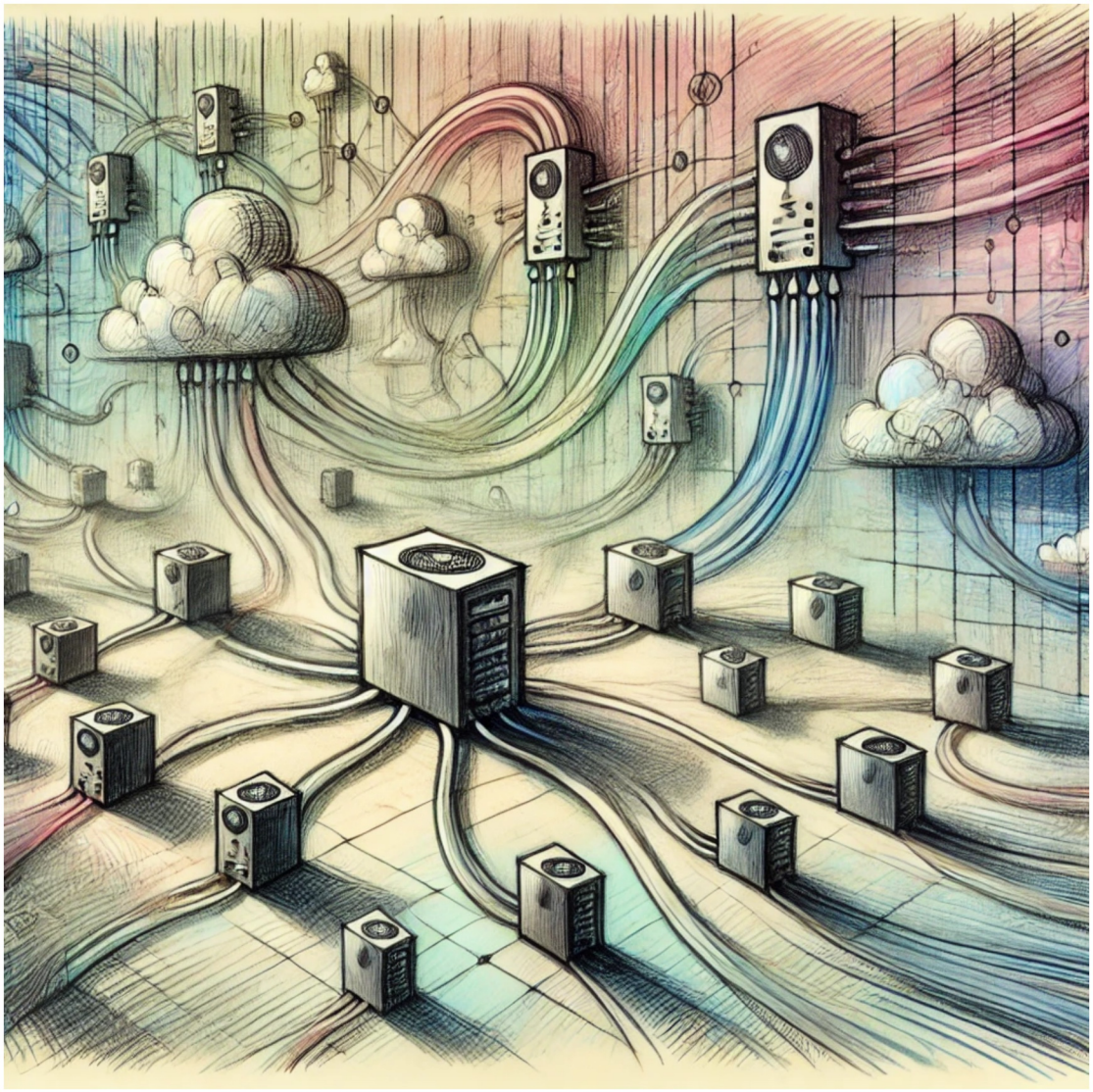


SPRING 18

UNIDAD 2

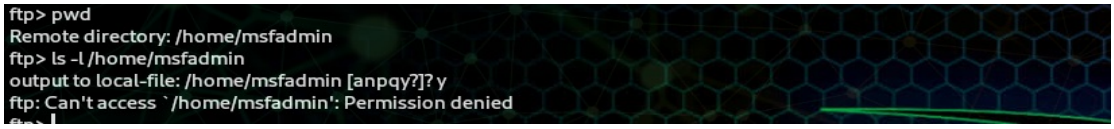
EJERCICIOS 1, 2 Y 3

NO TUNNELING-SSH

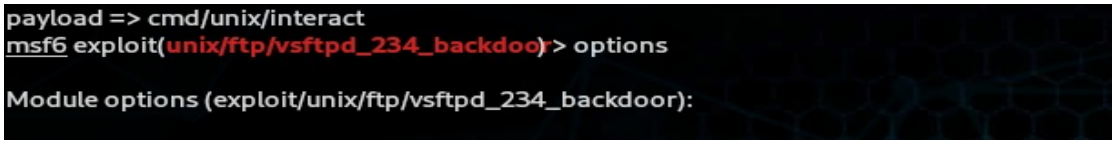
-- EJERCICIO_1.- Conseguir una shell en la Kali de la máquina Metasploitable2, sin usar la técnica de SSH Tuneling. Para ello deberás hacer uso de las herramientas vistas en la unidad 2 del Sprint.

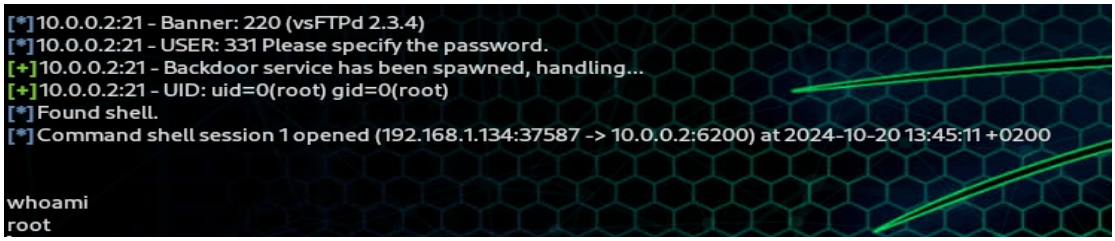
1. Se establece la infraestructura necesaria para llevar a cabo esta práctica, estando establecido como host principal el sistema Kali Linux con IP 192.168.1.134. al que se le ha añadido una 2º red en el rango 10.0.0.0/24 via hacia pivoting, por el método post-ip, es decir, que se conecta a esta 21 red una vez que se ha levantado la red DHCP principal. Porr otro lado e interconectadas a través de virtual-box, se encuentran las máquinas pivoting y meta 2 , la primera con 2 interfaces de red abiertas: una, en modo bridge con Kali (IP 