CURSO *ONLINE* DE CIBERSEGURIDAD_

Especialidad Administración de Sistemas de Ciberseguridad

Taller 2

Unidad 5. Seguridad en administración de sistemas

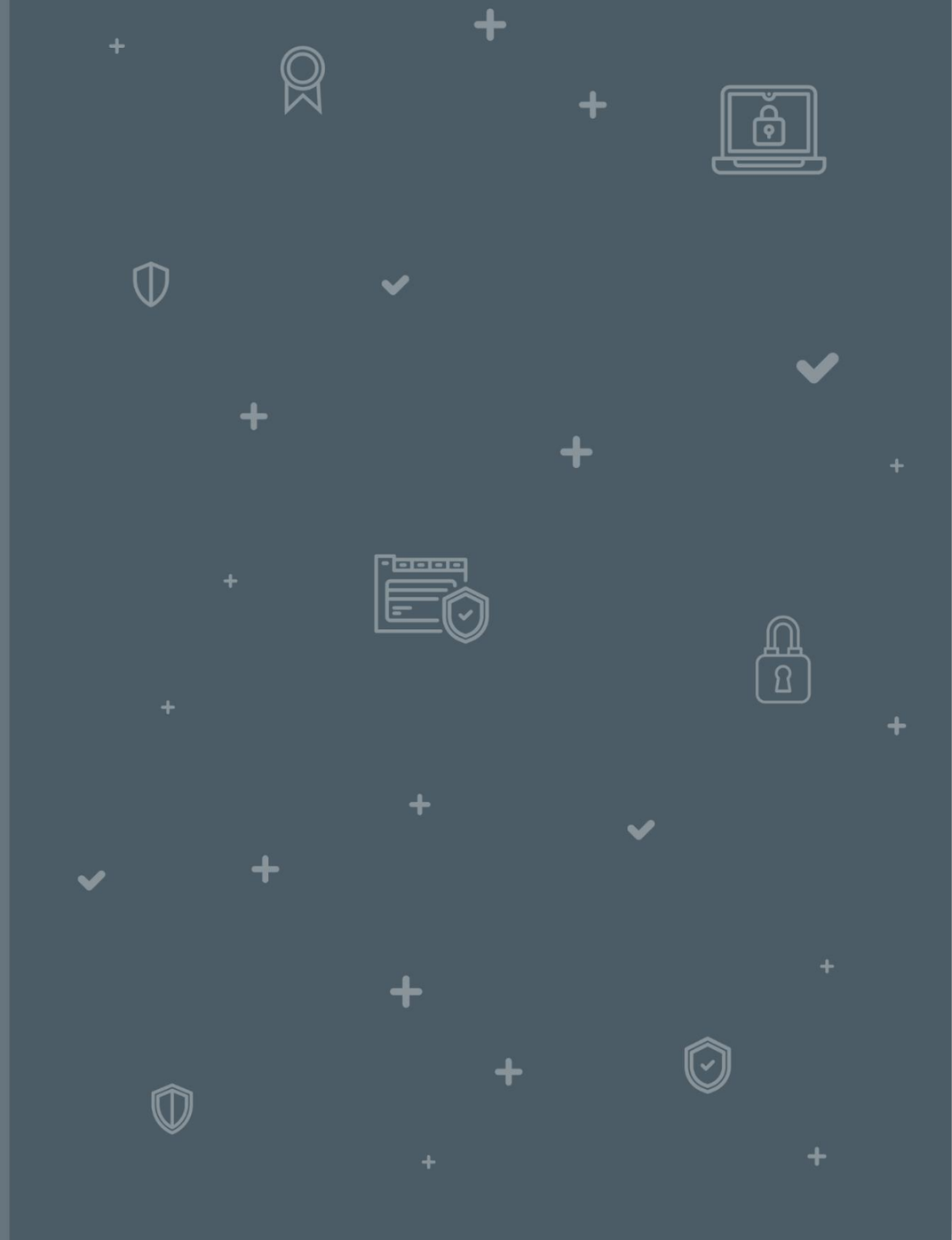
GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017

Contenidos

Duración total del taller: 1 hora 30 minutos

1

ATAQUE *«MAN IN THE MIDDLE»* DE PROTOCOLOS NO CIFRADOS



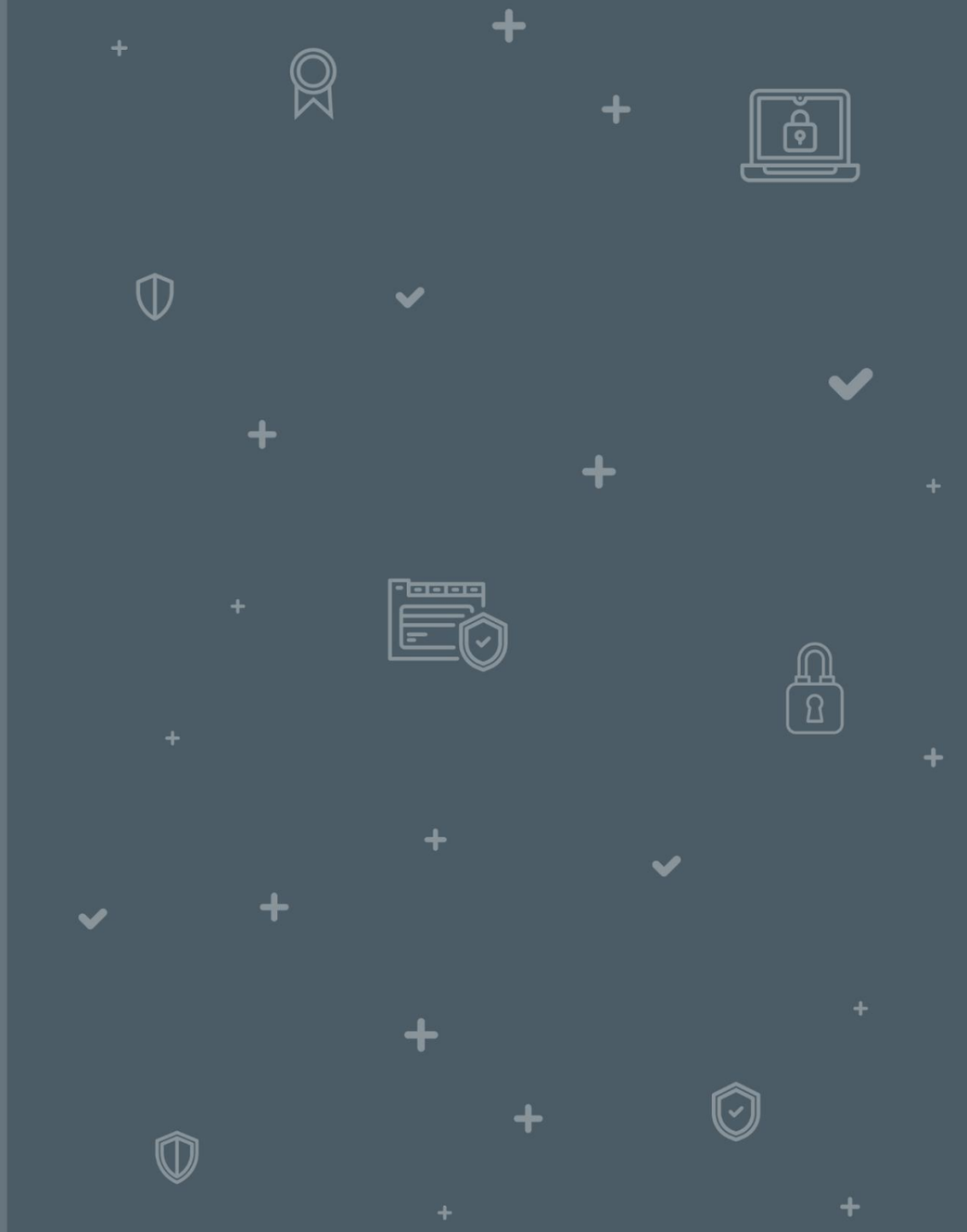
1 ATAQUE *«MAN IN THE MIDDLE»* DE PROTOCOLOS NO CIFRADOS

Man in the Middle es un ataque que consiste en introducirse en mitad de un intercambio de datos que se esté dando entre dos equipos o sistemas. La intención es que, conforme el tráfico pase por nosotros, interceptemos los paquetes y podamos obtener datos de interés. Adicionalmente, según el tipo de ataque *Man in the Middle*, también es posible que el atacante no solo intercepte la comunicación, sino que también la manipule antes de enviarla al destino.

Para realizar este ataque, necesitas tener tres máquinas encendidas, por lo que vas a utilizar la máquina virtual Kali Linux, Metasploitable3 y una máquina Ubuntu que instalarás a continuación.

2

CONSIDERACIONES PREVIAS



2 CONSIDERACIONES PREVIAS

Metasploitable3 deberías tenerlo descargado de la Unidad 3 para realizar las prácticas de dicha unidad, por lo que, si no la tienes instalada en tu equipo, accede a las prácticas de la Unidad 3 para ver el proceso.

3

INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

3 INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

Para instalar esta máquina debes acceder al siguiente enlace y descargar la primera versión. En esta misma página encontrarás la información de la contraseña para utilizarla más adelante.

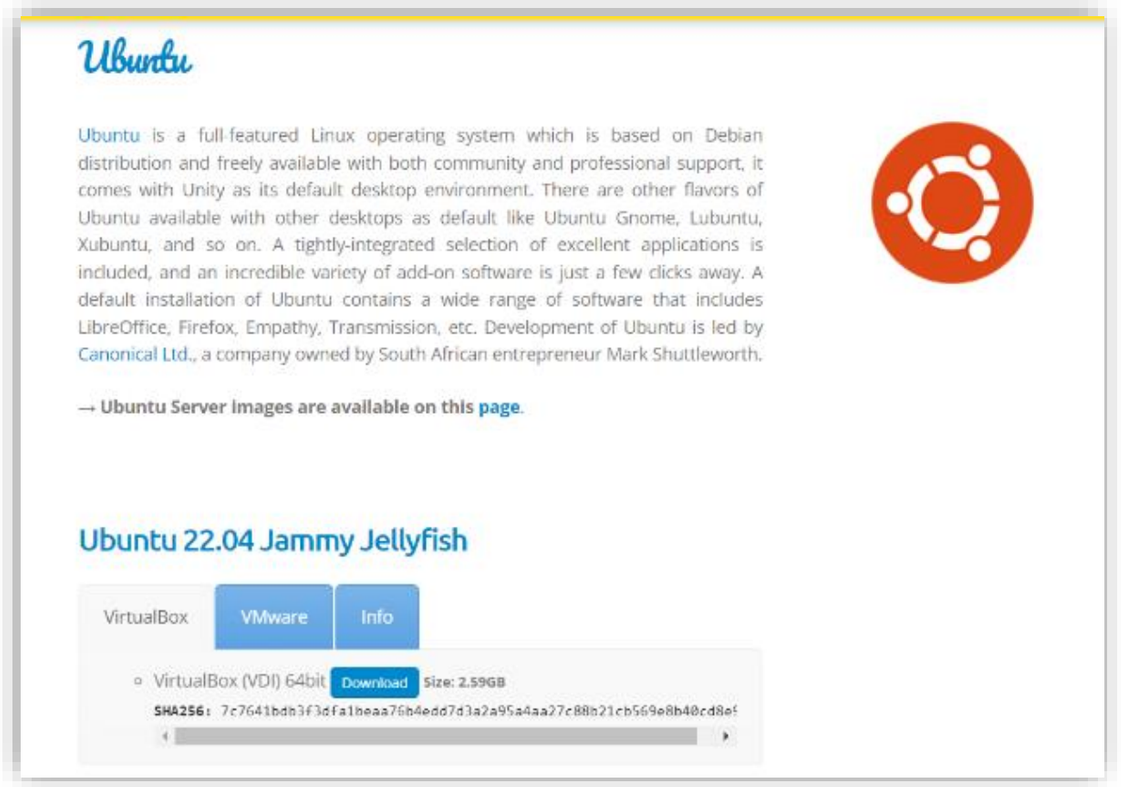


Ilustración 1: Página de inicio de descarga de Ubuntu.

3 INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

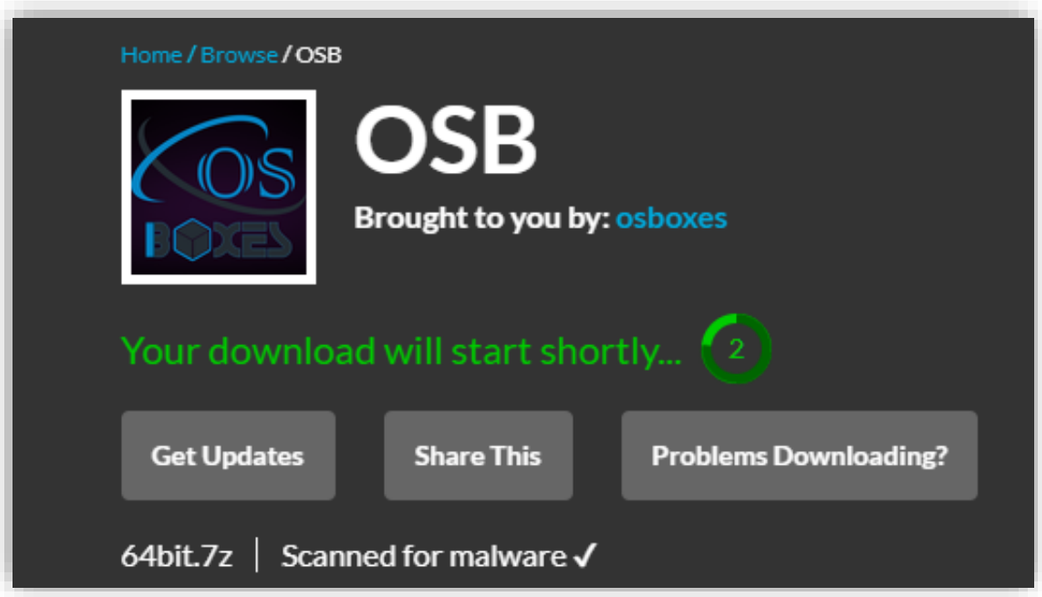


Ilustración 2: Proceso de descarga del archivo.

3 INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- Una vez descargado el archivo .vdi, debes configurar la máquina virtual y añadirla a VirtualBox.
  - Como te decimos siempre, una buena práctica es, en primer lugar, mover el archivo descargado a otra carpeta diferente de la de «Descargas». Por ejemplo, una que hayas creado para esta formación.
  - Para ello, abre VirtualBox y selecciona la opción «Nueva» en la parte superior de la pantalla.

