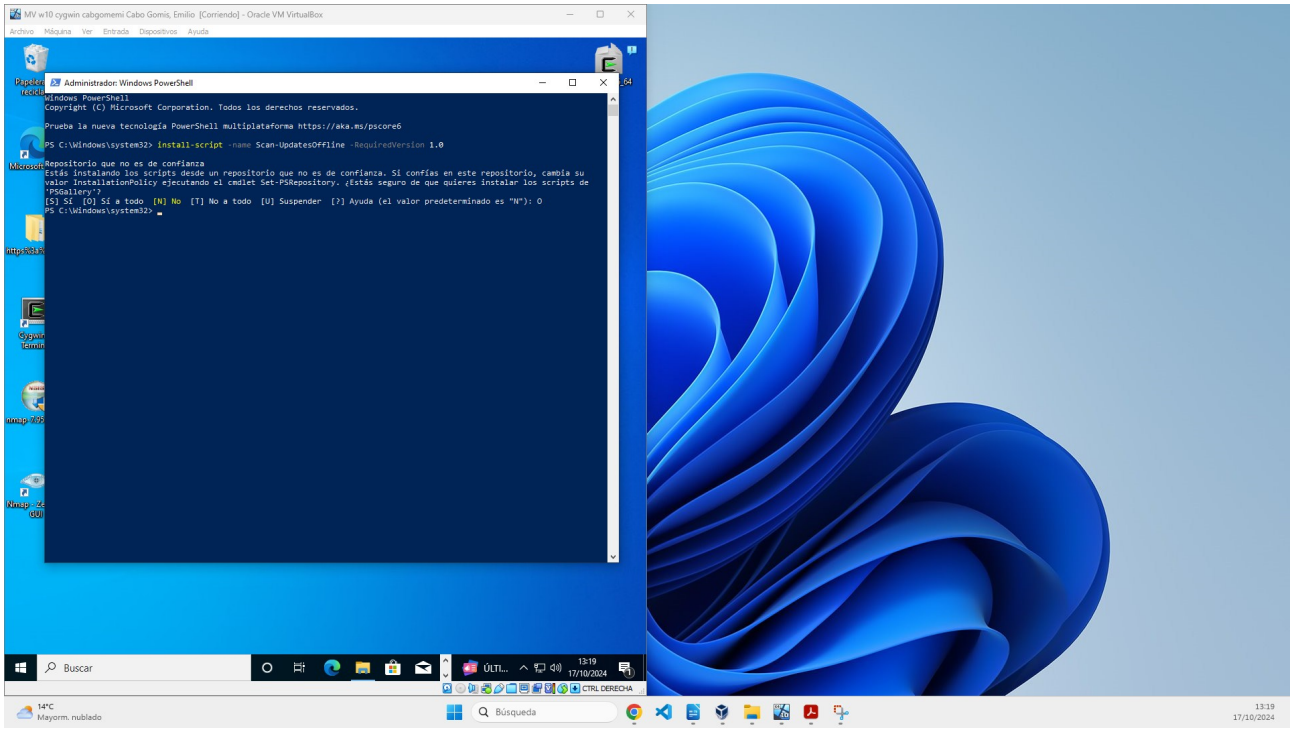
Pulsamos la tecla de Windows > escribimos “Powershell” > click derecho > ejecutar como administrador.



