# PROYECTO HACKING ÉTICO

**Trabajo realizado por** [**Lucas Falla Urtiaga**](mailto:falla.urluc24@triana.salesianos.edu) **y** [**Álvaro Castilla Cano**](mailto:castilla.caalv24@triana.salesianos.edu)**.**

**1  *EXPLOITS***

Un exploit es un software, un fragmento de datos o una secuencia de comandos que aprovecha un error o una vulnerabilidad de una aplicación o sistema para provocar un comportamiento involuntario o imprevisto.

Su nombre deriva del verbo inglés *“to exploit"*, que significa *“usar algo en beneficio propio”*. Básicamente, esto significa que el objetivo de un ataque padece un defecto de diseño que permite a ciertas personas crear los medios para acceder a él y utilizarlo en su propio interés.

La versión gratuita y limitada de Metasploit Framework Community es una herramienta que permite ejecutar y desarrollar exploits contra sistemas objetivos. Actualmente se encuentra integrado con Kali Linux, una distribución de Linux con diversas herramientas orientadas a la seguridad y es ampliamente utilizado para realizar pruebas de penetración.

Por lo que nosotros la usaremos para mostrar paso a paso la explotación de un servidor vulnerable.

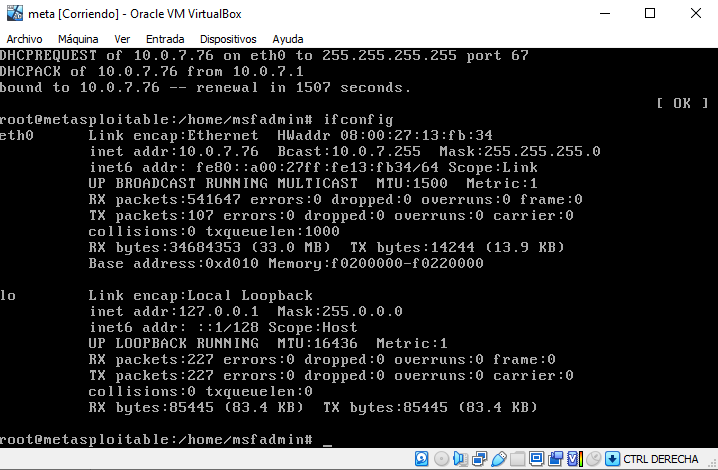
**2  *EXPLOTAR UNA VULNERABILIDAD CON METASPLOIT***

Para empezar a realizar el ataque, hemos necesitado de 2 máquinas virtuales (obviamente). Nosotros, personalmente, hemos utilizado **Kali Linux** y **Metasploitable 2**, siendo Álvaro el propietario de la primera y Lucas el de la segunda.

Hacemos un pequeño paréntesis para hacer saber que Metasploitable 2 es una máquina virtual creada con fines académicos, y que ya posee varias vulnerabilidades que permiten que sea sencillo realizar pruebas sobre ella.

Para continuar, es importante verificar que ambas máquinas tengan visibilidad entre sí (es decir, que puedan comunicarse). Esto puede corroborarse con un simple ping entre las dos.

