

Guía de instalación del entorno para la resolución de los *escape room* virtuales

En esta parte práctica del curso vamos a recrear el proceso por el cual accederíamos desde nuestro ordenador a otro en un entorno controlado, por lo que es necesario el uso de varias máquinas virtuales.

Una **máquina virtual** no es más que un software que emula un ordenador (con todos sus componentes físicos, sistema operativo, archivos independientes, etc) dentro de una ventana de tu sistema operativo como si fuese cualquier otro programa.

Podemos configurar nuestra propia máquina o bien descargarla de internet ya empaquetada con ciertas características. Después utilizaremos un software de virtualización, en nuestro caso **VMware Player**, para “encender” dichas máquinas y poder interactuar con ellas.

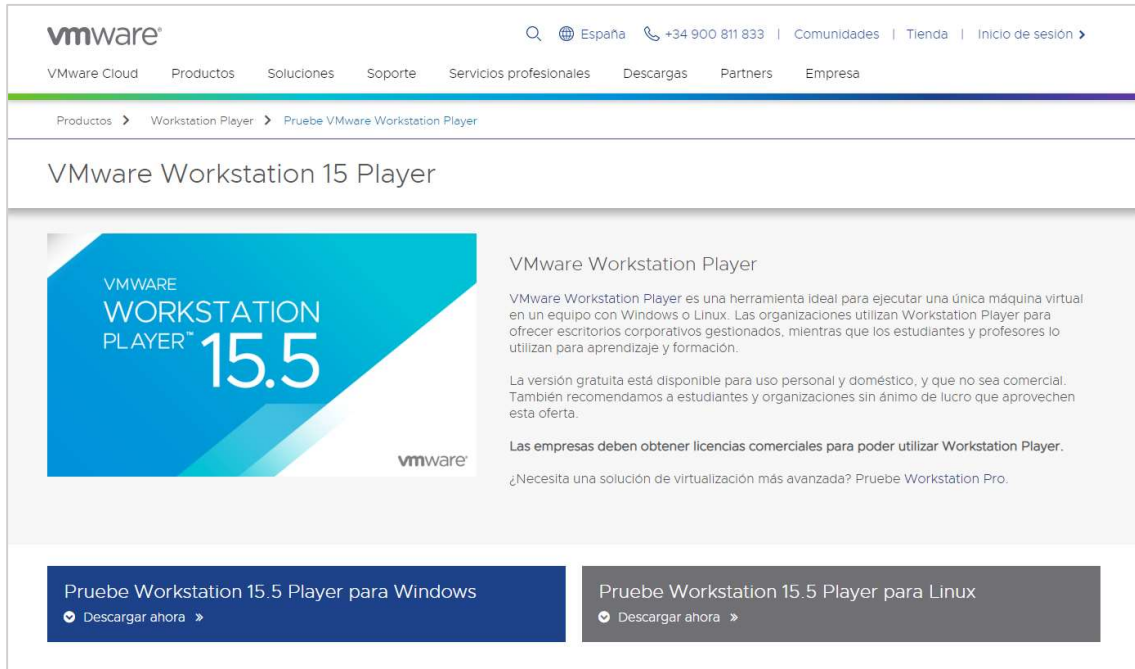
De esta forma, para resolver los *escape room* contaremos con una ventana con una primera máquina virtual desde la que realizaremos nuestras acciones de “ataque”, y una segunda ventana con la máquina a la que intentaremos acceder para encontrar las diferentes claves que esconde.

La presente guía cuenta con los siguientes apartados:

- Instalación de VMware Player
- Instalación del entorno de pentesting Kali Linux
- Introducción al entorno de pentesting Kali Linux
- Instalación de las máquinas objetivo

Instalación de VMware Player

En nuestro caso utilizaremos **VMware Player** para lanzar las máquinas virtuales desde nuestro ordenador, una herramienta gratuita para su uso no comercial.



The screenshot shows the VMware website's product page for Workstation 15 Player. The header includes the VMware logo, a search icon, and links for 'España', '+34 900 811 833', 'Comunidades', 'Tienda', and 'Inicio de sesión'. A navigation bar lists 'VMware Cloud', 'Productos', 'Soluciones', 'Soporte', 'Servicios profesionales', 'Descargas', 'Partners', and 'Empresa'. The breadcrumb trail reads 'Productos > Workstation Player > Pruebe VMware Workstation Player'. The main heading is 'VMware Workstation 15 Player'. On the left is a large blue graphic with 'VMWARE WORKSTATION PLAYER™ 15.5' and the VMware logo. To the right, the text describes the product as an ideal tool for running virtual machines on Windows or Linux, mentioning its use in corporate environments and education. It states that the free version is for personal and domestic use, while commercial licenses are required for businesses. A link to 'Pruebe Workstation Pro' is provided for those needing more advanced virtualization. At the bottom, there are two prominent buttons: 'Pruebe Workstation 15.5 Player para Windows' and 'Pruebe Workstation 15.5 Player para Linux', each with a 'Descargar ahora' (Download now) link and an arrow icon.

Podemos descargar la aplicación desde la siguiente dirección:

<https://www.vmware.com/es/products/workstation-player/workstation-playerevaluation.html>

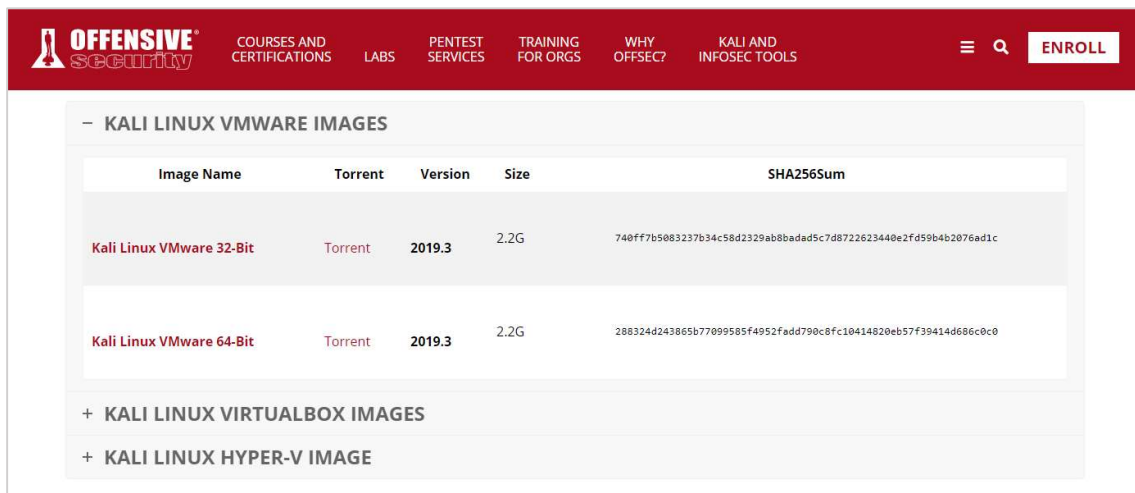
El proceso de instalación es automático y solo requiere que se reinicie el ordenador una vez finalizado.

Instalación del entorno de pentesting Kali Linux

El entorno de “ataque” o *pentesting* que utilizaremos para completar la práctica se trata de Kali Linux, una distribución del sistema operativo Linux muy utilizada para el testeo de seguridad de redes y de código libre.

Podemos descargar un paquete con la máquina virtual ya preparada para lanzarse en VMware Player en la siguiente dirección:

<https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/>



The screenshot shows the 'OFFENSIVE security' website header with navigation links: COURSES AND CERTIFICATIONS, LABS, PENTEST SERVICES, TRAINING FOR ORGS, WHY OFFSEC?, and KALI AND INFOSEC TOOLS. An 'ENROLL' button is in the top right. Below the header, a section titled '- KALI LINUX VMWARE IMAGES' contains a table with two rows of download links for Kali Linux VMware images.

