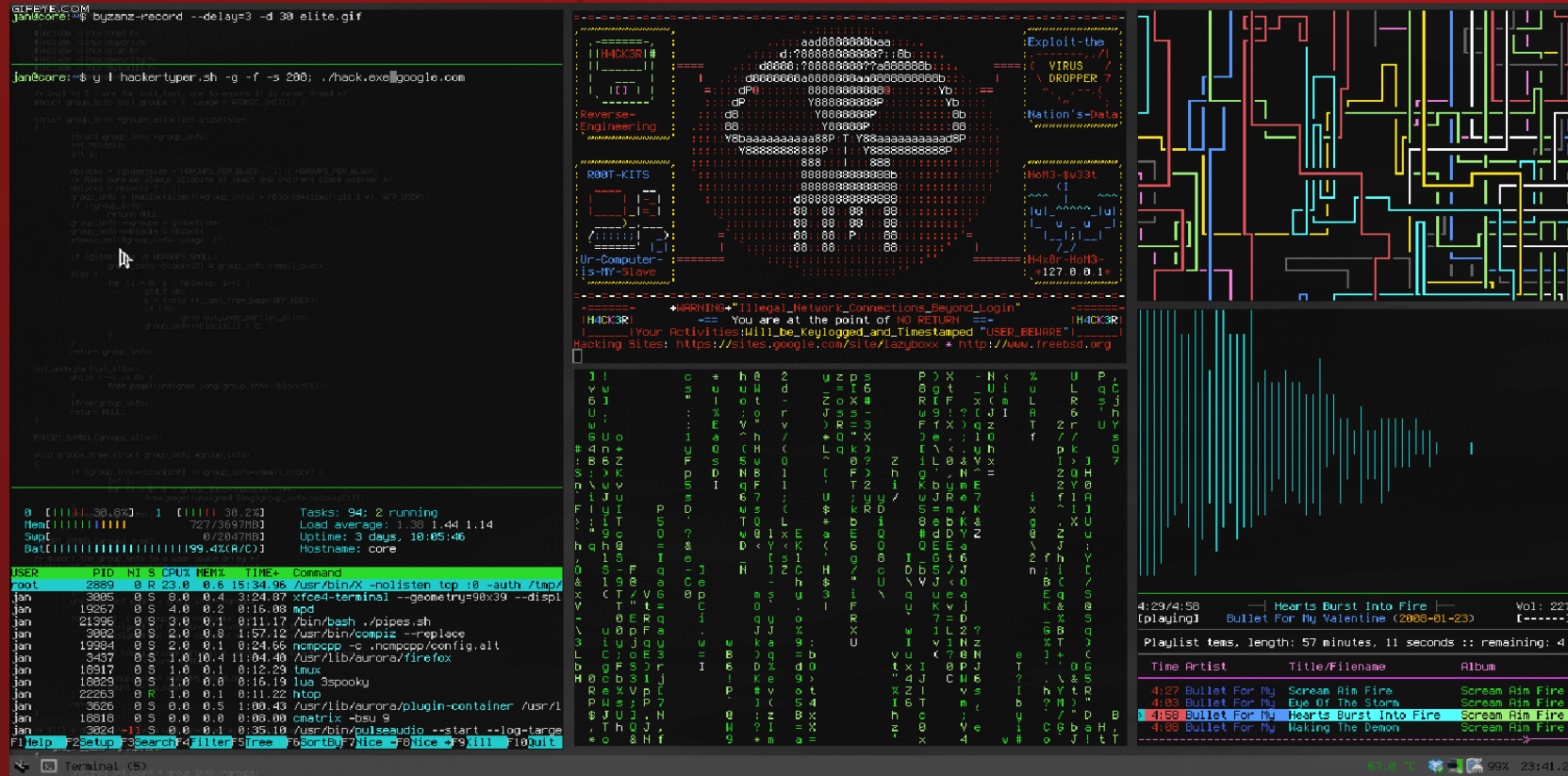


# KALI LINUX



Sergio Bravo Mora

# ¿QUÉ ES KALI LINUX?

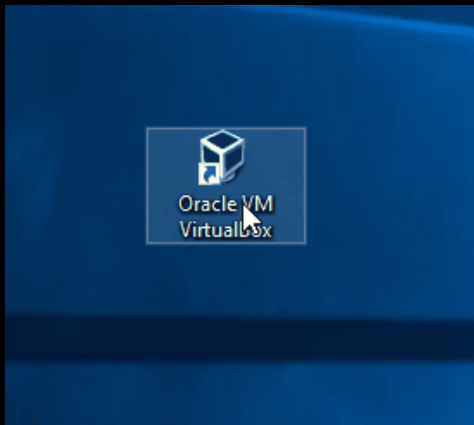


Kali Linux es una maquina virtual, que tiene una multitud de herramientas de hacking.