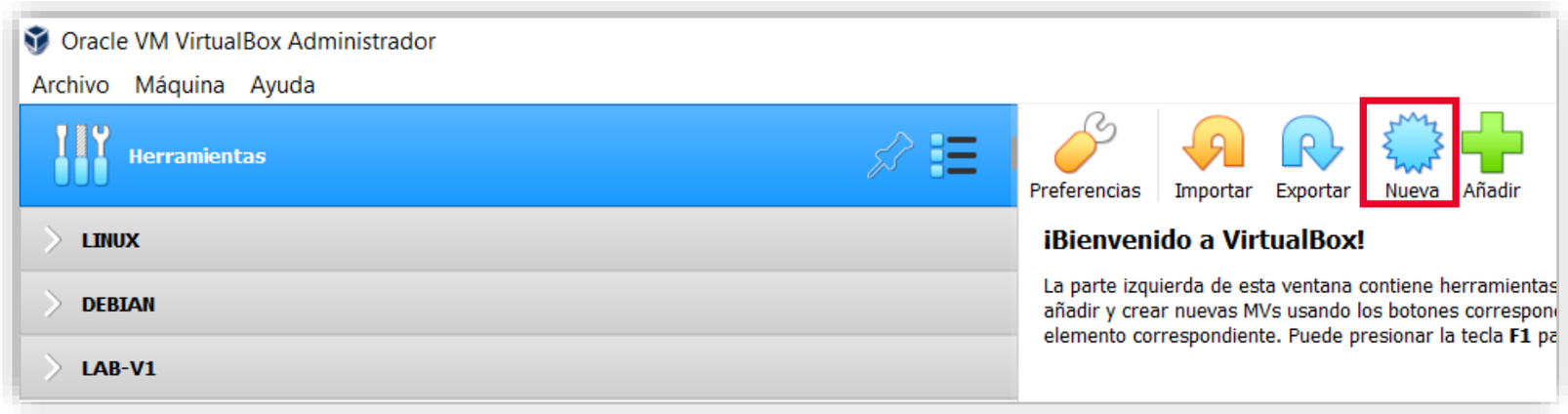


Ilustración 3: Opción «Nueva» dentro del menú de VirtualBox.

3 INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- Aparecerá una ventana en la que deberás poner el nombre de la máquina, dónde quieres guardarla y seleccionar el tipo y la versión de esta. Una vez completado, haz clic en «*Next*».

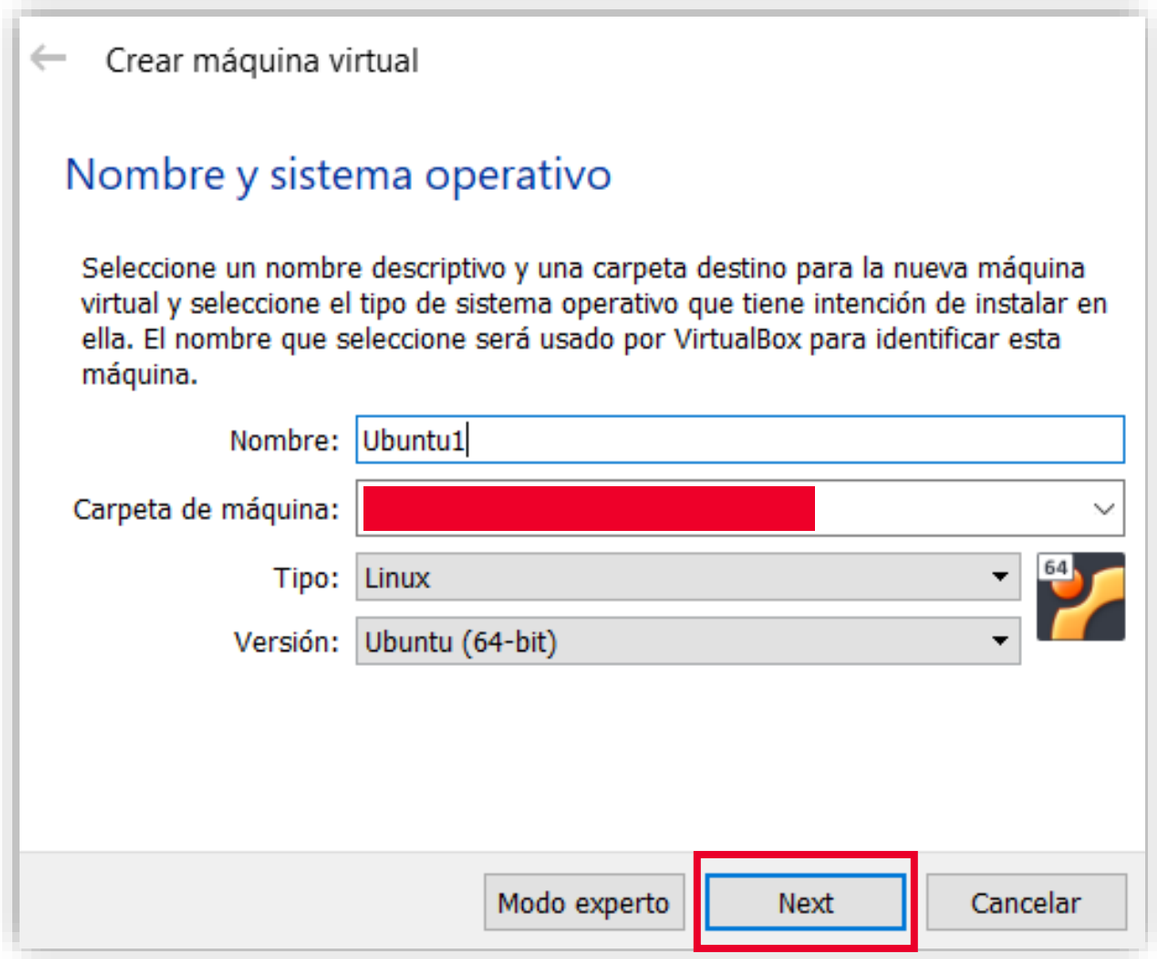


Ilustración 4: Campos a cumplimentar: nombre, carpeta de máquina, tipo y versión.

3 INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- El siguiente paso será configurar la memoria. Como no se necesita una gran capacidad para esta máquina, se indicará lo mínimo recomendado para evitar que consuma demasiados recursos. Cuando esté configurado haz clic en «*Next*».

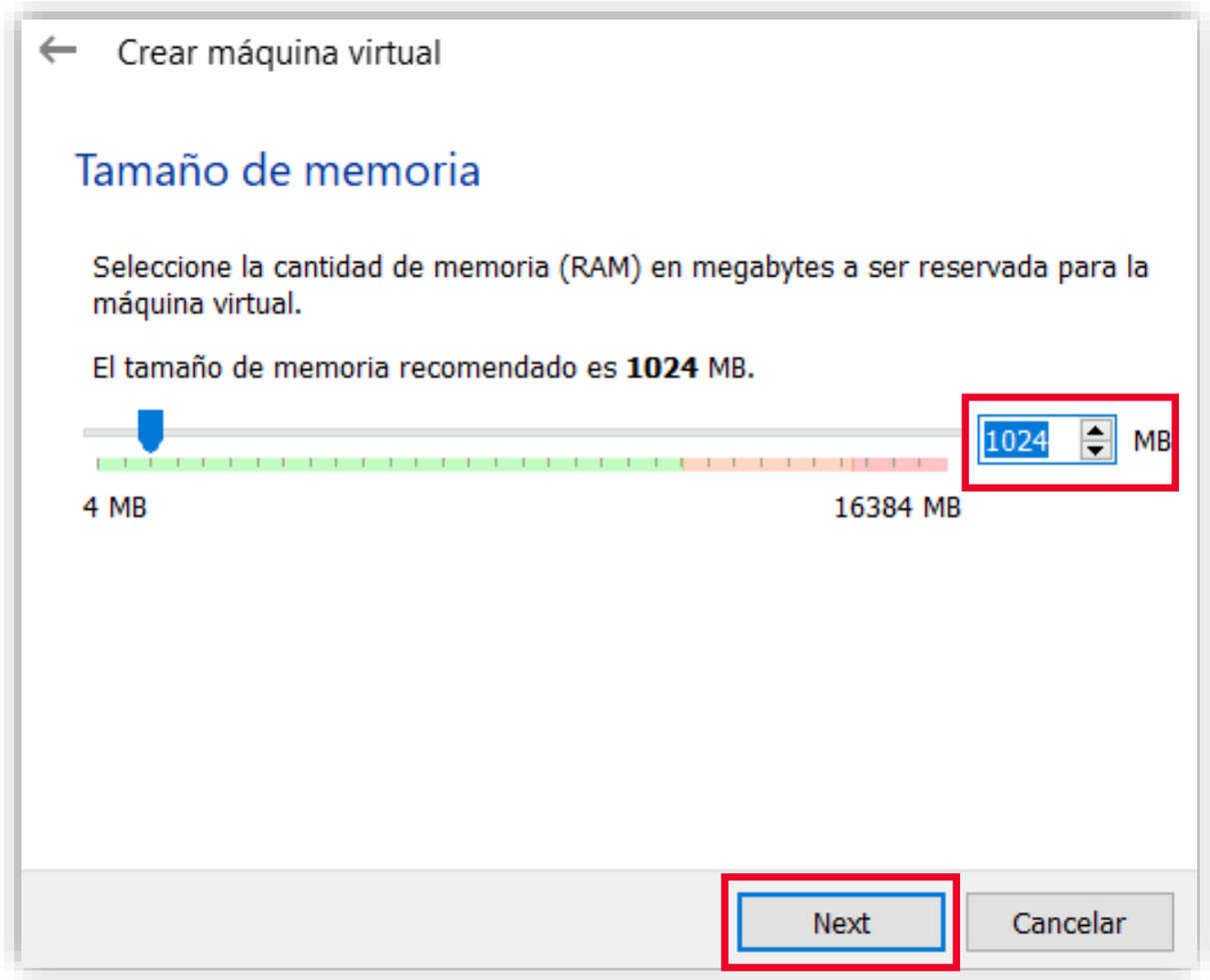


Ilustración 5: Capacidad del tamaño de la memoria.

3 INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- Después, debes configurar el disco duro, seleccionando «Crear un disco virtual ahora» y haciendo clic en «Crear».

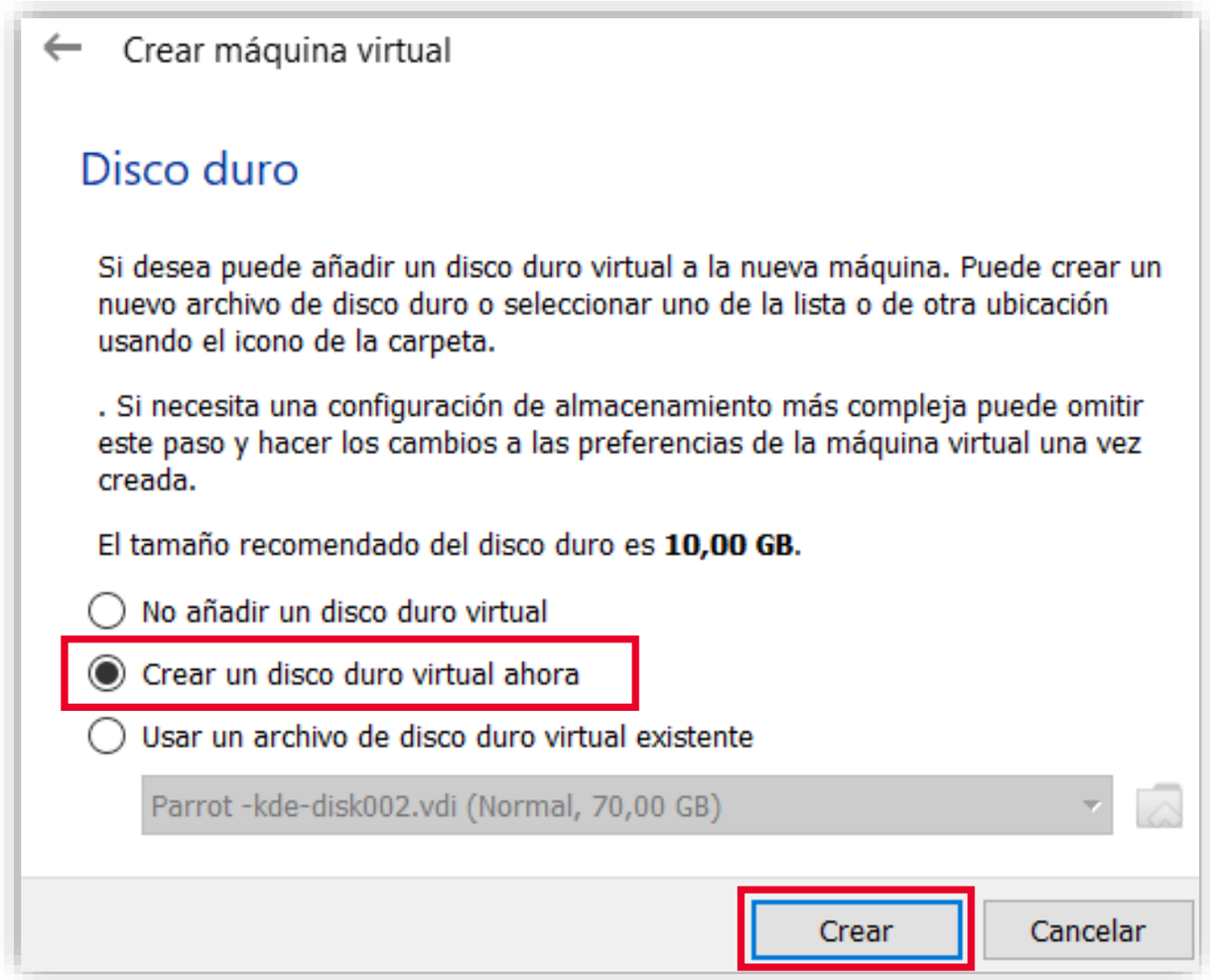


Ilustración 6: Opciones de disco duro de la máquina.

3 INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- Como el archivo que hemos descargado es un .vdi, selecciona la primera opción y haz clic en «*Next*».

