**Password guessing, funcionalidades y explotación de vulnerabilidades en sistemas**



Daniel Escaño Hernández CET Ciberseguridad

# 

# **1. Índice:**

[**1. Índice:**](#_4jq84lualx9d) **1**

[**2. Práctica 2-2**](#_ofiic1av8ddq) **2**

[**2.1 Ataque de Fuerza Bruta con fcrackzip.**](#_5d38uxjyswtl) **2**

[**2.2 Hydra, Medusa y Ncrack para Password cracking.**](#_n7d48m7xqom) **3**

[**2.3 Ataque de fuerza bruta sobre getway, correos y documentos**](#_p7kecyij5erd) **7**

[**2.4 Operaciones sobre DB**](#_pj8t73qmh6dv) **8**

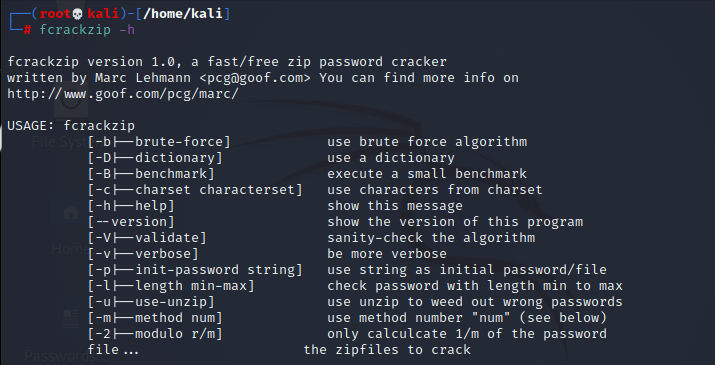
[**2.5 Módulos Auxiliares para acceder a máquinas Windows**](#_oy7ir09bwh7f) **10**

[**2.6 Explotar vulnerabilidades Client-side**](#_cf6udsowrd9h) **11**

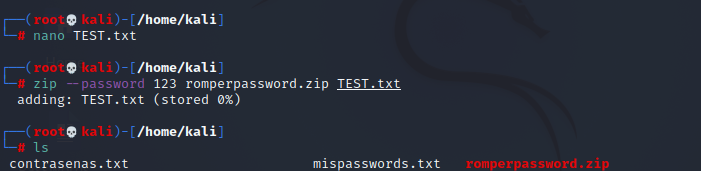
# **2. Práctica 2-2**

### **2.1 Ataque de Fuerza Bruta con fcrackzip**

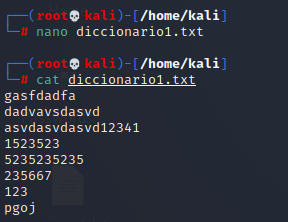
Descargamos fcrackzip y mostramos su manual de ayuda



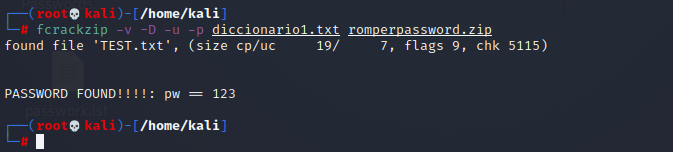
Creamos un documento y lo comprimimos utilizando una contraseña sencilla.

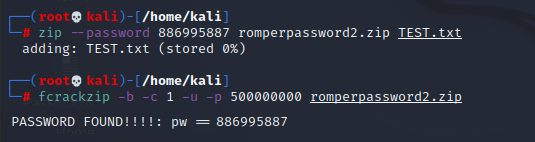


Creamos un diccionario con diferentes contraseñas, conteniendo la correcta,



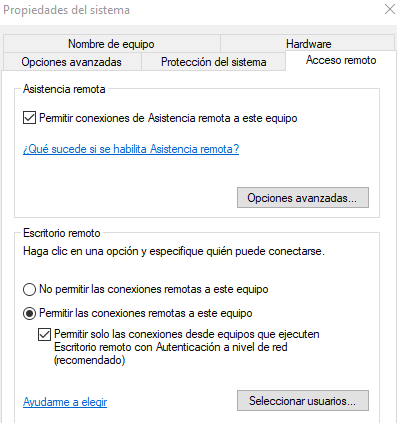
Realizamos el ataque con diccionario y otro con fuerza bruta

