Guía del auto-Hacker Galáctico

Fernando Méndez Torrubiano

10 de marzo de 2021

Índice

1. Introducción

Bienvenidos a la Guía del auto-Hacker Galáctico, un breve documento en el que se explicarán las nociones básicas para comenzar tu camino como *hacker* en **FDIst**.

1.1. Sistemas Operativos

He de comenzar diciendo que todo lo que se explique aquí, irá enfocado a la plataforma Linux, sin embargo, si usas **Windows**, no te preocupes, pues te enseñaremos a crear y usar una máquina virtual para que puedas trabajar sin necesidad de tener ninguna distribución de **GNU/Linux**.

Además, recalcar que cada uno es libre de usar la plataforma en la que más cómodo se sienta, no por usar **Windows o MacOS**, serás un informático de segunda, las herramientas están ahí y gracias a internet, toda la documentación está a vuestro alcance. Por tanto, si preferís usar otro Sistema Operativo (SO), que no esté basado en GNU/Linux, sabed que tenéis herramientas equivalentes a las que se van a detallar en esta guía. Eso sí, **tened cuidado con qué instaláis**, pues existen programas de dudosa seguridad y que incluyen spyware.

1.2. Advertencia y VPN

Por último advertíos de que **FDIst** tiene un acuerdo con el **CERN**, el **CSN** y el **Centro de Procesamiento de Datos (CPD)** de la Universidad Complutense de Madrid (UCM). Cualquier ataque a otra entidad o empresa, no estará respaldado por FDIst y **todo ataque que se realice a los centros anteriormente mencionados, deberá ser a través de la VPN** que se os proporcionará en este mismo manual y a la que previamente se os habrá dado acceso a través de vuestro correo UCM.

2. Instalación de Linux

En primer lugar, **si NO queréis instalar Linux**, porque no lo vais a usar para nada más, a parte de las actividades de FDIst, os recomiendo **leer el apartado *2.1***, saltaros el resto e ir al punto ***3.Instalación de una Máquina Virtual en Windows***.

2.1. Elección de la distribución

Existen múltiples distribuciones de Linux, nosotros os haremos una **lista de recomendaciones basadas en Debian y Arch**, pero podéis descargar la que más os guste:

- **Ubuntu**: Es la más popular y no es casualidad, pues esta distribución se creó para llevar Linux al público en general. Es la más sencilla de usar y la que dispone de un entorno más familiar, por contra, es de las que peor rendimiento tiene.
  Podéis descargar la última versión desde su página oficial:
  `https://ubuntu.com/download/desktop`.

- **Ubuntu Mate**: Una de mis favoritas, pues está pensada para equipos con peores prestaciones que Ubuntu, sin embargo, mantiene ese entorno familiar para los usuarios poco experimentados.
  Podéis descargar la última versión desde su página oficial:
  `https://ubuntu-mate.org/download/`.

- **Linux Mint**: Ligero y fácil de usar. Esa es la filosofía que marca a esta distribución, muy recomendada para equipos modestos y para amantes de Windows.
  Podéis descargar la última versión desde su página oficial:
  `https://linuxmint.com/download.php`.

- **Manjaro**: Bueno, bonito y gratis, pero no es tan sencillo de instalar como el resto de distribuciones. Si es la primera vez que instaláis Linux os costará, si no, esta distribución os encantará.
  Podéis descargar la última versión desde su página oficial:
  `https://manjaro.org/download/`.

- **Raspbian**: No es mala idea tener una Raspberry Pi conectada en casa y hacer ataques desde la FDI, conectado a ella mediante SSH (es lo que hago yo), para ello, os recomendamos el SO, creado exclusivamente para esta plataforma.
  Podéis descargar la última versión desde su página oficial:
  `https://www.raspberrypi.org/downloads/`.

- **Debian**: Por qué hablar de distribuciones para Debian, si tenemos el propio Debian. El *sistema operativo universal*, no apto para *noobs*. Realmente, sólo te recomendamos instalar este SO, si tienes experiencia en la plataforma Linux.
  Podéis descargar la última versión desde su página oficial:
  `https://www.debian.org/distrib/netinst`.

2.2. Preparación de la unidad de instalación

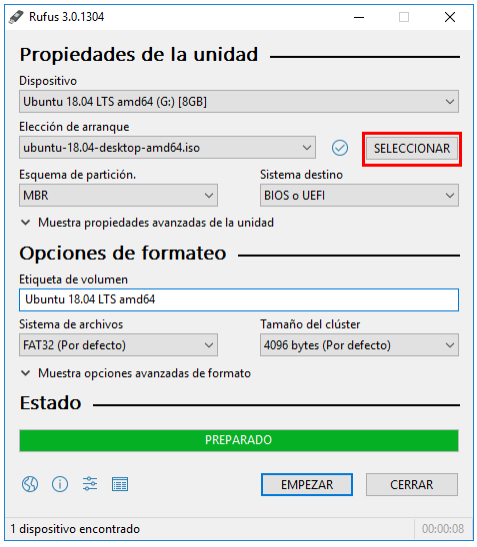
Una vez elegida nuestra distribución favorita y descargada la imagen de la misma (.ISO), podremos pasar a instalarla.

Para ello necesitaremos lo siguiente:

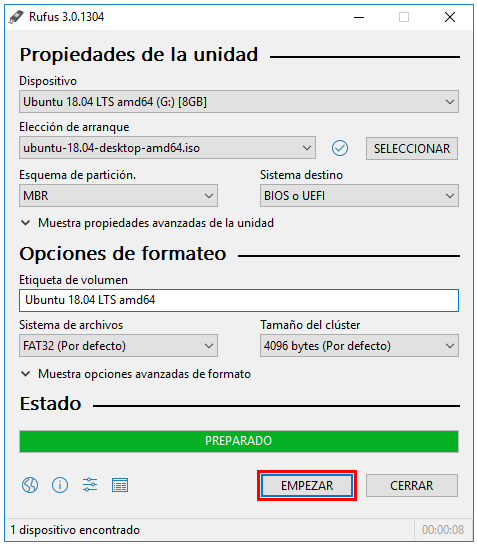
- Un **PenDrive** de al menos 8Gb (en algunos casos valdrá con menos capacidad).
- La **ISO** descargada de la distribución que queramos instalar.
- El programa **RUFUS**, para la preparación del PenDrive.
  Lo podéis descargar desde esta página: `https://rufus.ie/`

Preparación de la unidad USB (Advertencia, la unidad se formateará y se perderá toda la información contenida en su interior, por favor, realiza una copia de seguridad de tus archivos):

1. Introducimos la unidad USB en el PC donde hayamos descargado la ISO e iniciamos RUFUS.
2. Pulsamos *SELECCIONAR* y buscamos la el archivo ISO en la página donde lo hayamos guardado.