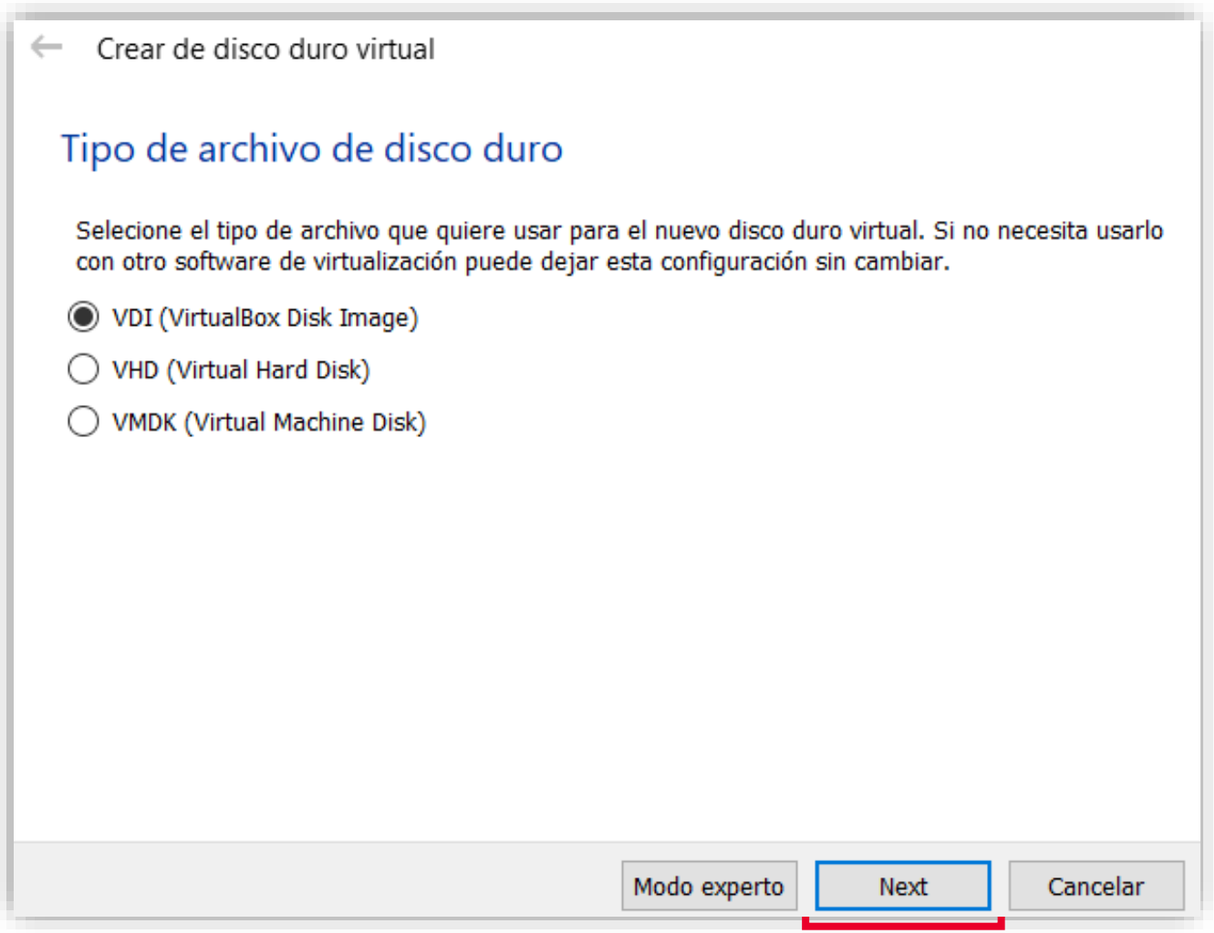


Ilustración 7: Tipo de archivo de disco duro.

3 INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- En el siguiente paso, vas a configurar el almacenamiento de disco duro. En este caso, selecciona la opción «Reservado dinámicamente».

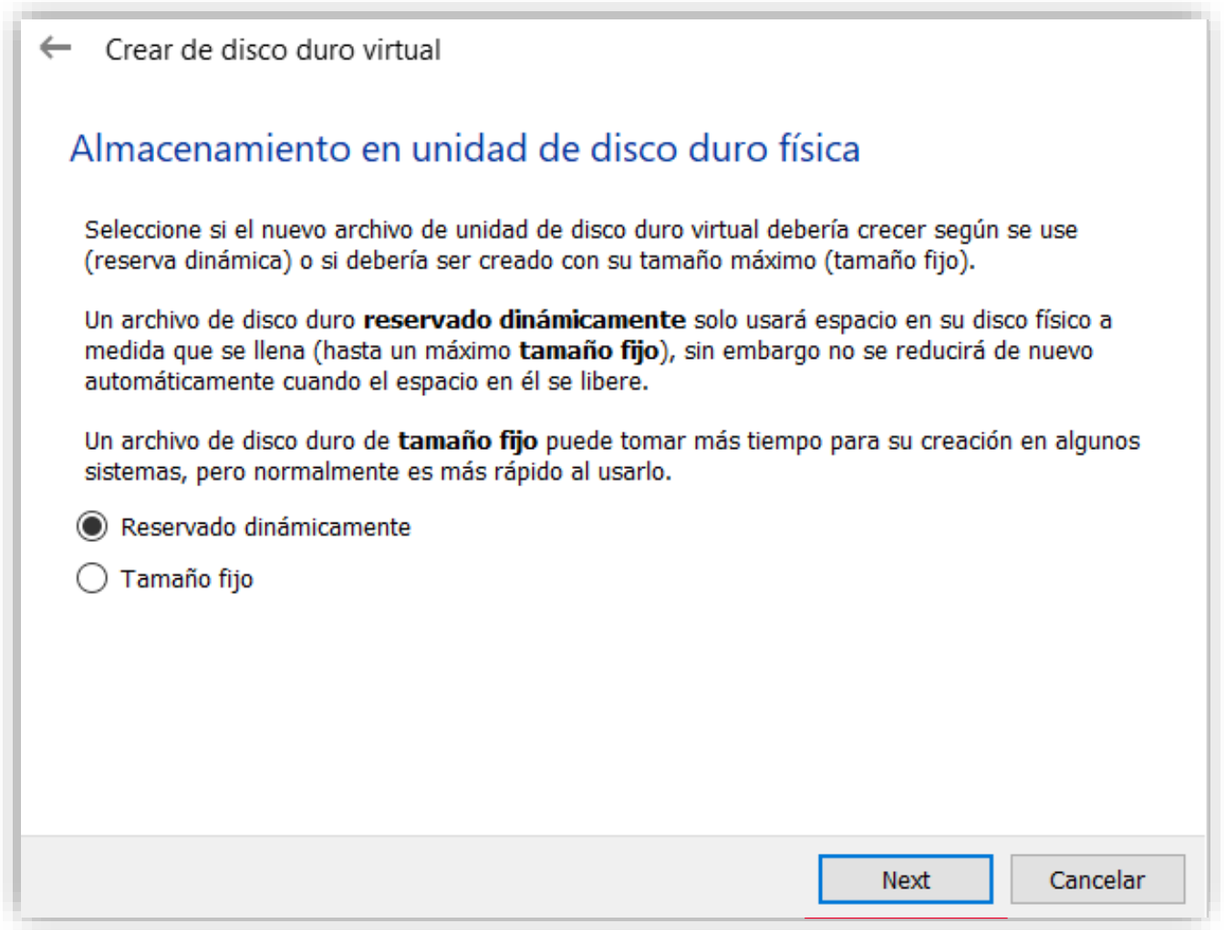


Ilustración 8: Capacidad de tamaño de disco duro.

3 INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- Ahora, selecciona la ubicación del archivo y el tamaño. En este caso, no necesitas una máquina con mucha capacidad por lo que solo indicarás 5GB. Después, haz clic en «Crear».

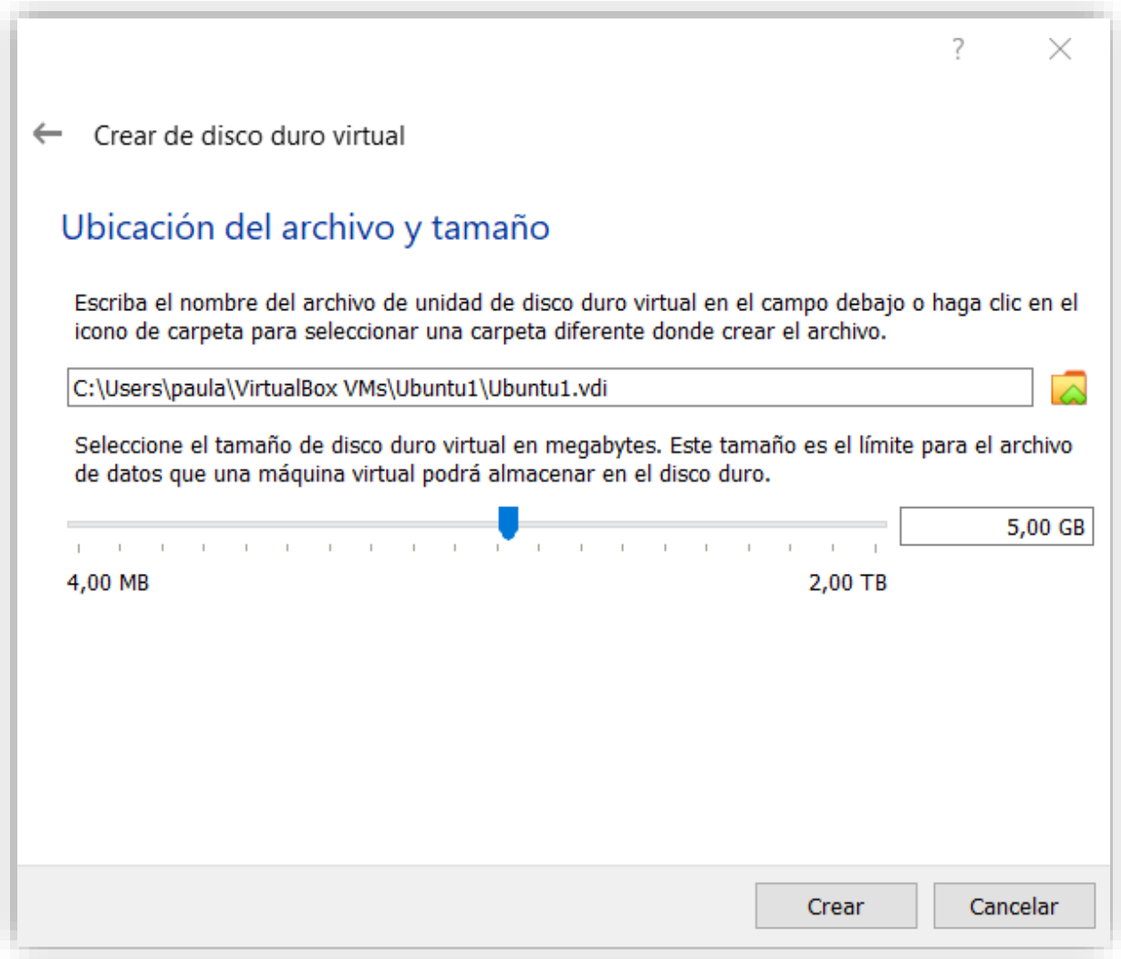


Ilustración 9:
Tamaño de disco duro.

3 INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- Una vez creada, configura la red de la misma forma que hicimos en la Unidad 3 en la máquina Metaiplotable3.
  - Para ello, haz clic derecho en la máquina virtual y pulsa sobre «Configuración».
- En la pestaña de Red, selecciona «Adaptador 1» y en Conectado a: «Red NAT». Por otro lado, en Nombre, selecciona la red NAT que has creado antes con la máquina Kali Linux.

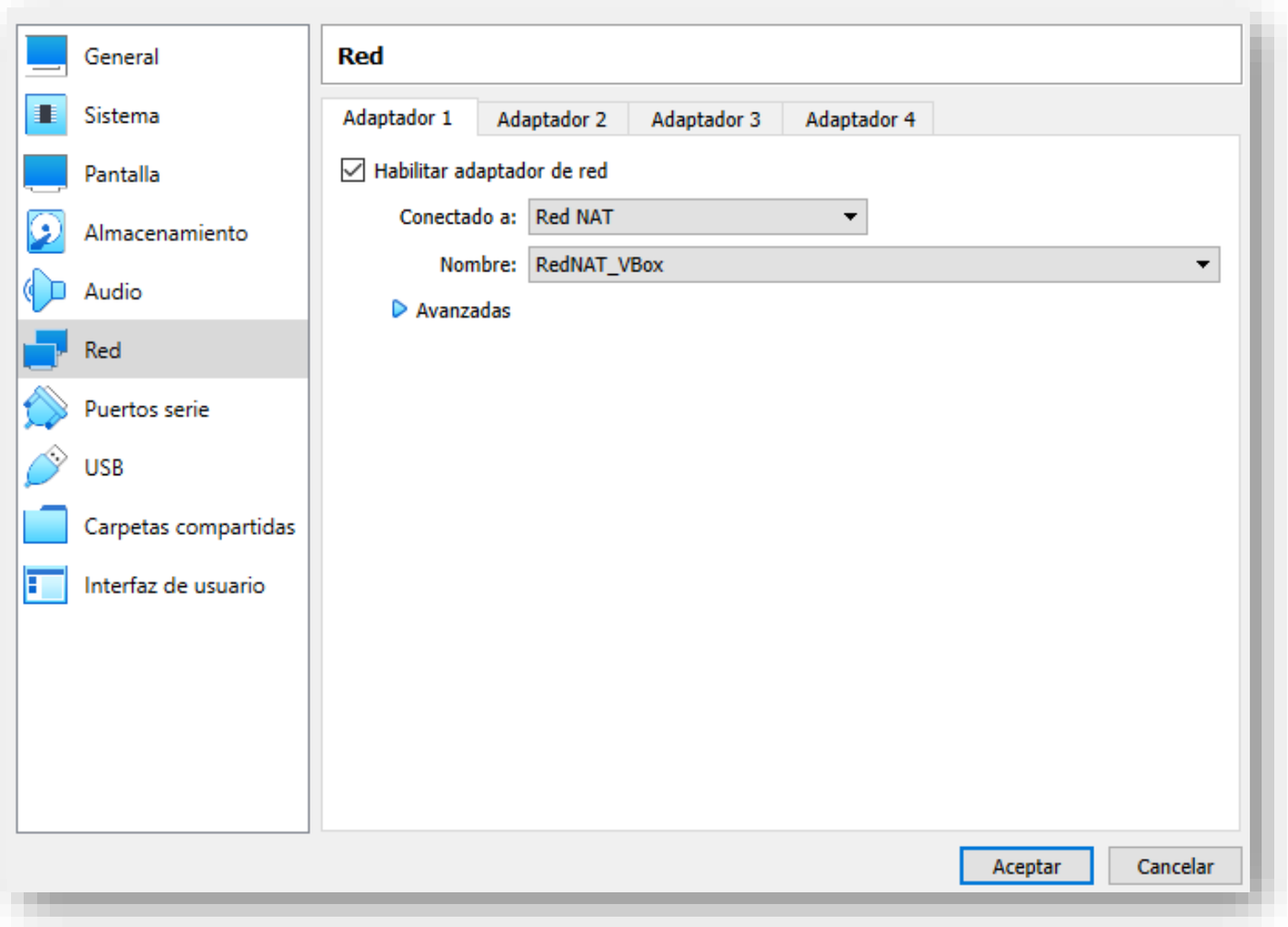


Ilustración 10:
Configuración de la red.