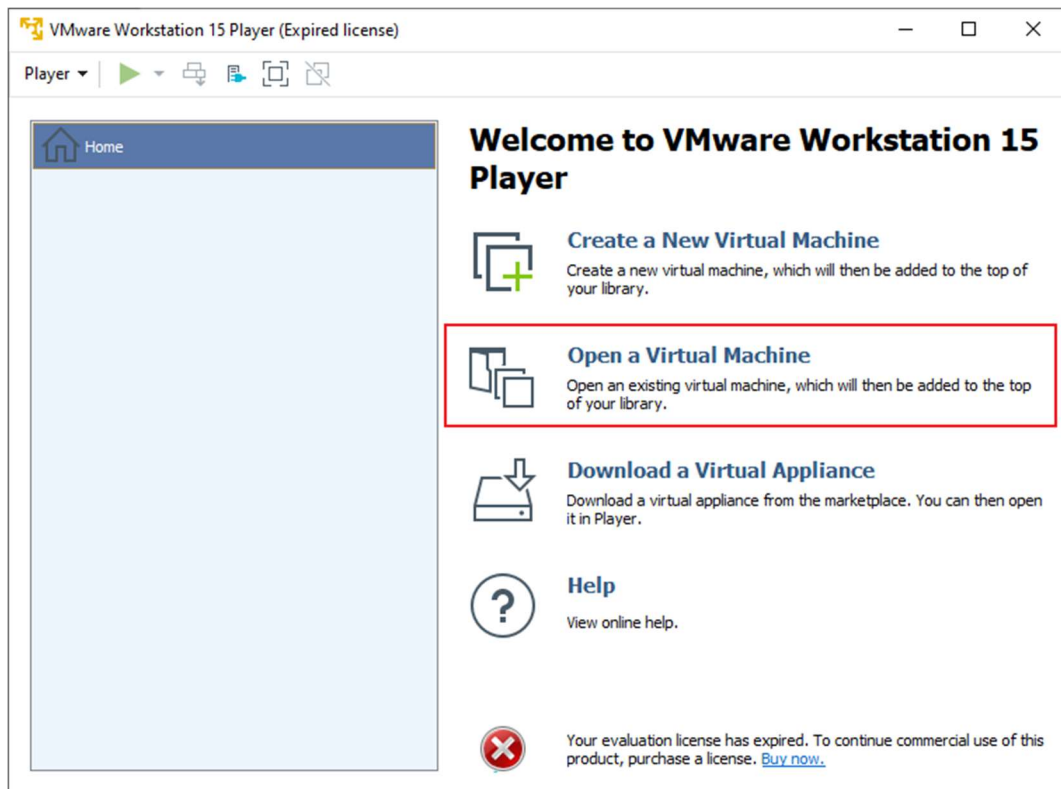
Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux VMware 32-Bit	Torrent	2019.3	2.2G	740ff7b5083237b34c58d2329ab8bad5c7d8722623440e2fd59b4b2076ad1c
Kali Linux VMware 64-Bit	Torrent	2019.3	2.2G	288324d243865b77099585f4952fadd790c8fc10414820eb57f39414d686c0c0

Below the table, there are expandable sections for '+ KALI LINUX VIRTUALBOX IMAGES' and '+ KALI LINUX HYPER-V IMAGE'.

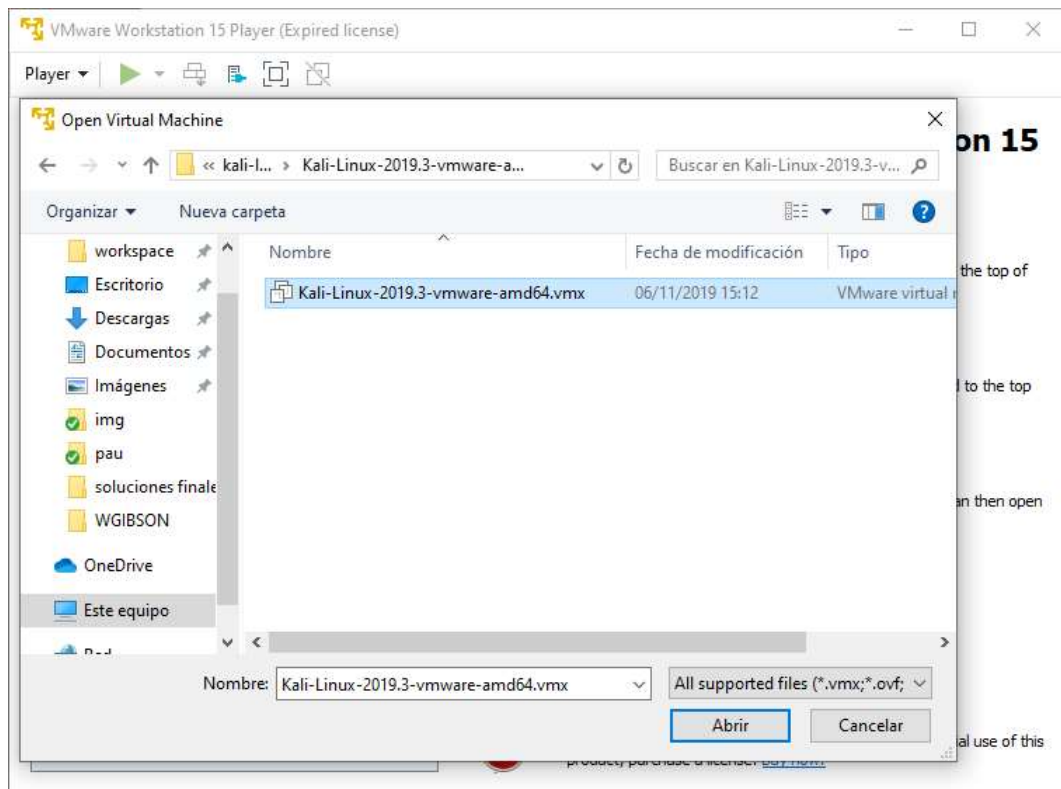
Una vez descargado el archivo, debemos descomprimirlo, ya que se trata de un archivo 7z. Para ello, si no contamos con la herramienta adecuada, podemos instalar **7-zip** en la siguiente dirección: <https://7-zip.es/descargar>

Ahora que ya tenemos los archivos correspondientes a la máquina virtual de Kali Linux, podemos proceder a importarla en VMware Player para poder lanzarla cuando queramos.

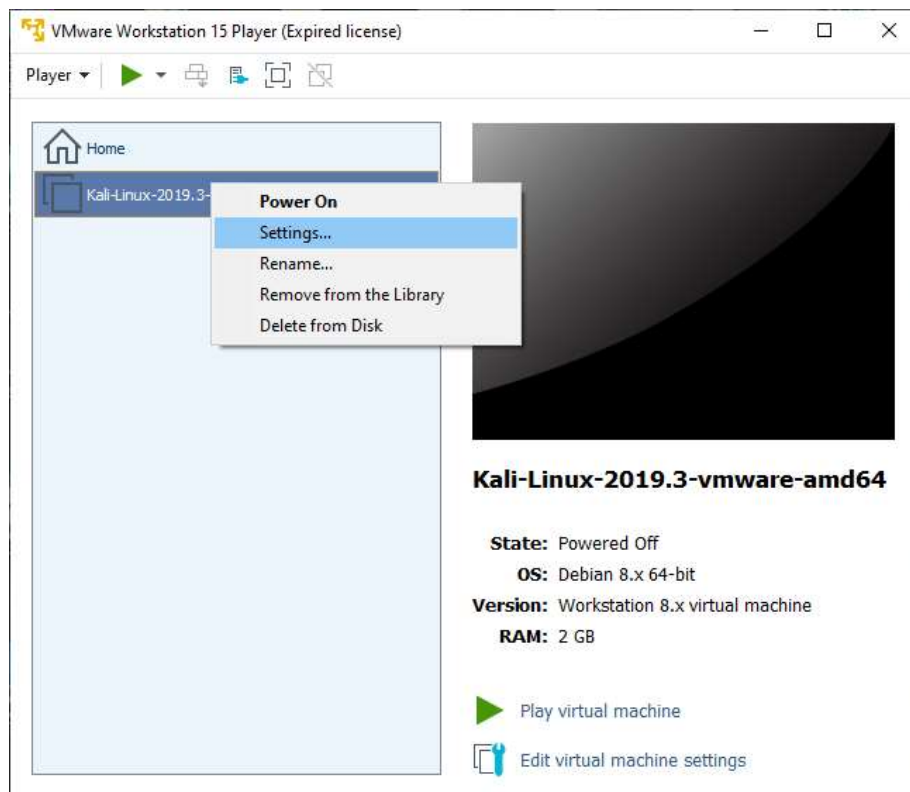
Abrimos **VMware Player** y seleccionamos la opción de **Abrir una Máquina Virtual / Open a Virtual Machine**.