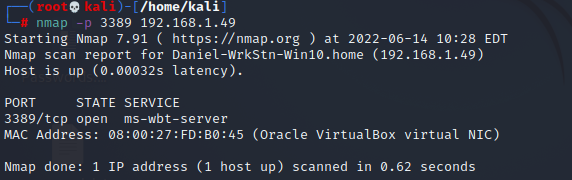


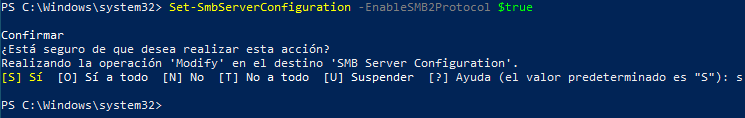


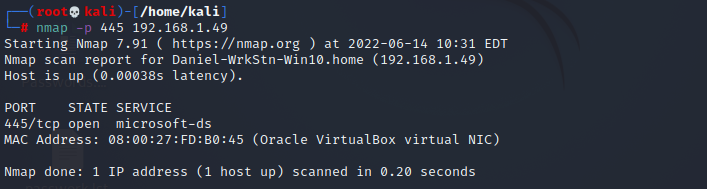
### **2.2 Hydra, Medusa y Ncrack para Password cracking**

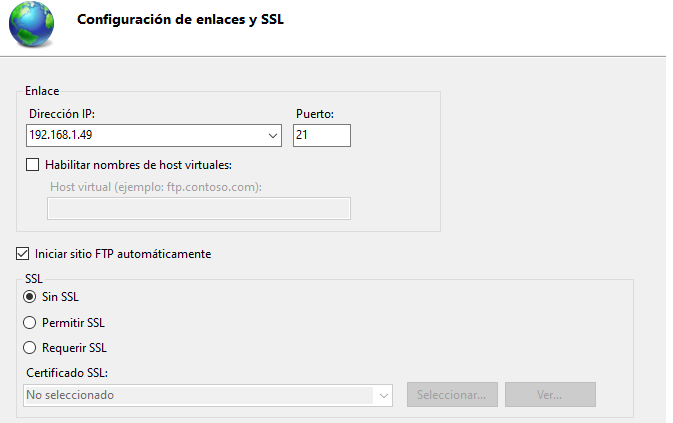
Comenzamos configurando los diferentes puertos y protocolos de Windows para realizar las pruebas, en este caso RDP, FTP y SMB. Además realizamos las comprobaciones correspondientes.