192.168.1.170) y otra, en red privada con meta 2(IP 10.0.0.1), y la segunda, conectada con una sola interfaz de rred en modo privado hacia pivoting (IP 10.0.0.2).
2. Se realiza conexión desde la máquina Kali a la Metaexploitable2, a traves del **servicio FTP** usando las credenciales conocidas, que en un caso real habría que usar técnicas de explotación para conocimiento de cradenciales, consiguiendo de esta forma, una forma sin usar técnicas de tunneling-ssh para llevar archivos hacia la maquina meta 2.

3. Se hacen una serie de comprobaciones con el ftp, no teniendo permisos para enviar archivos, solo lectura, por lo que buscamos otros medio parra hacer llegar el payload a meta 2 que no sea SSH.

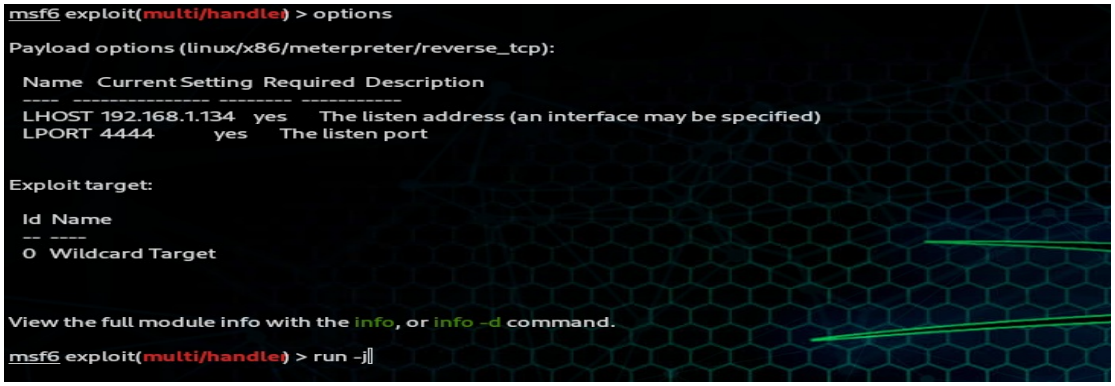


4. A traves de través del *“Framework Metaexploit”*, se utiliza una vulnerabilidad que tiene la versión vsftp 2., la cual usa la máquina meta 2, siendo la misma postiva consiguiendo una shell basica pero con permisos root:



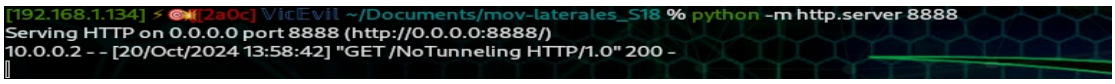


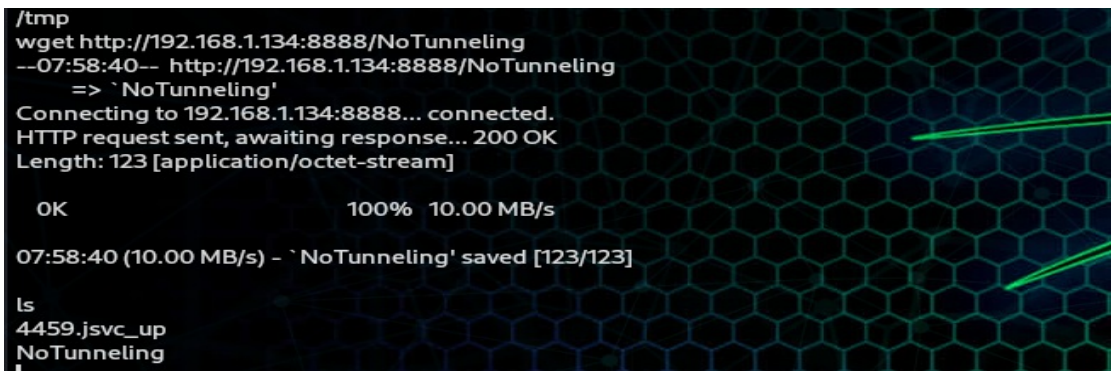
5. A través del mismo *Framework*, se apertura un **“handler”**, el cual pondremos a la escucha, ejecutando con el **flag -j,** hasta que le llegue la conexion del payload que vamos a configurar y enviar a meta2.



6. Se realiza con la herramienta “MSFvenom” un payolad que vamos a trrasferir via ftp a la máquina meta 2, dándole allí, permisos de ejecución, antes de ejecutarlo para recibir la conexión en el handler que tenemos a la escucha en Metaexploit.

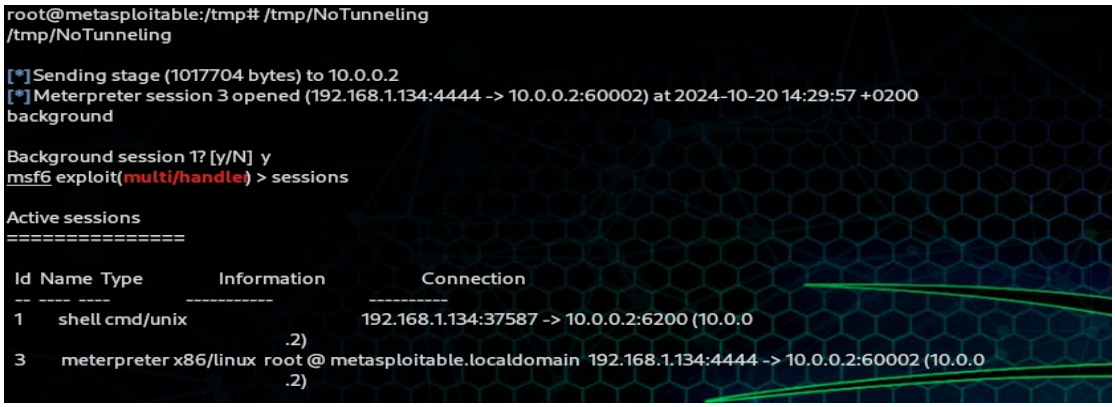
7. Ahora que tenemos la shell básica abierta con plenos permisos, se procede a enviar el payload desde Kali a meta2, usando el metodo servidor python - wget:





8. Se le conceden los permisos necesarios al payload para ser ejecutado, a través de la shell root conseguida y mejorada, procediendo a su ejecución:

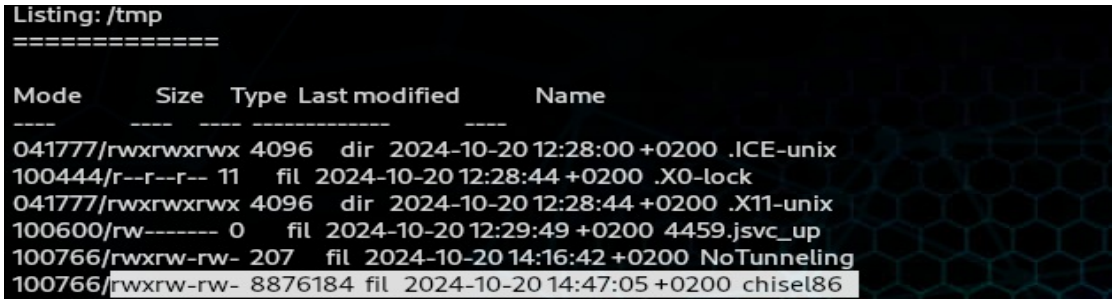
9. FinaLmente, se consigue una meterpreter con permisos root en meta 2 sin haber usado las técnicas del tunneling -SSH:



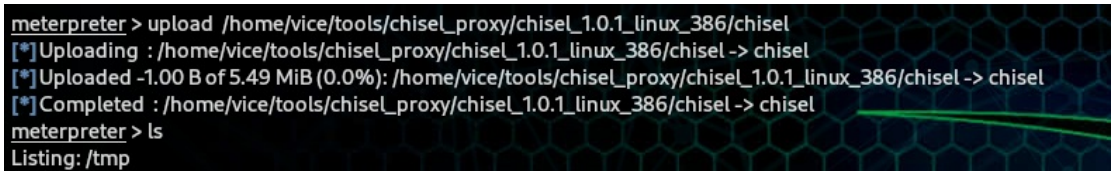
--EJERCICIO_2.- Conseguir acceder a la aplicación web de la Metasploitable2 desde la Kali, sin hacer uso de nuevo de un enrutamiento por SSH Tuneling.

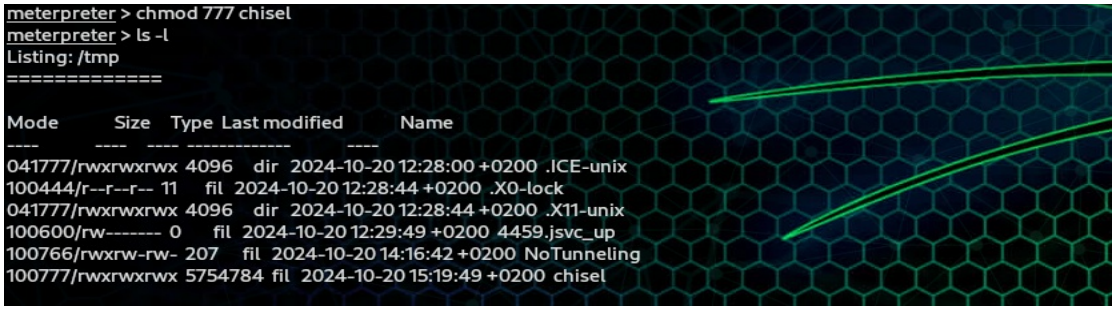
- En este caso, vamos a usar la herramienta “Chisel” que actúa como un proxy TCP/UDP, utilizándose para redirigir tráfico a través de una red. Aunque, puede ser usada para configurar túneles, no es específicamente una herramienta de tunneling en el sentido tradicional como SSH tunneling, sino mas bien una técnica de proxing.