3. Pulsamos *EMPEZAR* y esperamos al que el programa prepare la unidad. Una vez finalizado, **extraemos el pendrive con srguridad** y listo.

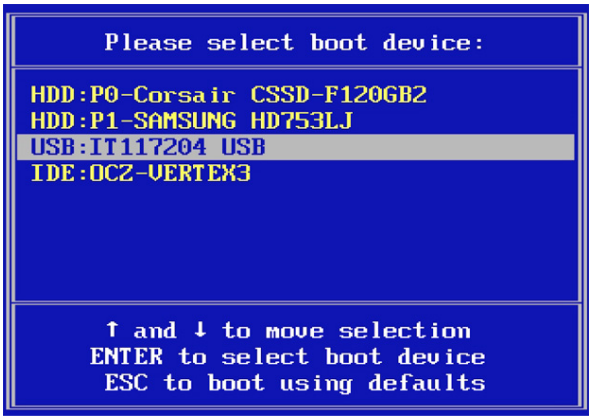


2.3. Arrancar el instalador del sistema

1. Introducimos la unidad de instalación USB que hemos preparado anteriormente en el ordenador en el que queramos instalar el SO.

2. Si en la BIOS no tenemos seleccionado que la unidad de arranque primaria sea el USB, pulsaremos rápidamente F12 hasta que nos aparezca el *"Boot Menu"* (en algunas placas base puede variar, consultar en la web oficial del fabricante).

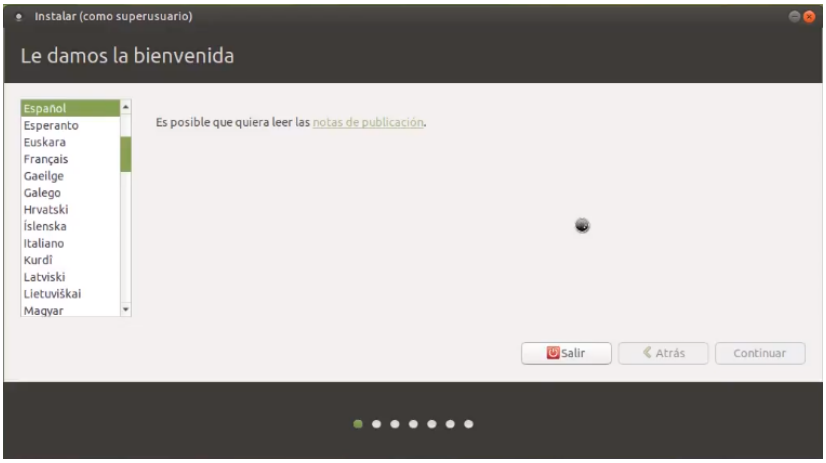
3. Seleccionamos el USB como unidad de arranque y se iniciará el instalador de la distribución de Linux elegida.



2.4. Opciones de instalación

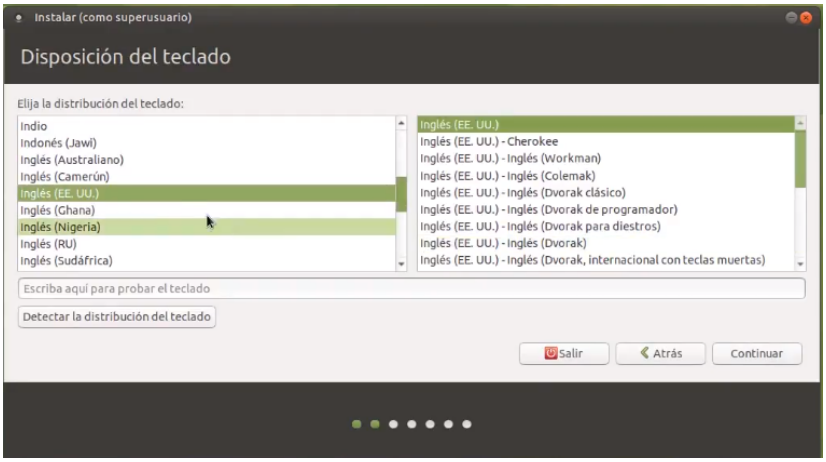
2.4.1. Idioma

Seleccionamos el idioma que deseemos para el sistema y pulsamos en *'Continuar'*.



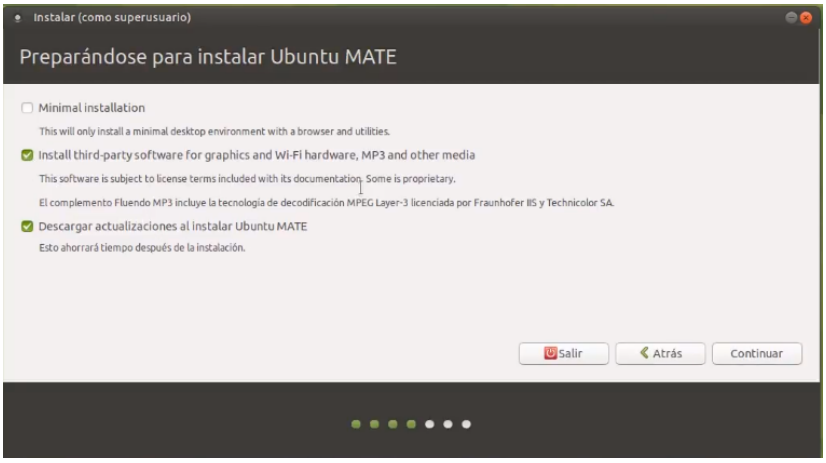
2.4.2. Distribución de teclado

Seleccionamos la distribución de teclado que queramos (aseguraos de que la distribución seleccionada es la **ESPAÑOLA**, si no luego tendréis muchos problemas a la hora de escribir) y pulsamos en *'Continuar'*.