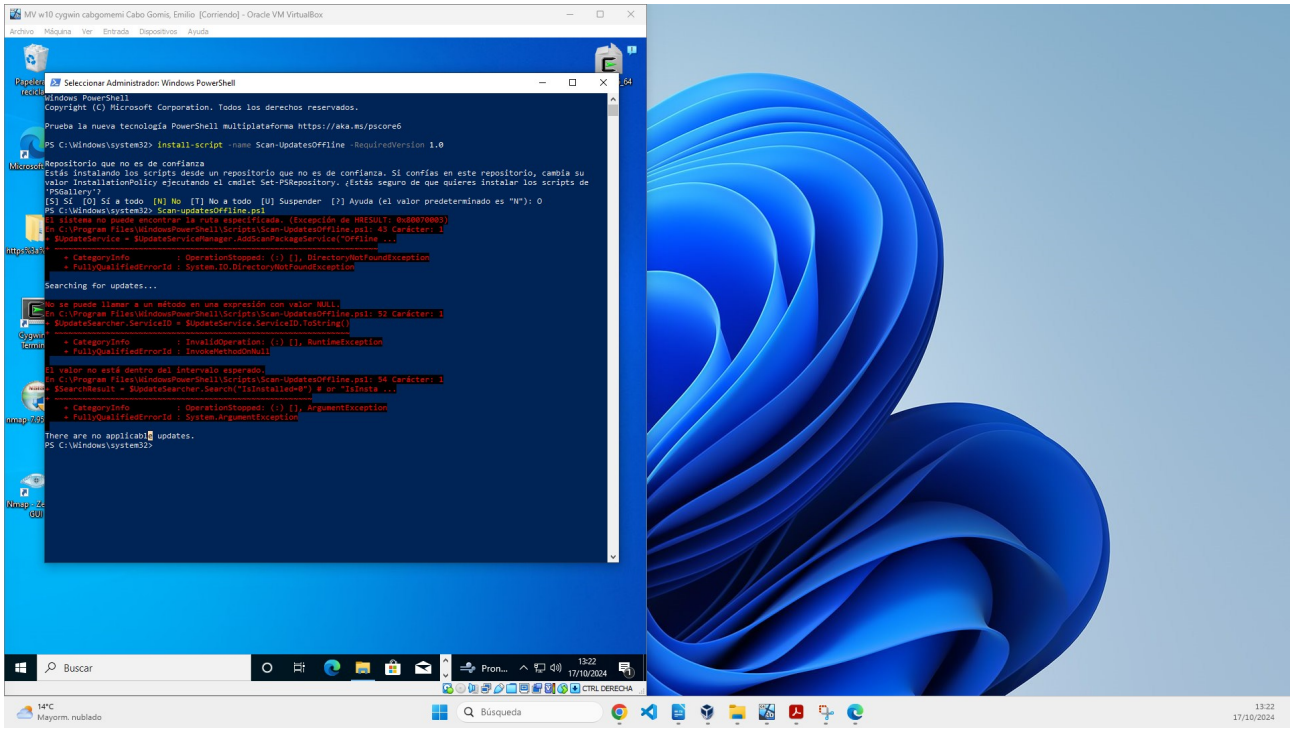
Instalamos el script.

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.