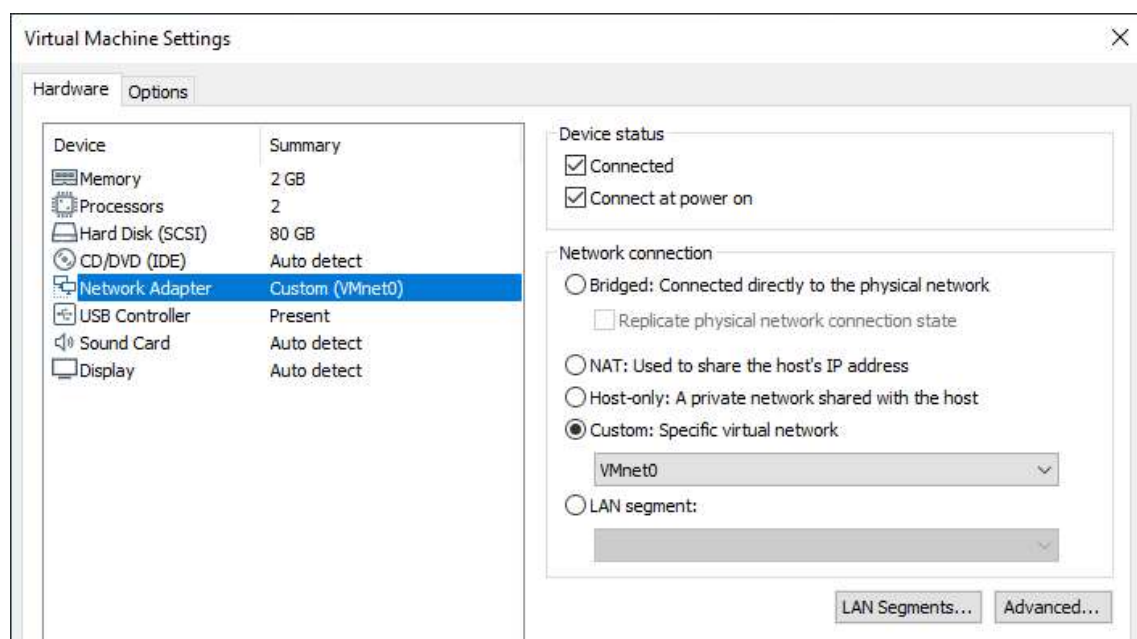
Seleccionamos el archivo con extensión **.vmx** que aparecerá en la carpeta donde hayamos descomprimido la máquina virtual anteriormente.



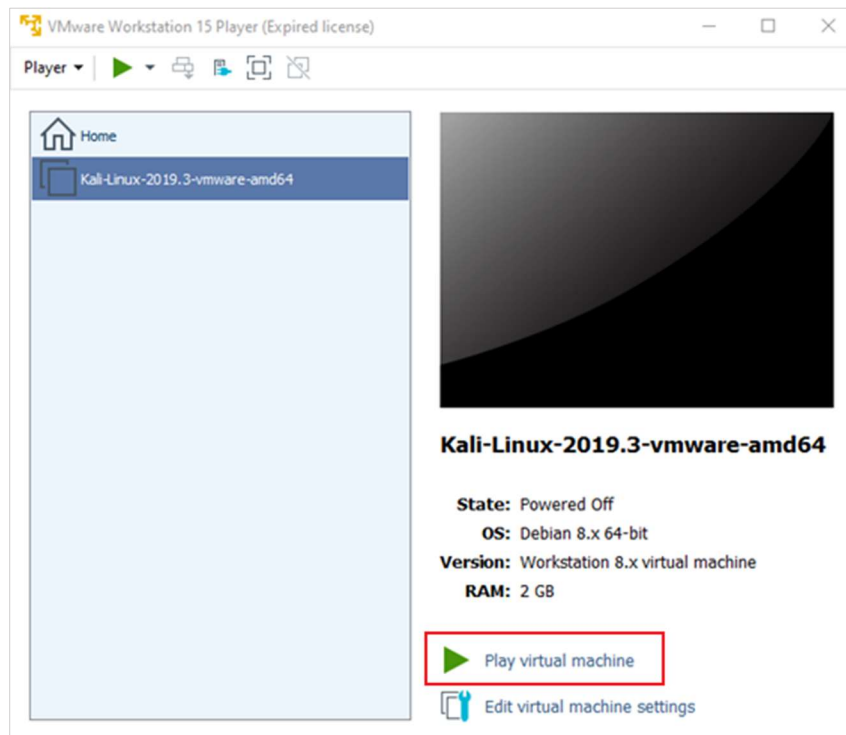
Ahora ajustaremos la configuración de hardware de la máquina virtual para que no sobrepase el rendimiento del ordenador en el que la estamos ejecutando. Para ello debemos pulsar con el botón derecho en la máquina virtual y seleccionar **Settings**.



Una posible configuración es la que se presenta en la siguiente captura de pantalla. Hay que prestar especial atención a que la configuración de red sea la indicada, para que tanto esta máquina como las que serán “atacadas” se encuentren en el mismo entorno de red y puedan verse entre sí. Seleccionaremos la conexión de red **Custom**, y ahí elegiremos la misma red en todas las máquinas que usemos, en nuestro caso la 8.



Una vez configurada podemos pulsar el botón de **Play virtual machine** para “encender” la máquina virtual e interactuar con ella.



Introducción al entorno de pentesting Kali Linux

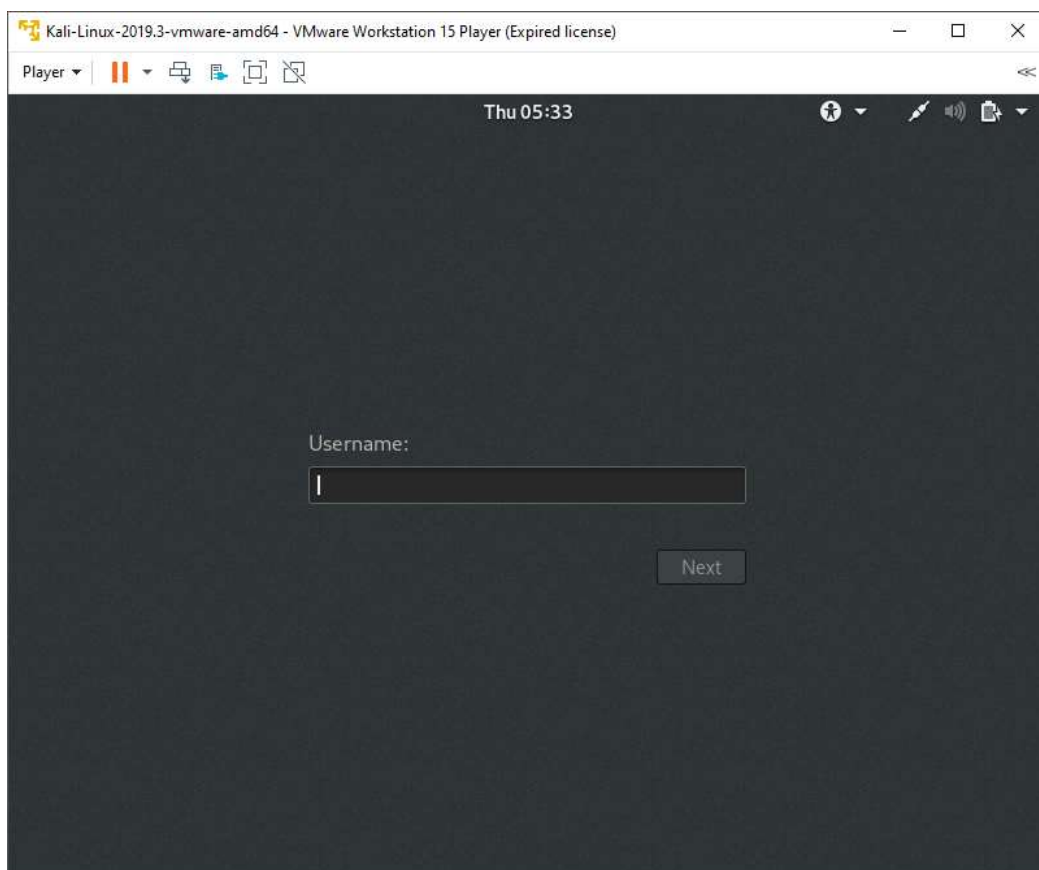
Al encender la máquina virtual, tendremos una ventana en la que se lanzará automáticamente el sistema operativo preinstalado. Podemos cambiarle el tamaño y las proporciones como a cualquier ventana o incluso trabajar a pantalla completa.