3 INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- Antes de ejecutar la máquina también deberás añadir en «Almacenamiento» el archivo .vdi que has descargado anteriormente.
  - Para ello, dentro del menú de «Almacenamiento», selecciona el icono marcado en la imagen.

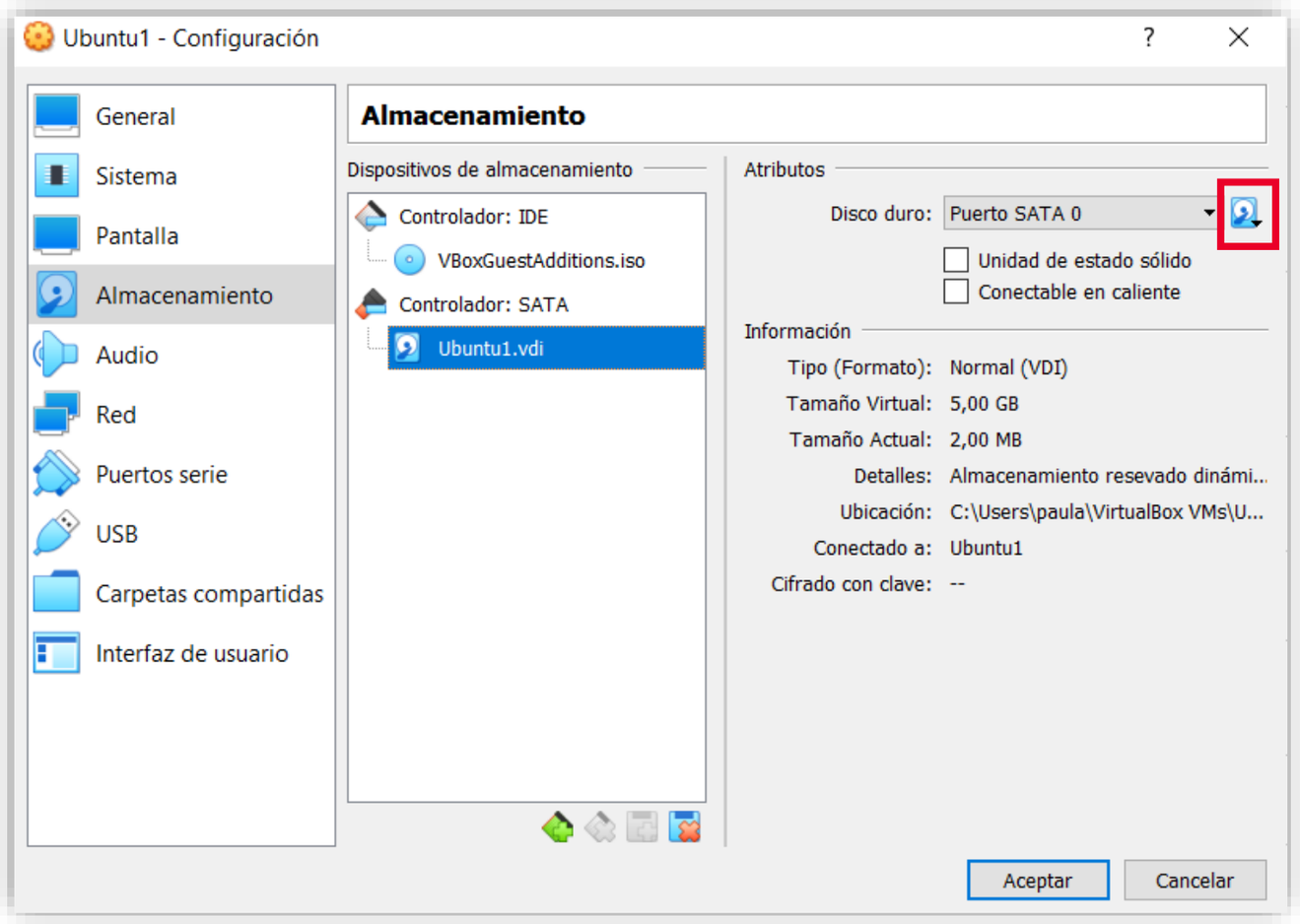


Ilustración 11: Configuración de almacenamiento Ubuntu.

3 INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- A continuación, se desplegará un menú. Haz clic en «Seleccionar a un archivo de disco».

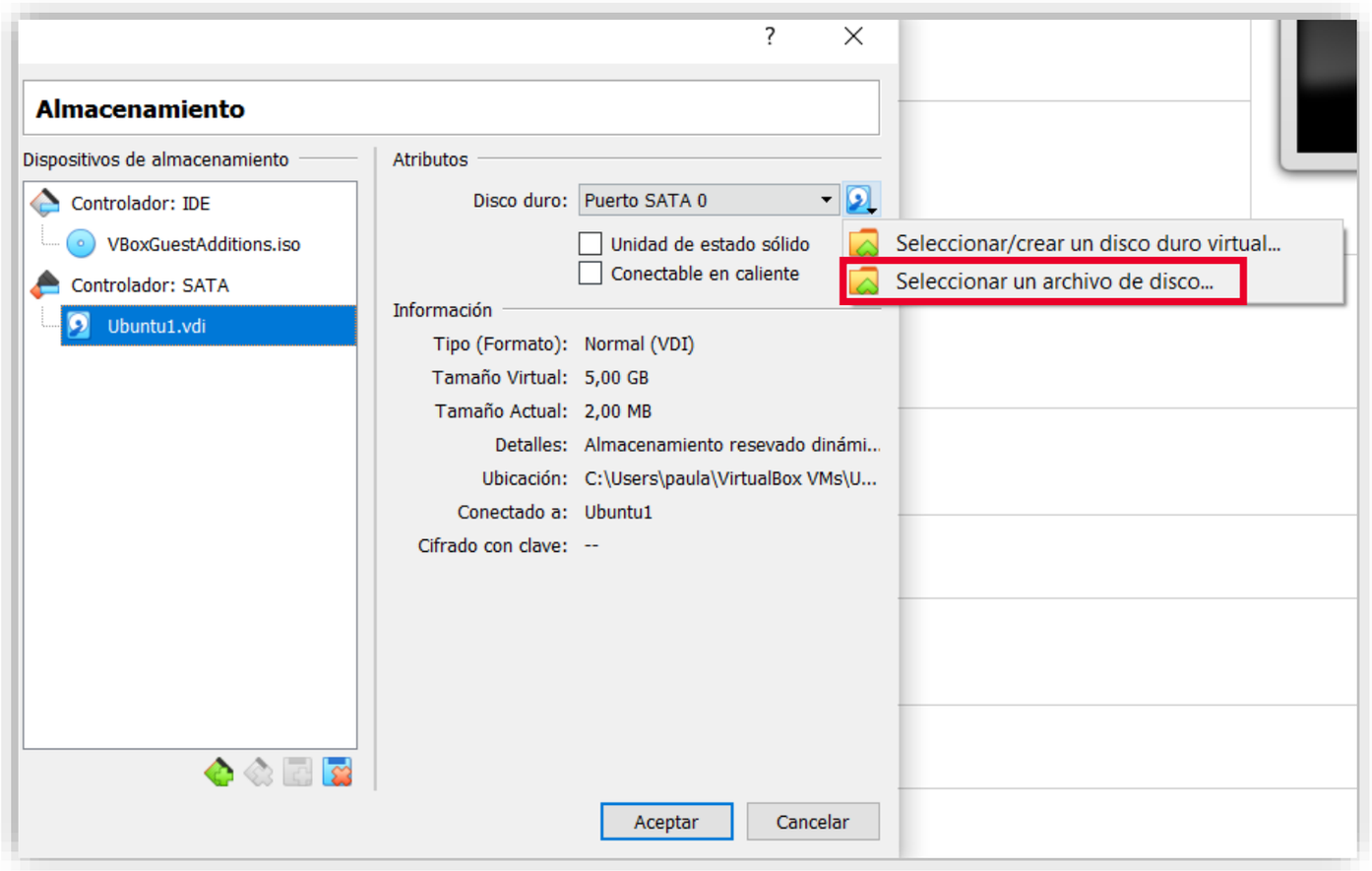


Ilustración 12: Configuración de almacenamiento.

3 INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- Se abrirá una ventana de explorador de archivos del equipo en la cual deberás desplazarte hasta localizar la carpeta en la que has guardado antes el archivo .vdi.
  - Selecciona el archivo y pulsa «Abrir».

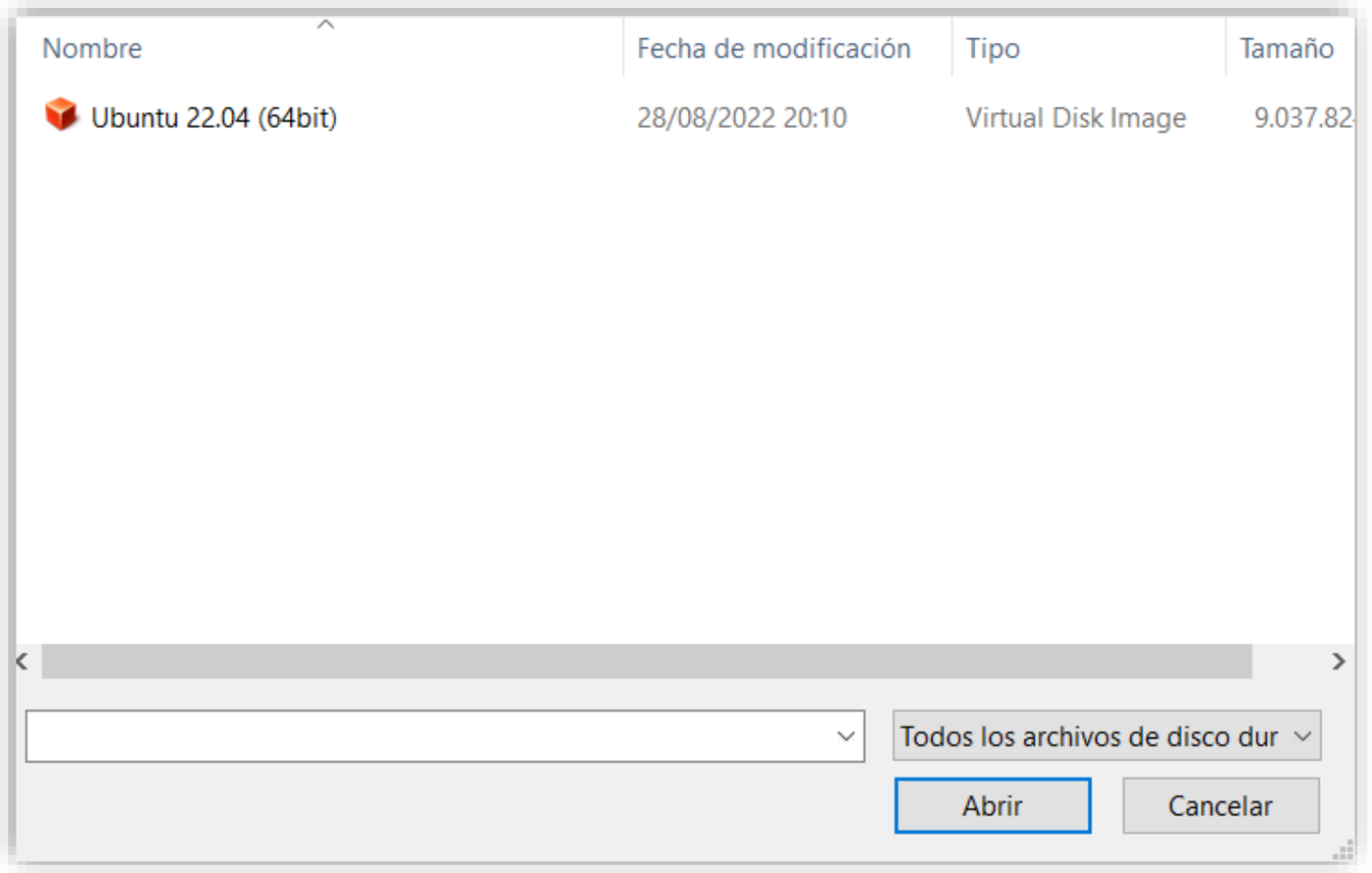


Ilustración 13: Ubicación del archivo archivo .vdi.

3 INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- Ya tienes configurada tu máquina Ubuntu. Ahora, haz clic en «Aceptar» para finalizar la configuración e inicia la máquina.