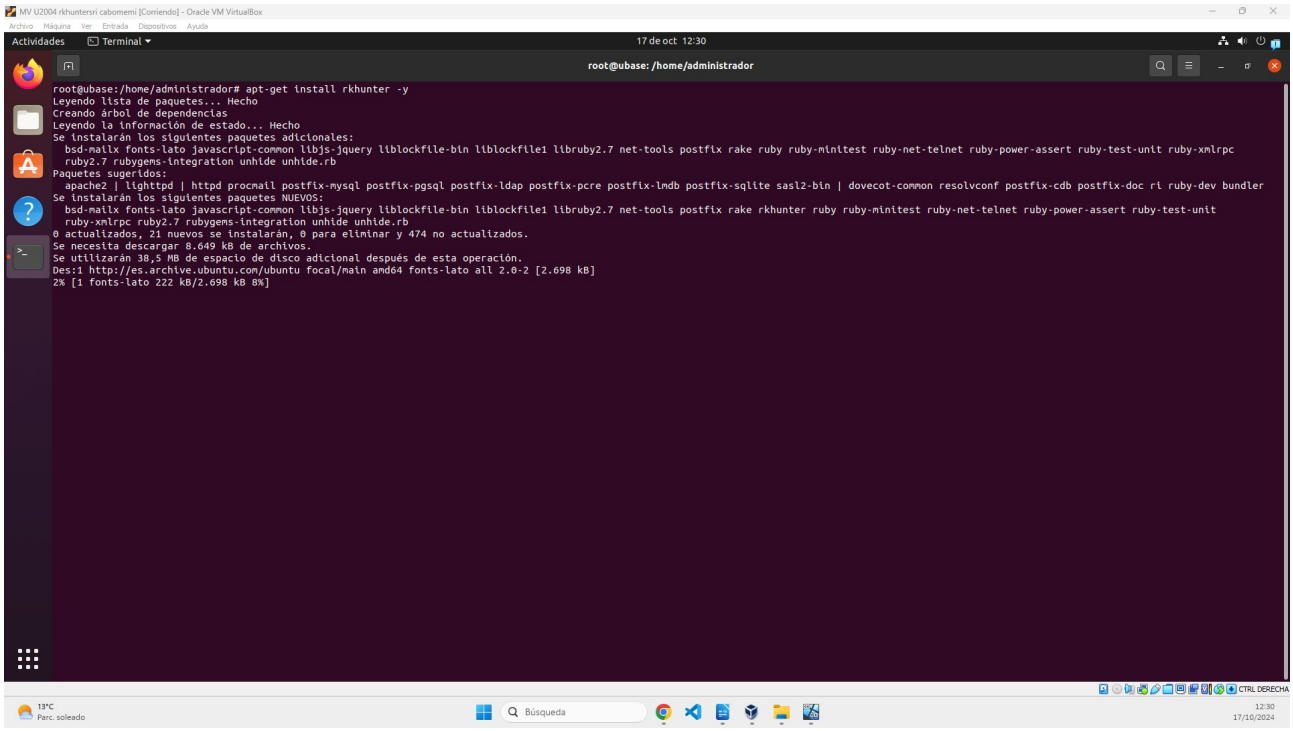
Linux

rkhunter

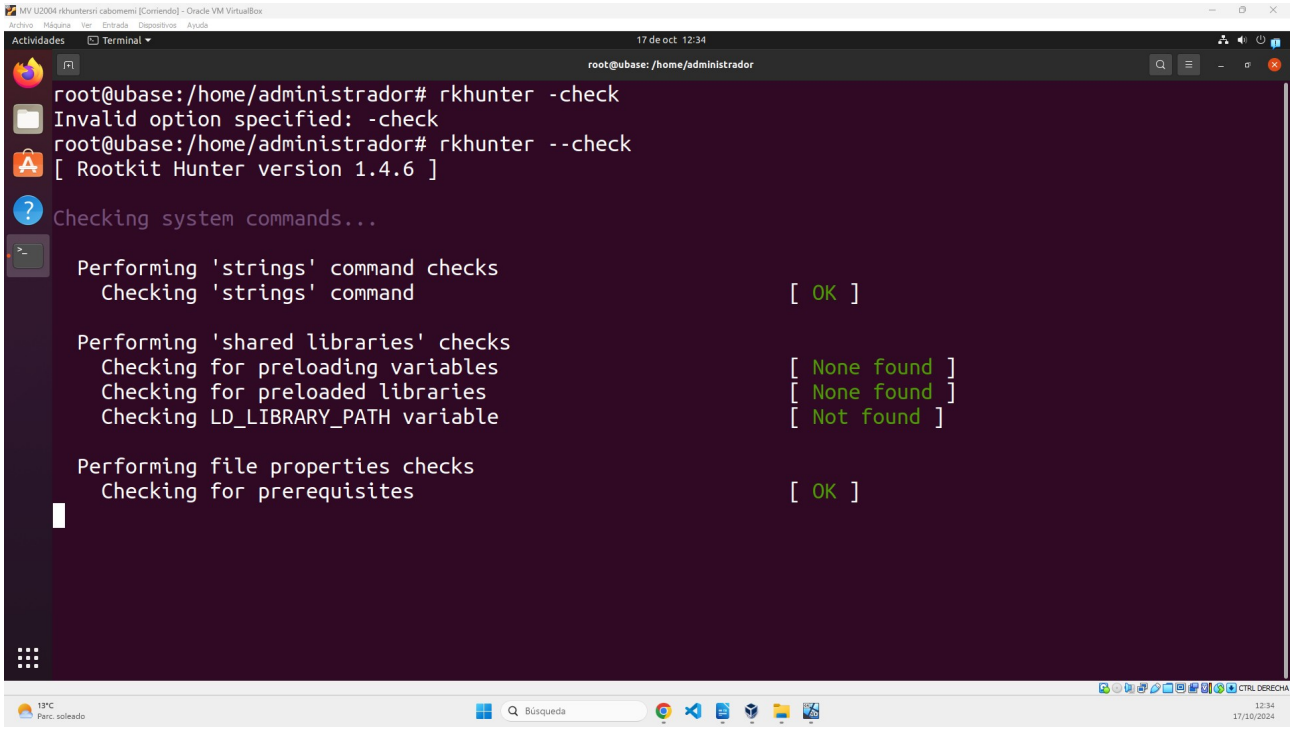
Abrimos un terminal mediante el shortcut ctrl + alt + t