En nuestro caso lo más cómodo sería dividir nuestro espacio de trabajo entre la ventana de la máquina virtual y la página con las instrucciones del *escape room*.

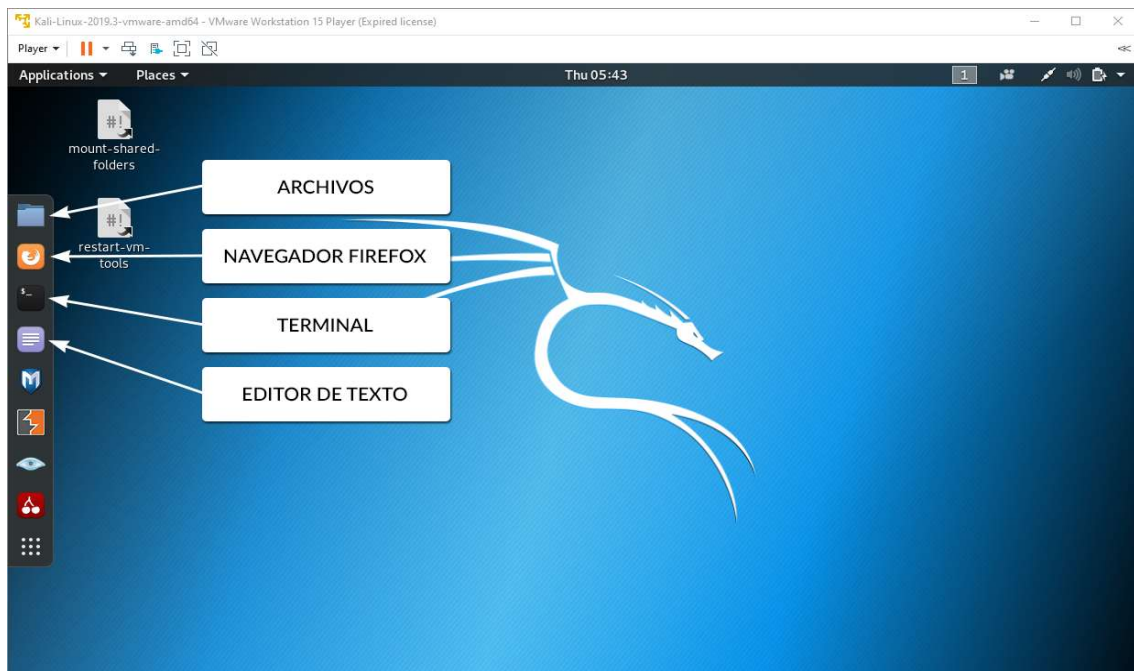
Cuando nos pida un usuario y contraseña, introduciremos los siguientes datos de acceso:

Username: **root**

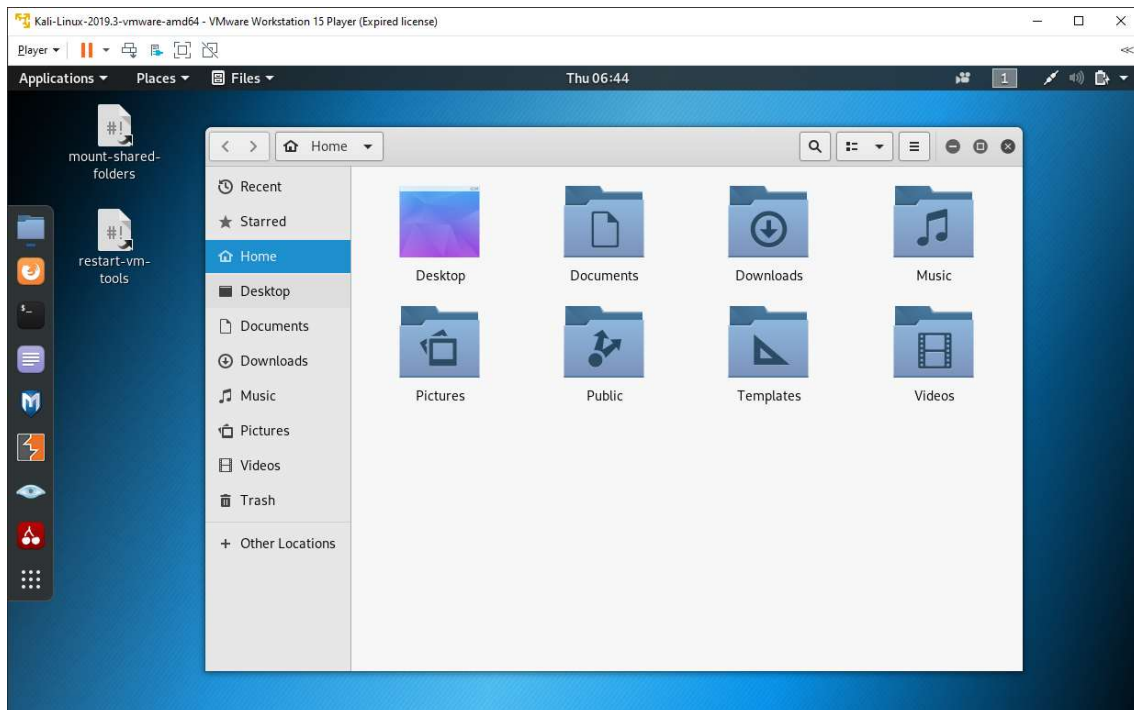
Password: **toor**



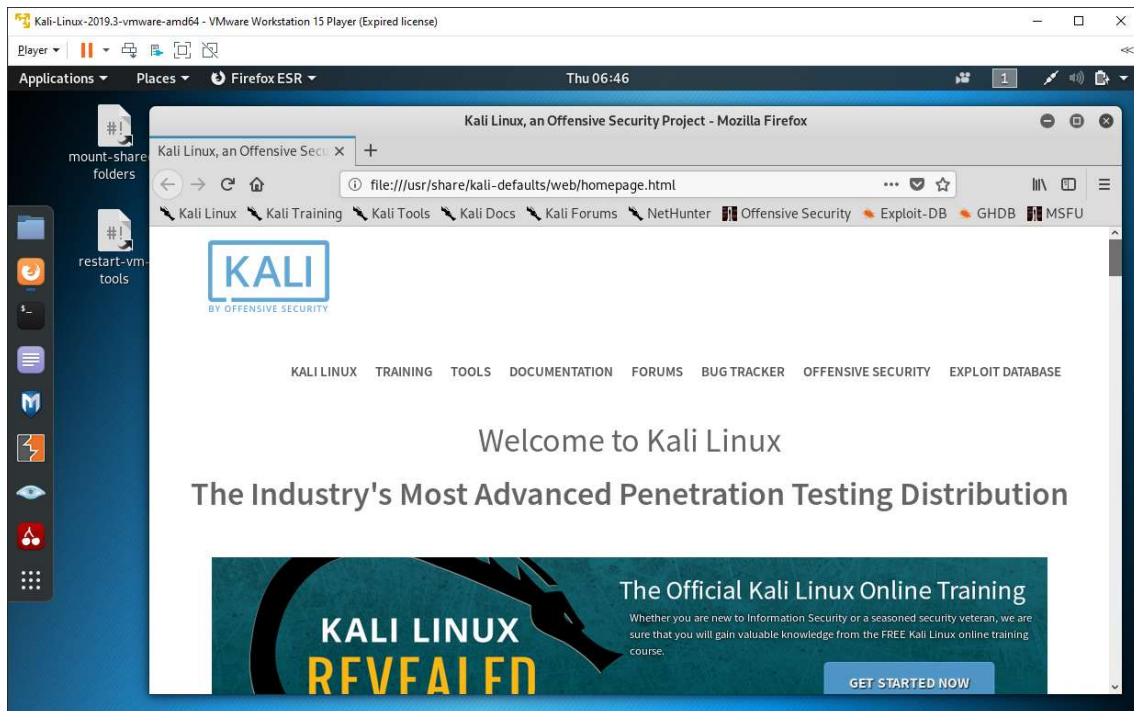
Nos encontraremos con una interfaz gráfica bastante similar a un entorno Windows o Mac en la que usaremos los siguientes elementos principales:



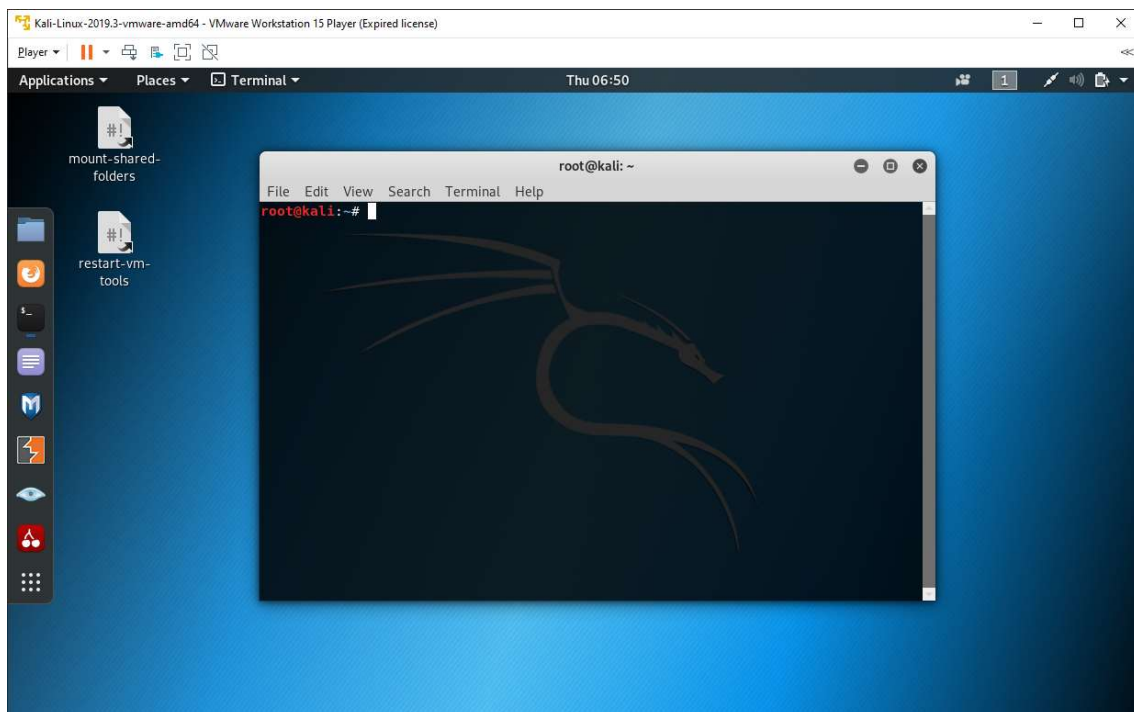
- **Archivos:** Sistema de carpetas donde están almacenados todos los ficheros.



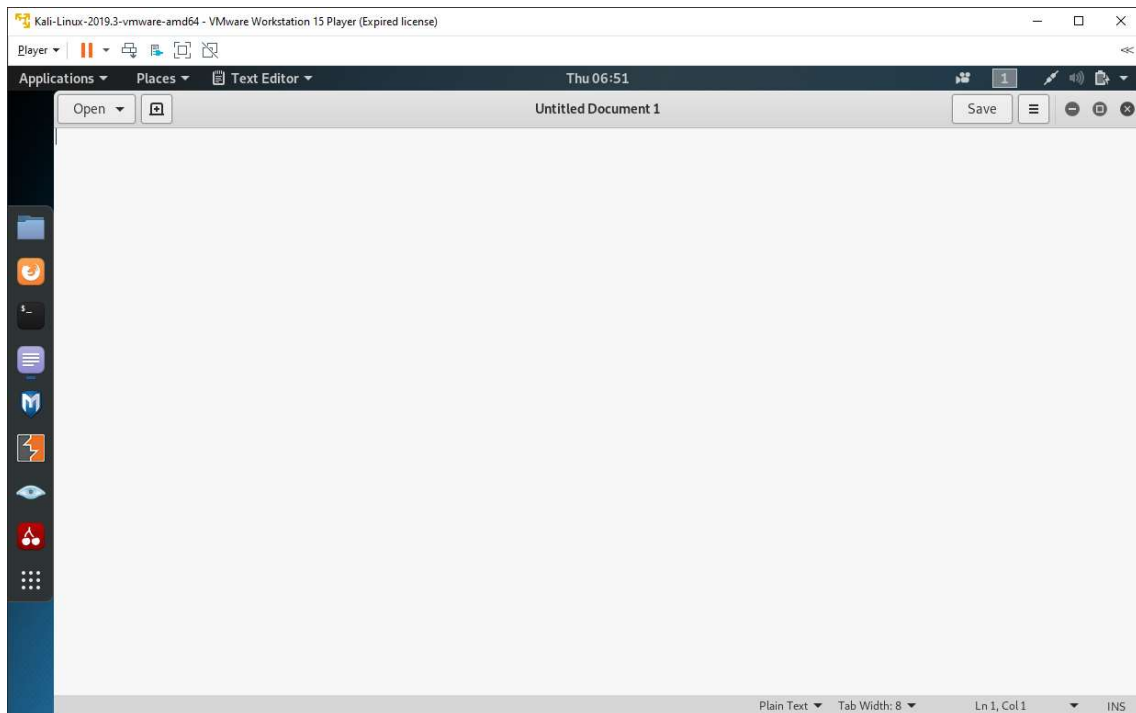
- **Navegador Firefox:** Aplicación con la que podremos abrir las aplicaciones web y otros archivos similares.



- **Terminal:** Aplicación que nos permite escribir y ejecutar comandos y scripts para realizar diversas tareas sin necesidad de una interfaz gráfica.



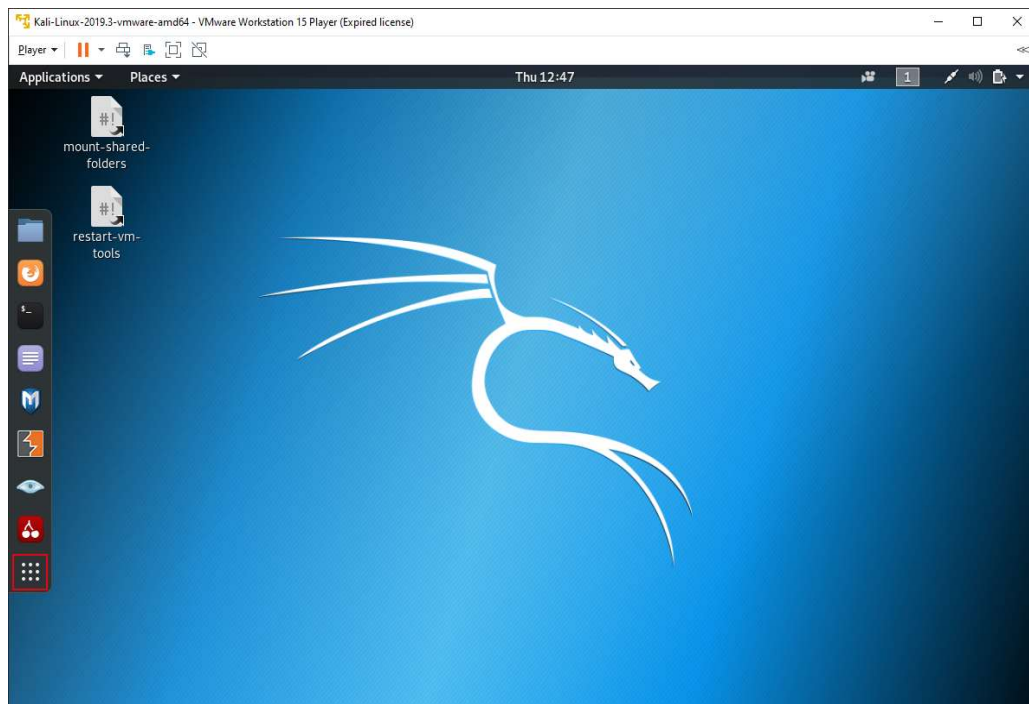
- **Editor de texto:** Programa que nos permite crear archivos de texto sin formato o de texto plano.