1) En primer lugar, vamos a transferir el archivo de la herramienta proxy a la máquina meta 2, aprovechando la meterpreter conseguida anteriormente entre Kali y meta 2:

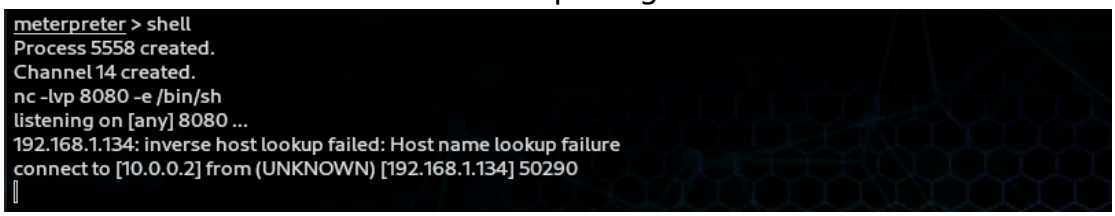


2) Ahora, configuramos Chisel, tanto en kali como en meta2, estableciendo un proxy inverso:



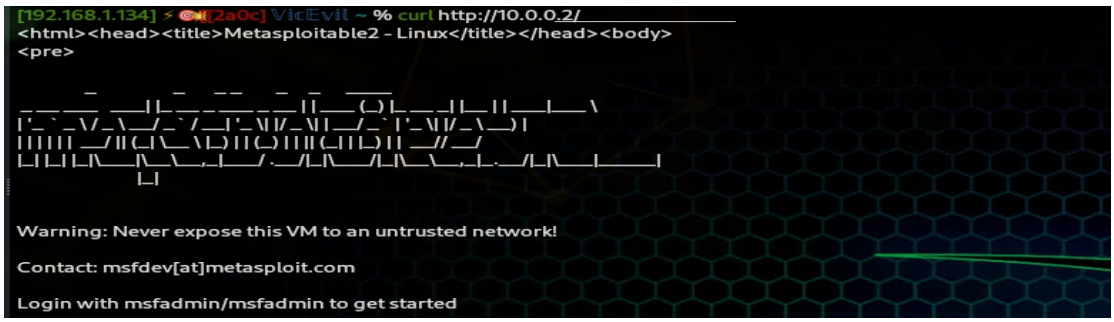


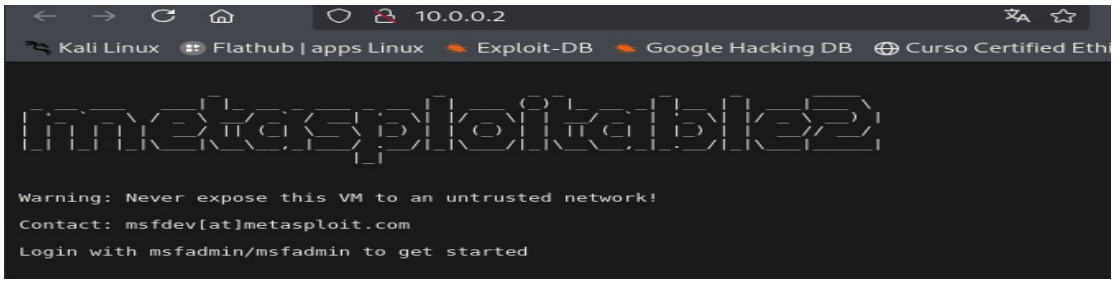
3) Se hacen varias pruebas con diferentes version de chisel para meta 2, que al tener un kernel obsoleto, no es compatible con muchas funciones que necesita el lenguaje go para ejecutar chisel, porr lo que se deja esta via y se busca una alternativa.
   Se plantea el uso de proxychains, pero una vez analizada esta posibilidad, entra dentro de las técnicas de tunelización por lo que se descarta.
   Finalmente, se decide **usar una herramienta de red** muy versátil: **netcat (nc)**, conocida como la "*navaja Suiza del TCP/IP*", que permite realizar diversas operaciones de red, entre las que se encuentra: permitir obtener una shell interactiva remota, funcionando un extremo de servidor y otro de cliente y la conexión a tros puertos y servicios de diferentes máquinas.
4) Por lo expuesto en al apartado anterior, a través de la shell meterpreter conseguida anteriormente con la máquina meta 2, ejecutamos el servidor de **netcat** por un **puerto libre en meta 2 (8080)**. En la **Kali**, ejecutamos el **cliente de netcat** para que se **conecte a la IP de meta2 por el mismo puerto**, consiguiendo otra nueva shell con maximos pivilegios.



