

Práctica 6

Arranque de Herramientas Forenses desde la Red (PXE)

Índice

Índice.....	2
Pasos Previos:.....	3
1. Creación de Máquinas Virtuales (VM):.....	3
a. Debian:.....	3
Instalar y Configurar los Servicios Necesarios:.....	5
1. Instalar y Configurar TFTP.....	5
2. Instalar y Configurar DHCP.....	7
3. Instalar DNSmasq.....	8
4. Configuración de la Distribución (Kali).....	10
5. Creación de la Máquina Objetivo.....	13

Pasos Previos:

1. Creación de Máquinas Virtuales (VM):

a. Debian:

Configuramos la máquina virtual para que tenga 2GB de memoria Ram, 25 GB de disco duro.

Usamos una ISO de Debian x64.

The screenshot shows the configuration window for a new virtual machine in Oracle VM VirtualBox. The window is divided into several tabs: General, Sistema, Almacenamiento, and Audio. The General tab is selected, showing the name 'forense_practica_6', type 'Linux', subtype 'Debian', and version 'Debian (64-bit)'. A red arrow points to the version dropdown. The Sistema tab is also visible, showing the memory base set to 2048 MB and the boot order with 'Disquete' and 'Óptica' selected. A red arrow points to the memory slider. The Almacenamiento tab is selected, showing the storage controller 'IDE' and the disk 'forense_practica_6.vdi'. A red arrow points to the disk name. The Attributes section shows the disk type as 'Puerto SATA 0' and the format as 'Normal (VDI)'. The Information section shows the virtual size as 25,00 GB and the actual size as 2,00 MB. The Audio tab is also visible, showing the 'Habilitar audio' checkbox checked.

General

Básico Avanzado Descripción Cifrado de disco

Nombre: forense_practica_6

Tipo: Linux x64

Subtipo: Debian

Versión: Debian (64-bit)

Sistema

Placa base Procesador Aceleración

Memoria base: 2048 MB

Orden de arranque: ☒ Disquete ☒ Óptica

Almacenamiento

Dispositivos

Controlador: IDE

debian-12.8.0-amd64-netinst.iso

Controlador: SATA

forense_practica_6.vdi

Atributos

Disco duro: Puerto SATA 0

☐ Unidad de estado sólido

☐ Conectable en caliente

Información

Tipo (formato): Normal (VDI)

Virtual size: 25,00 GB

Actual size: 2,00 MB

Detalles de almacenamiento: Almacenamiento reserva..

Ubicación: C:\Users\Fortuna_457\Vi...

Conectado a: forense_practica_6

Encryption key: --

Audio

☒ Habilitar audio

ANÁLISIS FORENSE

Red

Adaptador 1 Adaptador 2 Adaptador 3 Adaptador 4

☒ Habilitar adaptador de red

Conectado a: Red interna

Nombre: forense_interna

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

Modo promiscuo: Denegar

Dirección MAC: 080027B275DE

☒ Cable conectado

Puertos serie

Puerto 1 Puerto 2 Puerto 3 Puerto 4

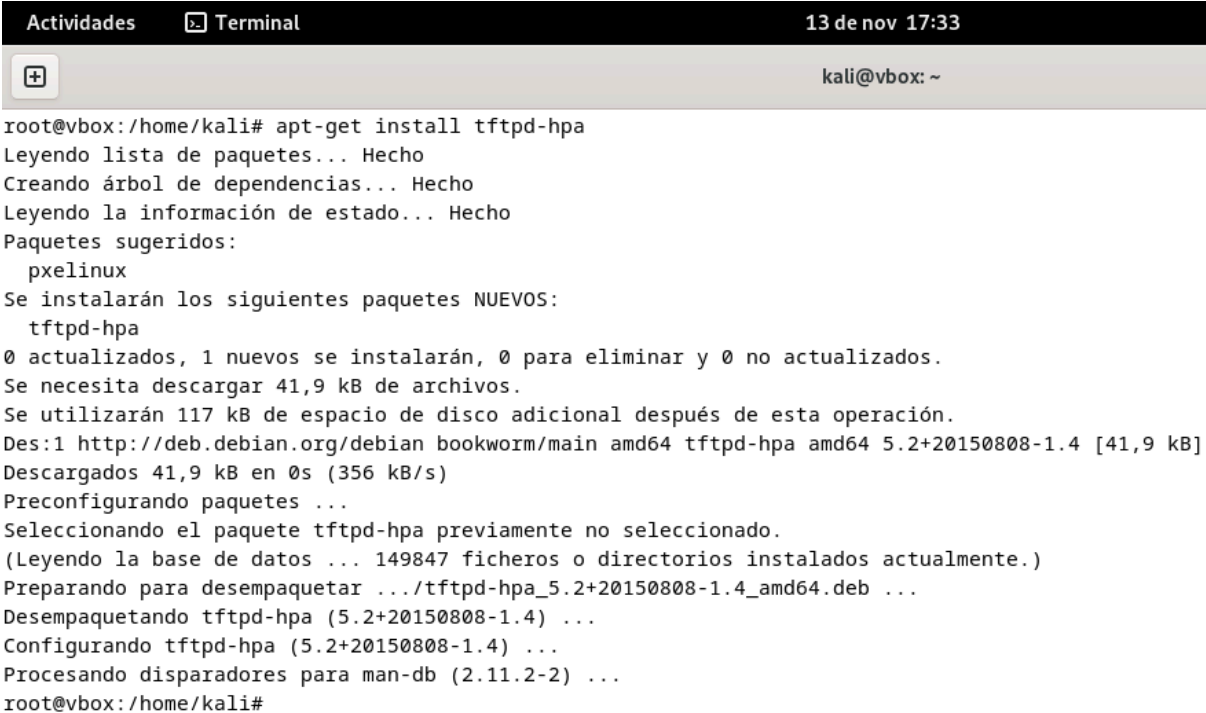
Aceptar Cancelar Ayuda

Instalar y Configurar los Servicios Necesarios:

1. Instalar y Configurar TFTP.

Ejecutamos el comando:

sudo apt-get install tftpd-hpa



```

Actividades  Terminal  13 de nov 17:33
kali@vbox: ~

root@vbox:/home/kali# apt-get install tftpd-hpa
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Paquetes sugeridos:
  pxelinux
Se instalarán los siguientes paquetes NUEVOS:
  tftpd-hpa
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 41,9 kB de archivos.
Se utilizarán 117 kB de espacio de disco adicional después de esta operación.
Des:1 http://deb.debian.org/debian bookworm/main amd64 tftpd-hpa amd64 5.2+20150808-1.4 [41,9 kB]
Descargados 41,9 kB en 0s (356 kB/s)
Preconfigurando paquetes ...
Seleccionando el paquete tftpd-hpa previamente no seleccionado.
(Leyendo la base de datos ... 149847 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../tftpd-hpa_5.2+20150808-1.4_amd64.deb ...
Desempaquetando tftpd-hpa (5.2+20150808-1.4) ...
Configurando tftpd-hpa (5.2+20150808-1.4) ...
Procesando disparadores para man-db (2.11.2-2) ...
root@vbox:/home/kali#
  