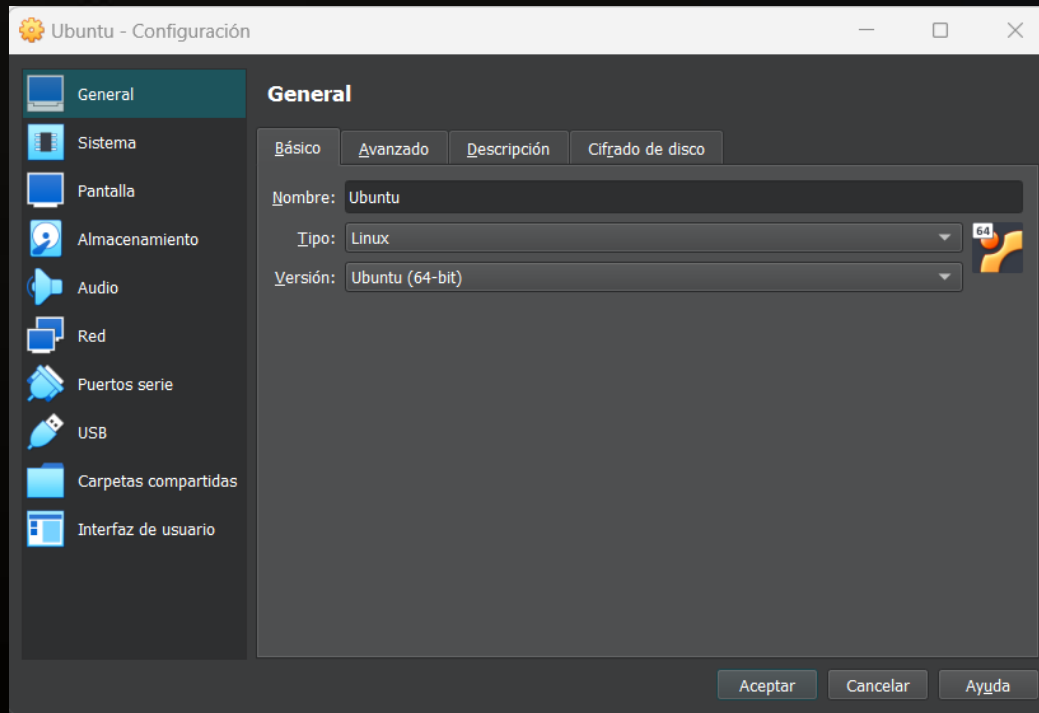
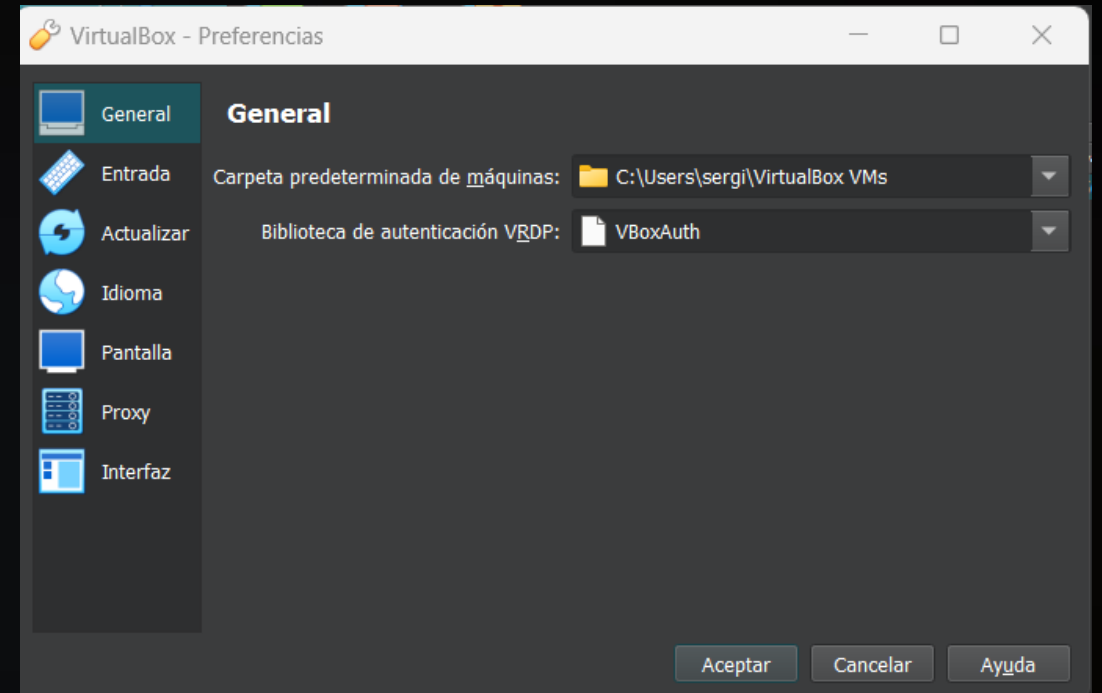
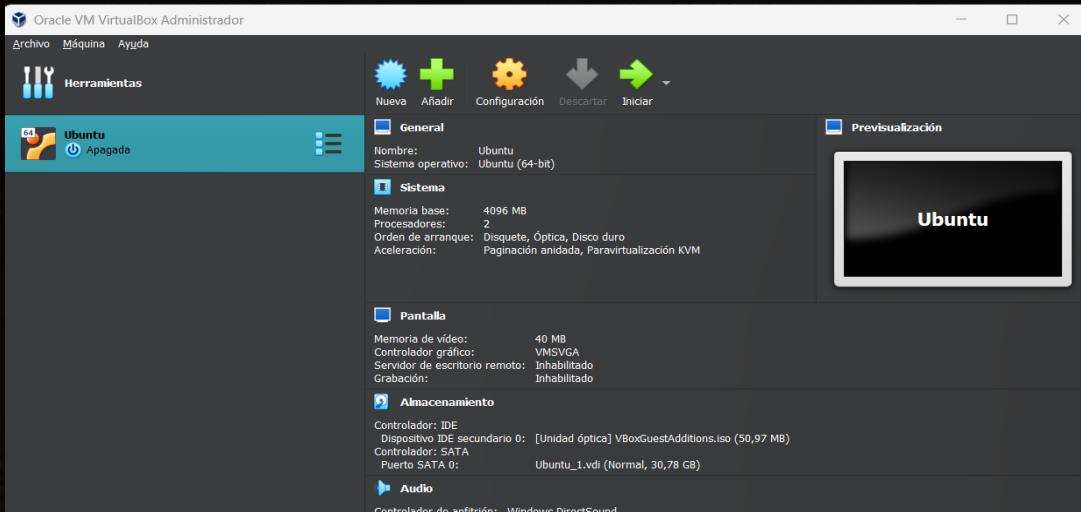
kali linux  
THE QUIETER YOU BECOME, THE MORE YOU ARE ABLE TO HEAR

# COMO DESCARGAR VIRTUAL BOX

- <https://www.virtualbox.org/>



<https://youtu.be/YFlowDwE-1E?feature=shared>



Una vez descargad0 nuestro virtual box, abra que seguir unos pasos para poder configurarlo bien, como por ejemplo, configuración de la pantalla, la memoria Ram que se le puede asignar y etc.

# COMO INSTALAR KALI



ISO.

MEMORIA.

ETHERNET.

ALMACENAMIENTO.

DISCO PARTICIONADOS.