2.4.3. Programas y drivers

A continuación nos aparecerán una serie de opciones:

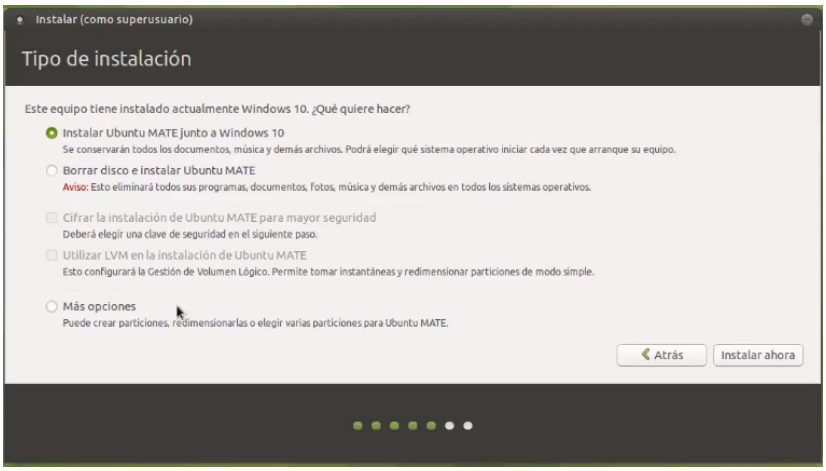


- **Instalación mínima**: esta opción es recomendable si vamos a instalar Linux junto con Windows y queremos dedicar poco espacio a la partición de Linux. Al seleccionar esta opción, se nos instalarán los programas básicos del sistema y nos ahorraremos espacio, pues no se instalarán herramientas como *LibreOffice* que no utilizaremos.
- **Instalación de software de terceros**: Importante marcar esta opción, pues descargará e instalará drivers que puedan necesitar componentes de nuestro hardware, como los de la tarjeta de red inalámbrica o nuestra tarjeta gráfica.
- **Descargar actualizaciones al instalar**: Opcional, pero recomendado marcarlo, la instalación tardará unos minutos más, pero luego no tendremos que buscar la última actualización manualmente.

Cuando hayamos seleccionado las opciones que deseemos, pulsamos en *'Continuar'*.

2.4.4. Tipo de instalación

Ahora es el momento de decidir si queremos instalar Linux junto con Windows, o por el contrario, formatear la unidad e instalar únicamente Linux (borrando Windows de forma permanente.



- **Instalar Linux junto a Windows**: Esta opción creará automáticamente una partición en nuestro disco duro, donde instalará la distribución de Linux, conservando Windows. Al arrancar el equipo, el GRUB de Linux nos permitirá elegir que sistema arrancar (por defecto pondrá Linux, pero más tarde, podremos modificar el orden de arranque si por defecto queremos poner Windows).

- **Borrar disco e instalar Linux**: Formateará por completo la unidad, eliminará Windows y todos los archivos que contenga, perderemos la licencia del SO.
  Si seleccionamos esta opción, se nos habilitarán las siguientes opciones:

- **Cifrar la instalación de Linux para mayor seguridad**: Esto hará que los datos contenidos en el disco sean cifrados, la instalación tardará un poco más y tendrá un impacto en el rendimiento del equipo, por tanto, si tenemos un ordenador con componentes de baja calidad, no es recomendable. Por el contrario, si queremos proteger muy bien nuestros archivos, entonces es recomendable seleccionar esta opción.

- **Utilizar LVM**: Esto no es más que un sistema que administración de discos, es recomendable seleccionar esta opción, pues en un futuro puede que queramos volver a instalar Windows o otra distribución de Linux junto con la actual.

Por otra parte, si queremos instalar Linux junto con Windows, pero queremos seleccionar nosotros mismos el espacio que se le dedica a cada Sistema Operativo, seleccionaremos la siguiente opción:

- **Más opciones**: Nos permitirá crear la partición de Linux con el tamaño que queramos, ajustando así, cuánto espacio del disco le dejamos a Windows. Es recomendable usar al menos 30GB para la mayoría de distribuciones de Linux, aunque con menos podrían funcionar.

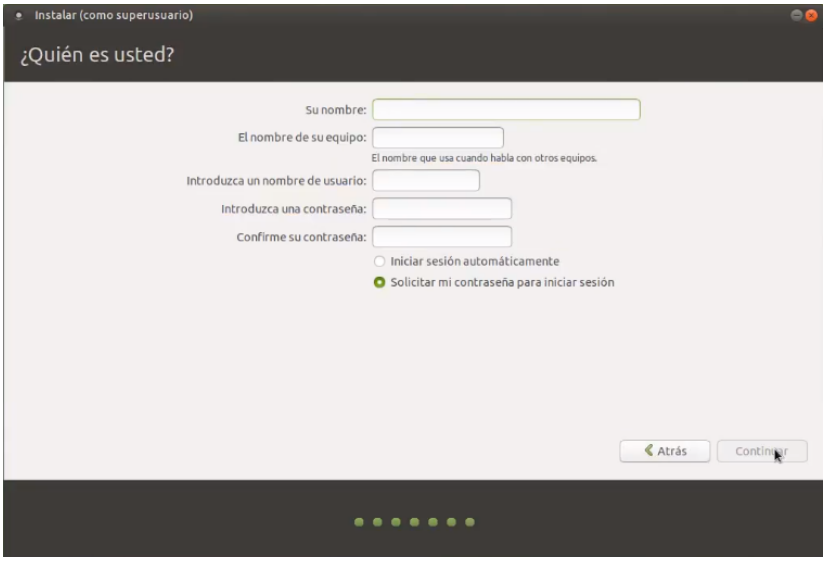
Por último, pulsamos en *'Instalar ahora'*.

2.4.5. Zona horaria

Seleccionaremos la región donde nos encontremos, en nuestro caso, Madrid. Y pulsamos en *'Continuar'*.

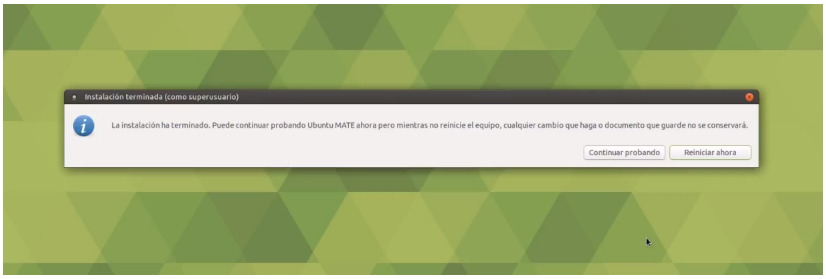
2.5. Usuario y contraseña

Por último, le asignaremos un nombre al equipo, crearemos el usuario con el nombre que queramos e creamos una nueva contraseña. Si queremos podemos seleccionar la opción de *'Iniciar sesión automáticamente'*, para que no nos pida nuestra contraseña al iniciar nuestro ordenador (más cómodo, pero mucho más inseguro).
Pulsamos en *'Continuar'* y comenzará la instalación.