```

Editamos el archivo **/etc/default/tftpd-hpa** y cambiamos el puerto a 70 en caso de que el puerto por defecto esté ocupado.



```

Actividades  Terminal
GNU nano 7.2
# /etc/default/tftpd-hpa

TFTP_USERNAME="tftp"
TFTP_DIRECTORY="/srv/tftp"
TFTP_ADDRESS=":70"
TFTP_OPTIONS="--secure"
  
```

Creamos la siguiente carpeta.

```
root@vbox:/home/kali# mkdir -p /srv/tftp/
```

Ejecutamos el siguiente comandos para instalar el pxelinux:

apt install pxelinux syslinux-common

```
root@vbox:/home/kali# apt install pxelinux syslinux-common
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
syslinux-common ya está en su versión más reciente (3:6.04~git20190206.bf6db5b4+dfsg1-3).
fijado syslinux-common como instalado manualmente.
Se instalarán los siguientes paquetes NUEVOS:
  pxelinux
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 156 kB de archivos.
Se utilizarán 246 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

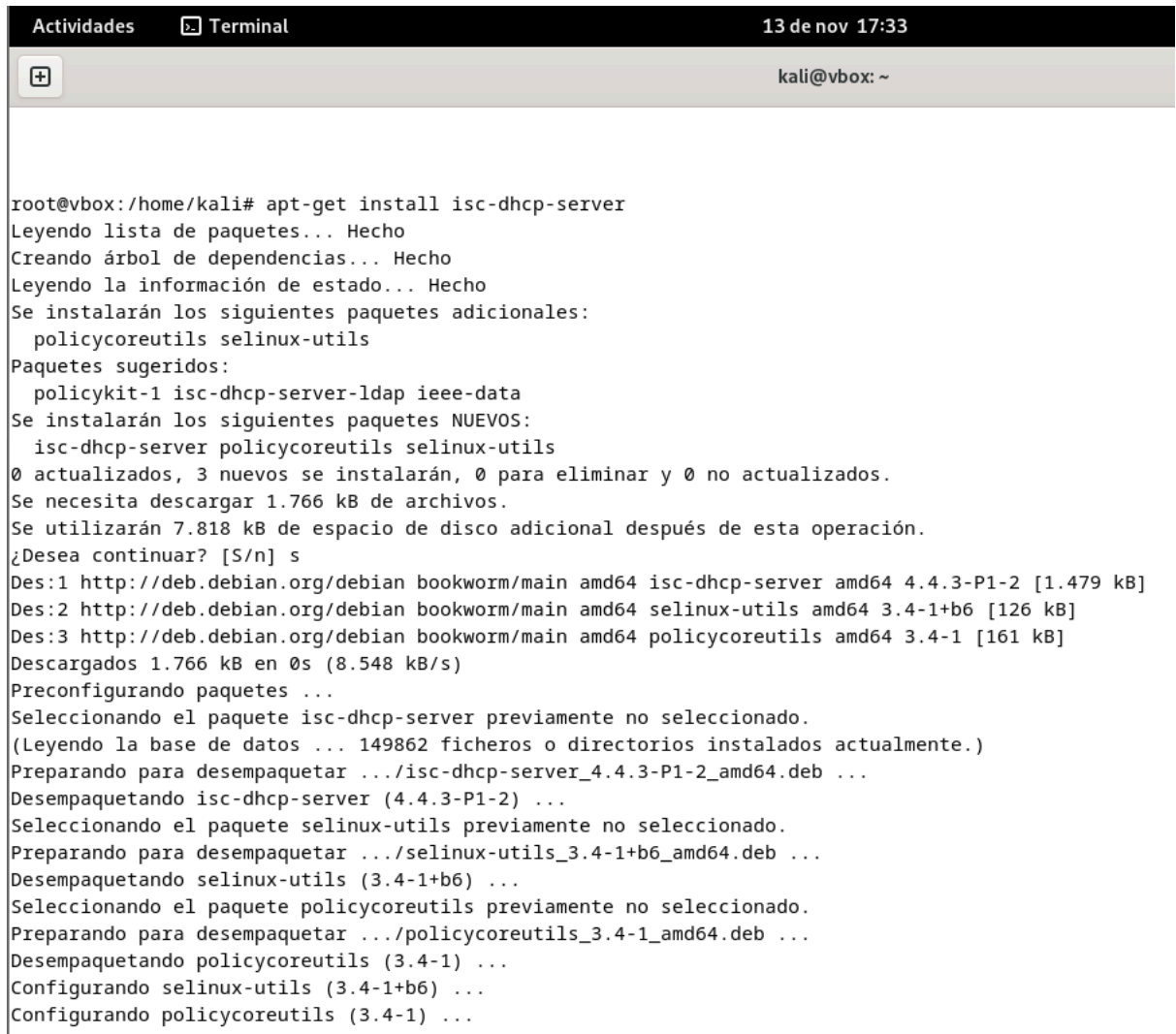
Copiamos el contenido de lo que acabamos de instalar en la carpeta anterior.

```
root@vbox:/home/kali# cp /usr/lib/PXELINUX/pxelinux.0 /srv/tftp/
```

2. Instalar y Configurar DHCP.

Ejecuta:

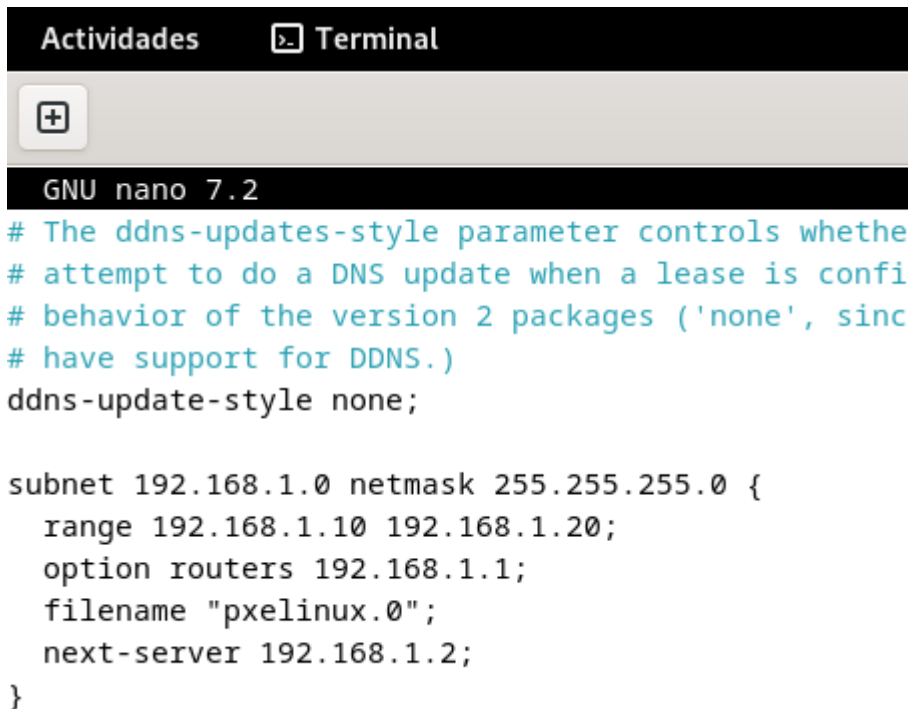
```
sudo apt-get install isc-dhcp-server
```



The screenshot shows a terminal window titled 'Terminal' with the date and time '13 de nov 17:33'. The user is logged in as 'kali@vbox: ~'. The terminal output shows the command 'apt-get install isc-dhcp-server' being executed. The output includes the following text:

```
root@vbox:/home/kali# apt-get install isc-dhcp-server
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  policycoreutils selinux-utils
Paquetes sugeridos:
  policykit-1 isc-dhcp-server-ldap ieee-data
Se instalarán los siguientes paquetes NUEVOS:
  isc-dhcp-server policycoreutils selinux-utils
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 1.766 kB de archivos.
Se utilizarán 7.818 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://deb.debian.org/debian bookworm/main amd64 isc-dhcp-server amd64 4.4.3-P1-2 [1.479 kB]
Des:2 http://deb.debian.org/debian bookworm/main amd64 selinux-utils amd64 3.4-1+b6 [126 kB]
Des:3 http://deb.debian.org/debian bookworm/main amd64 policycoreutils amd64 3.4-1 [161 kB]
Descargados 1.766 kB en 0s (8.548 kB/s)
Preconfigurando paquetes ...
Seleccionando el paquete isc-dhcp-server previamente no seleccionado.
(Leyendo la base de datos ... 149862 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../isc-dhcp-server_4.4.3-P1-2_amd64.deb ...
Desempaquetando isc-dhcp-server (4.4.3-P1-2) ...
Seleccionando el paquete selinux-utils previamente no seleccionado.
Preparando para desempaquetar .../selinux-utils_3.4-1+b6_amd64.deb ...
Desempaquetando selinux-utils (3.4-1+b6) ...
Seleccionando el paquete policycoreutils previamente no seleccionado.
Preparando para desempaquetar .../policycoreutils_3.4-1_amd64.deb ...
Desempaquetando policycoreutils (3.4-1) ...
Configurando selinux-utils (3.4-1+b6) ...
Configurando policycoreutils (3.4-1) ...
```

Configura el archivo **/etc/dhcp/dhcpd.conf** para asignar direcciones IP y proporcionar la ubicación de los archivos PXE.



```

GNU nano 7.2
# The ddns-updates-style parameter controls whethe
# attempt to do a DNS update when a lease is confi
# behavior of the version 2 packages ('none', sinc
# have support for DDNS.)
ddns-update-style none;

subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.10 192.168.1.20;
    option routers 192.168.1.1;
    filename "pxelinux.0";
    next-server 192.168.1.2;
}

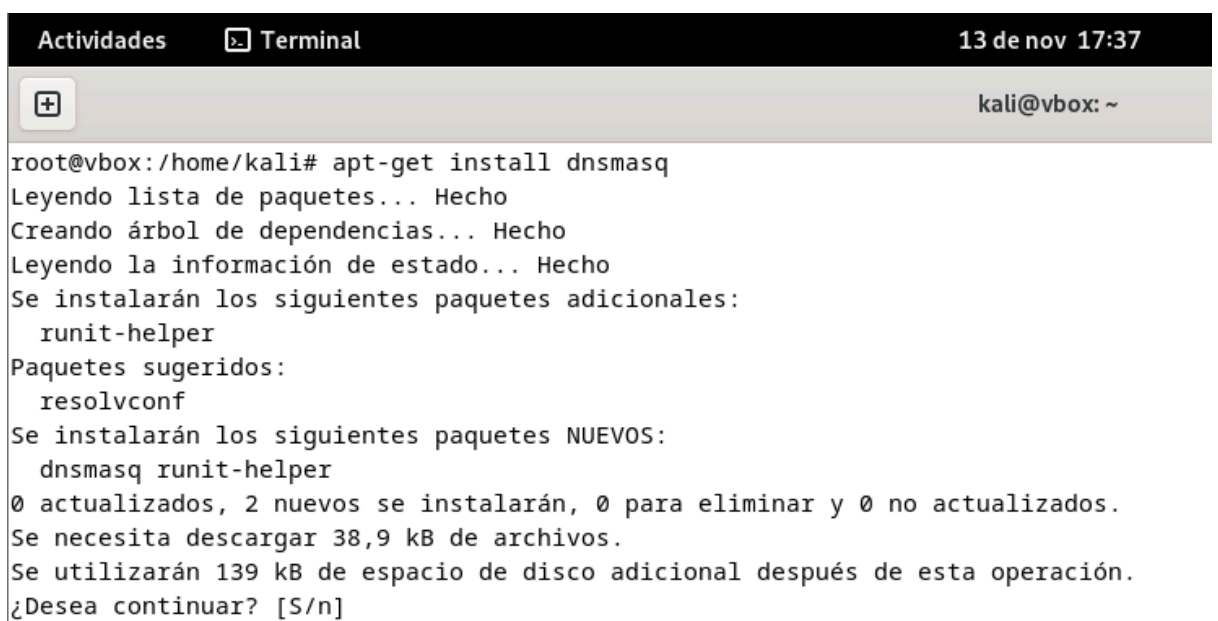
```

3. Instalar DNSmasq.

DNSmasq puede combinar DHCP y TFTP en un solo servicio, simplificando la configuración.

Lo instalamos con:

sudo apt-get install dnsmasq

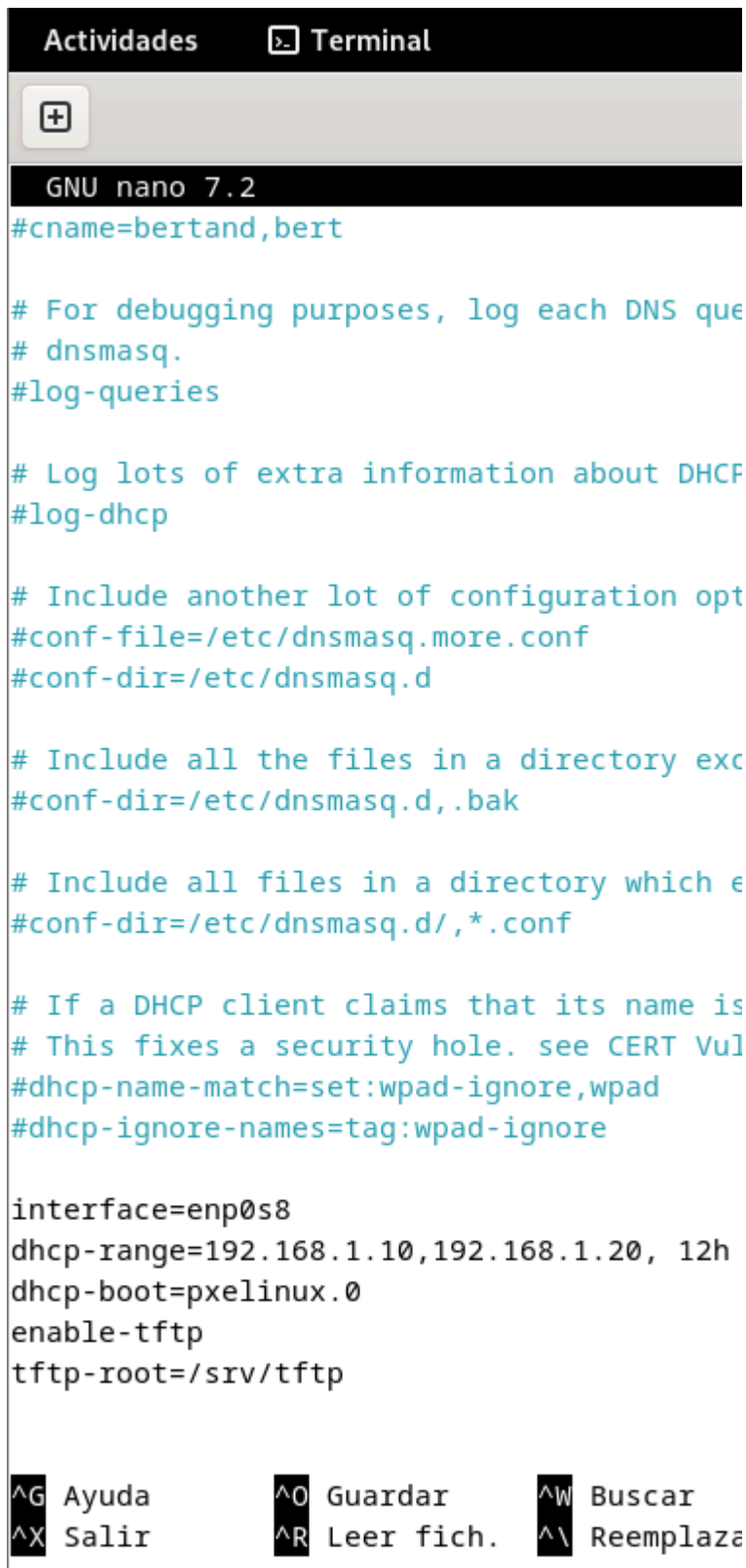