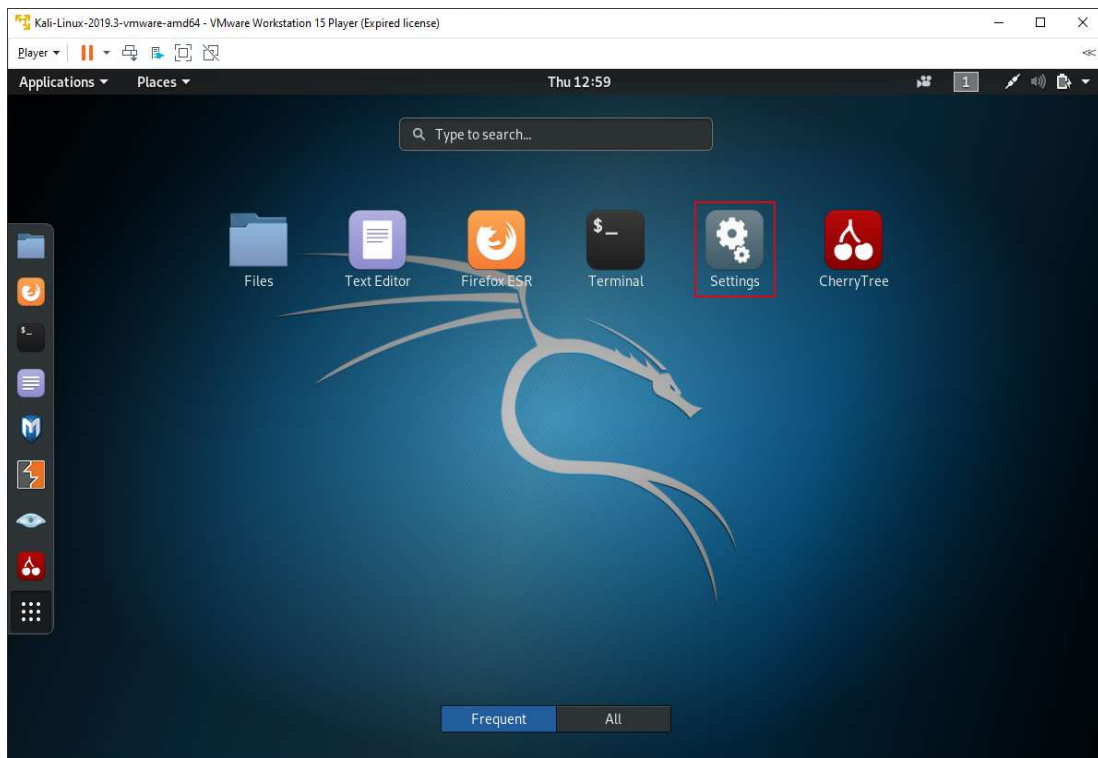
Con estas herramientas intentaremos acceder a la máquina que contiene el *escape room*, en la que no podremos realizar ninguna acción, pero que tendrá que estar activa.

Para facilitarnos la tarea, **debemos configurar el teclado al español**, ya que el que viene por defecto es el inglés y no se corresponde con nuestros símbolos.

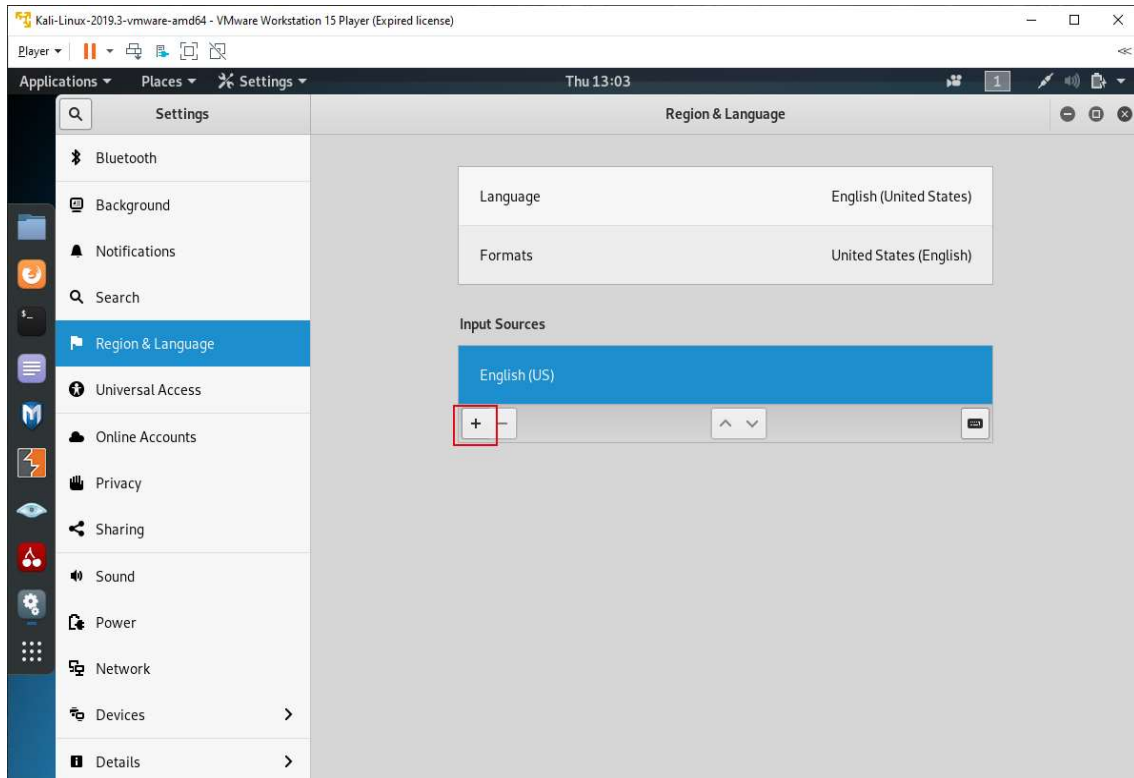
Para ello pulsaremos el **último icono de la barra lateral**, que nos mostrará todas las aplicaciones disponibles.



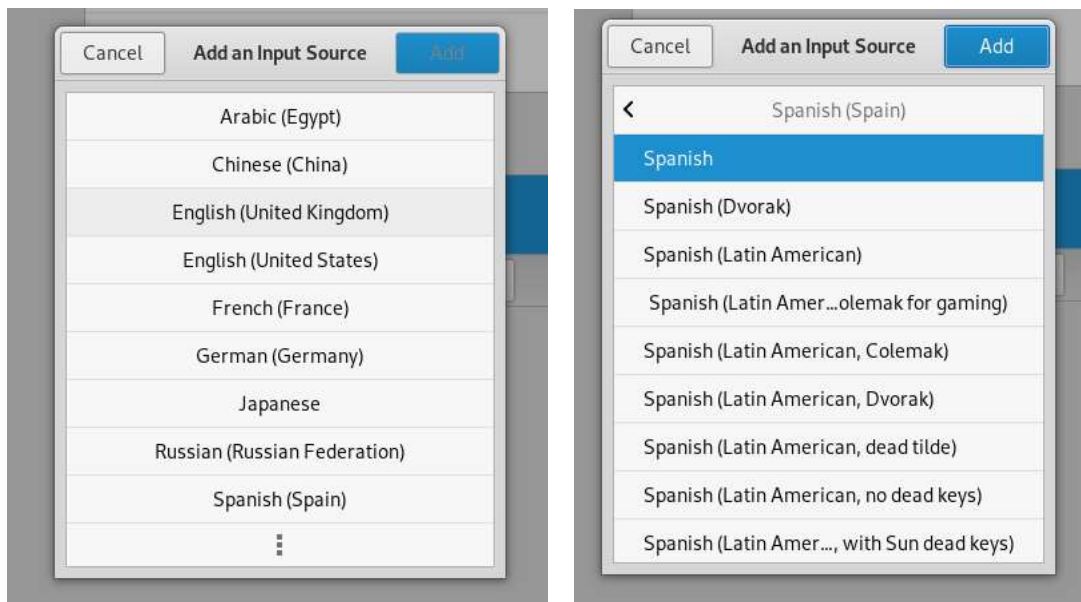
Después accederemos a las **opciones**, seleccionando el icono correspondiente.