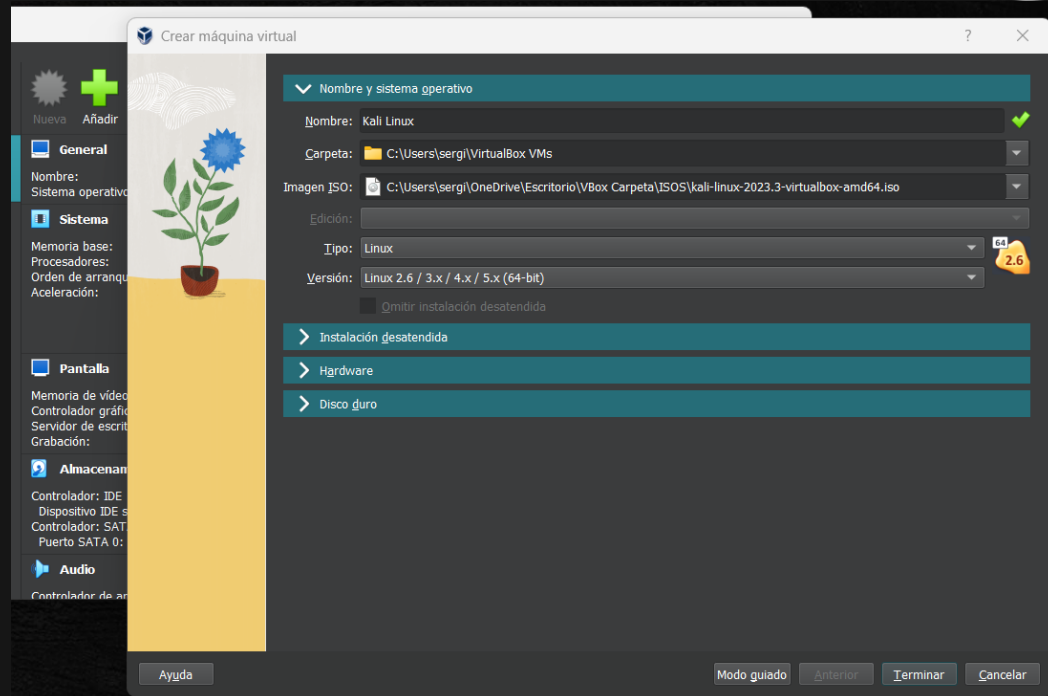
# DONDE DESCARGAR LA ISO



En el enlace que he dejado abajo a la izquierda se puede descargar nuestra maquina virtual Kali Linux, y la captura de la izquierda es la que yo recomiendo descargar.

- <https://www.kali.org/get-kali/#kali-virtual-machines>

# COMO AGREGAR LA ISO AL VIRTUAL BOX

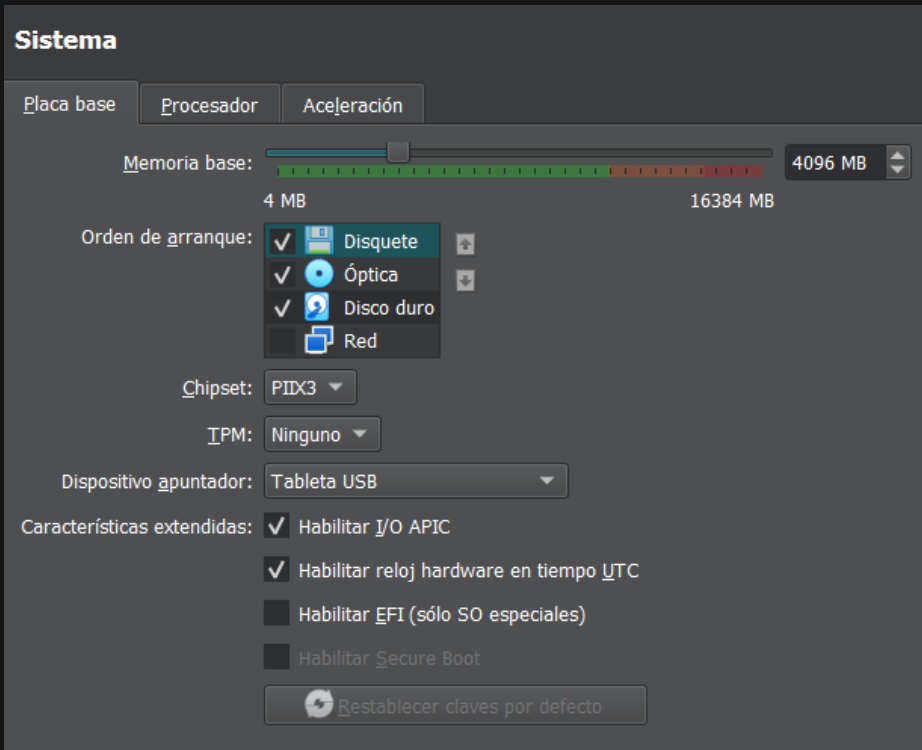


Una vez descargada nuestra Kali Linux debemos seguir unos pasos para poder configurarla bien para así hacer que funcione bien y de rendimiento.



# CONFIGURACIÓN DE MEMORIA


Para la Memoria RAM, yo le he asignado 4GB, depende del portátil o torre que tengas le podremos asignar mas o menos memoria RAM.





# CONFIGURACIÓN DE ETHERNET

En el tema de ETHERNET, yo he usado el de clase, pero sin problema se le puede asignar cualquier wifi etc.



**Red**

Adaptador 1   Adaptador 2   Adaptador 3   Adaptador 4

☒ **H**abilitar adaptador de red


Conectado a: Adaptador puente

Nombre: TP-LINK Gigabit Ethernet USB Adapter

▼ **A**vanzado

Tipo de adaptador: Intel PRO/1000 MT Desktop (82540EM)

Modo promiscuo: Denegar

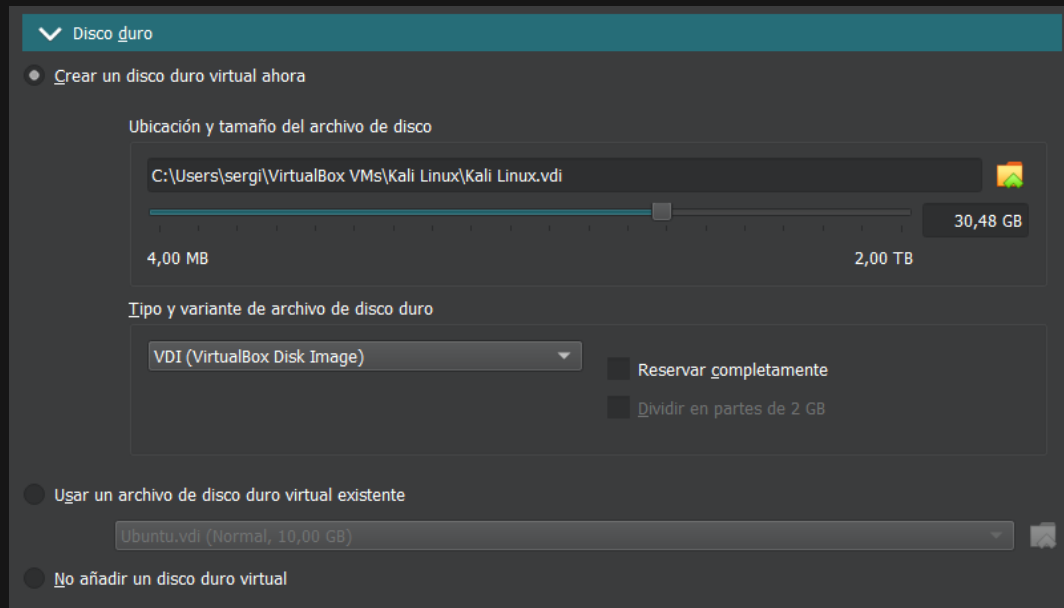
Dirección MAC: 080027AA8390 

☒ **C**able conectado

Aceptar   Cancelar   Ayuda

# CONFIGURACIÓN DE ALMACENAMIENTO

El almacenamiento, es el espacio que le vamos a dar a nuestra maquina virtual y el espacio que usaremos para nuestro trabajo etc. Por eso yo le he asignado 30GB ya que no la usaremos mucho.