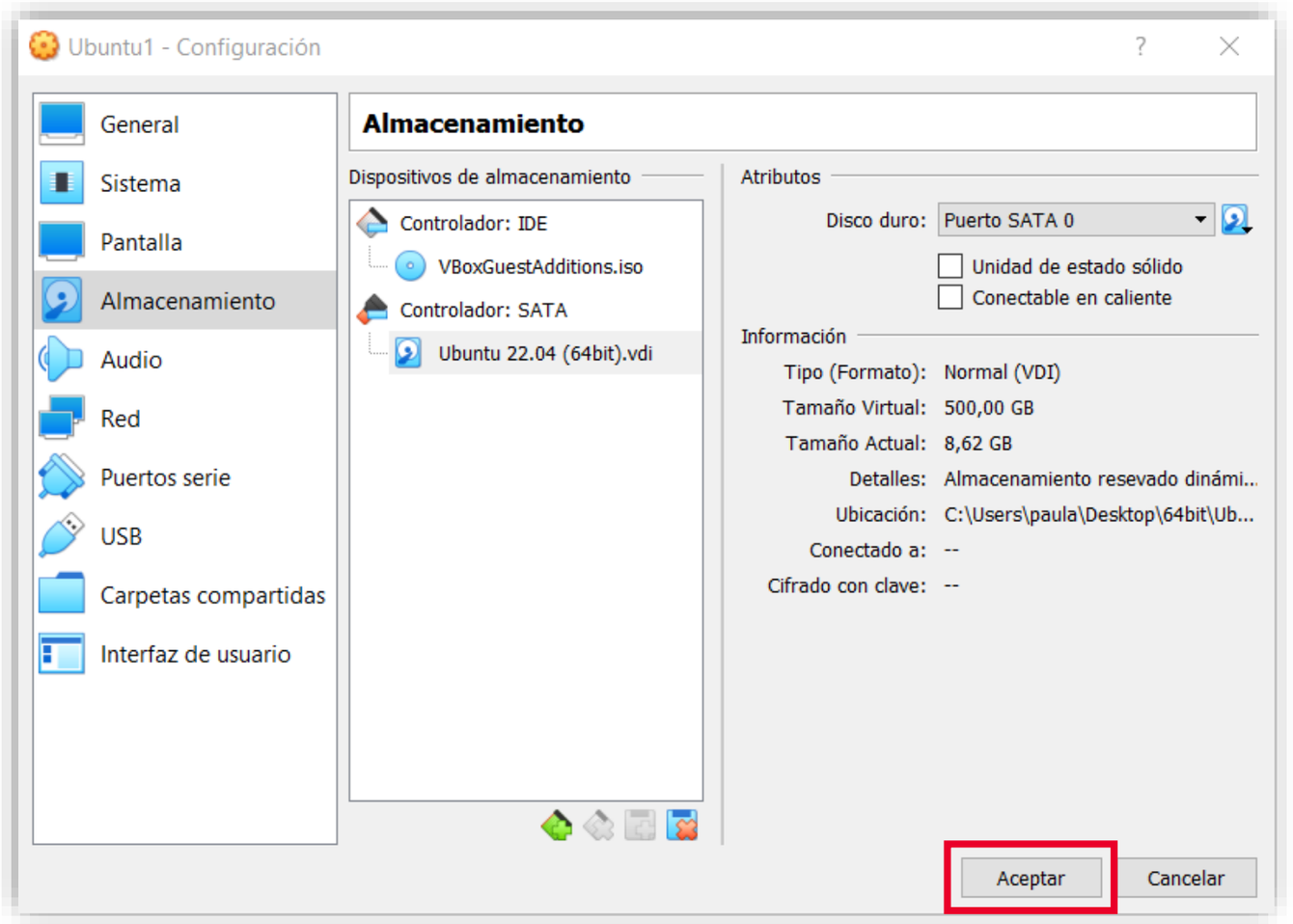
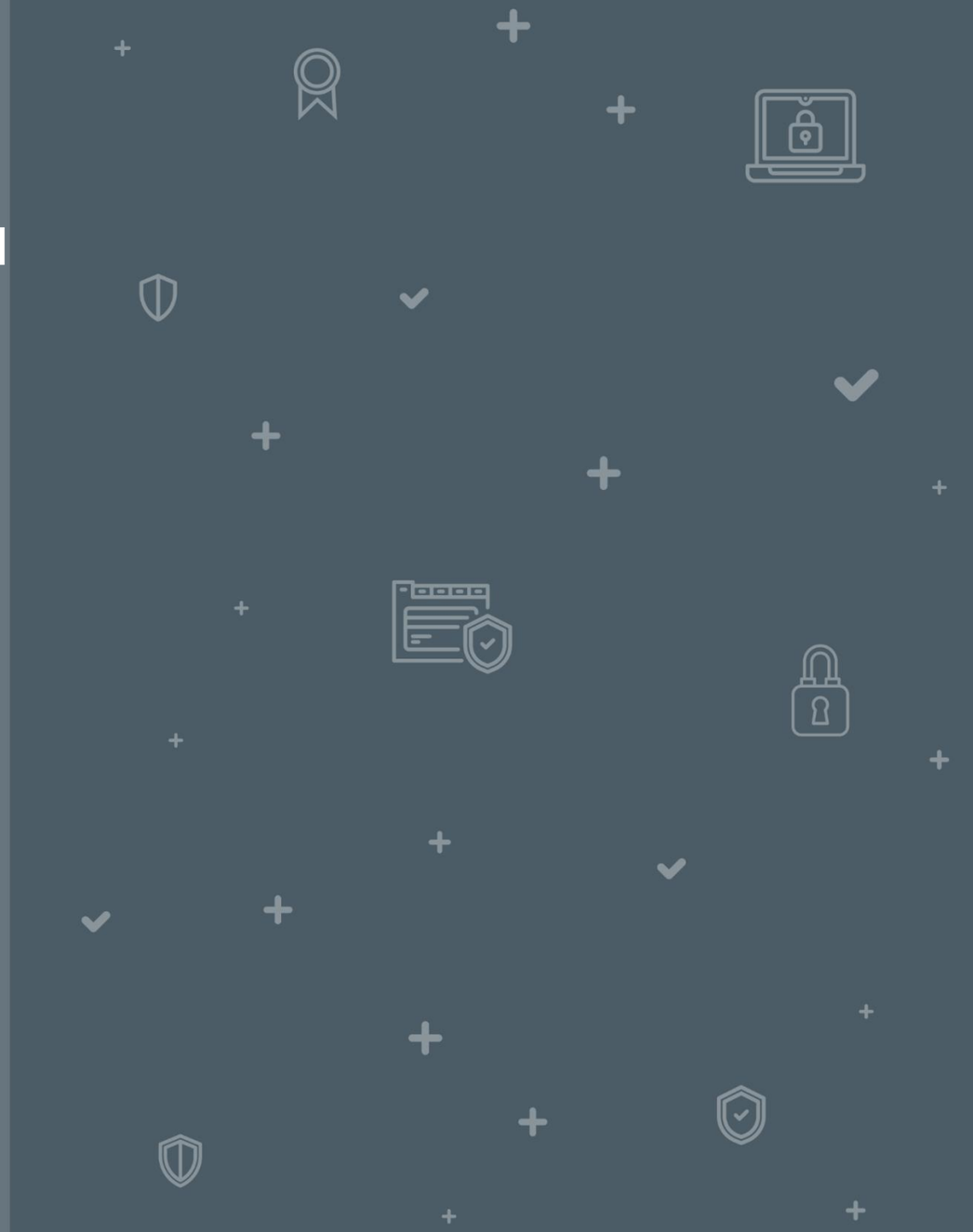


Ilustración 14: Botón de «Aceptar» para finalizar la configuración.

4

ENUNCIADO EJERCICIO PRÁCTICO 1



4 ENUNCIADO EJERCICIO PRÁCTICO 1

- Para realizar el ataque *Man in the Middle* utilizaremos el programa **Ettercap**, que es un programa gratuito y de código abierto.
- Para que funcione este tipo de ataque, todas las máquinas deben estar en el mismo segmento de red, por lo que deberás comprobar que has configurado bien todas las máquinas en la Red NAT. Es decir, que todas las máquinas tengan la configuración que puedes ver en la imagen:

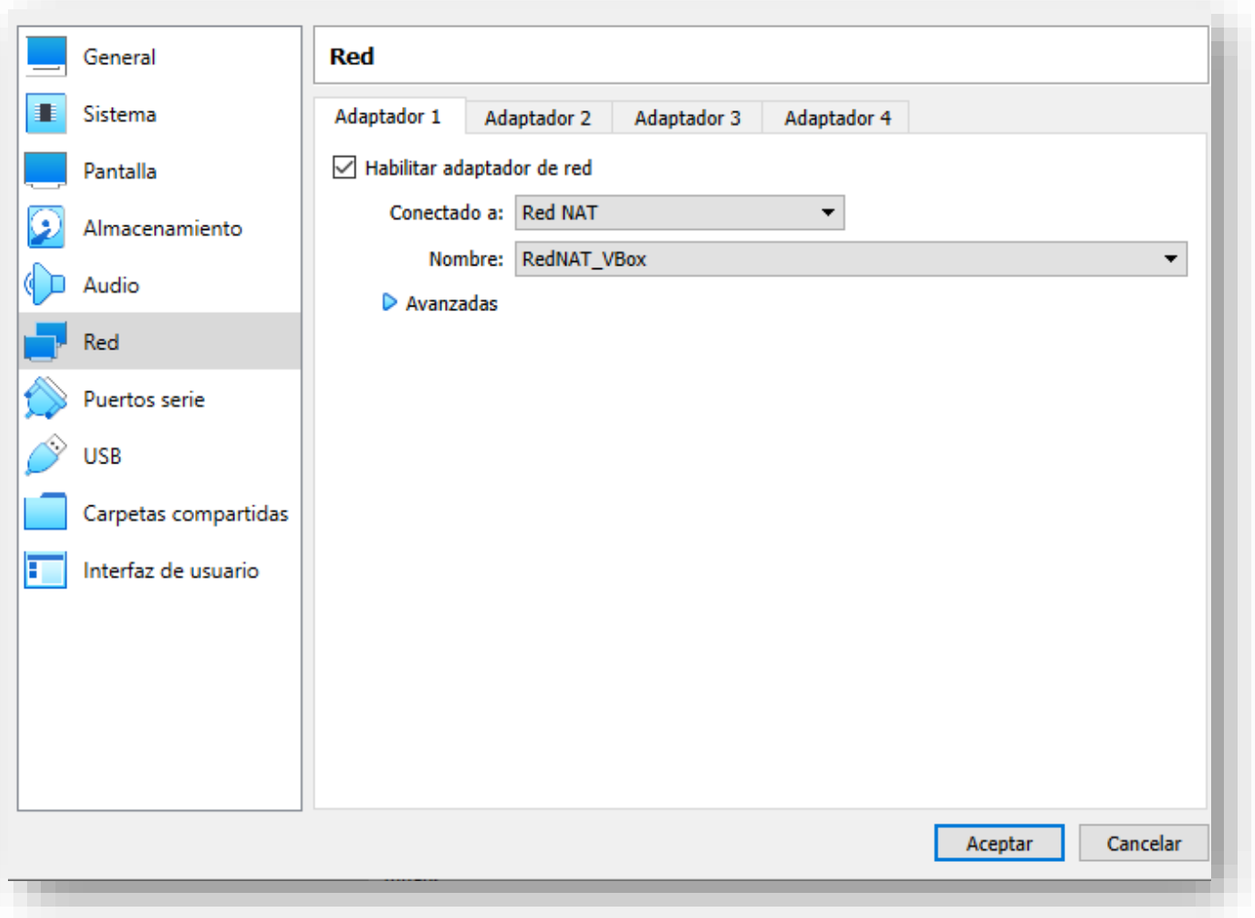
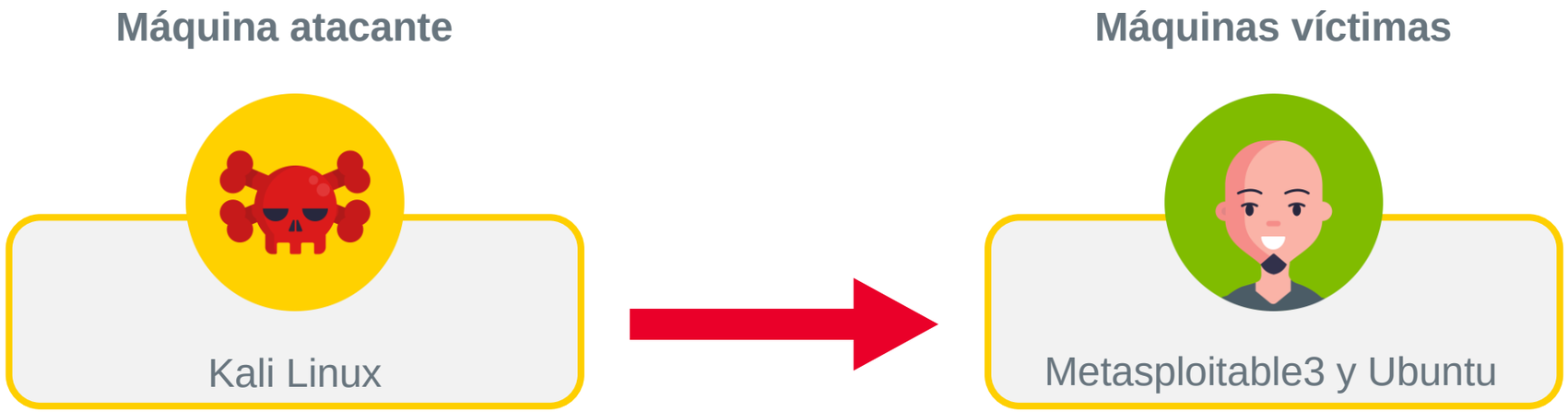


Ilustración 15: Configuración de la red para todas las máquinas.

4 ENUNCIADO EJERCICIO PRÁCTICO 1

- Para entender mejor este ataque, las máquinas instaladas anteriormente (Metasploitable3 y Ubuntu) serán las máquinas víctima y la máquina Kali Linux actuará como atacante. Es decir, la conexión normal se hará entre las máquinas Metasploitable3 y Ubuntu, y Kali Linux será quien realice el ataque *Man in the Middle*.



5

SOLUCIONARIO EJERCICIO PRÁCTICO 1

5 SOLUCIONARIO EJERCICIO PRÁCTICO ACTIVIDAD 1

- Lo primero que debes saber es cuál es la dirección IP que pertenece a cada máquina con la que estamos trabajando.
  - Para ello, ejecuta el comando **ifconfig** en cada una de las máquinas.