```

Actividades Terminal 13 de nov 17:37
kali@vbox: ~
root@vbox:/home/kali# apt-get install dnsmasq
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  runit-helper
Paquetes sugeridos:
  resolvconf
Se instalarán los siguientes paquetes NUEVOS:
  dnsmasq runit-helper
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 38,9 kB de archivos.
Se utilizarán 139 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]

```


Configura **/etc/dnsmasq.conf** para establecer el entorno de PXE.



```

GNU nano 7.2
#cname=bertand,bert

# For debugging purposes, log each DNS que
# dnsmasq.
#log-queries

# Log lots of extra information about DHCP
#log-dhcp

# Include another lot of configuration opt
#conf-file=/etc/dnsmasq.more.conf
#conf-dir=/etc/dnsmasq.d

# Include all the files in a directory exc
#conf-dir=/etc/dnsmasq.d,.bak

# Include all files in a directory which e
#conf-dir=/etc/dnsmasq.d/*.conf

# If a DHCP client claims that its name is
# This fixes a security hole. see CERT Vul
#dhcp-name-match=set:wpad-ignore,wpad
#dhcp-ignore-names=tag:wpad-ignore

interface=enp0s8
dhcp-range=192.168.1.10,192.168.1.20, 12h
dhcp-boot=pxelinux.0
enable-tftp
tftp-root=/srv/tftp