Instalamos el programa necesario escribiendo el comando

sudo apt-get install rkhunter -y



Ejecutamos el comando rkhunter --check

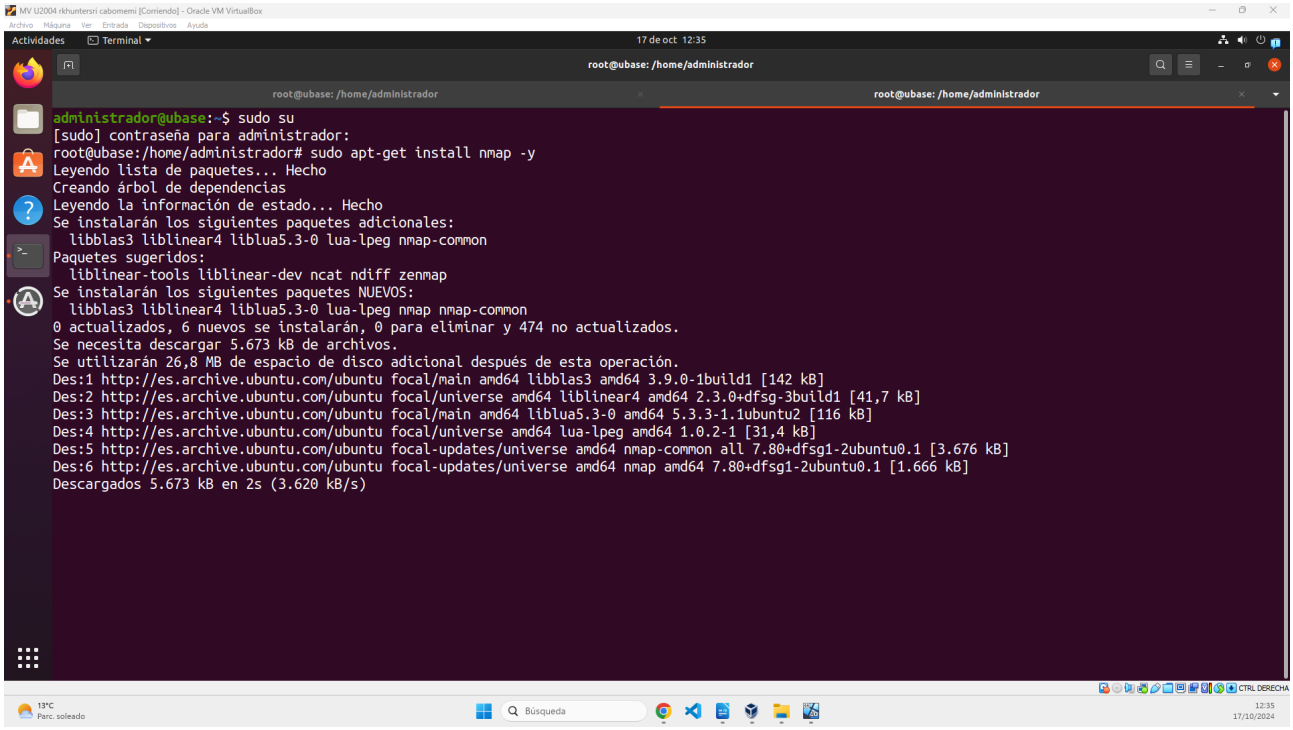


Nmap

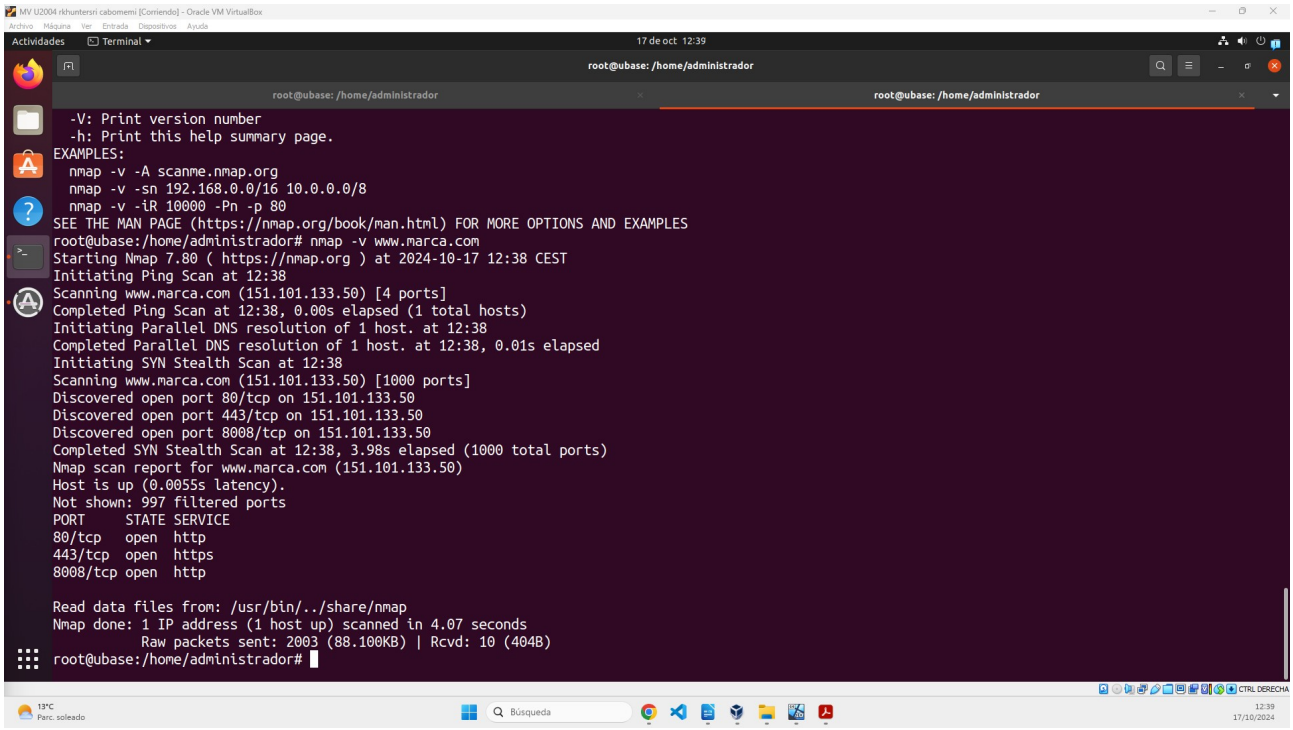
Abrimos un terminal mediante el shortcut ctrl + alt + t

Instalamos el programa necesario escribiendo el comando

sudo apt-get install nmap -y



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



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