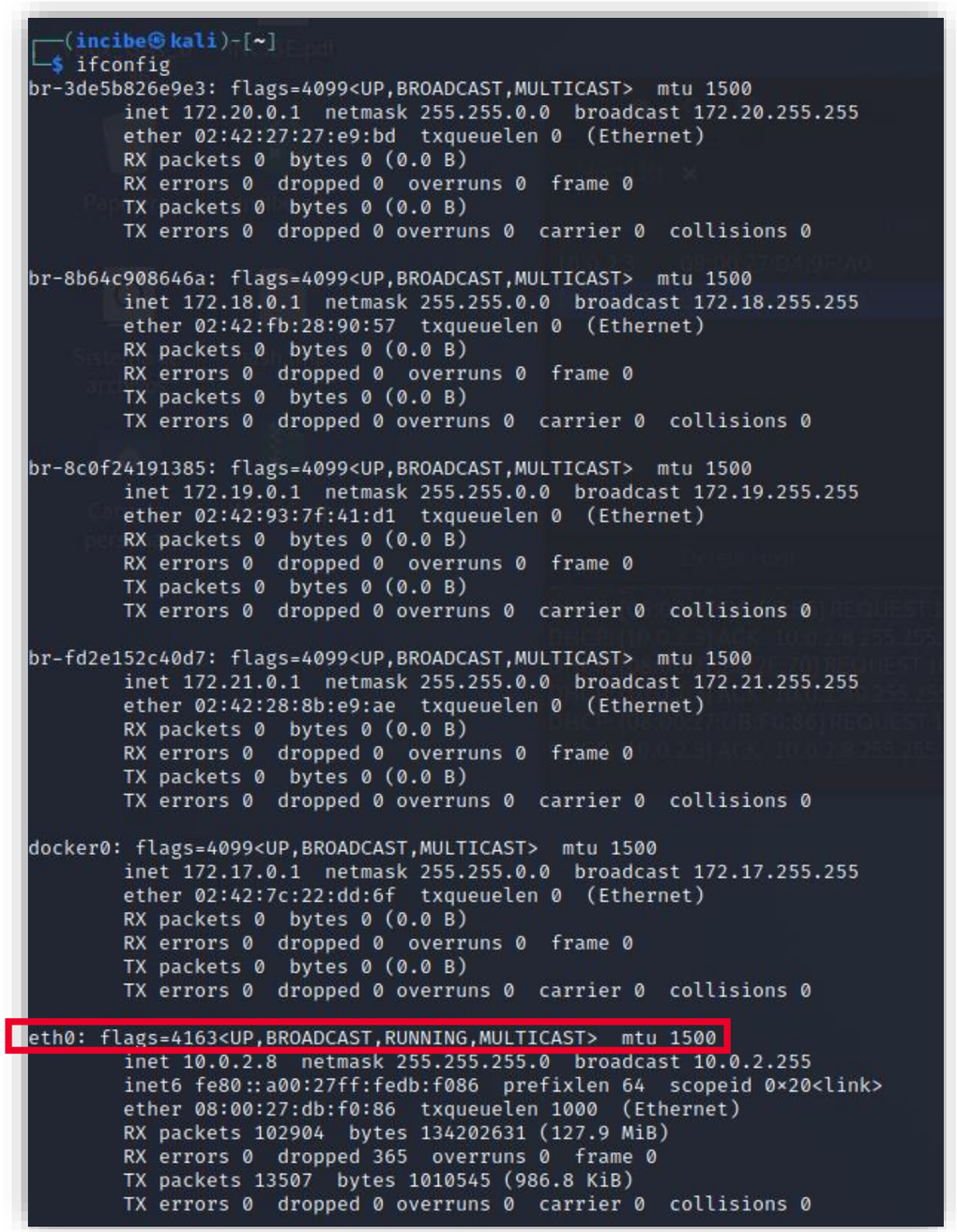


Ilustración 16: Ejecución del comando ifconfig en Kali Linux.

5 SOLUCIONARIO EJERCICIO PRÁCTICO ACTIVIDAD 1

- En Ubuntu, sería de la siguiente manera:

```
osboxes@osboxes:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.41  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::1348:a0b1:cf96:4c11  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:42:77:5d  txqueuelen 1000  (Ethernet)
        RX packets 531006  bytes 795262879 (795.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 105579  bytes 6449420 (6.4 MB)
        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 226  bytes 26536 (26.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 226  bytes 26536 (26.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Ilustración 17: Ejecución del comando ifconfig en Ubuntu.

5 SOLUCIONARIO EJERCICIO PRÁCTICO ACTIVIDAD 1

- En Metasploitable3, sería:

```
vagrant@metasploitable3-ub1404:~$ ifconfig
docker0   Link encap:Ethernet  HWaddr 02:42:4a:7a:b1:17
          inet addr:172.17.0.1  Bcast:172.17.255.255  Mask:255.255.0.0
          inet6 addr: fe80::42:4aff:fe7a:b117/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:738 (738.0 B)