▼ Disco duro

● Crear un disco duro virtual ahora

Ubicación y tamaño del archivo de disco

C:\Users\sergi\VirtualBox VMs\Kali Linux\Kali Linux.vdi

4,00 MB 2,00 TB 30,48 GB

Tipo y variante de archivo de disco duro

VDI (VirtualBox Disk Image)

Reservar completamente

Dividir en partes de 2 GB

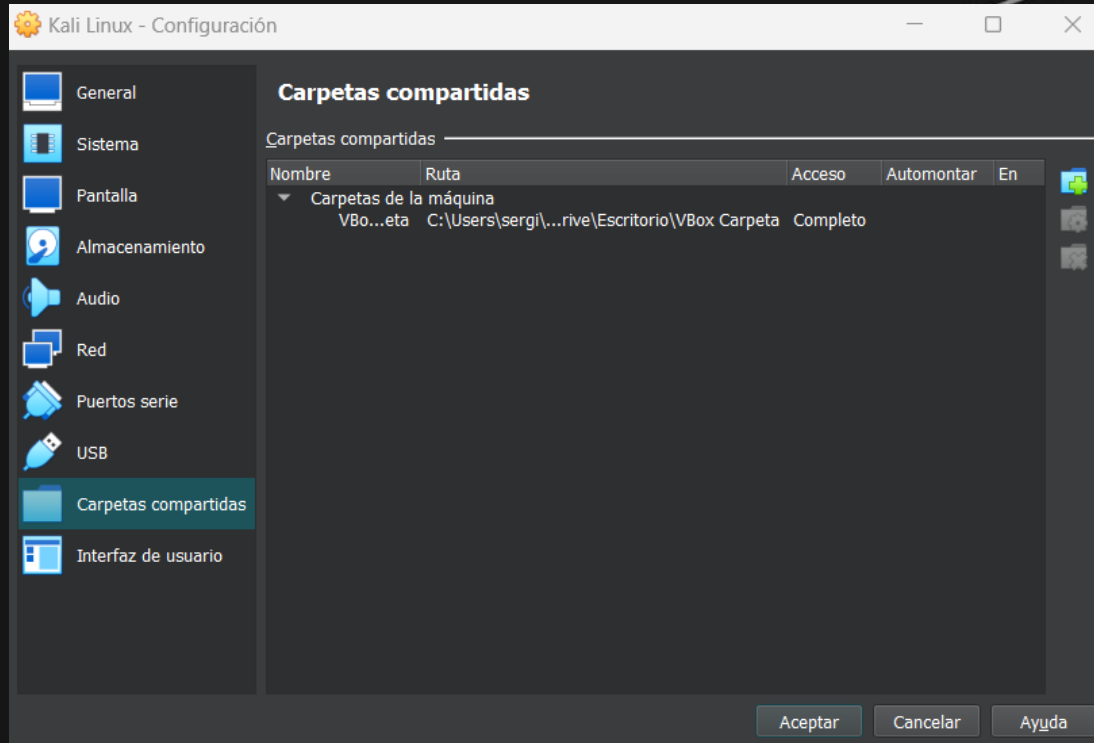
● Usar un archivo de disco duro virtual existente

Ubuntu.vdi (Normal, 10,00 GB)

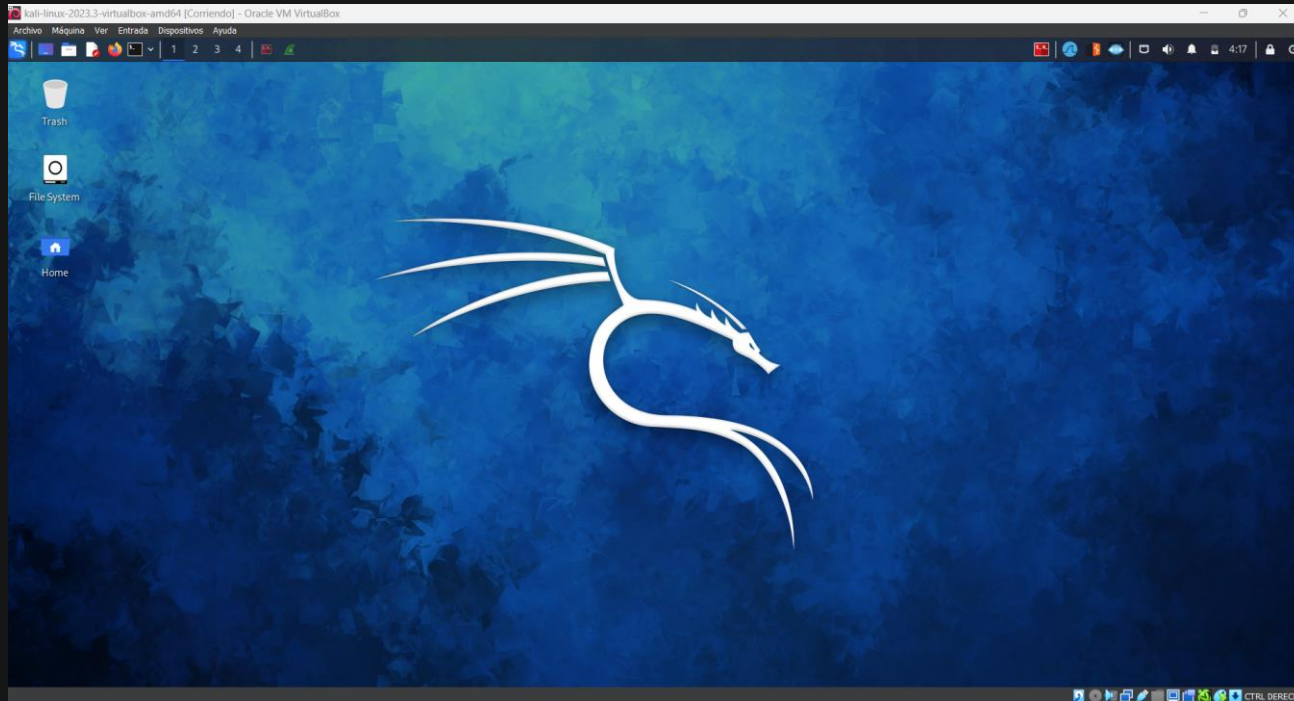
● No añadir un disco duro virtual

# CONFIGURACIÓN COMPARTICIÓN DE CARPETAS

En este apartado os enseñare como se puede crear una carpeta compartida para poder pasarnos cosas de nuestro propio ordenador o portátil a nuestra maquina virtual y viceversa.(Recomiendo ponerlo en Bidireccional).