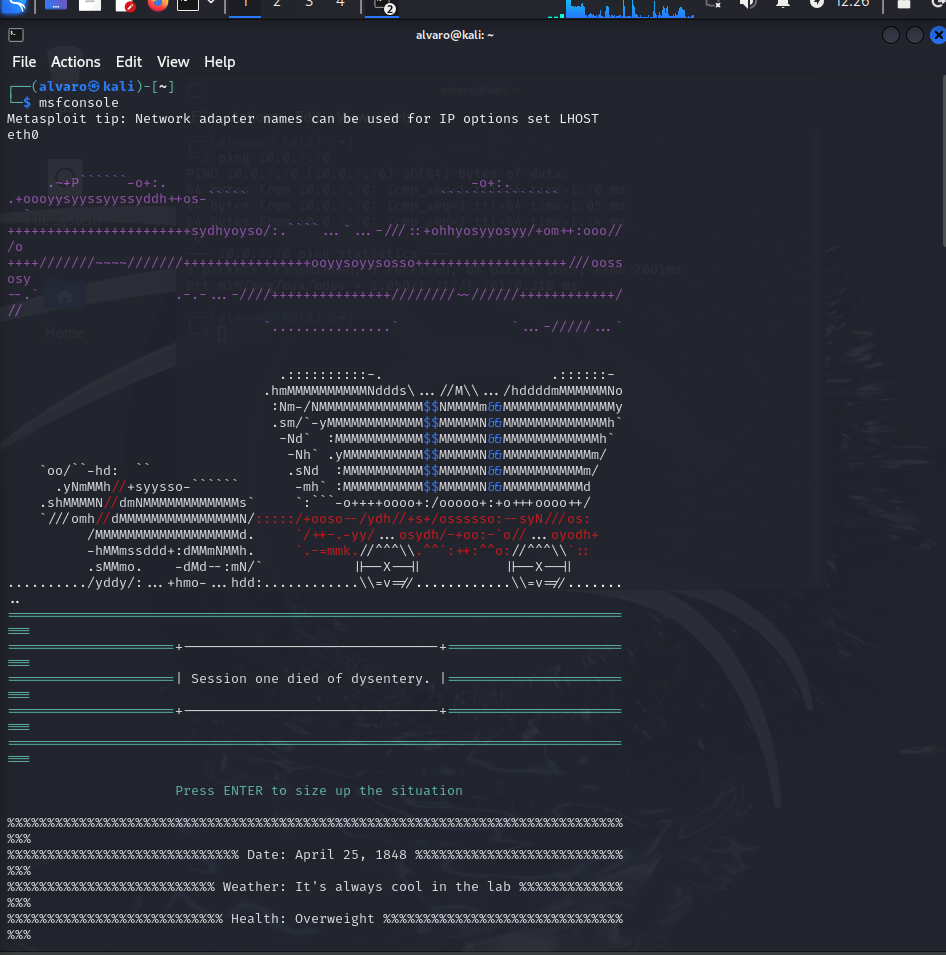
En la siguiente imagen podemos ver el estado de las interfaces de red en el ordenador que tiene Metasploitable 2, pudiendo observar que la dirección de red es: **10.0.7.76**.

****

Después, desde la máquina en Kali Linux (que por cierto, todo el ejercicio se desarrolla en esta máquina, ya que la segunda solo oficia como objetivo del ataque, por lo que no se vamos a realizar acciones en esta más allá de activarla para *“atacarla”*) utilizaremos la consola de Metasploit (msfconsole) desde donde se lanzarán todos los comandos correspondientes sobre el servidor en el que se desea realizar la prueba de penetración. Para abrir la consola, solo hace falta utilizar el comando:

***msfconsole***

Aquí se puede ver cómo lo usamos:



**Information gathering**

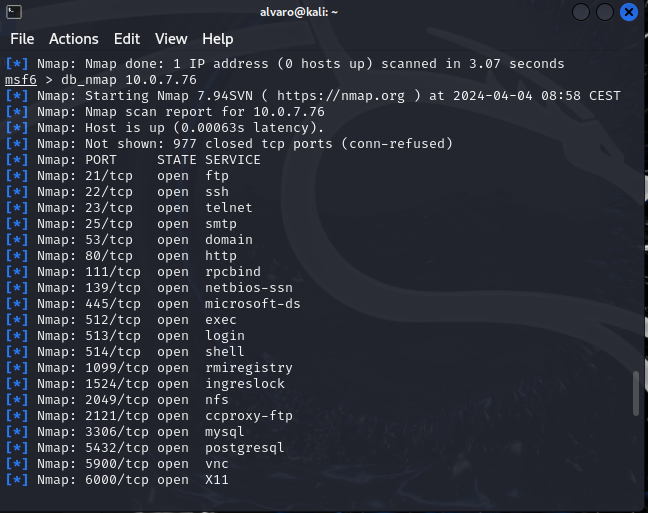
Para el que no lo sepa, el término *“Information gathering”* se refiere a recabar la máxima cantidad de información posible de fuentes abiertas.