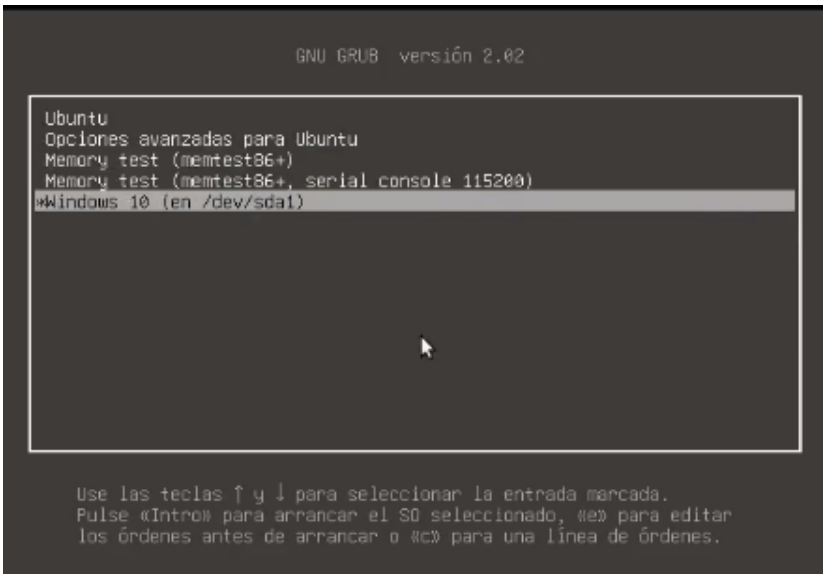
2.6. Finalizar la instalación

Cuando la instalación finalice, nos aparecerá un nuevo cuadro de diálogo, en el que pulsaremos en *'Reiniciar ahora'* y ya podremos comenzar a usar nuestra distribución de Linux.



2.6.1. Poner Windows como primera opción del GRUB

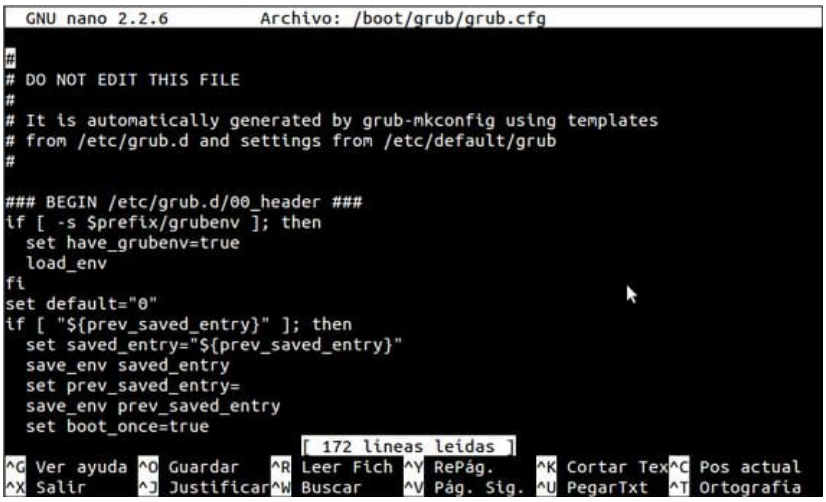
Como habremos observado, al reiniciar el equipo (si hemos instalado Linux junto con Windows, nos aparecerá la ventana en la que nos permite escoger que SO iniciar. Por defecto viene seleccionada la distrubución de Linux que hayamos instalado y hay una cuenta atrás que iniciará está automáticamente, a no ser que toquemos alguna flecha del teclado para seleccionar otra opción.



A continuación os explico cómo poner Windows por defecto:

1. Abriremos una terminal desde nuestra distribución de Linux y escribiremos el siguiente comando: **sudo nano /boot/grub/grub.cfg**

2. Se nos abrirá un documento editable como este:



En donde tendremos que modificar sólo la linea `set default='0'`. Cambiando el '0' por el '4', que es el número que, en mi caso, corresponde a la partición de Windows que esta instalada junto a tu sistema Linux.

3. Hecho esto, pulsamos 'CTRL+X' para salir, pulsamos la tecla 'S' para guardar y a continuación la tecla 'ENTER' para confirmar.

Y listo, la próxima vez que iniciemos el equipo, Windows será la opción por defecto.

3. Máquina Virtual de Linux en Windows

Lo primero, debemos descargar un programa de virtualización, como **VirtualBox** (de Oracle), aunque existen muchos e incluso Windows dispone de forma nativa de un método de virtualización, creemos que VirtualBox es el que mejor funciona:
`https://www.virtualbox.org/`

Otra de las alternativas muy buenas es **VMware**:
`https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html`

3.1. Maquina Virtual de FDIst

Aunque a continuación vamos a explicar cómo crear una máquina virtual, también tenemos la opción de **importar la máquina virtual ya preparada de FDIst**.
Está creada sobre Debian 10 con una interfaz gráfica KDE. Es muy ligera y vienen instalados los paquetes más básicos que usaremos (como nmap).

Aunque esta máquina viene por defecto con 2Gb de RAM asignados, si tu PC lo permite, te recomendamos que le asignes más.

El *usuario* es **fdist** y la *contraseña* es **fdist**.
Aquí os dejamos el enlace de **descarga**: `https://fdist.ucm.es/vm/FDIst.ova`

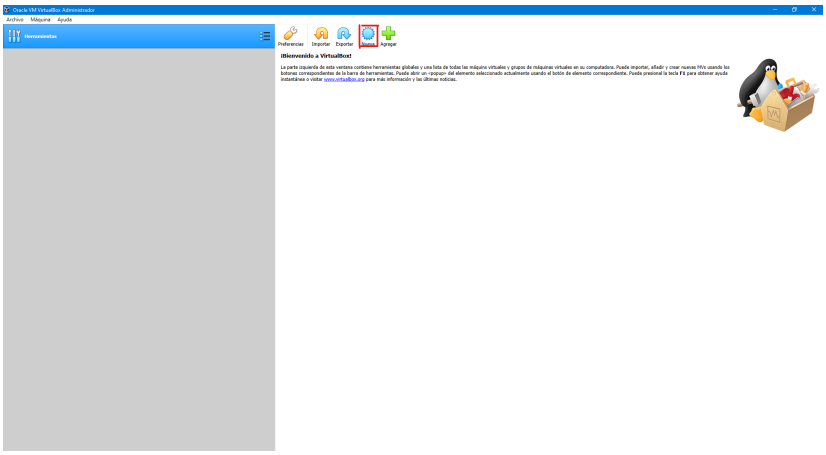
Para añadirla es muy sencillo, una vez descargado el archivo .OVA:

- En **VirtualBox**: Archivo >> Importar servicio virtualizado... >> *Y seleccionamos el archivo.*
- En **VMware**: Player >> File >> Open... >> *Y seleccionamos el archivo.*