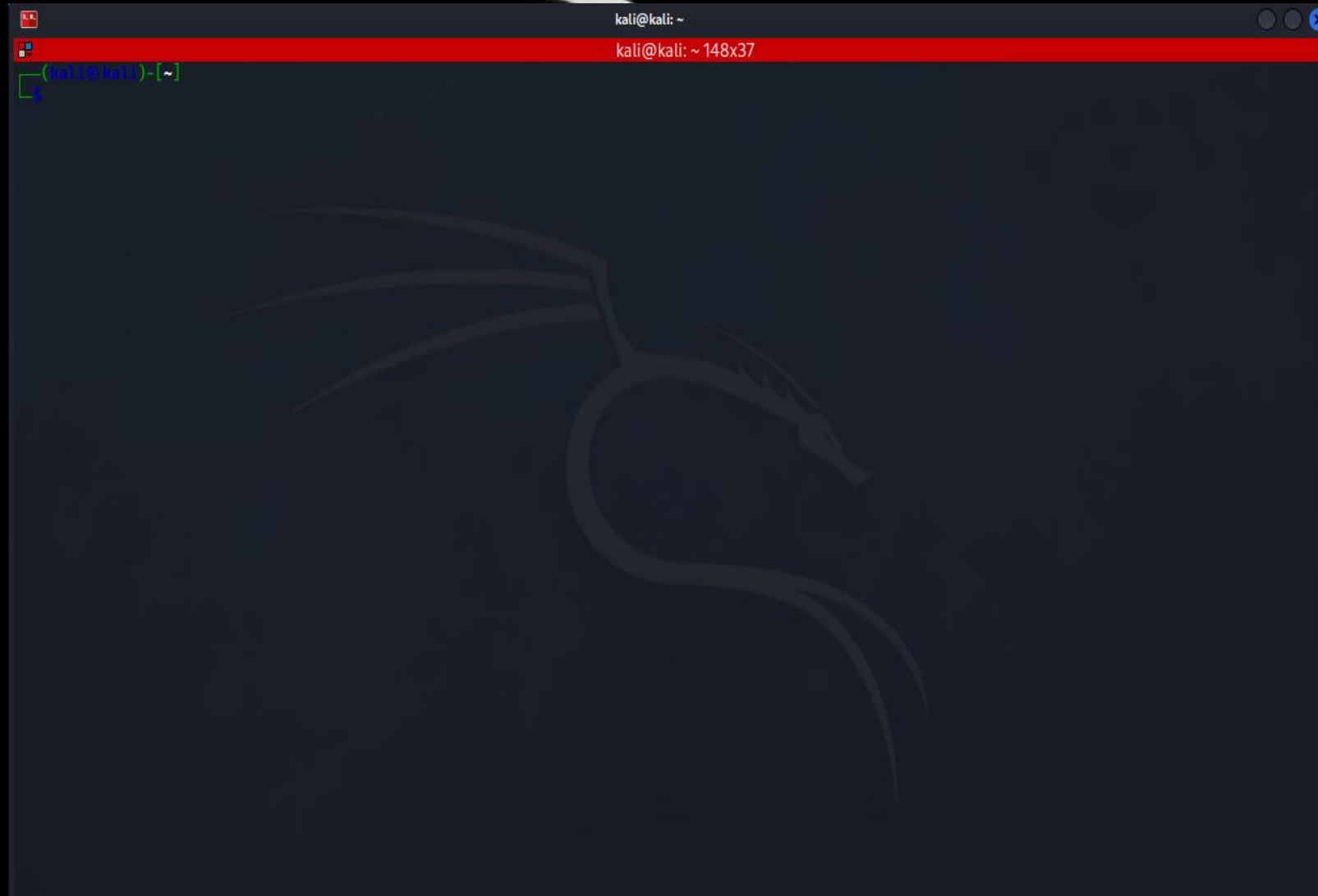
# KALI LINUX



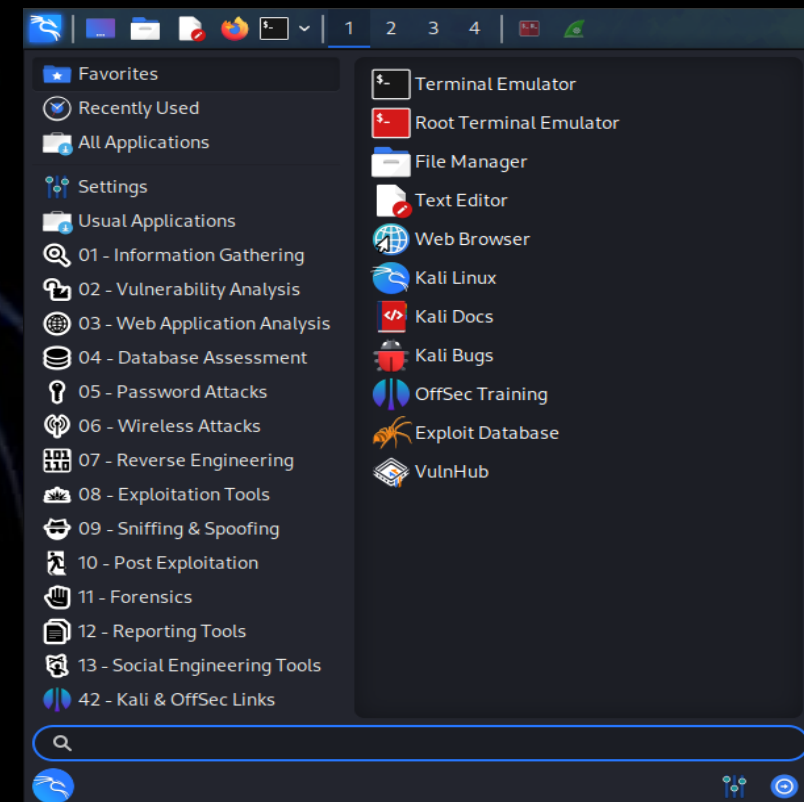
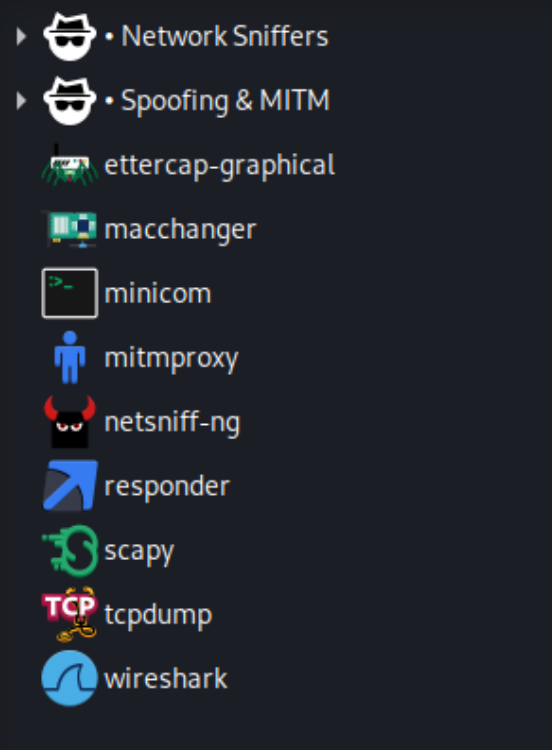
Una vez configurada nuestra Kali Linux, toca ejecutarla, y así se vería nuestro entorno dentro de la maquina virtual.