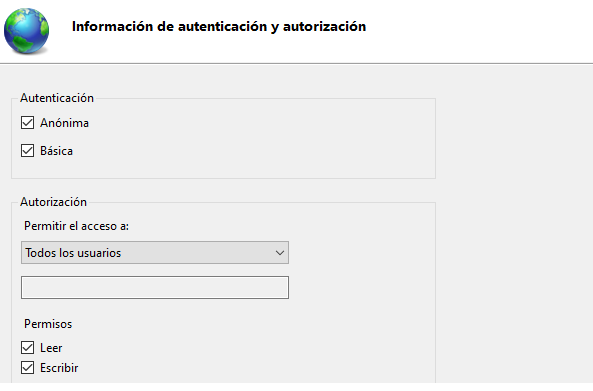


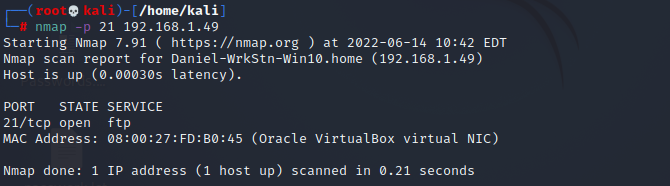




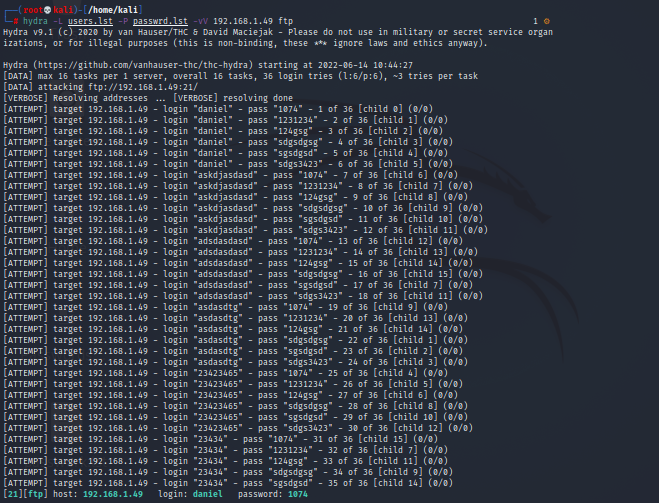


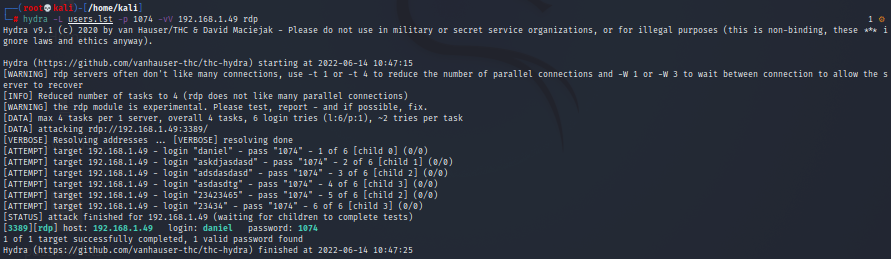




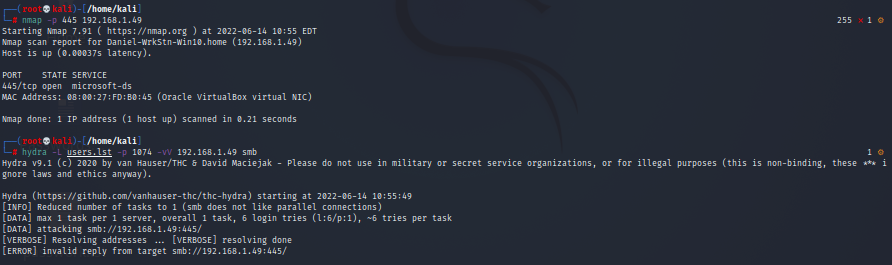


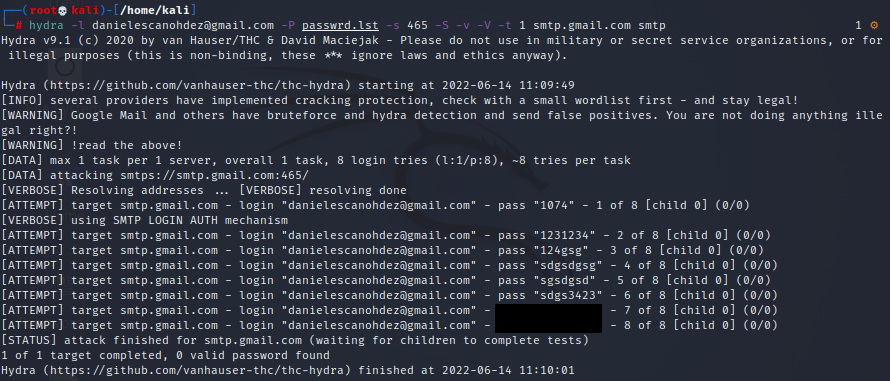
Una vez comprobado realizamos los ataques a los diferentes puertos, y también a una dirección de correo electrónico.