eth0      Link encap:Ethernet  HWaddr 08:00:27:b8:2f:70
          inet addr:10.0.2.40  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb8:2f70/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8741 errors:0 dropped:0 overruns:0 frame:0
          TX packets:640 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:579992 (579.9 KB)  TX bytes:96237 (96.2 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:12299 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12299 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4852762 (4.8 MB)  TX bytes:4852762 (4.8 MB)
```

Ilustración 18: Ejecución del comando ifconfig en Metaespoitable3.

5 SOLUCIONARIO EJERCICIO PRÁCTICO ACTIVIDAD 1

- Una vez tengas las direcciones IP de las máquinas víctimas, abre una terminal en Kali que deberás dejar abierta mientras se esté utilizando el programa Ettercap. Este viene instalado por defecto en la máquina Kali.
  - Para abrirlo, deberás escribir en la terminal el comando **sudo ettercap -G** y se abrirá su entorno gráfico.

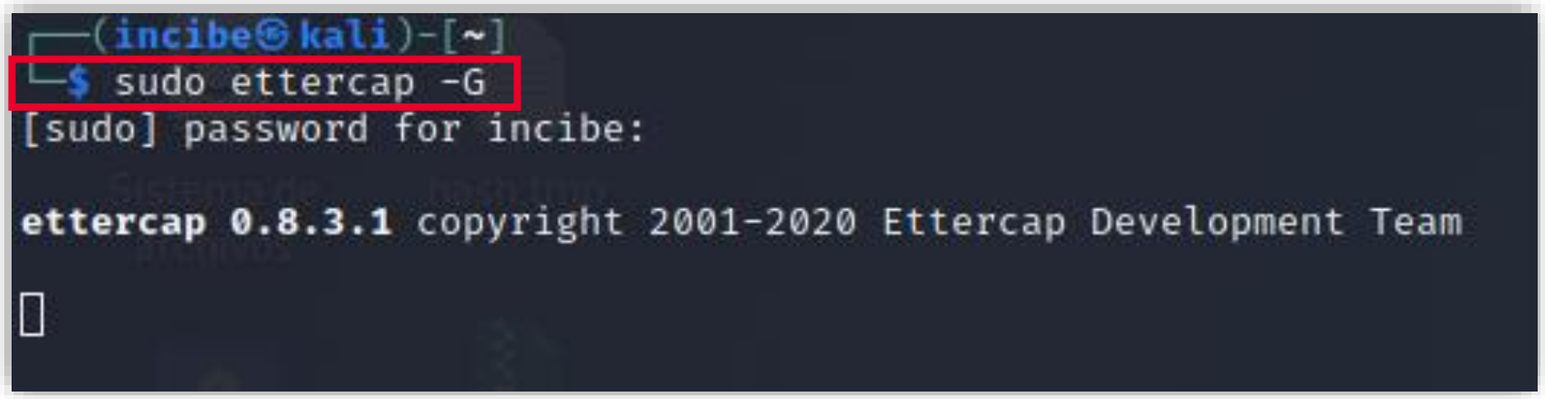


Ilustración 19: Comando sudo ettercap -G.

5 SOLUCIONARIO EJERCICIO PRÁCTICO ACTIVIDAD 1

- Una vez abierto, haz clic sobre el símbolo ✓.

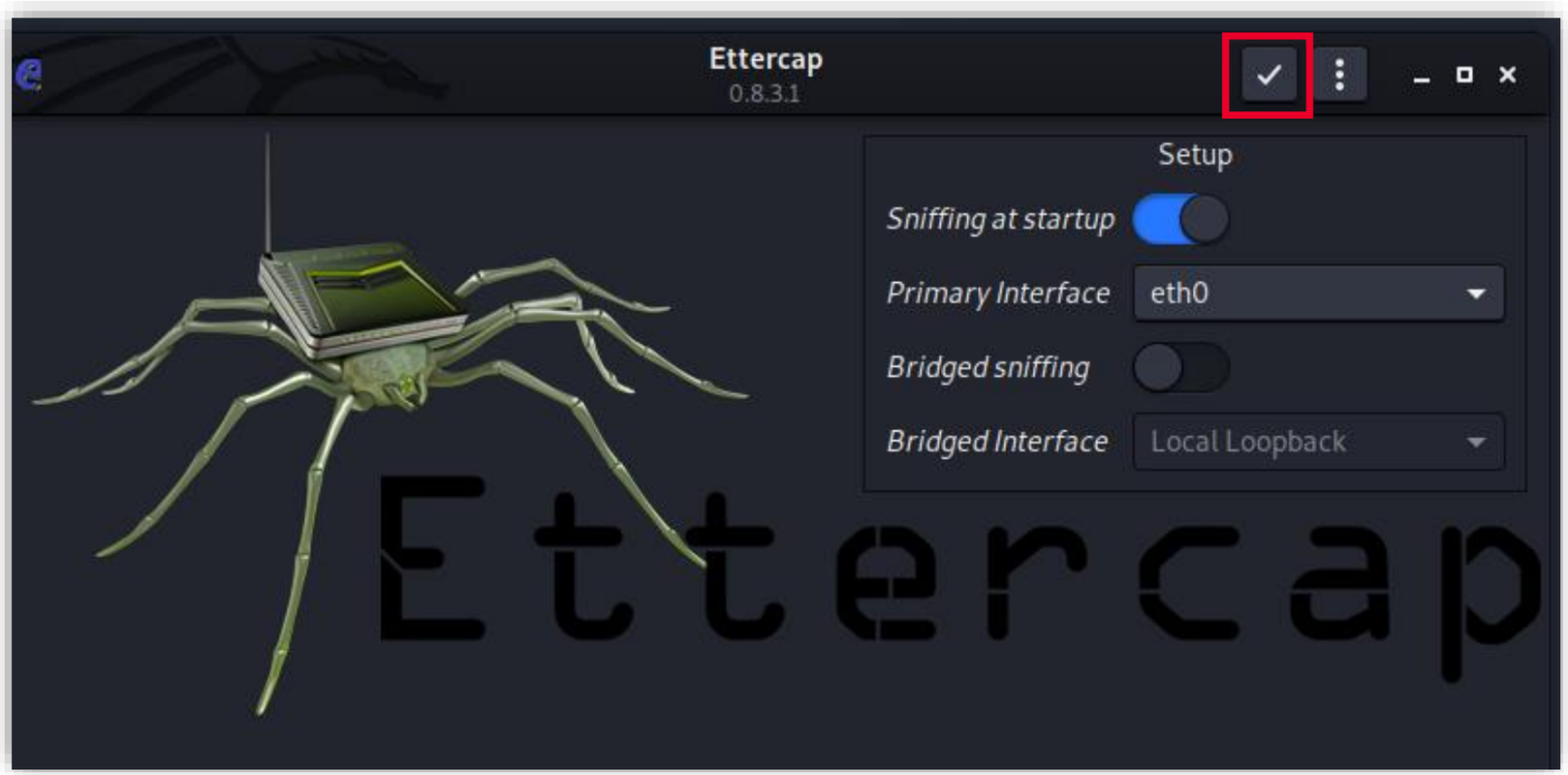


Ilustración 20: Ettercap.

5 SOLUCIONARIO EJERCICIO PRÁCTICO ACTIVIDAD 1

- Automáticamente el programa empezará a capturar el tráfico, pero antes deberás configurarlo.
  - Haz clic en el botón «*Stop*» que se encuentra en la parte superior izquierda.

Ilustración 21: Clic en «*Stop*» para configurar el programa Ettercap.

5 SOLUCIONARIO EJERCICIO PRÁCTICO ACTIVIDAD 1

- Para empezar el ataque, debes comprobar que aparecen las direcciones IP de las máquinas víctima.
  - Para ello, pulsa en el icono de tres puntos que hay en la parte superior derecha del programa, donde se desplegará un menú. Selecciona *Host* > *Scan for Host*. Espera a que Ettercap escanee la red.

Ilustración 22: Icono del menú desplegable en Ettercap.

5 SOLUCIONARIO EJERCICIO PRÁCTICO ACTIVIDAD 1

- Selecciona, en el mismo menú, *Host* > *Host List*, donde podrás ver la lista de las diferentes direcciones IP que ha detectado dentro de la red.

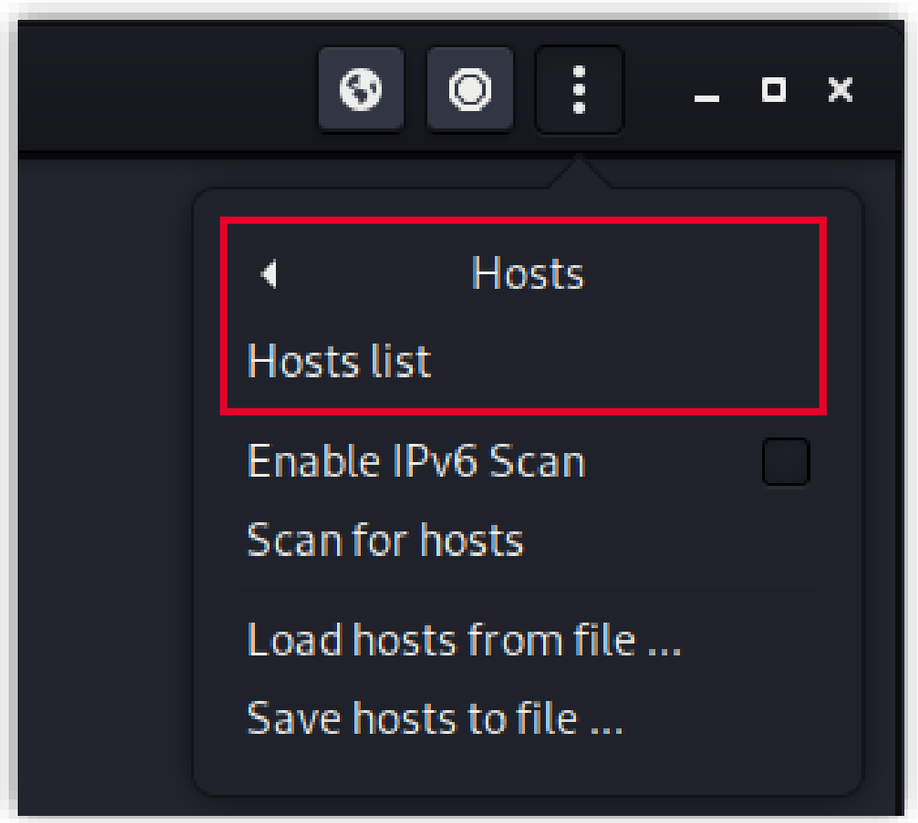


Ilustración 23: Menú *Host* > *Host List*

5 SOLUCIONARIO EJERCICIO PRÁCTICO ACTIVIDAD 1

- En esta lista, selecciona la dirección IP de la primera máquina víctima como *Target*1, que en este caso será la IP de la Metasploitable3. Para seleccionarlo, haz clic derecho sobre la IP de la Metasploitable3 y selecciona «*Add to Target* 1».

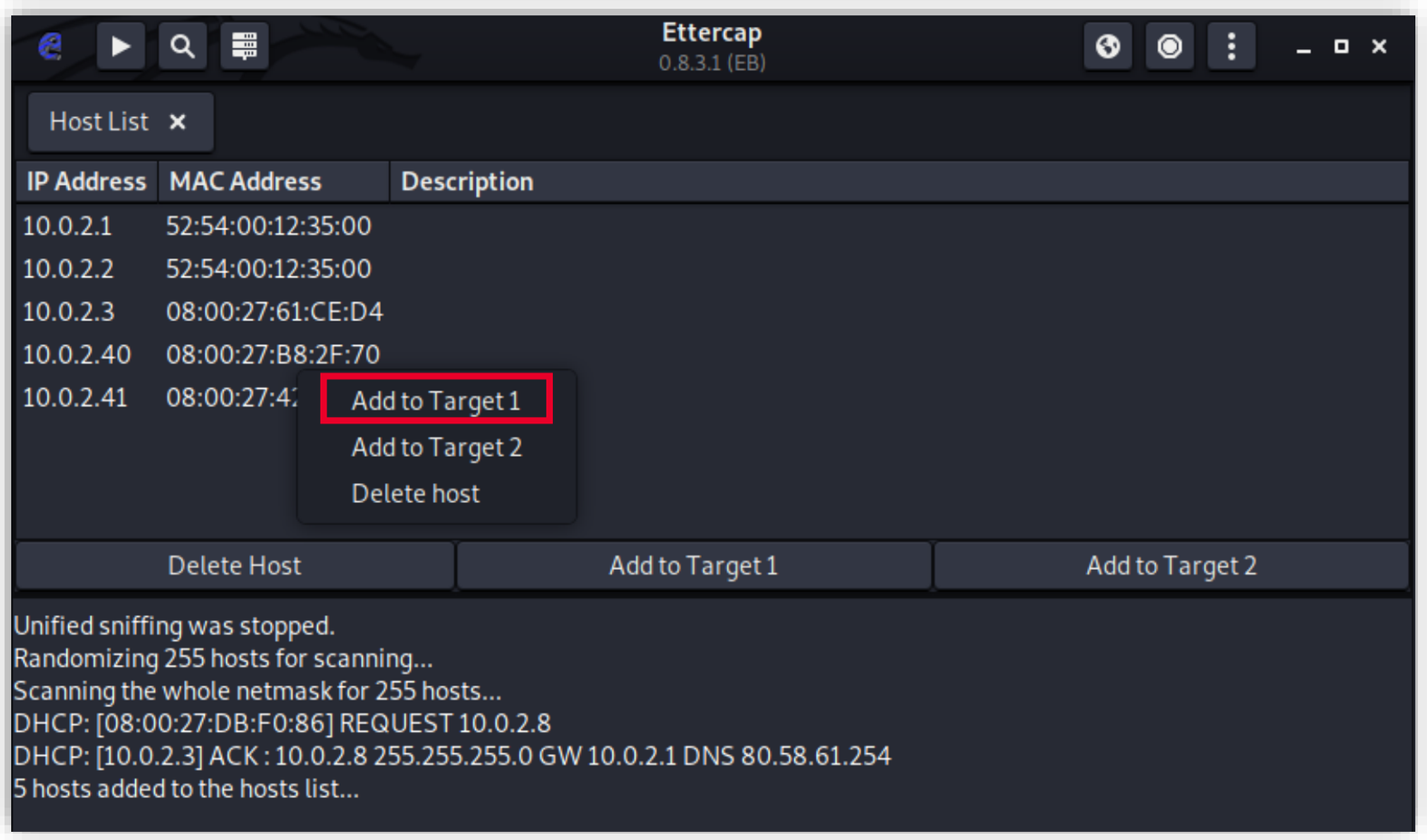


Ilustración 24: Menú Metasploitable3 > *Add to Target* 1.

5 SOLUCIONARIO EJERCICIO PRÁCTICO ACTIVIDAD 1

- Realiza el mismo paso con la IP de la máquina Ubuntu, pero en este caso añádela como *Target*2.
- Una vez tengas tus objetivos definidos, abre el menú seleccionando el símbolo con la bola del mundo marcado en la imagen y después «ARP *poisoning*».

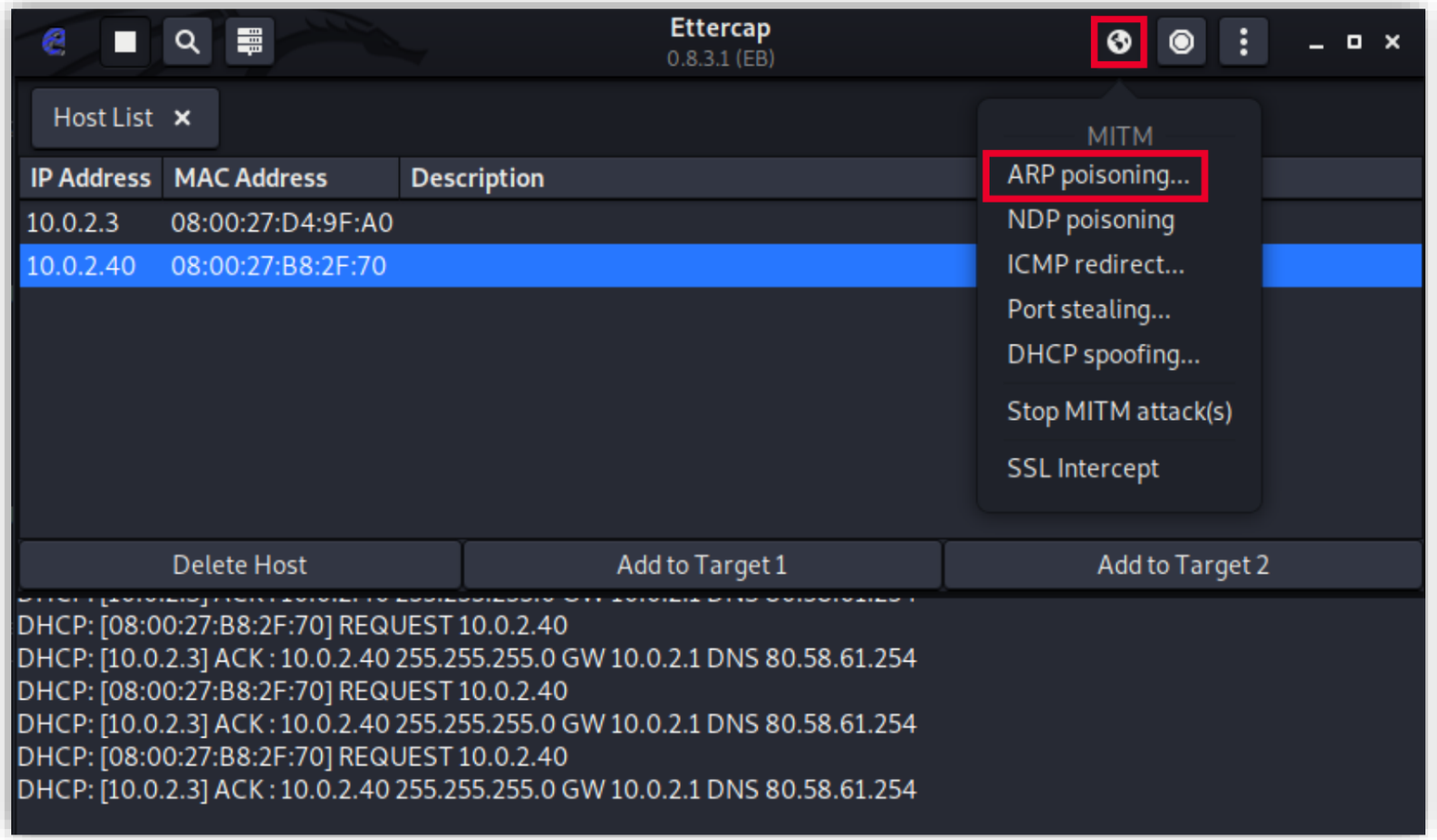


Ilustración 25: Ubicación del símbolo con la bola del mundo > ARP *poisoning*.