3.2. Creación de una Máquina Virtual

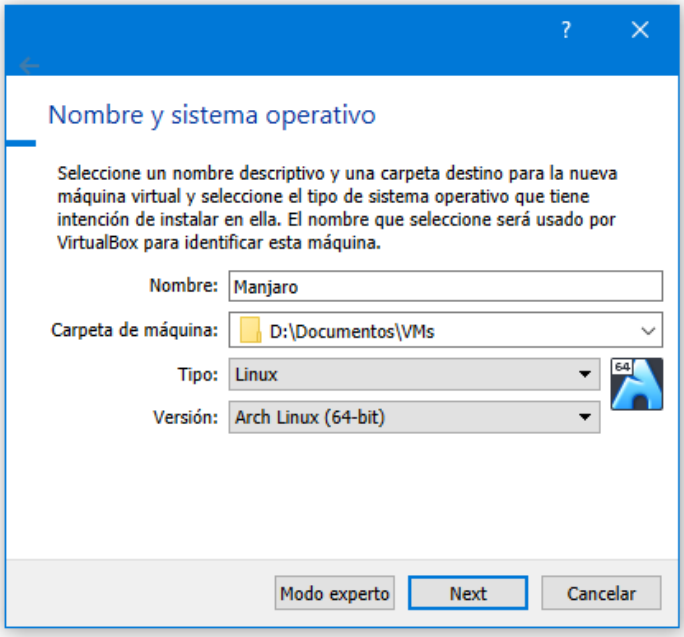
A pesar de que vayamos a utilizar una máquina virtual, **es necesario tener una ISO de la distribución de Linux que queramos usar**.
Para ello, os recomiendo leer el apartado ***2.1. Elección de la distribución***.

Una vez instalado VirtualBox, procedemos a crear una máquina virtual.
Para ello pulsamos sobre el icono *'NUEVA'*.



3.3. Configuración Inicial

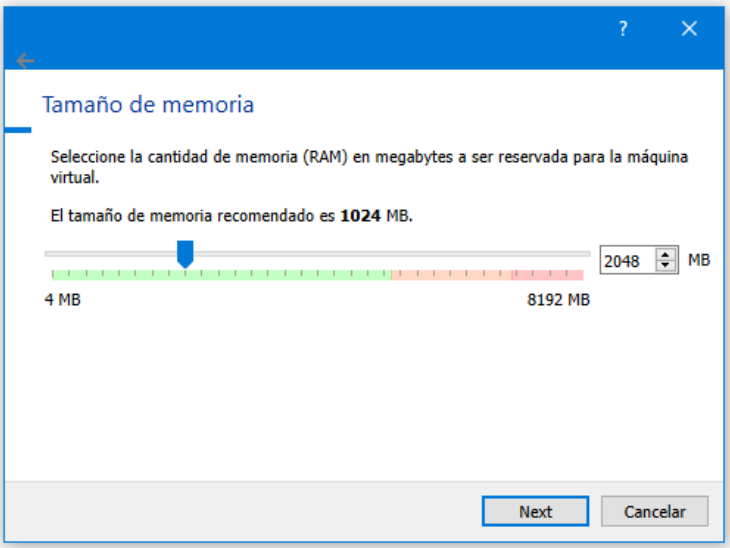
A continuación daremos un nombre a nuestra Máquina Virtual, seleccionaremos la carpeta donde la vamos a crear y escogeremos el tipo de máquina (en nuestro caso Linux) y su versión (la distribución principal a la que corresponda, en nuestro caso ARCH Linux, pues instalaremos Manjaro).



Pulsamos sobre el botón *'Siguiente'*.

3.4. Tamaño de la memoria

Ahora seleccionaremos el tamaño de memoria RAM que queremos asignar a nuestra Máquina Virtual. Por defecto nos pone 1024MB, yo os recomiendo subir al menos a 2048MB si vuestro PC tiene 8GB o más de memoria RAM instalada. Tened en cuenta que debéis dejar memoria suficiente para que Windows administre el resto del sistema.

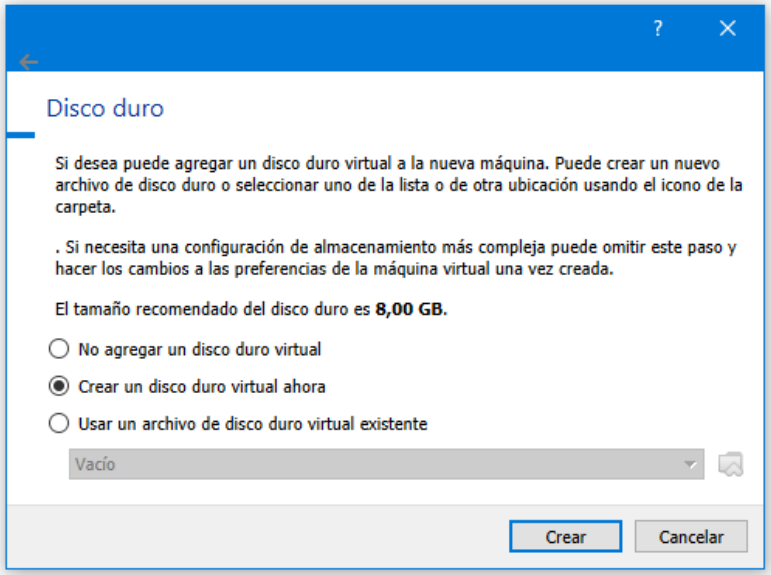


Pulsamos sobre el botón *'Siguiente'*.

3.5. Creación de un Disco Duro Virtual

3.5.1. Creación

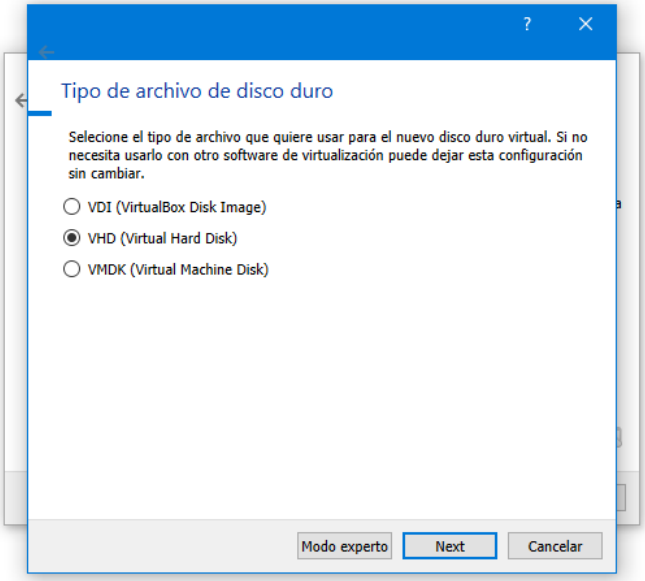
Nuestra máquina necesita estar alojada en algún espacio físico, para ello crearemos una pequeña partición en nuestro disco (un Disco Duro Virtual).



Pulsamos sobre el botón *'Crear'*.