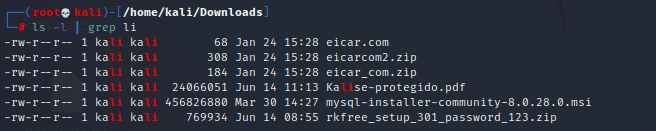
[Error en servicio smb]

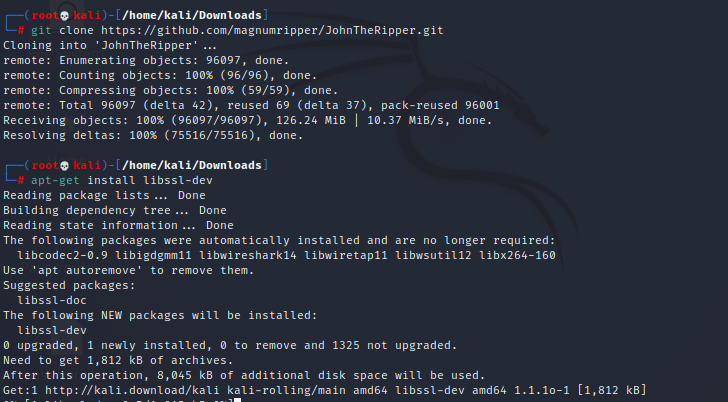




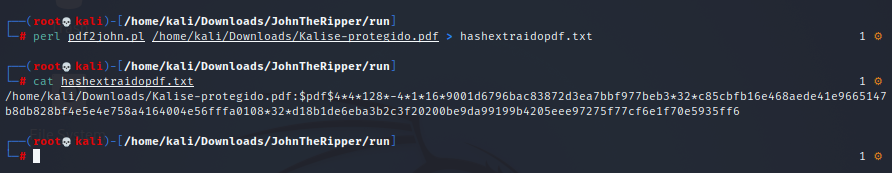
### **2.3 Ataque de fuerza bruta sobre getway, correos y documentos**

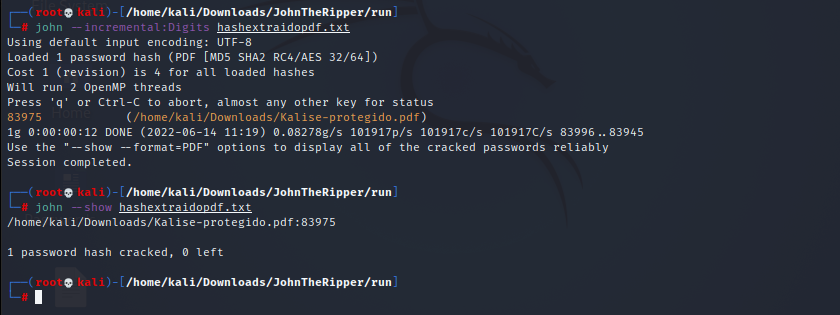
Descargamos el fichero con extensión PDF protegido por contraseña, descargamos e instalamos JohnTheRipper





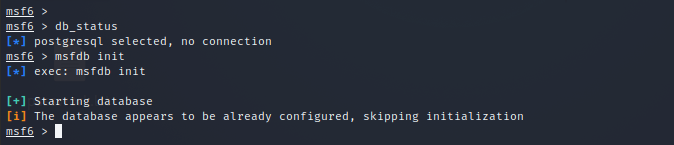
Procedemos a obtener el hash del archivo para conseguir la contraseña