# TERMINAL

La terminal,  
es nuestro  
entorno de  
trabajo, ya  
que en ella  
se pueden  
hacer  
multitud de  
cosas con  
una serie de  
comando  
etc.



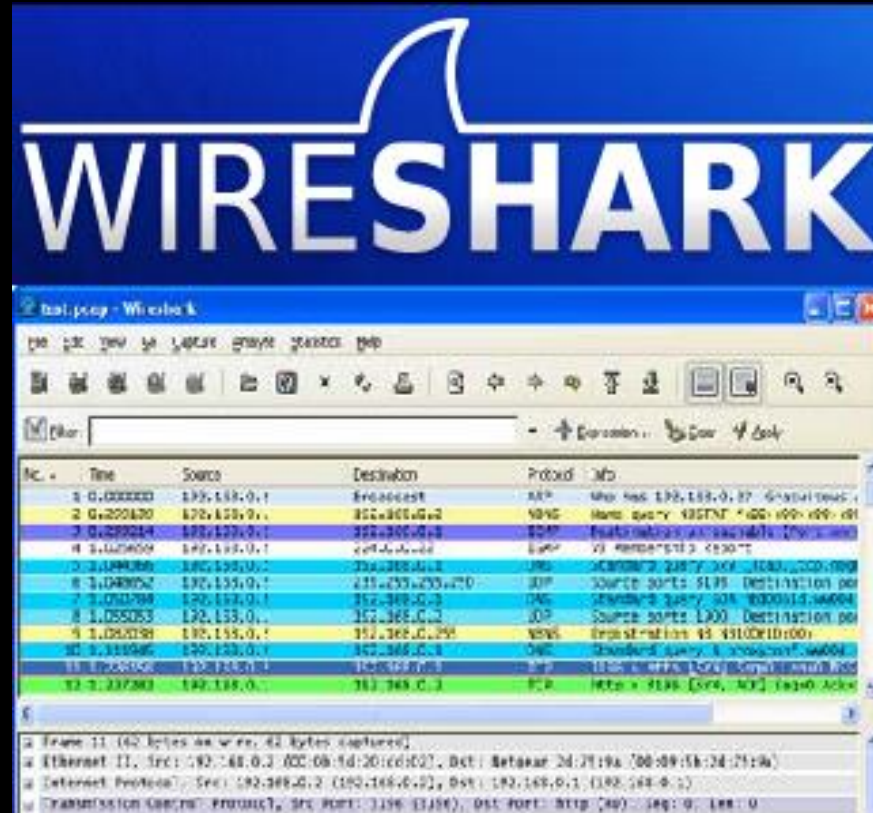
# HERRAMIENTAS DE HACKING





# HERRAMIENTAS DE HACKING

Las herramientas de hacking son usadas para diferentes tipos de hacking, ya sea forense, spoofing, MITM, o escaneos de red y muchos mas tipos de hacking.

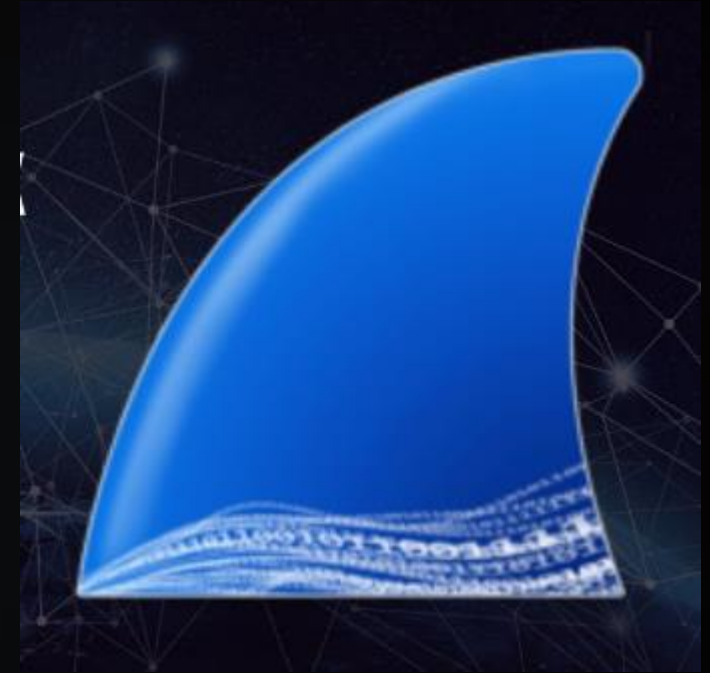
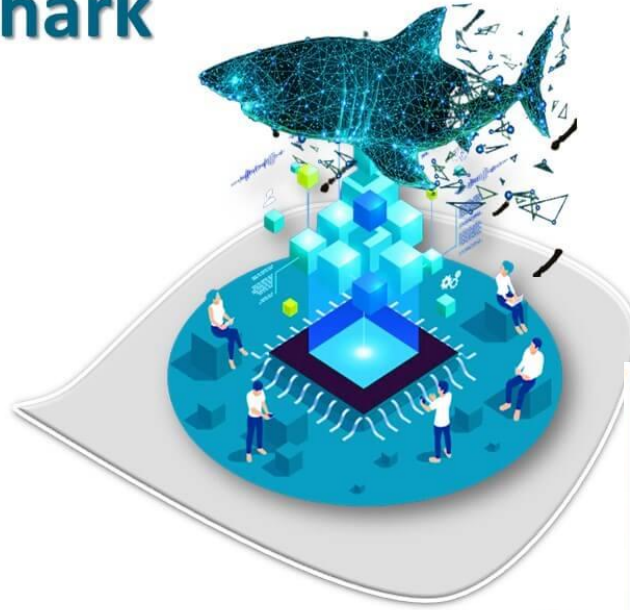


En la siguiente diapositiva, os mostrare Wireshark, una aplicación de hacking el cual se puede hacer escaneos de red y por así decirlo un seguimiento de cualquier ordenador que este en nuestra red, podríamos ver donde se mete en internet incluso, ver sus usuarios y contraseñas.