Volviendo con la penetración y una vez utilizado el comando “*msfconsole”*, necesitamos recopilar información, y para lo cual es posible utilizar Nmap desde la propia consola de Metasploit (Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos). Para ello, basta con solo invocar el comando *“db\_nmap”*. Los parámetros que pueden utilizarse son los mismos que acepta Nmap. De esta manera, los resultados serán almacenados en la base de datos de Metasploit.

Para obtener una observación rápida del sistema objetivo, se ingresa el siguiente comando:

***db\_nmap direcciónIP***

En nuestro caso sería: *“db\_nmap 10.0.7.76”*.

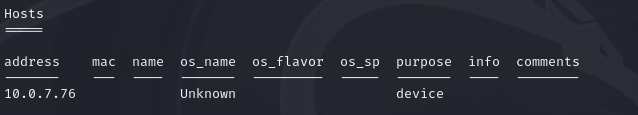


Con el comando anterior se realiza un escaneo sobre todos los puertos del sistema objetivo. De esta manera, tal como se especificó anteriormente, los resultados serán almacenados en la base de datos.

Para consultar la información de todos los sistemas que han sido analizados utilizamos el comando:

***hosts***

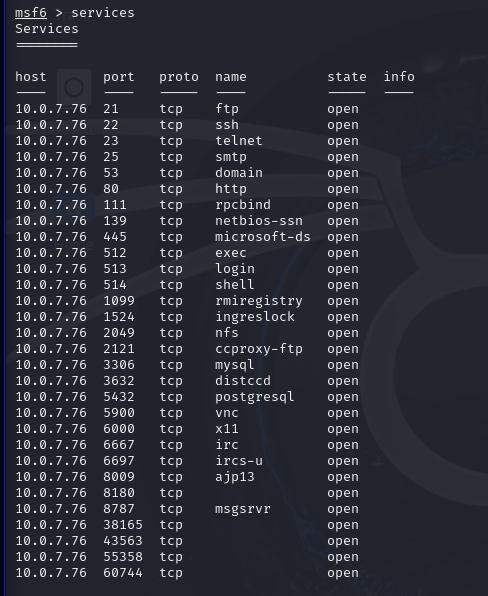
De esta forma se nos imprimen dichos datos por pantalla:



También podemos imprimir por pantalla todos los puertos y servicios asociados que han sido descubiertos durante el análisis con Nmap usando el comando:

***services***

De esta forma:



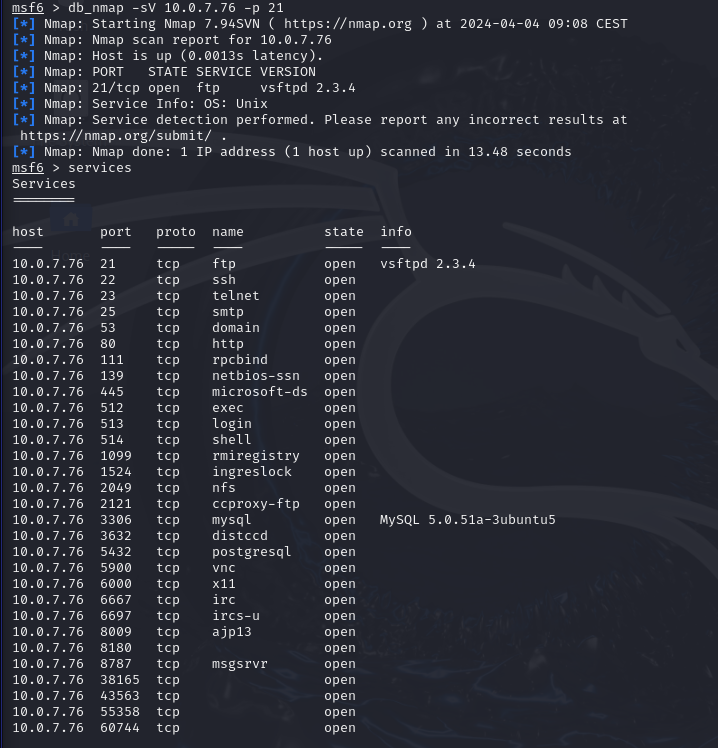
Sin embargo, en esta instancia es posible que no se cuente con demasiada información sobre los servicios descubiertos en el sistema objetivo. Pero utilizando la misma herramienta (Nmap) es posible determinar, por ejemplo, la versión específica de un servicio. Esto se puede lograr mediante el siguiente comando:

***db\_nmap –sV direcciónIP –p puertoDeInterés***

El parámetro *“sV”* indica que se examine la versión específica del servicio. En nuestro caso podríamos elegir cualquier puerto de entre todos los disponibles, por lo que a modo de ejemplo, vamos a ejecutar dicho comando para averiguar la versión sobre el servicio que se está ejecutando en el puerto 21, utilizado comúnmente por el servicio FTP ( aquel protocolo VISTO EN CLASE que se utiliza para transferir todo tipo de archivos entre equipos conectados a una red).

Introducimos el comando: *“db\_nmap -sV 10.0.7.76 -p”*.

Si ahora ejecutamos el comando *“services”* nuevamente, se obtendrá información específica del servicio analizado (añadiéndose en el campo *“info”*).



Como podemos observar, la versión del servicio del puerto 21 ahora es visible.

Cabe destacar que el puerto 3306 también tiene información visible porque hicimos con él una pequeña prueba para comprobar que el comando anteriormente mencionado funcionara correctamente. Así que vamos a ignorarlo para el resto de la explicación ya que carece de importancia para esta.

**Explotación**

Puesto que hemos encontrado información de un servicio en especial, es posible determinar a partir de esta, si el mismo es vulnerable. Utilizando la consola, podemos realizar la búsqueda de un exploit en particular para ese servicio y luego llevar a cabo la explotación del mismo. Para realizar la búsqueda se ingresa el siguiente comando:

***search versionInfo***

En nuestro caso: *“search vsftp 2.3.4”*.



Tras utilizar el comando, podemos visualizar tras toda esa información que efectivamente podemos utilizar un exploit. Y para ello, utilizaremos el último comando de la última línea que se nos imprime por pantalla en color azul.

O sea: use exploit/unix/ftp/vsftpd\_234\_backdoo r..

Explicándolo brevemente, para seleccionar el exploit se introduce el comando *“use”* seguido de la ruta del exploit seleccionado:

**use rutaDelExploitSeleccionado**

En nuestro caso, el comando que debemos introducir sería el anteriormente mencionado.



Una vez seleccionado el exploit que se va a utilizar, se deben configurar aquellos parámetros necesarios a través de la consola. Para ver las opciones, debemos ingresar el comando:

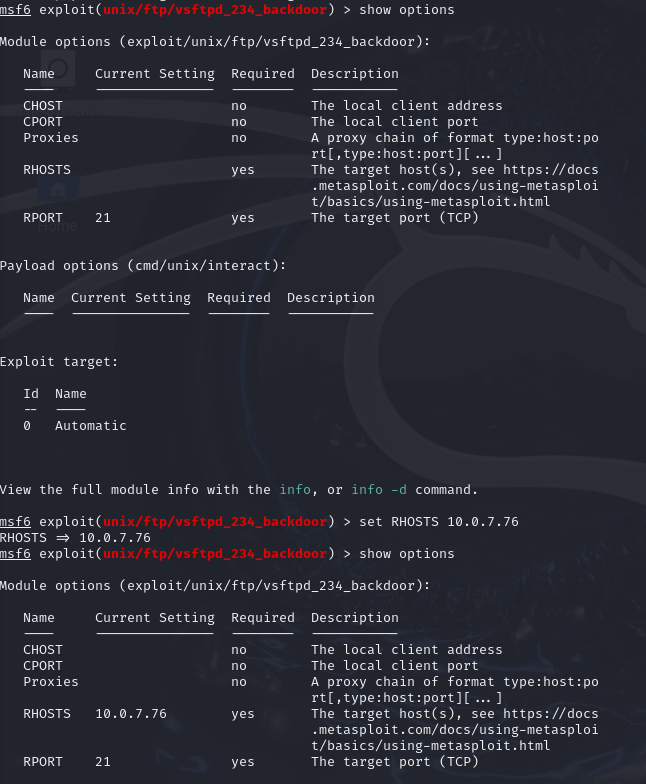
***show options***

el cual enumera todos los parámetros indicando si son opcionales u obligatorios mediante el campo *“required”*.

En esta instancia, ya es posible configurar los parámetros. Para realizar esta tarea se debe utilizar el comando *“set”* seguido del parámetro y el valor que se desea establecer:

***set parámetroDeseado valorDeseado***

Para nosotros, el comando sería el siguiente: *“set RHOSTS 10.0.7.76”*.



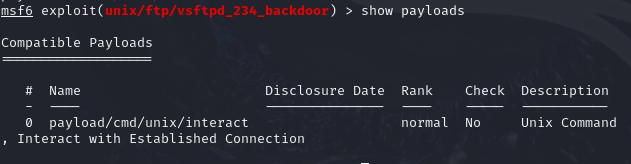
**Payload**

Básicamente, el *“payload”* es la secuencia de instrucciones que se ejecutarán una vez que se haya explotado con éxito la vulnerabilidad. Metasploit Framework posee diversos payloads con diferentes funcionalidades para cada tipo de arquitectura.

Si nos fijamos en la imagen anterior, podremos observar que tras la información impresa por pantalla tras el comando “show options” encontraremos esta sentencia que hace referencia a los payloads que podemos usar: Payload options (cmd/unix/interact) :.

En este caso, usaremos el payload sugerido: el payload cmd/unix/interact. Sin embargo, para conocer todos los payloads que son compatibles con el exploit que se va a utilizar, existe un comando para realizar el listado correspondiente:

***show payloads***



En este caso, sólo podemos utilizar el sugerido por Metasploit, ya que es el único que aparece en la lista.

Así que dejémonos de rollos y utilicemos el siguiente comando para establecer el payload:

***set payload nombreDelPayload***

En nuestro caso, el comando sería: *“set payload cmd/unix/interact payload”*.

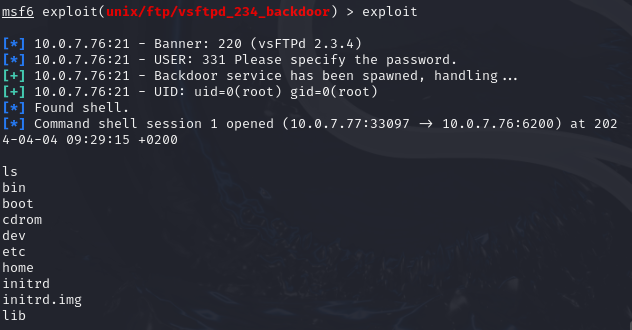


Luego de que todos los parámetros ya han sido configurados (por fin) será posible llevar a cabo la explotación. Para ello, basta con ejecutar el comando:

***exploit***

y esperar que Metasploit haga su trabajo.

En esta instancia, si todo ha salido bien, se obtiene una shell de comandos sobre el sistema que ha sido atacado, permitiendo ejecutar cualquier comando en dicho sistema. Por ejemplo, a continuación se puede observar un comando de listado de directorios (hecho con el comando *“ls”*):



**3  *CONCLUSIÓN***

En este caso hemos obtenido acceso a un servidor a través de un servicio FTP vulnerable. Mediante la identificación de la versión del servicio se pudo encontrar el exploit adecuado y de la misma manera, hemos inyectado un payload capaz de disponer una shell de comandos a merced del atacante.