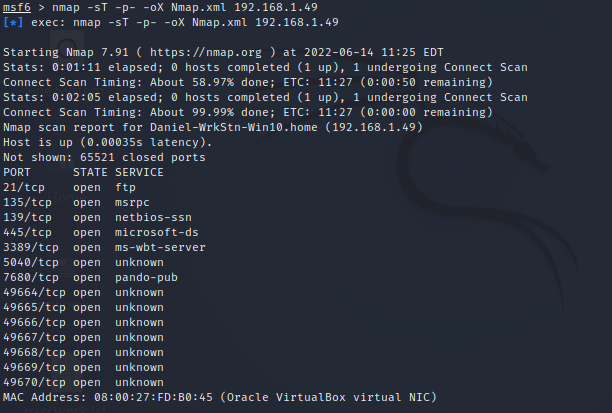


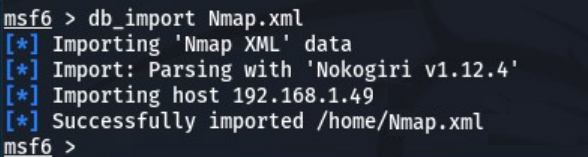


### **2.4 Operaciones sobre DB**

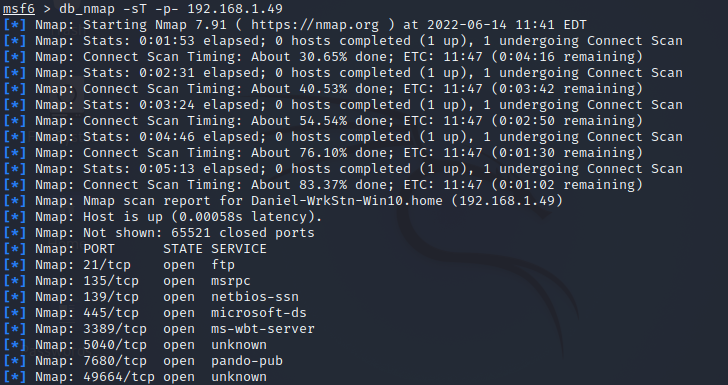
Iniciamos la base de datos, realizamos un escaneo de puertos e importamos el archivo generado.

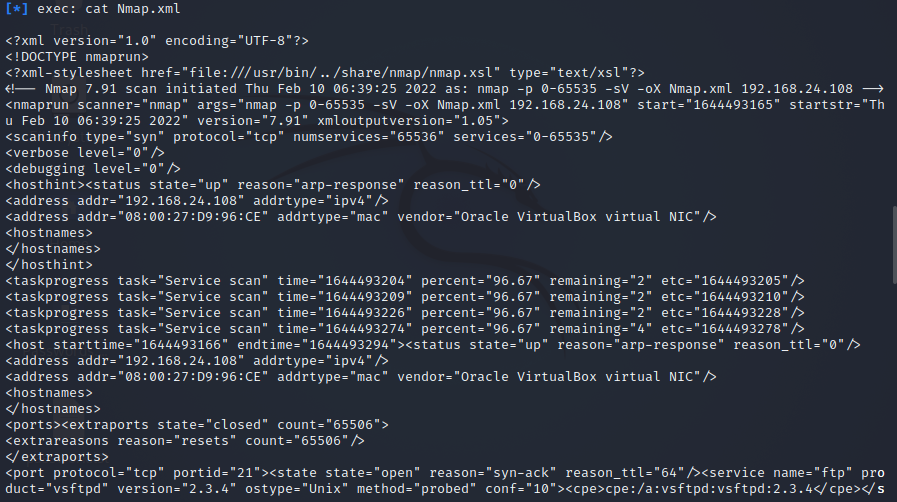






Otra forma de importar los datos es utilizar el comando db\_nmap, registramos resultados y podemos comprobarlo accediendo al archivo Nmap.xml