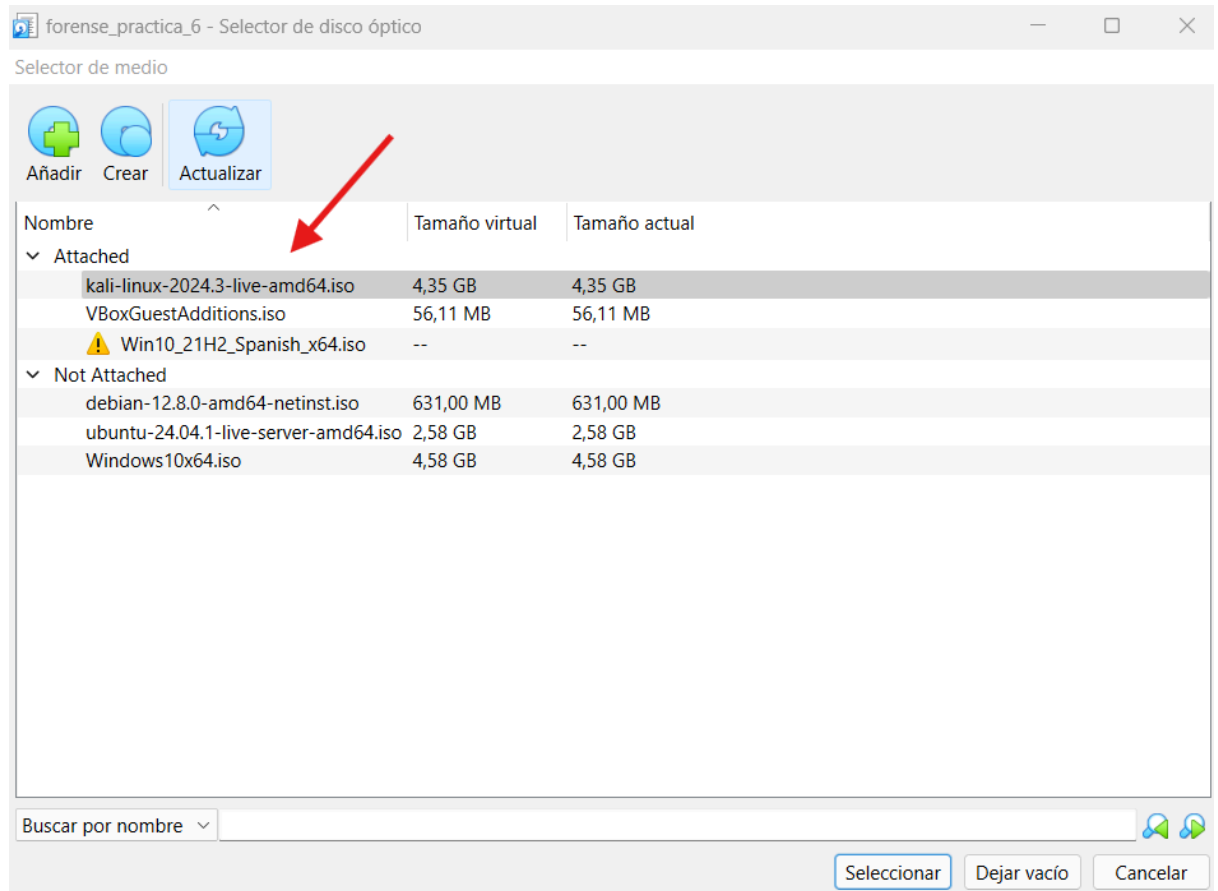
^G Ayuda      ^O Guardar    ^W Buscar
^X Salir      ^R Leer fich. ^\ Reemplaza
  
```

Reiniciamos el servicio.

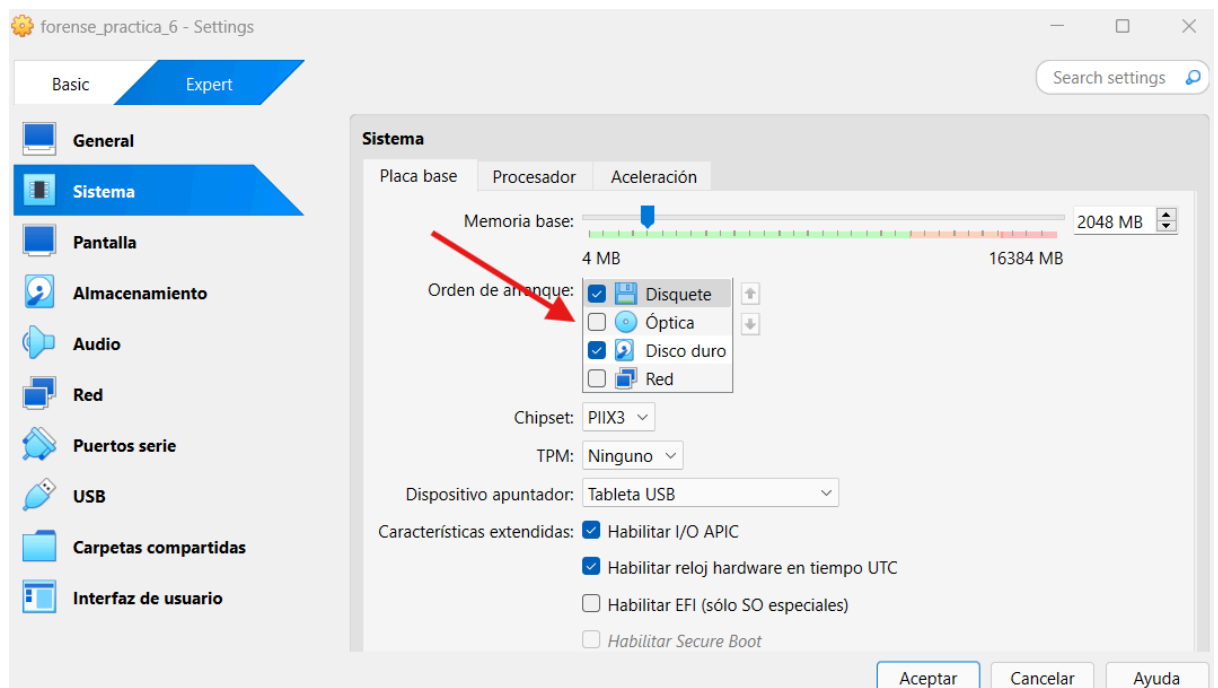
```
root@vbox:/home/kali# systemctl restart dnsmasq
```

4. Configuración de la Distribución (Kali).

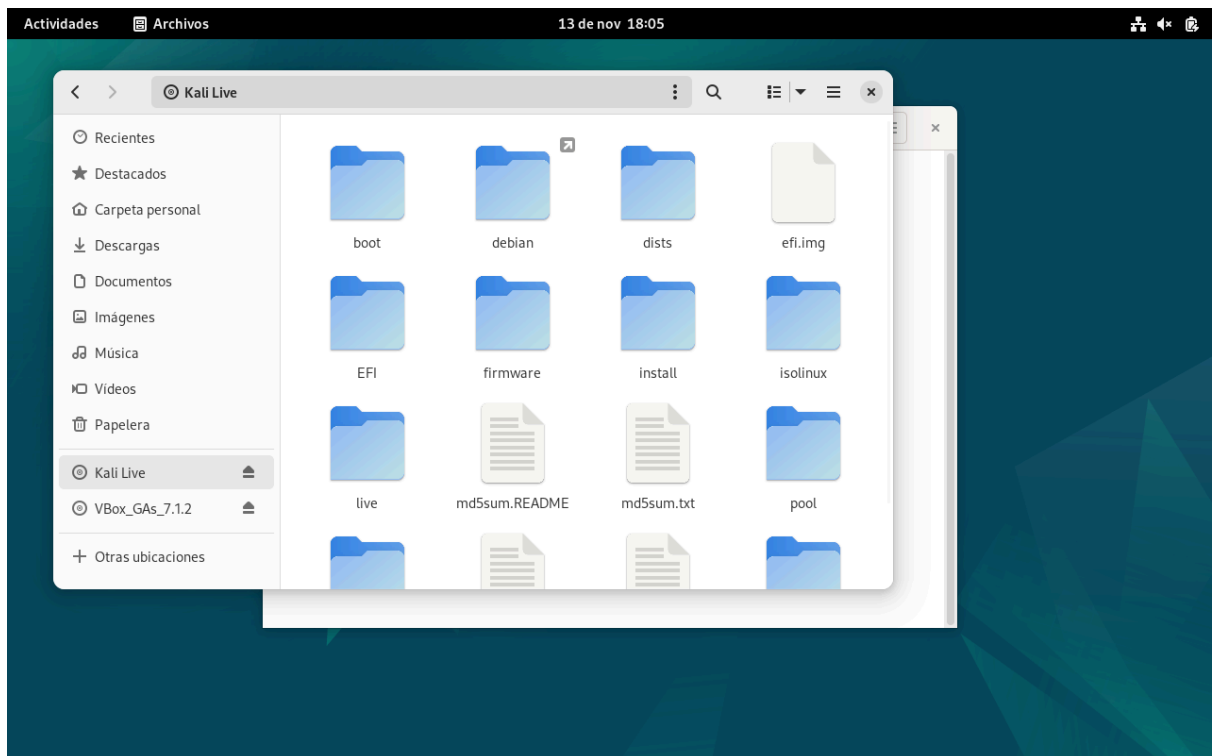
Cargamos el kali-live en la unidad óptica.



Quitamos el arranque desde unidad óptica.



Comprobamos que se ha cargado el disco del kali-live.



Ejecutamos el comando:

lsblk

Para saber dónde está el disco con el kali-live.

Y así poder montarlo con el comando:

mount /dev/sr1 /mnt/

```
root@vbox:/home/kali# lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda          8:0    0   25G  0 disk
├─sda1       8:1    0   24G  0 part /
├─sda2       8:2    0    1K  0 part
└─sda5       8:5    0   975M  0 part [SWAP]
sr0         11:0    1 56,1M  0 rom
sr1         11:1    1  4,3G  0 rom  /media/kali/Kali Live
root@vbox:/home/kali# mount /dev/sr1 /mnt/
```

Comprobamos que se ha montado.