# WHIRESHARK

## Kali Linux Wireshark



\*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length
2	0.000018035	172.24.63.50	172.24.48.1	DNS	8
3	0.044615102	172.24.48.1	172.24.63.50	DNS	21
4	0.045852665	172.24.48.1	172.24.63.50	DNS	16
5	0.047579187	172.24.63.50	195.154.174.209	NTP	9
6	0.059622993	195.154.174.209	172.24.63.50	NTP	9
7	2.681316440	fe80::215:5dff:fede...	ff02::2	ICMPv6	6

# ESCANEEO DE RED TCP

```
kali@kali: ~  
kali@kali: ~ 106x44  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 24 bytes 1240 (1.2 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 24 bytes 1240 (1.2 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)~  
$ nmap -P 10.0.2.15/8  
Command 'nmap' not found, did you mean:  
  command 'wamp' from deb python3-autobahn  
  command 'nam' from deb nam  
  command 'pamp' from deb paml  
  command 'nmap' from deb nmap  
  command 'nama' from deb nama  
Try: sudo apt install <deb name>  
  
(kali@kali)~  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255  
    inet6 fe80::34e0:d8ad:2eac:5da9 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)  
    RX packets 6833 bytes 9704049 (9.2 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 1140 bytes 106594 (104.0 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 24 bytes 1240 (1.2 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 24 bytes 1240 (1.2 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)~  
$
```

\*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
2161	16.894202002	10.0.2.15	104.18.5.159	TCP	54	47518 → 443 [ACK] Seq=
2162	16.907138779	104.18.5.159	10.0.2.15	TLSv1.3	85	Application Data
2163	16.907213395	10.0.2.15	104.18.5.159	TCP	54	47518 → 443 [ACK] Seq=
2164	16.930787857	10.0.2.15	142.250.184.163	QUIC	82	Handshake, DCID=e659b6
2165	16.935543773	10.0.2.15	142.250.184.163	QUIC	82	Handshake, DCID=e659b6
2166	16.945554073	142.250.184.163	10.0.2.15	QUIC	85	Handshake, DCID=a015d0
2167	16.951022017	142.250.184.163	10.0.2.15	QUIC	85	Handshake, DCID=a015d0
2168	16.961383049	10.0.2.15	142.250.184.170	TLSv1.3	118	Change Cipher Spec, Ap
2169	16.961824721	10.0.2.15	142.250.184.170	TLSv1.3	224	Application Data
2170	16.962140277	142.250.184.170	10.0.2.15	TCP	60	443 → 54270 [ACK] Seq=
2171	16.962526743	10.0.2.15	142.250.200.131	OCSP	473	Request
2172	16.972949618	142.250.184.170	10.0.2.15	TLSv1.3	668	Application Data, Appl
2173	16.973074065	10.0.2.15	142.250.184.170	TCP	54	54270 → 443 [ACK] Seq=
2174	16.973532979	10.0.2.15	142.250.184.170	TLSv1.3	85	Application Data
2175	16.975879358	142.250.184.170	10.0.2.15	TLSv1.3	85	Application Data
2176	16.984169589	10.0.2.15	142.250.184.163	QUIC	82	Handshake, DCID=e659b6
2177	16.984310187	10.0.2.15	142.250.184.163	QUIC	82	Handshake, DCID=e659b6
2178	16.998578401	142.250.184.163	10.0.2.15	QUIC	84	Handshake, DCID=a015d0
2179	17.017235849	10.0.2.15	142.250.184.170	TCP	54	54270 → 443 [ACK] Seq=
2180	17.029209396	10.0.2.15	142.250.184.163	QUIC	82	Handshake, DCID=e659b6
2181	17.029462179	10.0.2.15	142.250.184.163	QUIC	82	Handshake, DCID=e659b6
2182	17.042466467	142.250.184.163	10.0.2.15	QUIC	84	Handshake, DCID=a015d0
2183	17.064261018	10.0.2.15	104.18.5.159	TLSv1.3	255	Application Data
2184	17.069766880	10.0.2.15	142.250.184.163	QUIC	82	Handshake, DCID=e659b6
2185	17.069988772	10.0.2.15	142.250.184.163	QUIC	82	Handshake, DCID=e659b6
2186	17.082743744	142.250.184.163	10.0.2.15	QUIC	84	Handshake, DCID=a015d0

Frame 2168: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface eth0  
Ethernet II, Src: PcsCompu\_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: 10.0.2.15  
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.250.200.131  
Transmission Control Protocol, Src Port: 54270, Dst Port: 443  
Transport Layer Security

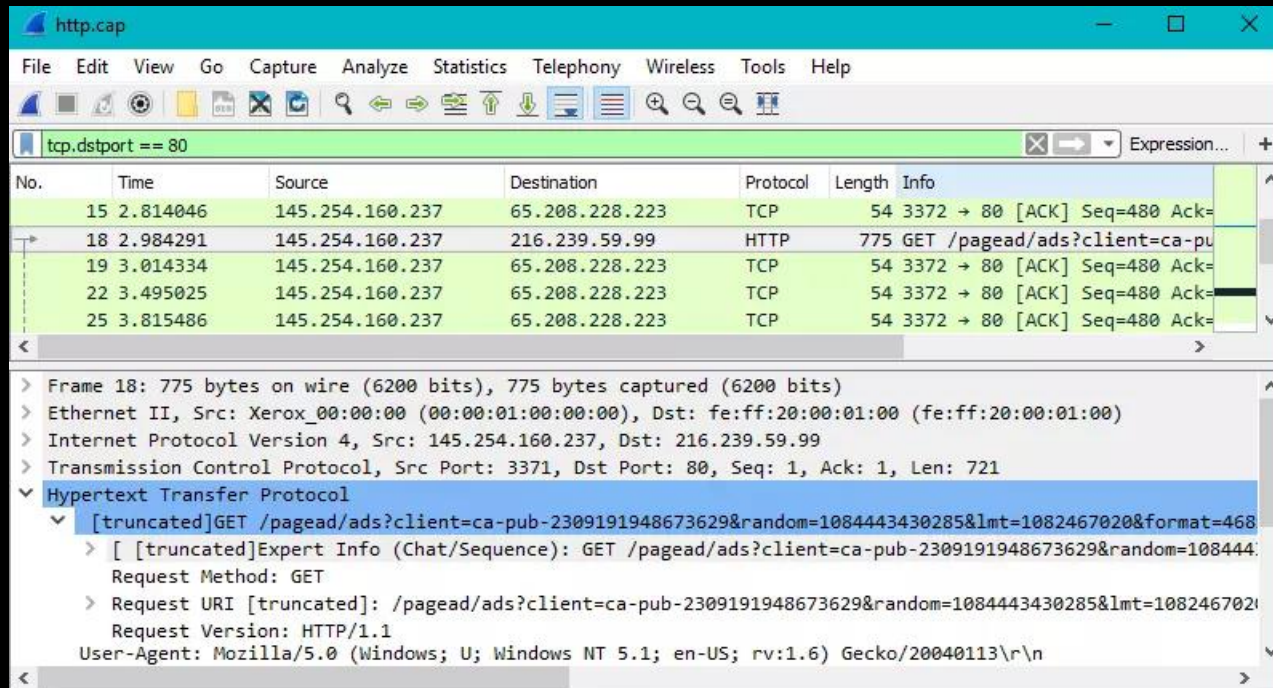
0000 52 54 00 12 35 00 08 00 27 cb 7e f5 08 00 45  
0010 00 68 20 c8 40 00 40 06 c6 14 0a 00 02 0f 8e  
0020 b8 aa d3 fe 01 bb 24 60 50 a4 00 00 2c 5e 50  
0030 f5 3c 54 0e 00 00 14 03 03 00 01 01 17 03 03  
0040 35 80 e9 fa 24 f5 bb 36 13 d0 a6 0d 44 1d 08  
0050 ac 69 94 29 6c 12 0d f1 7f d1 22 ee 05 ae 3c  
0060 13 86 62 7c a9 d2 5a c8 4c 38 d9 1a 50 b2 57  
0070 9d c8 34 cf c1 05