El parámetro -e le dice al servidor netcat que ejecute un programa cuando se establezca la conexión, es decir, se ejecuta una shell de bash al efectuarse la misma

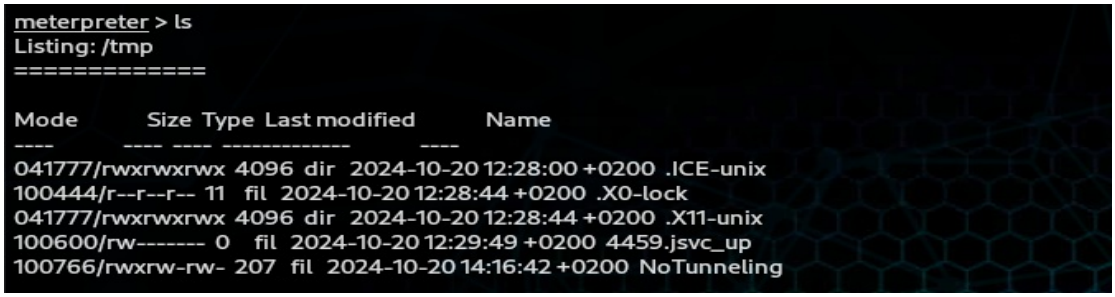
5) Una vez conectados, ejecutamos el comando **“curl”** con la **direccion web de la metaexplotable2**, consiguiendo respuesta satisfactoria, al igual que a ejecutando, directamente, a través del **navegador web** de la Kali:



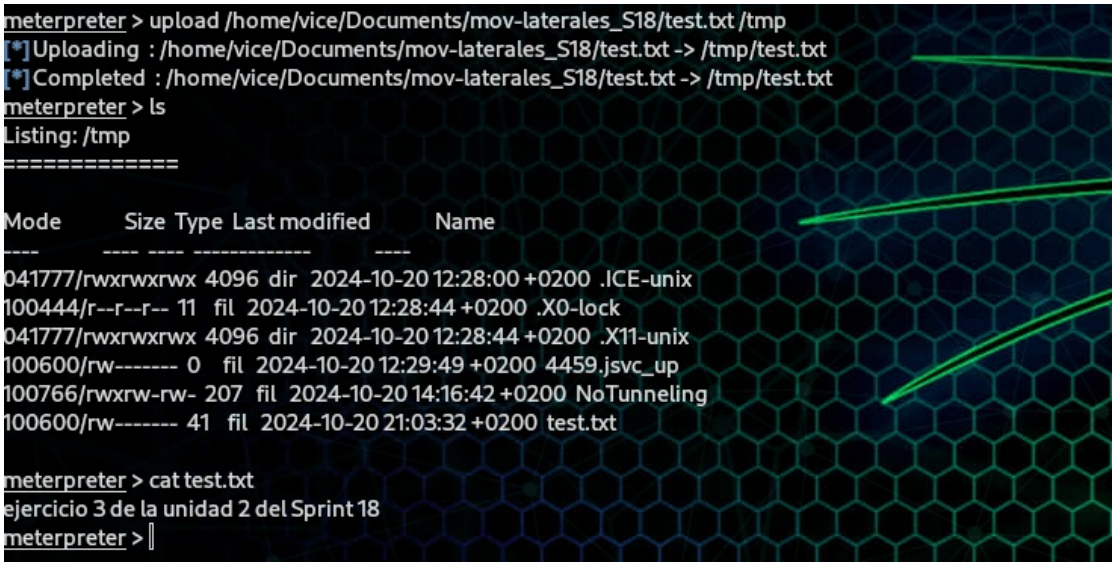


-- EJERCICIO_3.- Conseguir llevar el fichero “test.txt” desde la Kali hasta la Metasploitable 2 a través de un Meterpreter o la herramienta Chisel.

- Se ha provado con diferentes versiones de chisel para la metasploitable 2 con resultado infructuoso, debido al kernel obsoleto que tiene la citada maquina del año 2010.
- Se ha intentado establecer la conexión a través de la maquina pivoting con Chisel, pero pivoting no tiene servidor web abierto y el servicio ftp por el 21 no funciona, por lo que, no se puede transferir el archivo correspondiente de chisel, obteniendo el mismo resultado que el anterior.
- Por todo lo manifestado, se procede a usar la sesión de meterpreter que tenemos abierta con meta2, para la transferencia del archivo “test.txt” indicado en el ejercicio, con resultado positivo:



Directorio /tmp de Meta2 antes de la transferencia mediante meterpreter



Envio del archivo mediante el comando “upload” de meterpreter desde Kali a Meta2, ejecutando su contenido mediante cat en esta última máquina.