```
root@vbox:/home/kali# ls /mnt/
boot    EFI        install  md5sum.README  pool-udeb      tools
debian  efi.img     isolinux md5sum.txt      sha256sum.README
dists   firmware  live     pool            sha256sum.txt
root@vbox:/home/kali#
```

Creamos la siguiente carpeta.

```
root@vbox:/home/kali# mkdir /srv/tftp/kali
root@vbox:/home/kali#
```


Y movemos todo el contenido que hemos montado en mnt a la carpeta que acabamos de crear.

```
root@vbox:/home/kali# cp -r /mnt/* /srv/tftp/kali/
```

Creamos la siguiente carpeta, y creamos el archivo indicado.

```
root@vbox:/home/kali# mkdir -p /srv/tftp/pxelinux.cfg
root@vbox:/home/kali# nano /srv/tftp/pxelinux.cfg/default
```

Escribimos la siguiente configuración.



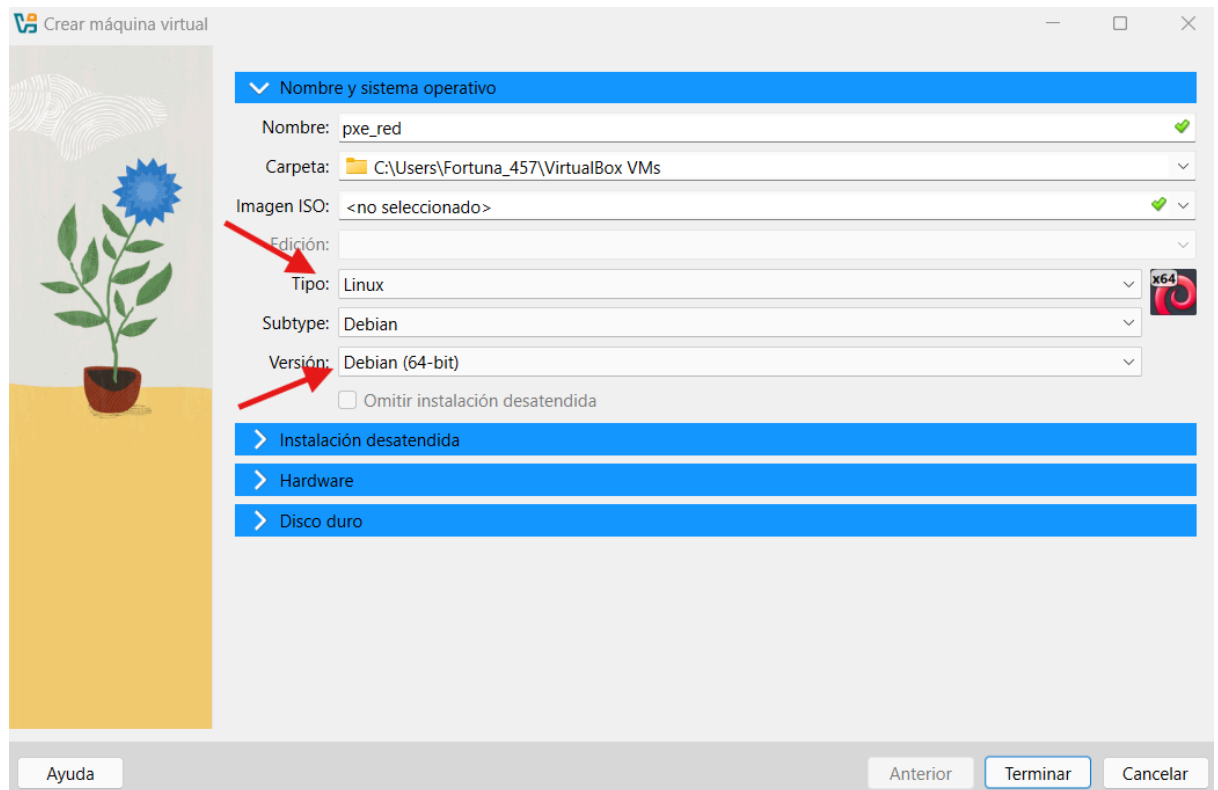
```
Actividades  Terminal  13 de nov 18:19
kali@vbox: ~
GNU nano 7.2 /srv/tftp/pxelinux.cfg/default *
DEFAULT kali
LABEL kali
    KERNEL /kali/live/vmlinuz