3.5.2. Tipo de Disco Duro

VirtualBox nos ofrece 3 opciones, de las cuales, tanto la primera (*VirtualBox Disk Image*, como la segunda (*Virtual Hard Disk*, son recomendables. Lo dejamos a vuestra elección.



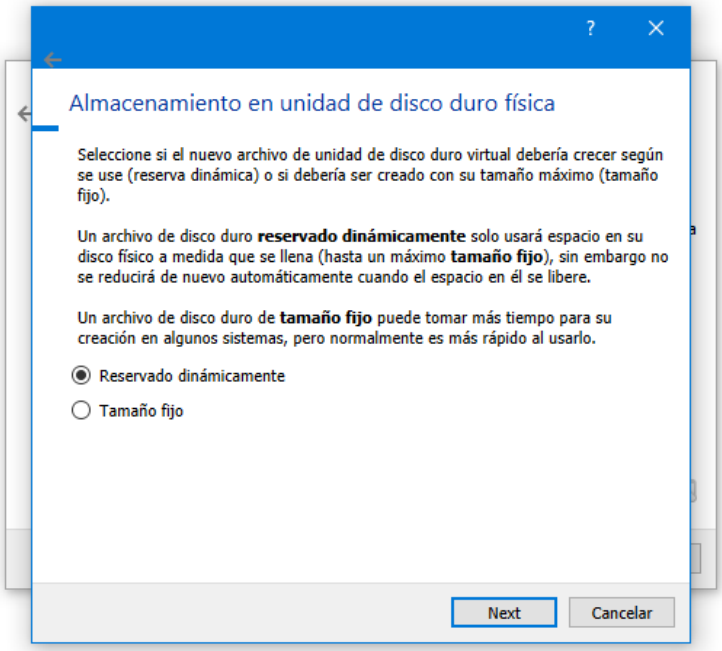
Pulsamos sobre el botón *'Siguiente'*.

3.5.3. Tipo de Almacenamiento

En este caso, VirtualBox nos ofrece 2 opciones:

1. Reservado dinámicamente: esto irá ocupando espacio en nuestro disco según la Máquina Virtual necesite, hasta el máximo que le asignaremos a continuación.

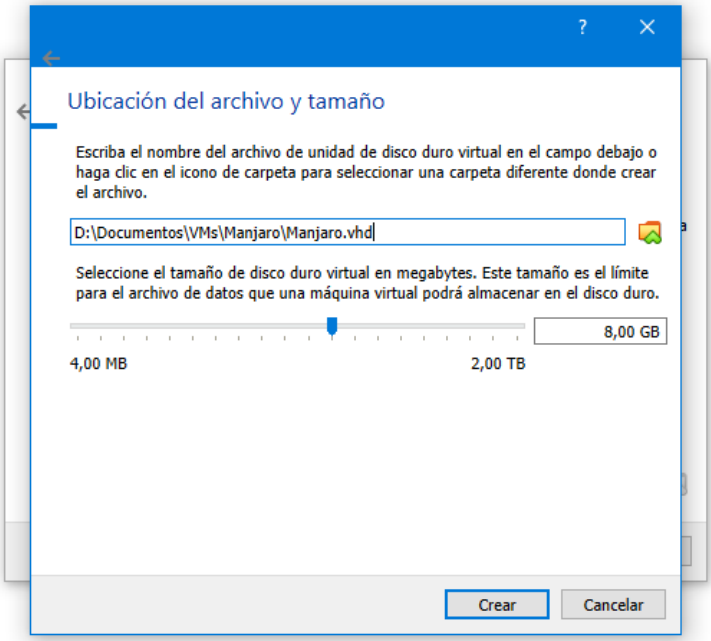
2. Tamaño fijo: reservará directamente todo el espacio que le digamos a continuación, tanto si la Máquina Virtual lo está usando, como si no.



Pulsamos sobre el botón *'Siguiente'*.

3.5.4. Ubicación y tamaño

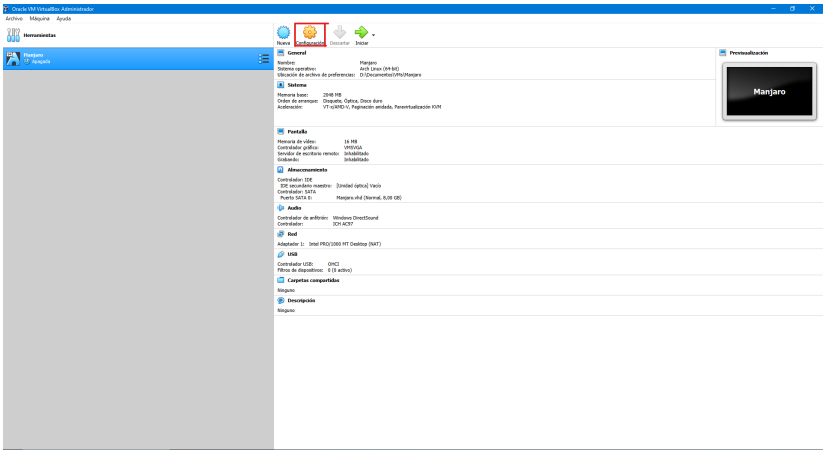
En este apartado podremos seleccionar la ubicación en la que se creará el Disco Duro Virtual. Además, VirtualBox nos recomienda el tamaño mínimo para que la Máquina Virtual funcione, podemos asignar más si así lo queremos.



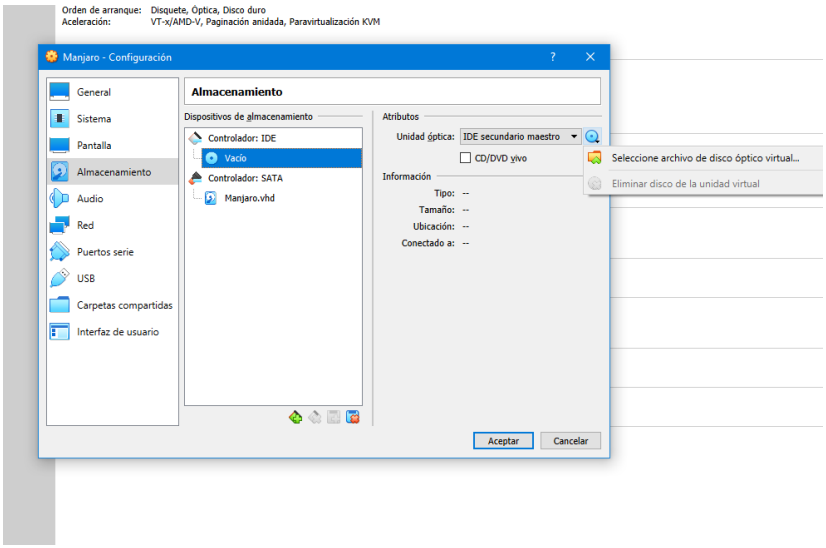
Pulsamos sobre el botón *'Crear'*.