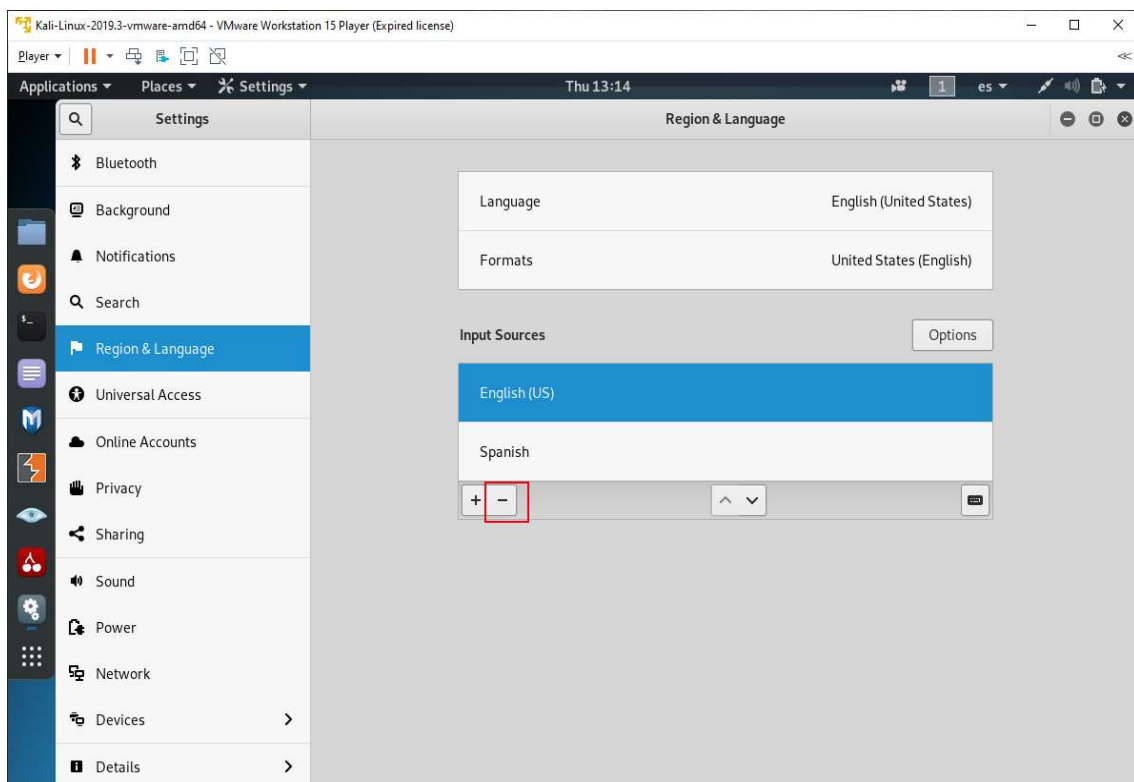
Seleccionaremos **Region & Language** y después, en **Input Sources** hacemos click en el **botón con el símbolo +** para añadir un nuevo idioma.



Seleccionamos **Spanish (Spain)**, después **Spanish** y añadimos el idioma.



Por último, borraremos el idioma inglés para menor confusión, seleccionándolo y pulsando el **botón con el símbolo -** y cerramos la ventana.

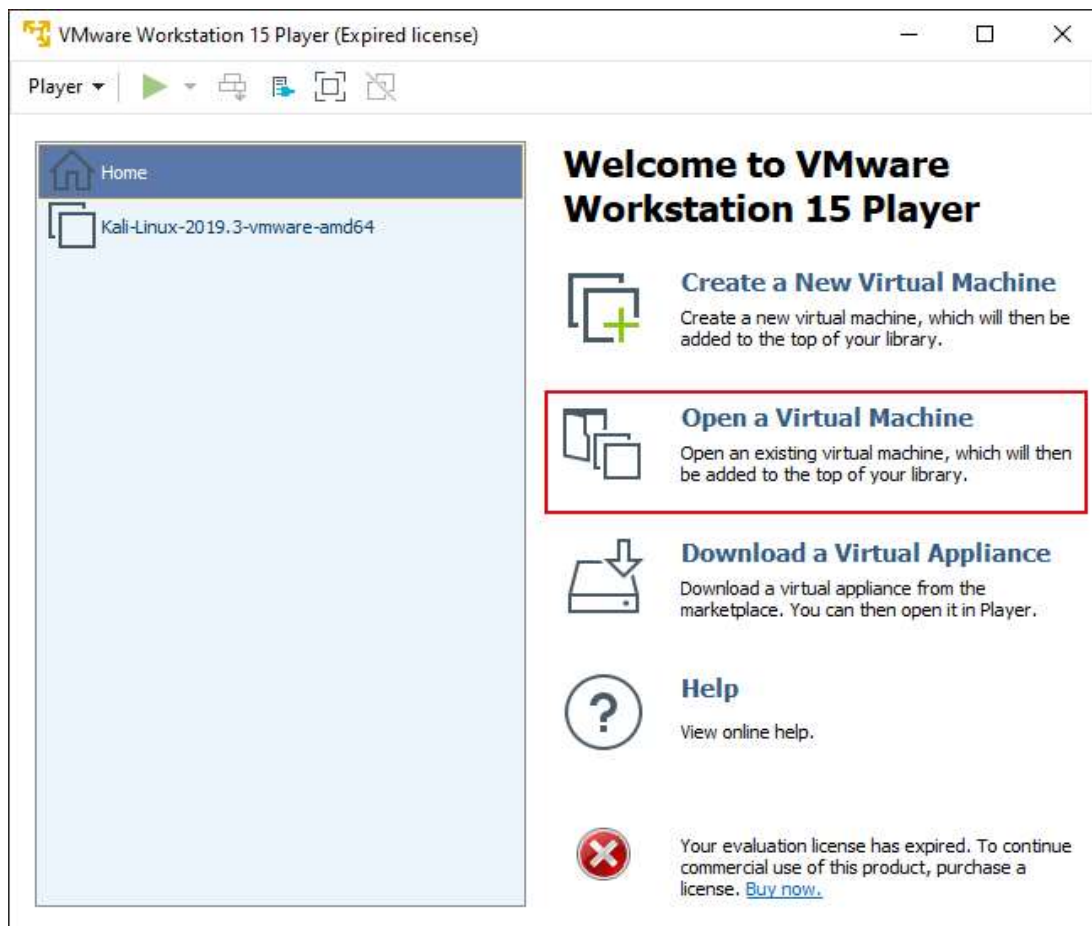


Instalación de la máquinas objetivo

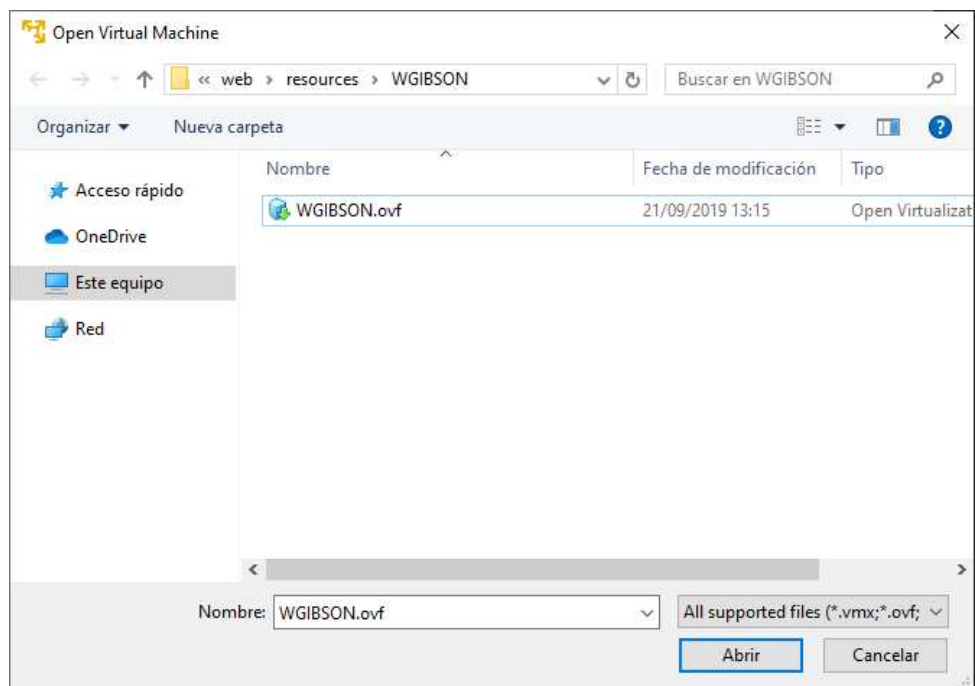
Sin cerrar la máquina que ya tenemos activa, desde la que realizaremos nuestras acciones, debemos instalar y lanzar una nueva máquina que será la que debemos atacar, la que contiene el *escape room*.

El proceso es similar al anterior.