    APPEND initrd=/kali/live/initrd.img boot=live fetch=tftp://192.168.1.1/kali/live/filesystem.squashfs ip=dhcp
    PROMPT 0
    TIMEOUT 50
```

Y cambiamos los permisos a la carpeta tft.

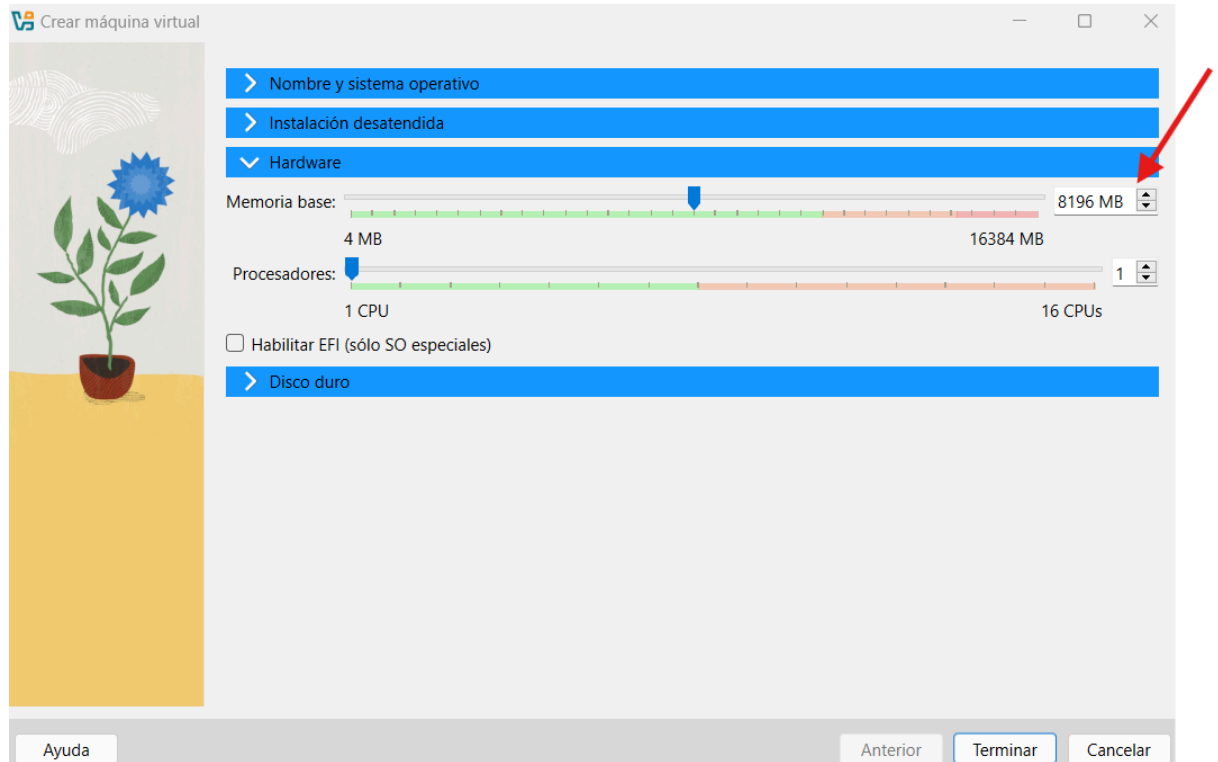
```
root@vbox:/home/kali# chmod -R 755 /srv/tftp/
root@vbox:/home/kali#
```

5. Creación de la Máquina Objetivo.

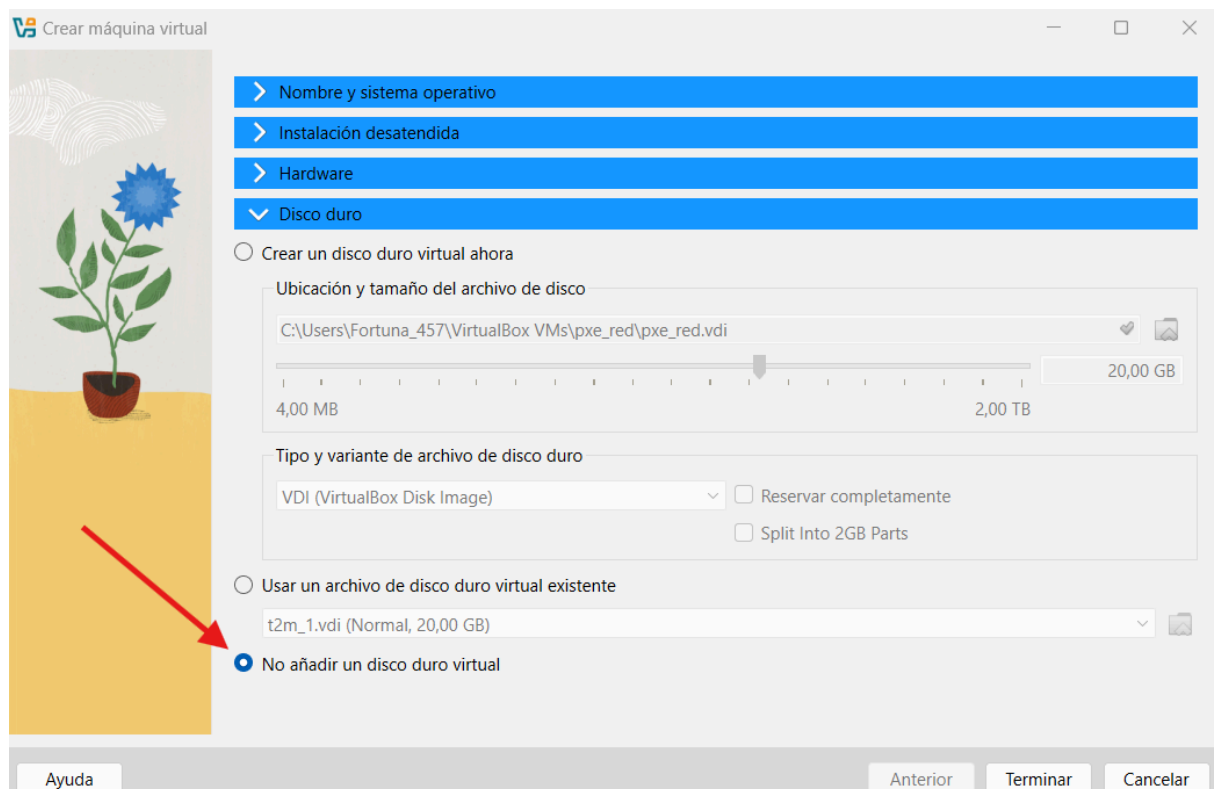
Seleccionamos una distribución de Debian x64.



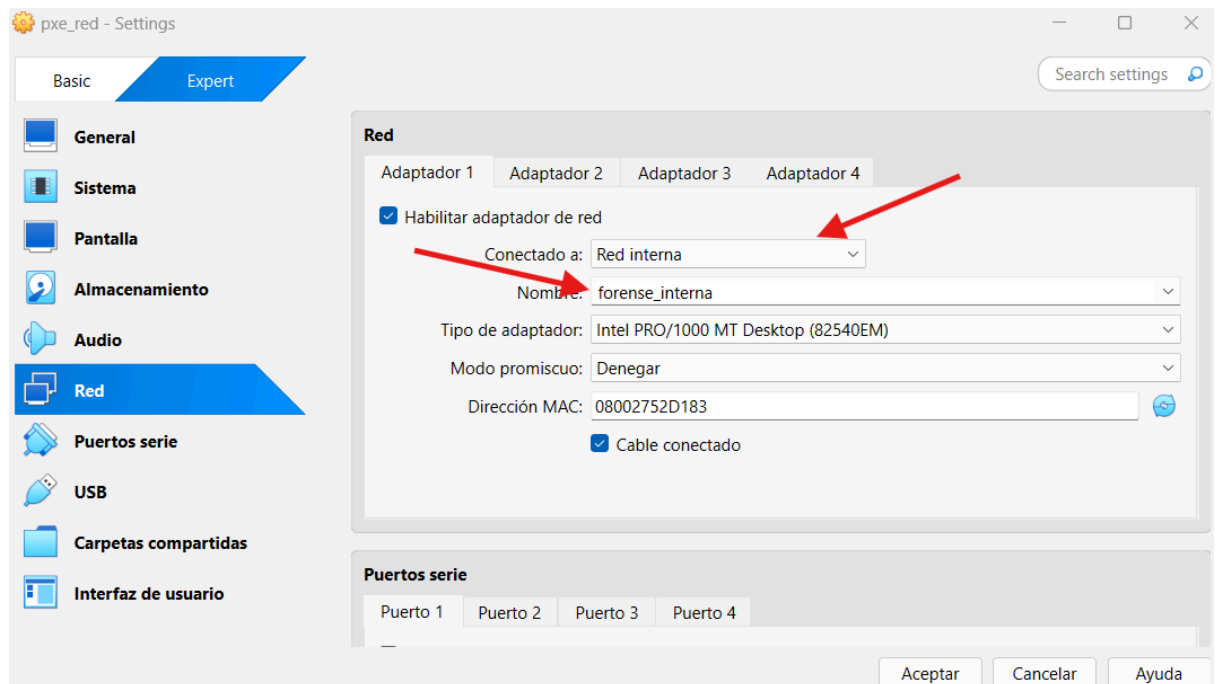
Le ponemos hasta 8 Gb de RAM, ya que el sistema operativo se cargará inicialmente en la RAM.



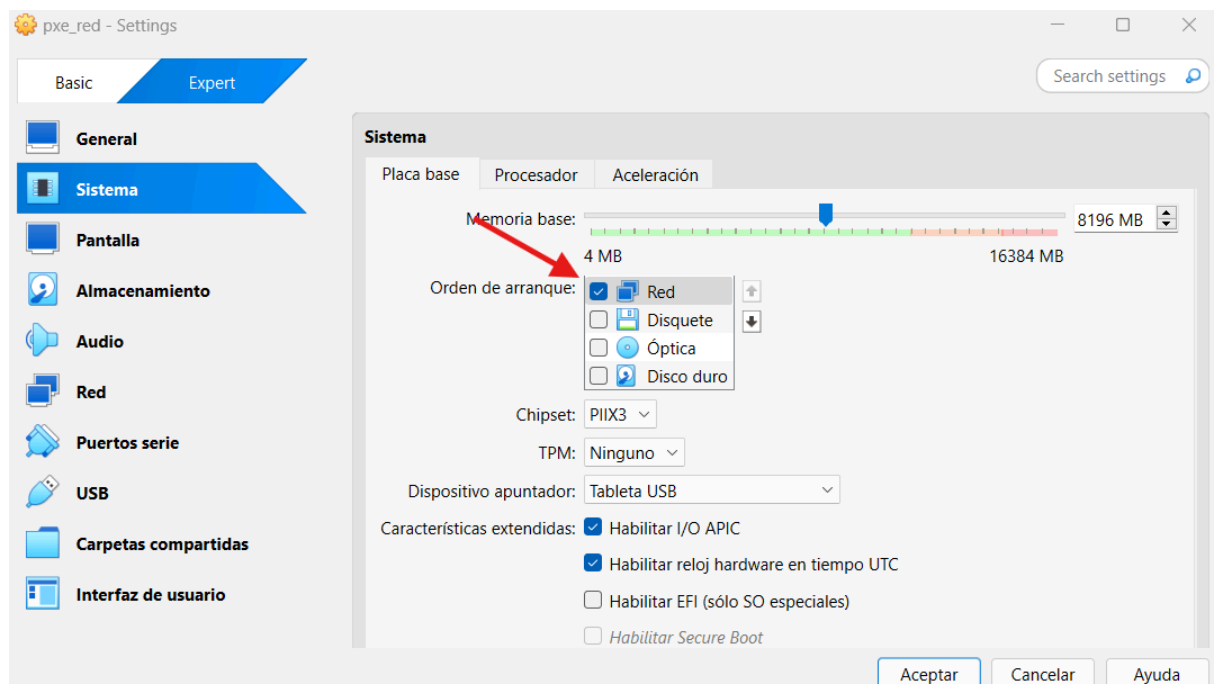
Por último, no añadimos disco. Pues todo se va a hacer desde la memoria RAM.



Especificamos que ha de estar en la misma red interna que nuestra estación forense.



Por último, solo dejamos seleccionado el arranque por red.



Al arrancar la máquina virtual desde la red nos dará este fallo.