5 SOLUCIONARIO EJERCICIO PRÁCTICO ACTIVIDAD 1

- Selecciona «*Sniff remote connections*» y pulsa «*OK*».

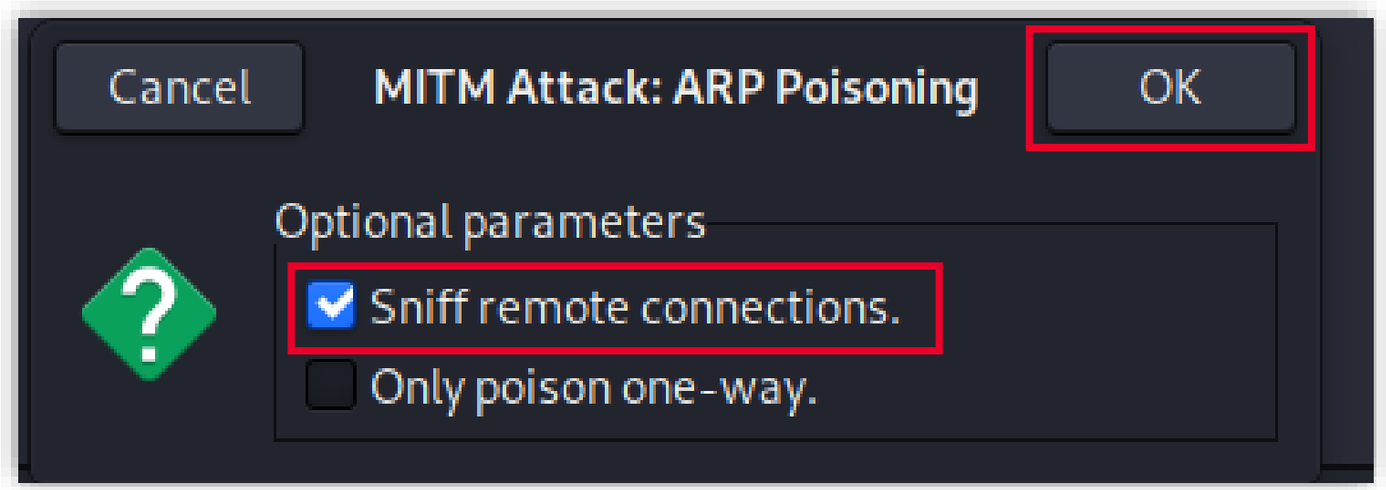


Ilustración 26: Opción «*Sniff remote connections*».

5 SOLUCIONARIO EJERCICIO PRÁCTICO ACTIVIDAD 1

- Para empezar a hacer el proceso de *sniffing*, haz clic sobre el icono de *Play* (marcado en la imagen) y empezará automáticamente.

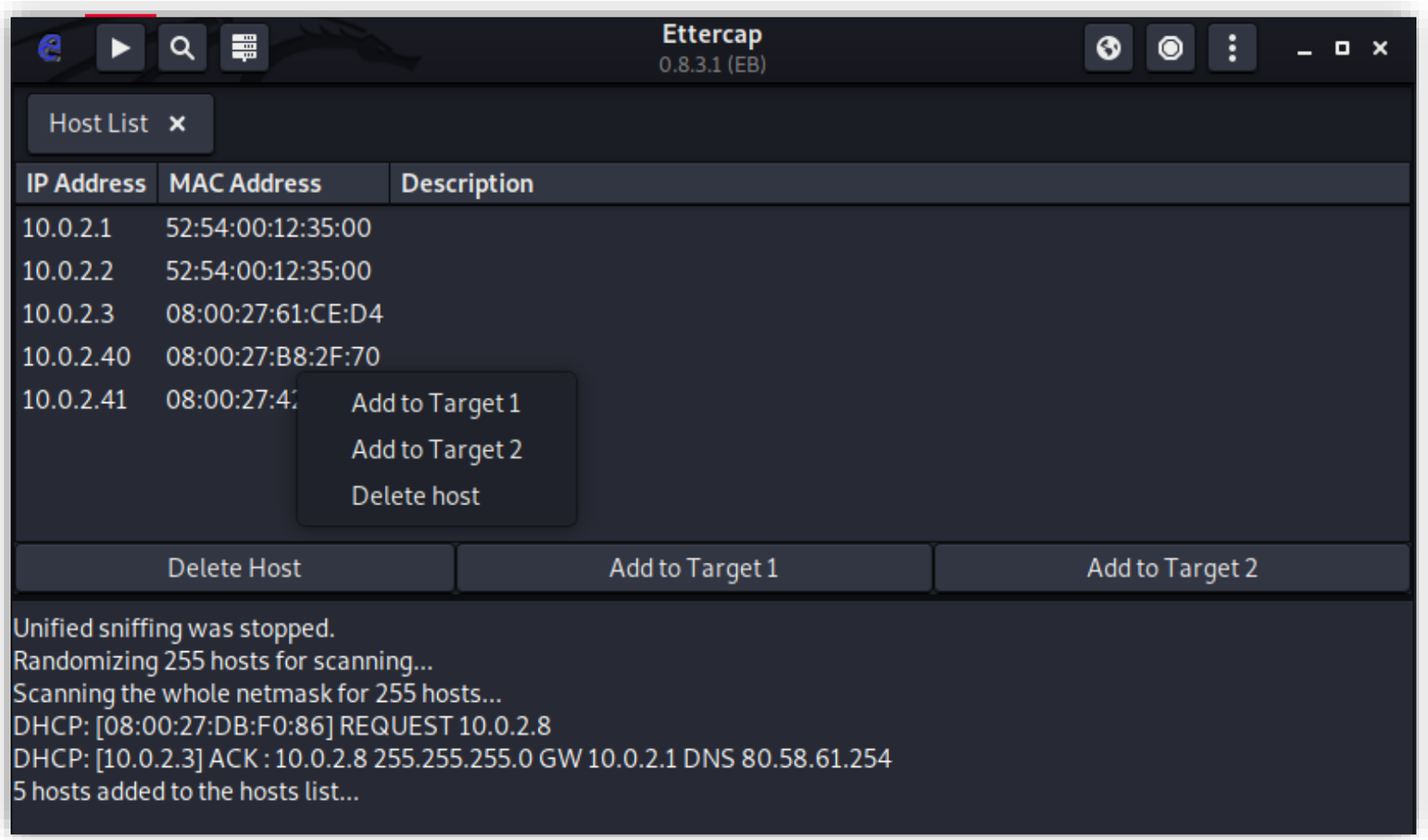


Ilustración 27: Clic en el icono de *Play*.

5 SOLUCIONARIO EJERCICIO PRÁCTICO ACTIVIDAD 1

- Para comprobar que ha funcionado correctamente, accede a la máquina Metasploitable3 y ejecuta el comando **arp –a**, con él podrás ver que ha otorgado la misma MAC a la dirección IP de la máquina atacante Kali que a la dirección IP de la máquina Ubuntu. Este comando muestra las tablas del protocolo ARP, que es el encargado de convertir las direcciones IP de cada ordenador en direcciones MAC. Con el sufijo -a podemos ver todas (all).

Dirección IP Ubuntu

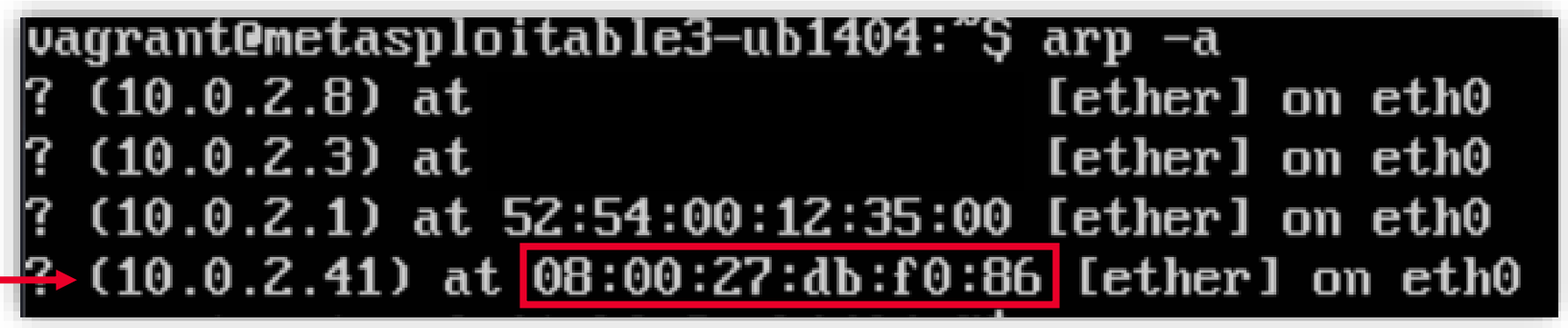


Ilustración 28: Direcciones IP de la máquina Kali y Ubuntu.

5 SOLUCIONARIO EJERCICIO PRÁCTICO ACTIVIDAD 1

- Si accedes a la máquina Ubuntu y ejecutas el mismo comando, vas a comprobar que sucede lo mismo, pero en este caso le otorga la misma MAC a la Metasploitable3 y a Kali.

Dirección IP Metasploitable

Dirección IP Kali Linux

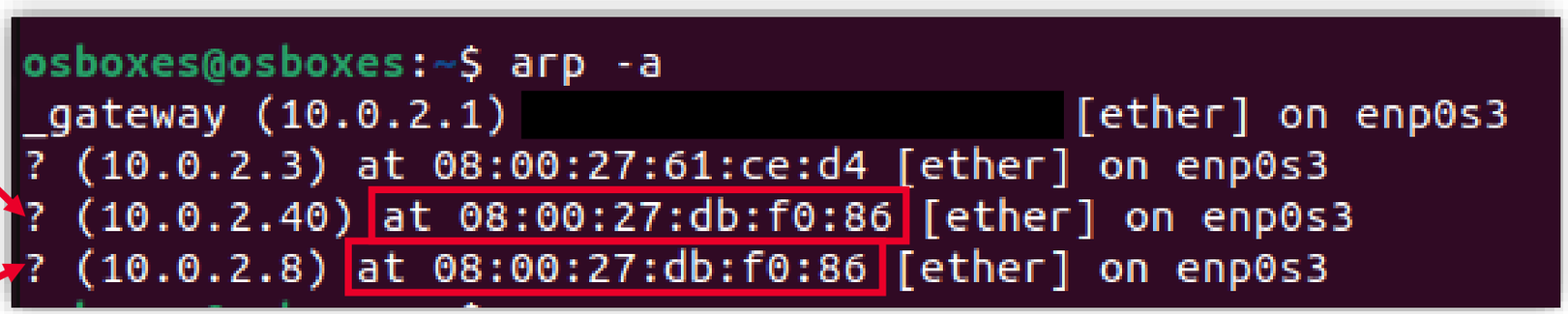


Ilustración 29: MAC de la máquina Kali y Ubuntu.

5 SOLUCIONARIO EJERCICIO PRÁCTICO ACTIVIDAD 1

- Por último, desde la máquina Metasploitable3, si accedes al navegador y escribes la dirección IP de la máquina Metasploitable3, es decir, 10.0.2.40 o *localhost*, vas a acceder a una interfaz virtual que te mostrará un listado de directorios del servidor del propio equipo, en este caso Metasploitable3. Es como si tu equipo se estuviese haciendo una petición a sí mismo. Así, vas a observar cómo funciona el ataque si la víctima hiciese *log in* en alguna página web.

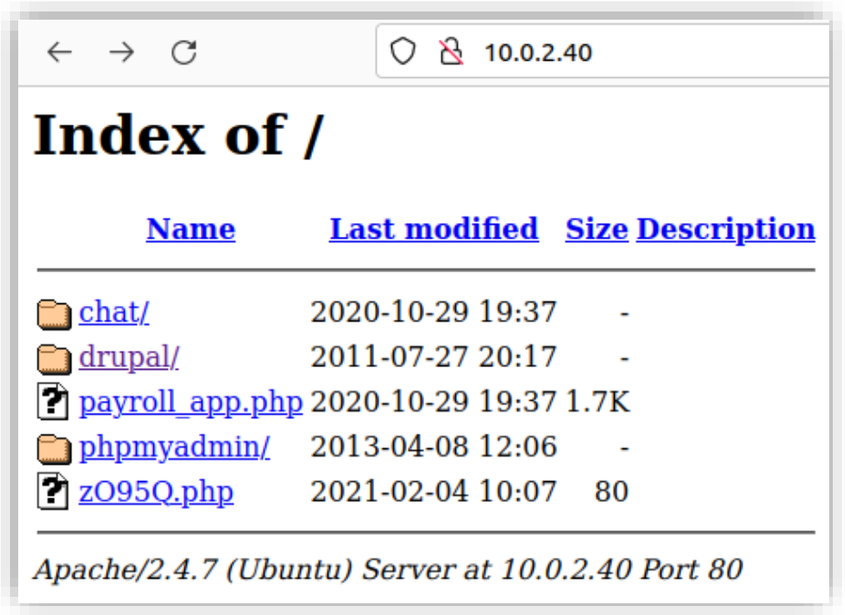


Ilustración 30: Dirección IP de páginas web.

5 SOLUCIONARIO EJERCICIO PRÁCTICO ACTIVIDAD 1

- Después, haz clic en el directorio «**drupal/**», donde encontrarás una página de *Log in* que podrás utilizar para comprobar si el ataque ha funcionado.

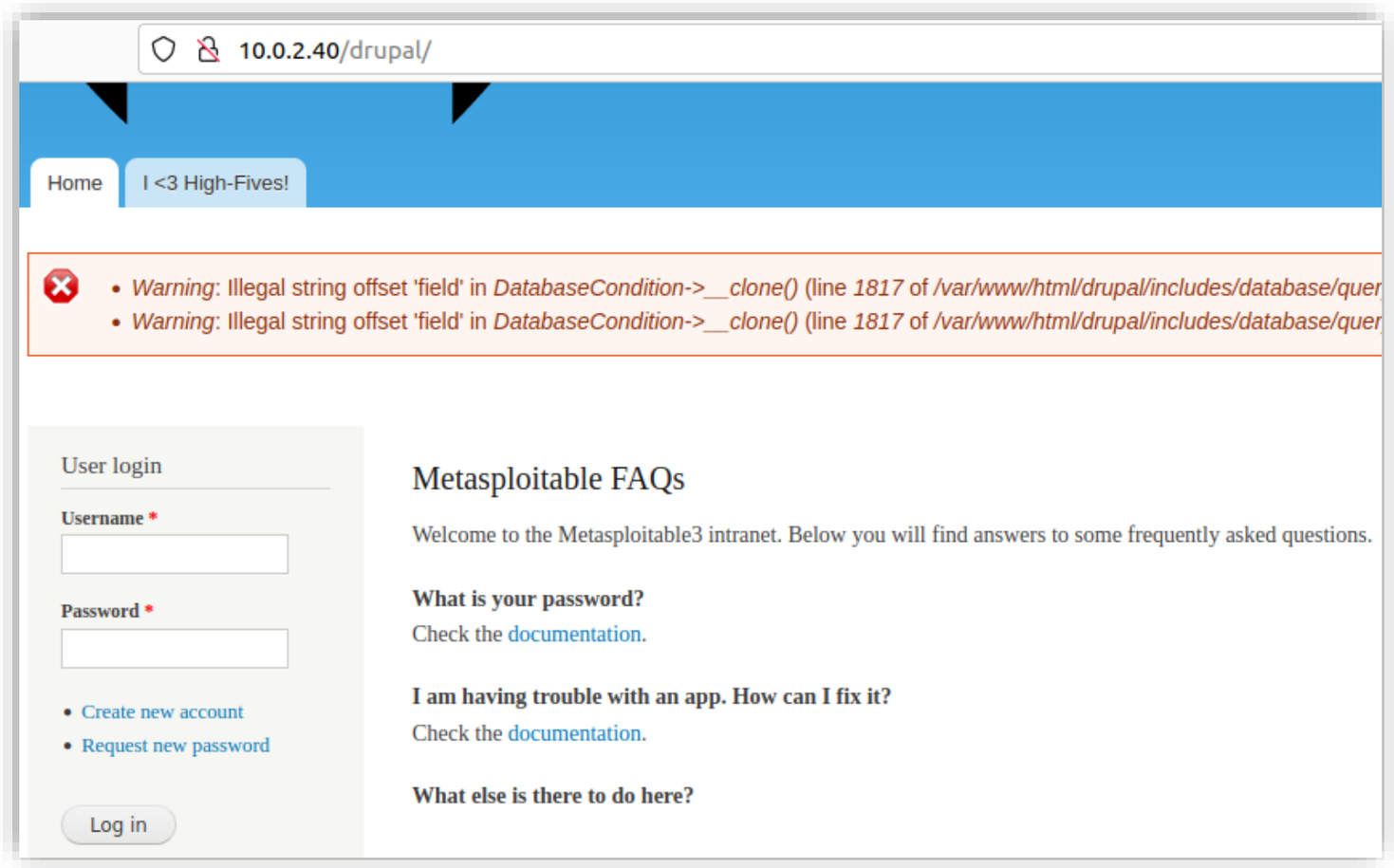


Ilustración 31: Página de inicio de una página web.

5 SOLUCIONARIO EJERCICIO PRÁCTICO ACTIVIDAD 1

- Introduce un usuario y contraseña aleatorio y haz clic en «*Log in*».
- Cuando se haya enviado el *Log in*, accede a la máquina Kali.
- En Ettercap aparecerá la captura de tráfico con los datos que has enviado desde la máquina víctima Ubuntu, incluidos los datos introducidos de usuario y contraseña.

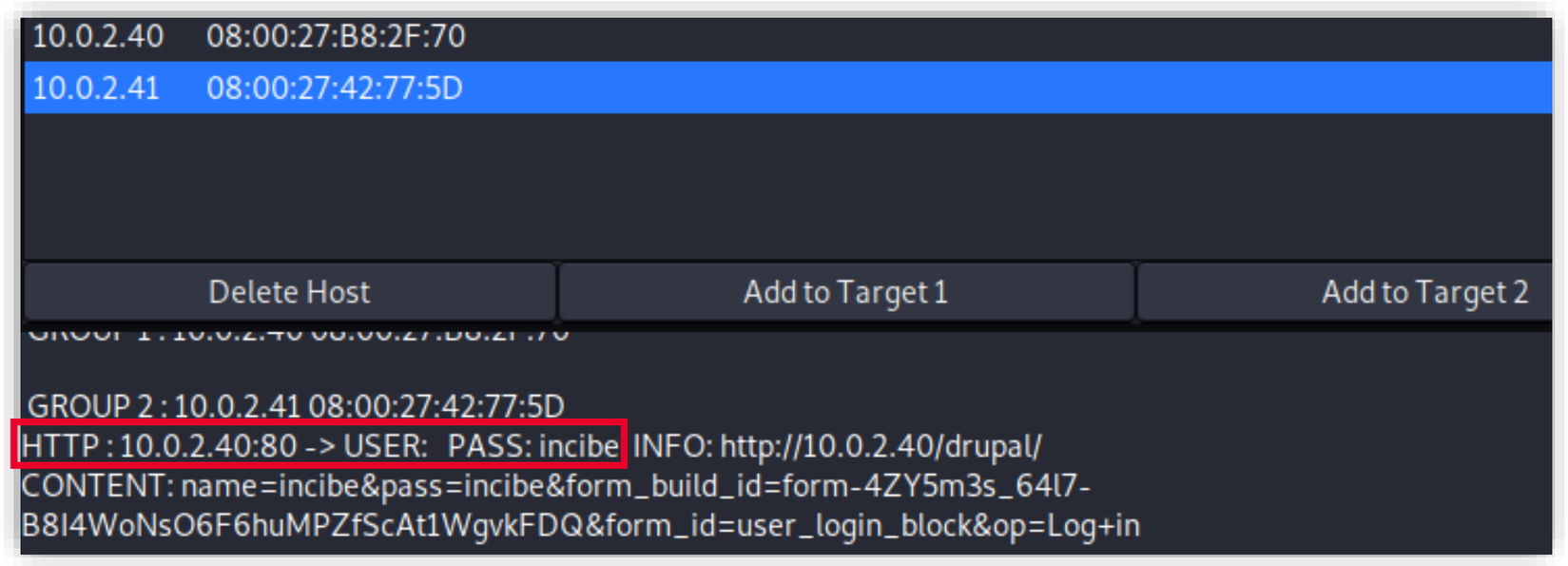


Ilustración 32: Captura de tráfico con los datos enviados desde la máquina Ubuntu.

5 SOLUCIONARIO EJERCICIO PRÁCTICO ACTIVIDAD 1

- Finalmente, se comprueba que cualquier acción que se realice entre estas máquinas será capturada por Ettercap.

¡GRACIAS!

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

017