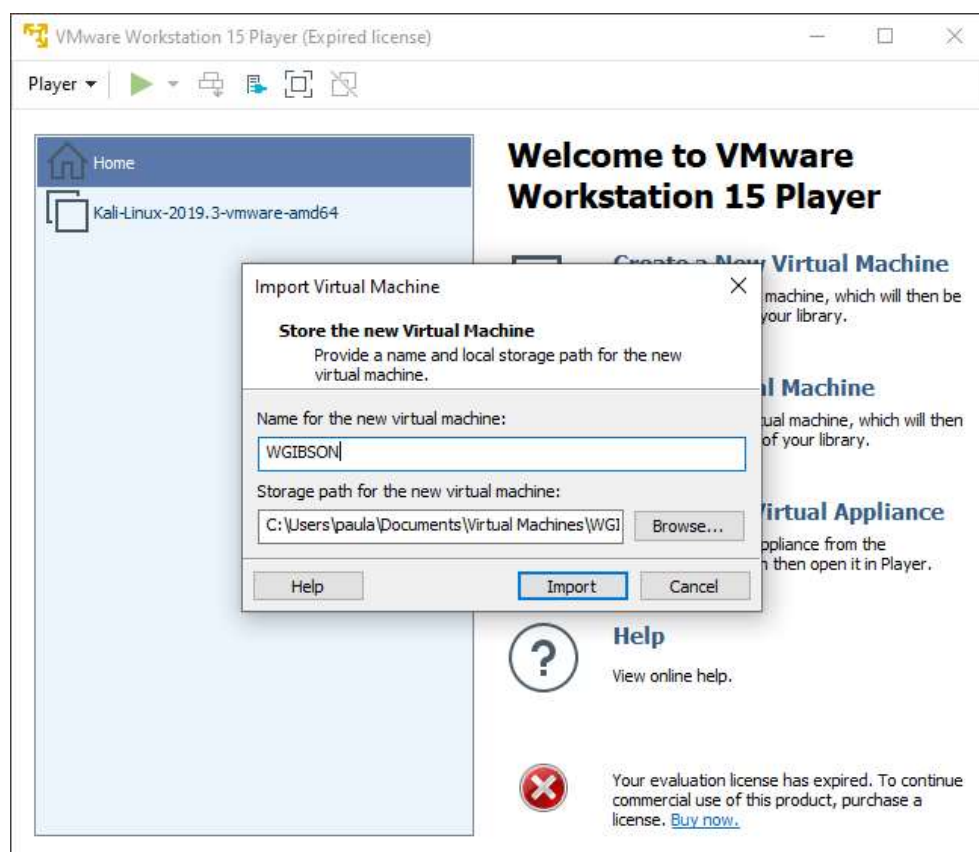
Después de descargar el archivo con la máquina a resolver de la web del curso, procedemos a abrir otra sesión de **VMware** y elegimos la opción de **abrir una máquina virtual**.



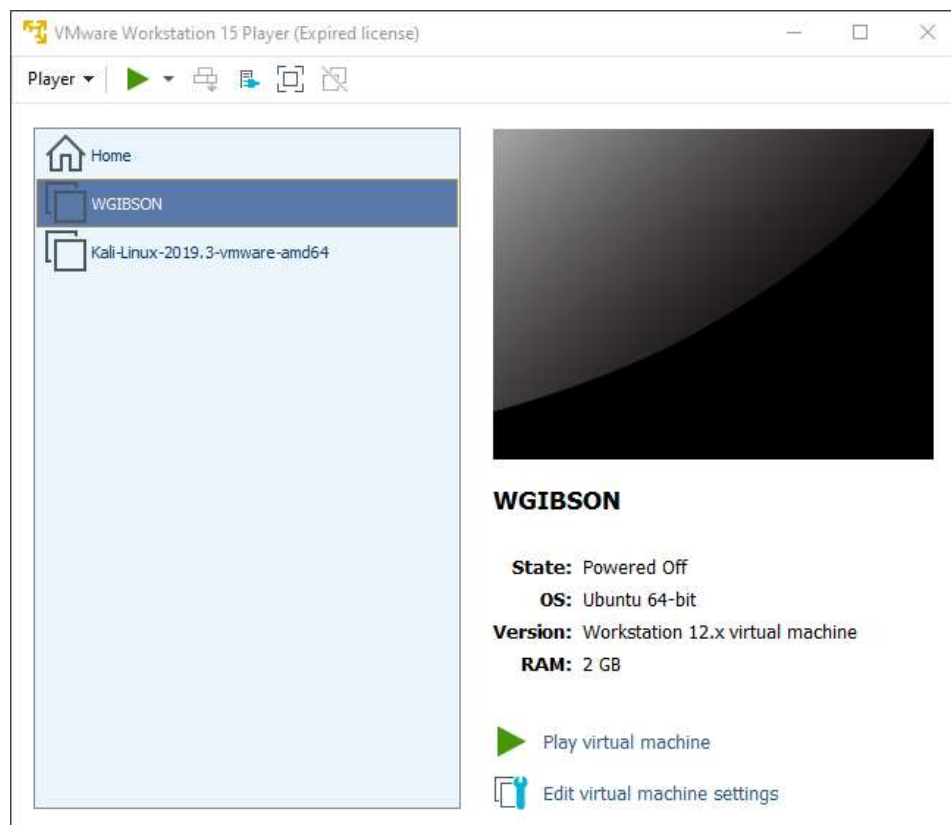
Después, elegiremos el archivo con extensión **.ovf** que contiene la máquina.



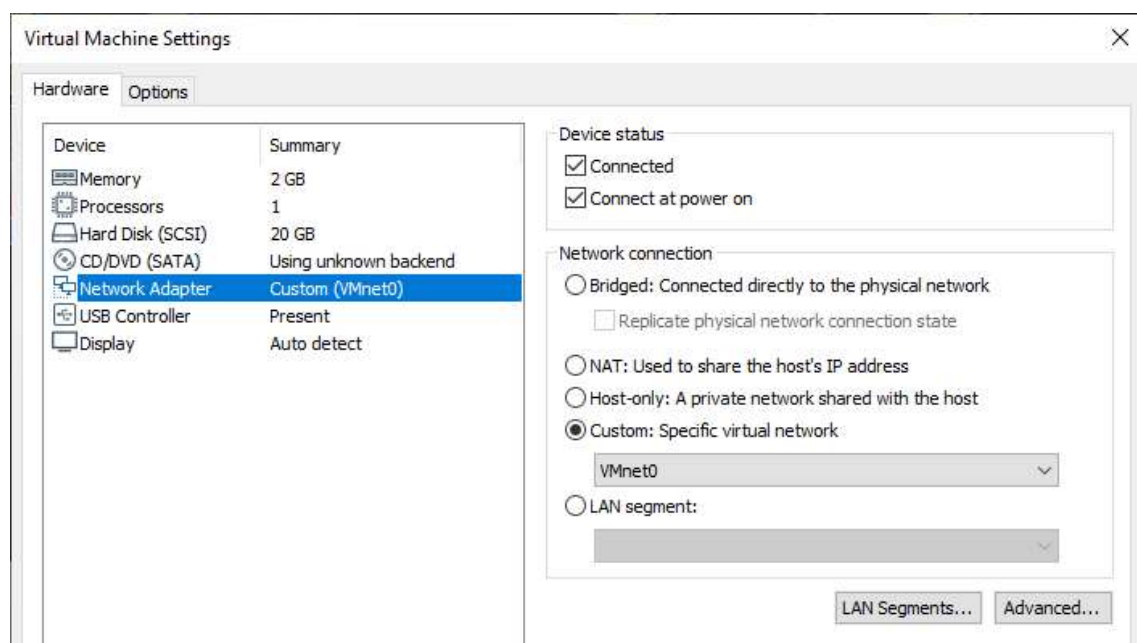
Indicamos la carpeta donde queremos que se guarde la máquina, por defecto, la carpeta de sistema de la aplicación donde también está alojado el entorno de pentesting.



Una vez finalizada la importación de la máquina la importación de la máquina, ya podemos ejecutarla del mismo modo que el entorno de pentesting.



Es **muy importante recordar** que hay que configurar la máquina para que trabaje en el mismo entorno de red que hemos elegido para nuestra máquina con el entorno de pentesting para que se puedan ver entre ellas.



Para instalar la otra máquina objetivo, seguiríamos el mismo proceso, importando su archivo **.ovf** correspondiente y configurando después el mismo entorno de red que las anteriores.