```

iPXE (PCI E2:00.0) starting execution...ok
iPXE initialising devices...ok

iPXE 1.21.1 -- Open Source Network Boot Firmware -- http://ipxe.org
Features: DNS TFTP PXE PXEXT

net0: 08:00:27:52:d1:83 using 82540em on 0000:00:03.0 (open)
  [Link:down, TX:0 TXE:0 RX:0 RXE:0]
  [Link status: Down (http://ipxe.org/38086101)]
Waiting for link-up on net0.... ok
Configuring (net0 08:00:27:52:d1:83).... ok
net0: 192.168.1.12/255.255.255.0 gw 192.168.1.1
Next server: 192.168.1.1
Filename: pxelinux.0
tftp://192.168.1.1/pxelinux.0... ok
pxelinux.0 : 42430 bytes [PXE-NBP]

PXELINUX 6.04 PXE 20200816 Copyright (C) 1994-2015 H. Peter Anvin et al

Failed to load ldlinux.c32
Boot failed: press a key to retry, or wait for reset...
....._

```

Para solucionarlo hacemos lo siguiente.

Instalamos los utils de syslinux

```
|root@vbox:/home/kali# apt install syslinux-utils
```

Copiamos el contenido a la carpeta tftp, y comprobamos que se han movido correctamente.

```

root@vbox:/home/kali# cp /usr/lib/syslinux/modules/bios/ldlinux.c32 /srv/tftp/
root@vbox:/home/kali# ls /srv/tftp/
kali ldlinux.c32 pxelinux.0 pxelinux.cfg
root@vbox:/home/kali#

```

Y reiniciamos el servicio.

```
|root@vbox:/home/kali# systemctl restart tftpd-hpa
```


Y ahora sí nos funcionará.

```
iPXE (PCI E2:00.0) starting execution...ok
iPXE initialising devices...ok

iPXE 1.21.1 -- Open Source Network Boot Firmware -- http://ipxe.org
Features: DNS TFTP PXE PXEXT

net0: 08:00:27:52:d1:83 using 82540em on 0000:00:03.0 (open)
  [Link:down, TX:0 TXE:0 RX:0 RXE:0]
  [Link status: Down (http://ipxe.org/38086101)]
Waiting for link-up on net0..... ok
Configuring (net0 08:00:27:52:d1:83)..... ok
net0: 192.168.1.12/255.255.255.0 gw 192.168.1.1
Next server: 192.168.1.1
Filename: pxelinux.0
tftp://192.168.1.1/pxelinux.0... ok
pxelinux.0 : 42430 bytes [PXE-MBP]

PXELINUX 6.04 PXE 20200816 Copyright (C) 1994-2015 H. Peter Anvin et al
Loading /kali/live/vmlinuz...
```