wireshark\_eth0NUTGD2.pcapng Packets: 2218 · Displayed: 2218 (100.0%) · Dropped: 0 (0.0%) Profile: Default

# ESCANEEO DE RED TCP

Un escaneo de puerto es tráfico TCP o UDP que se envía a una serie de puertos.

El escaneo de puertos típicamente clasificará los puertos en una de tres categorías:



No.	Time	Source	Destination	Protocol	Length	Info
15	2.814046	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=
18	2.984291	145.254.160.237	216.239.59.99	HTTP	775	GET /pagead/ads?client=ca-pu
19	3.014334	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=
22	3.495025	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=
25	3.815486	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=

Frame 18: 775 bytes on wire (6200 bits), 775 bytes captured (6200 bits)
Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
Internet Protocol Version 4, Src: 145.254.160.237, Dst: 216.239.59.99
Transmission Control Protocol, Src Port: 3371, Dst Port: 80, Seq: 1, Ack: 1, Len: 721
Hypertext Transfer Protocol
[truncated]GET /pagead/ads?client=ca-pub-2309191948673629&random=1084443430285&mt=1082467020&format=468
[ [truncated]Expert Info (Chat/Sequence): GET /pagead/ads?client=ca-pub-2309191948673629&random=108444
Request Method: GET
Request URI [truncated]: /pagead/ads?client=ca-pub-2309191948673629&random=1084443430285&mt=108246702
Request Version: HTTP/1.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113\r\n

**Abierto:** el host deseado responde con un paquete que indica que está activo en ese puerto. También indica que el servicio que se usó para el escaneo (típicamente TCP o UDP) también está en uso.

**Cerrado:** el host de destino recibe el paquete de solicitud e indica que no hay ningún servicio activo en ese puerto.

**Filtrado:** un escáner de puertos categorizará un puerto como filtrado cuando se envié un paquete de solicitud, pero no se reciba una respuesta. Esto generalmente indica que el paquete de solicitud ha sido filtrado y eliminado por un firewall.



# CONCEPTOS BÁSICOS Y CURIOSIDADES.

- También podemos usar la terminal para hacer escaneos de red, y ver que puertos están abiertos:

```
File Actions Edit View Help

    valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:cb:7e:f5 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 526sec preferred_lft 526sec
    inet6 fe80::34e0:d8ad:2eac:5da9/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
$ nmap -sT -p- 10.0.2.15/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-02 05:13 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00094s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT      STATE SERVICE
53/tcp    open  domain

Nmap scan report for 10.0.2.15
Host is up (0.0031s latency).
All 65535 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 65535 closed tcp ports (conn-refused)

Nmap done: 256 IP addresses (2 hosts up) scanned in 16.38 seconds

(kali㉿kali)-[~]
$ nmap -sT -p- 10.0.2.15
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-02 05:13 EDT
Nmap scan report for 10.0.2.15
Host is up (0.000028s latency).
All 65535 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 65535 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds

(kali㉿kali)-[~]
$ |
```

# CURIOSIDADES QUE NO SABIAS.

¿Sabias que desde la terminal o consola del propio Windows puedes actualizar todos los programas que tienes instalados?

```
C:\Windows\System32>winget upgrade --all
Nombre                               Id                               Versión   Disponible  Origen
-----
Google Chrome                       Google.Chrome                   119.0.6045.105 119.0.6045.106 winget
Microsoft Visual C++ 2015-2019 Redistributable (x64)... Microsoft.VCRedist.2015+.x64 14.28.29334.0 14.38.32919.0 winget
Microsoft Visual C++ 2015-2019 Redistributable (x86)... Microsoft.VCRedist.2015+.x86 14.28.29334.0 14.38.32919.0 winget
3 actualizaciones disponibles.
1 paquete(s) tienen números de versión que no se pueden determinar. Use --include-unknown para ver todos los resultados.

Instalando dependencias:
(1/2) Encontrado Microsoft Visual C++ 2015-2022 Redistributable (x64) [Microsoft.VCRedist.2015+.x64] Versión 14.38.32919.0
El propietario de esta aplicación le concede una licencia.
Microsoft no es responsable, ni tampoco concede ninguna licencia de paquetes de terceros.
Descargando https://download.visualstudio.microsoft.com/download/pr/02a6d5c5-3e10-47de-8025-d97a1321d3e3/5F60592799FAE0C82578112D48621438FFC976AB39D848D8F7623F5705A83E27/VC_redist.x64.exe
24.1 MB / 24.1 MB
El hash del instalador se verificó correctamente
Iniciando instalación de paquete...

Google Chrome                       Google.Chrome                   119.0.6045.105 119.0.6045.106 winget
Microsoft Visual C++ 2015-2019 Redistributable (x64)... Microsoft.VCRedist.2015+.x64 14.28.29334.0 14.38.32919.0 winget
Microsoft Visual C++ 2015-2019 Redistributable (x86)... Microsoft.VCRedist.2015+.x86 14.28.29334.0 14.38.32919.0 winget
3 actualizaciones disponibles.
1 paquete(s) tienen números de versión que no se pueden determinar. Use --include-unknown para ver todos los resultados.

C:\Windows\System32>
```

\$winget upgrade, y despues \$winget upgrade --all (Para actualizas las aplicaciones de windows 10 desde cmd, lo abrimos como administrador)

\$cleanmgr (Limpiar archivos basura)

\$sudo apt full-upgrade -y (Para actualizar kali desde la terminar)

\$Sudo apt upgrade (Actualizar kali)