3.6. Selección de la ISO

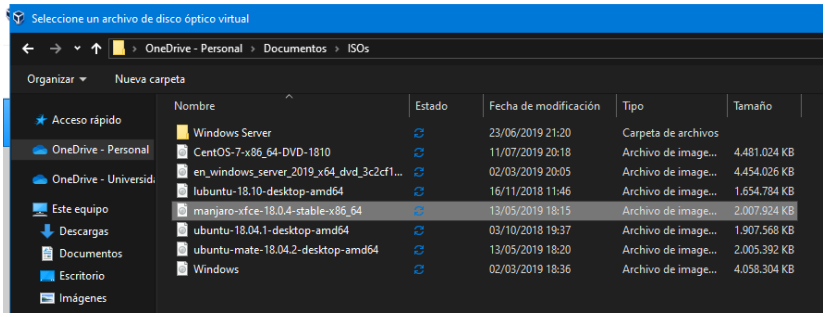
Ahora vamos a decirle a VirtualBox de dónde tiene que leer la ISO para instalar la Máquina Virtual.



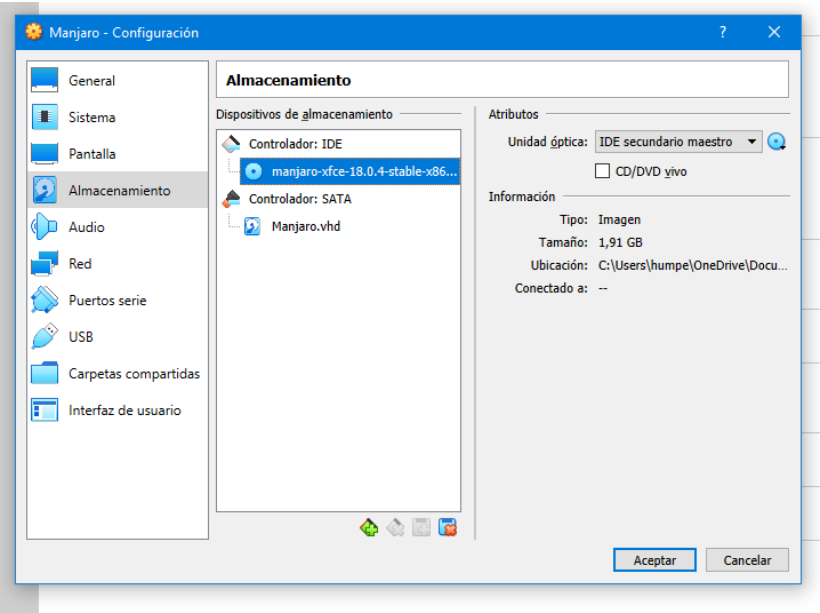
Pulsamos sobre el botón *'Configuración'*.



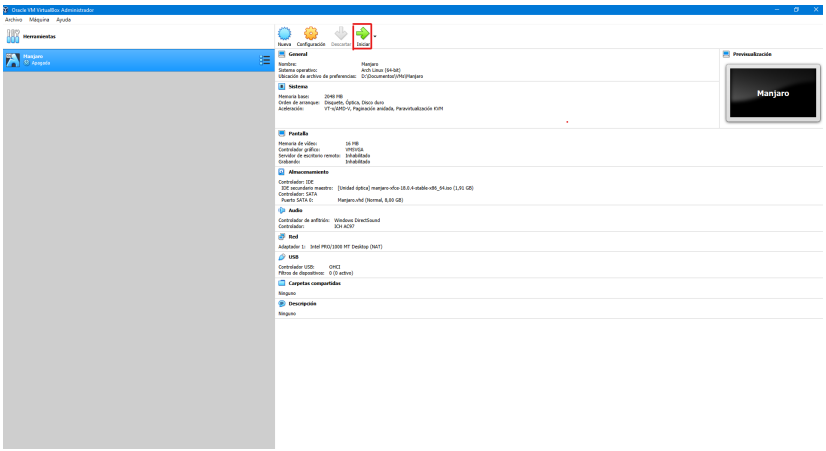
Vamos a la sección de *'Almacenamiento'* y en el *'Controlador'*, seleccionamos el archivo de disco óptico virtual (lo que sería el medio de instalación).



Buscamos la carpeta donde habíamos guardado la ISO y la seleccionamos.



Pulsamos sobre el botón *'Aceptar'* y listo.



Ahora ya sólo tenemos que pulsar sobre el botón *'Iniciar'* de la Máquina Virtual y comenzará la instalación. Para guiaros, podéis seguir la guía de instalación del apartado ***2.Instalación de Linux***, a partir del punto ***2.4.Opciones de Instalación***.

4. Conexión a la VPN, HackTheCERN / HackTheCSN / HackTheUCM

4.1. Código ético

Antes de comenzar, os adjuntamos el *Manual de Código Ético* proporcionado por el **CERN** y por el **CSN**. Es muy recomendable que les echéis un vistazo, pues explica las direcciones IPs a las que debéis enfocar vuestros ataques y cómo debéis realizar estos mismos:

```
https://cv4.ucm.es/moodle/pluginfile.php/4672494/mod_resource/
content/1/CERNCodeOfEthics.pdf
```

```
https://cv4.ucm.es/moodle/pluginfile.php/7094461/mod_resource/
content/1/CodigoEtico.pdf
```

4.2. Registro

Para poder tener acceso a la VPN, **es necesario que rellenéis este formulario** con vuestra cuenta UCM y esperéis una confirmación mediante correo electrónico de que se os ha concedido acceso, **hasta entonces, no podréis realizar ningún ataque**.

```
https://fdist.ucm.es/registro/
```

4.3. Configuración de la VPN

4.3.1. En distribuciones Linux

(Basadas en Debian: Ubuntu, Linux Mint, Raspbian...)

1. Abrimos un terminal y escribimos el siguiente comando:

   sudo apt-get install vpnc network-manager-vpnc

2. Si tenemos un escritorio basado en GNOME, escribiremos:

   sudo apt-get install network-manager-vpnc-gnome

(En otras versiones como RedHat, Arch, Manjaro...)

1. Abrimos un terminal y escribimos el siguiente comando:

   yum install vpnc

2. Si no funciona, escribiremos:

   yum install NetworkManager-vpnc

   (Esto instalará los paquetes para servidor VPN).

- Una vez instalados todos los paquetes, escribiremos el comando:

  sudo vpnc

- A continuación nos pedirá los credenciales, debemos escribir lo siguiente:

  - Pasarela / Gateway: **reservado2.vpn.ucm.es**
  - Nombre del grupo: **ucm**
  - Contraseña del grupo: **ucm**
  - Nombre de usuario: **Vuestro correo @ucm.es**
  - Contraseña del usuario: **Vuestra contraseña del correo**

- Una vez que queramos desconectarnos, debemos escribir el siguiente comando:

  sudo vpnc-disconnect

  (O simplemente reiniciar el equipo).

4.3.2. En Windows 10

Si estamos usando una máquina virtual de Linux en Windows 10 y conectamos Windows a la VPN, la máquina virtual (que está soportada por Windows 10 como SO principal), también estará conectada a la VPN.

- En primer lugar, es necesario bajar e instalar el programa *Global Protect* desde la página:

  `https://galeria.ucm.es/global-protect/login.esp`

- Su instalación es muy sencilla y una vez instalado introducimos las credenciales:

  - Pasarela / Gateway: **reservado2.vpn.ucm.es**
  - Nombre de usuario: **Vuestro correo @ucm.es**
  - Contraseña del usuario: **Vuestra contraseña del correo**

- Y cuando queramos cerrar la VPN, es tan sencillo como pulsar en *'Desconectar'*.

5. Uso de la herramienta NMAP

Nmap es un programa de código abierto que **sirve para efectuar rastreo de puertos**. Fue creado originalmente para Linux aunque **actualmente es multiplataforma**.
Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática, para ello NMAP envía unos paquetes definidos a otros equipos y analiza sus respuestas.
Ha llegado a ser una de las herramientas imprescindibles para todo administrador de sistemas, y es usado para pruebas de penetración y tareas de seguridad informática en general. Como muchas herramientas usadas en el campo de la seguridad informática, es también una herramienta muy utilizada para hacking.

A continuación mostramos un ejemplo de uso:

```
sudo nmap -Pn localhost
```

Explicación de cada campo:

- **sudo**: ejecuta el comando con permisos de súper-usuario.
- **namp**: comando para ejecutar la herramienta NMAP.
- **-Pn**: no realiza *ping* antes del escaneo (evita descartar máquinas levantadas detrás de firewall que bloquea ICMP).
- **localhost**: IP a la que realizaremos el excanéo, en este caso, LOCALHOST es nuestra propia máquina.

Aunque tanto para esta, como para cualquier otra herramienta que uséis, os recomendamos no quedaros en los ejemplos que aquí os proponemos y buscar más información de uso. Un buen comienzo para buscar ayuda en cualquier comando es el uso '-h' (help), el cual nos mostrará por pantalla todo lo que puedes hacer con ese comando.

6. Ataque de Denegación de Servicio (DDoS)

DDoS son las siglas de "**Distributed Denial of Service**". Traducido al castellano, significa literalmente "Ataque distribuido denegación de servicio".

Un **ataque DDoS o ataque de denegación de servicio**, es aquel cuyo principal objetivo es **inhabilitar el uso de un determinado sistema** o infraestructura para que no pueda prestar el servicio para el que está destinado. El ataque puede ir dirigido a la red informática o al servidor web, por ejemplo.

En términos más sencillos, un ataque DDoS **consiste en saturar al receptor de paquetes hasta que este colapse** y no pueda prestar servicio.

Este ataque puede ser realizado tanto desde la consola de comandos de **Windows** (CMD o PowerShell), como desde la terminal de **Linux**.
No os voy a enseñar a realizar un ataque real, porque además necesitaréis de herramientas externas para ello, pero podéis probar a relizar algunas peticiones a servidores con lo que os explico a continuación.

6.1. Desde Windows

Aunque a muchos les sorprenda, un ataque DDoS se puede hacer desde la consola de Windows, pues al fin y al cabo, no es más que un envío masivo de paquetes y la herramienta PING, sirve para ello (aunque su finalidad real sea la de comprobar el estado de un host).
A continuación vemos un ejemplo de como hacerlo (ejecutando un CMD en modo Administrador):

```
ping DISKOBOLO.FDI.UCM.ES -t -l 65500
```

Explicación de cada campo:

- **ping**: comando para realizar el ataque.
- **diskobolo.fdi.ucm.es**: IP a la que se dirige el ataque.
- **-t**: campo que sirve para hacer que los envíos de paquetes no se detengan hasta que pulsemos *'CTRL+C'*.
- **-l 65500**: comando para elegir el tamaño (en bytes) de datos que se envían. Tened en cuenta que los servidores con un sistema de seguridad bien implementado, no os dejarán enviar paquetes tan pesados, por tanto, deberéis disminuir el tamaño de los paquetes y usar muchas máquinas diferentes a la vez para realizar un ataque efectivo.

6.2. Desde Linux

Para llevar a cabo un ataque de este tipo desde una máquina Linux, debemos descargar el paquete HPING3, para ello introducimos el siguiente comando:

```
sudo apt install hping3
```

A continuación vemos un ejemplo de cómo realizar un ataque:

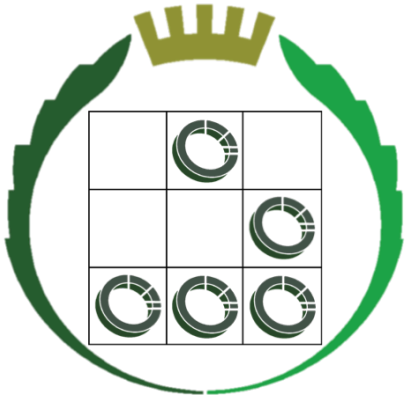
```
sudo hping3 –rand-source -p 80 -S –flood ESPORTS.FDI.UCM.ES
```

Explicación de cada campo:

- **sudo**: ejecuta el comando con permisos de súper-usuario.
- **hping3**: comando para realizar el ataque.
- **–randsource**: genera IPs falsas de forma aleatoria para no dejar un rastro de nuestra IP real, que es desde la que se está realizando el ataque-
- **-p 80**: puerto al que se va a realizar el ataque, en este caso el 80 (http).
- **-S**: activa el flag syn.
- **–flood**: le indica a HPING3 que envie los paquetes a la máxima velocidad posible.
- **esports.fdi.ucm.es**: IP de la víctima.

7. El juramento hacker de FDIst

FDI$_{ST}$
JURAMENTO



Yo _____ prometo participar en las actividades del FDI Security Team y contribuir a ellas en la medida de lo posible, y respetando los principios de la ética hacker.

Por ello, en mi camino para satisfacer mi curiosidad, no destruiré ningún sistema y alertaré a su legítimo propietario de cualquier vulnerabilidad que en el mismo hubiera podido encontrar. Así mismo, prometo respetar la legalidad vigente.

Por último, prometo disfrutar con todo el proceso.