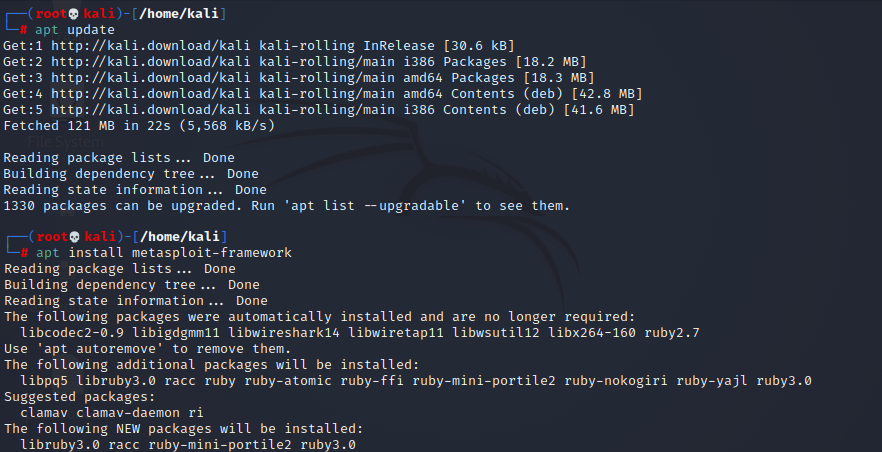


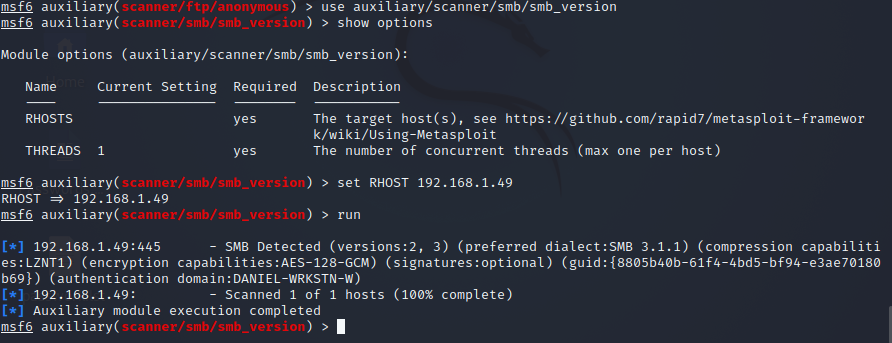
### **2.5 Módulos Auxiliares para acceder a máquinas Windows**

Descargamos e instalamos metasploit-framework

Vamos a utilizar el módulo auxiliary/scanner/smb/smb\_version con:

use auxiliary/scanner/smb/smb\_version y acceder a ver las opciones del módulo con show options... se verá que solicita el rango de direcciones que queremos analizar sobre la máquina con Windows 7 y Metasploitable

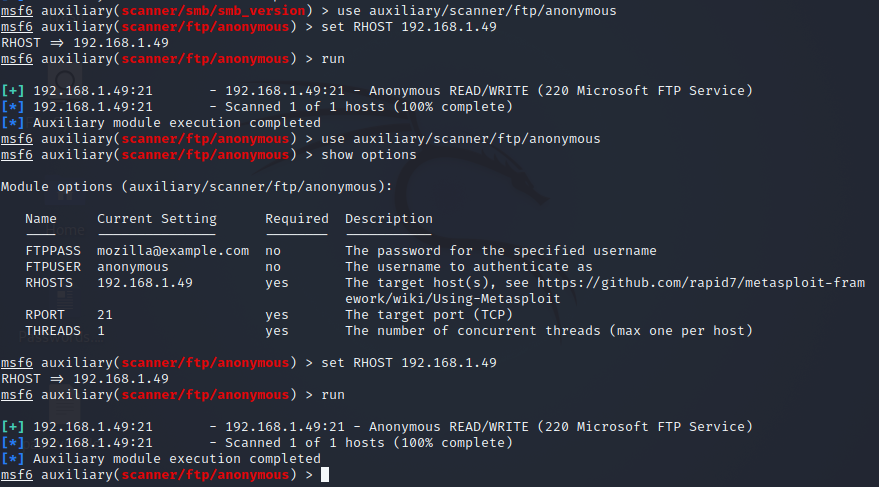




Además usamos el módulo auxiliar ftp Anonymous, para analizar los ftp anonimos con el comando siguiente:

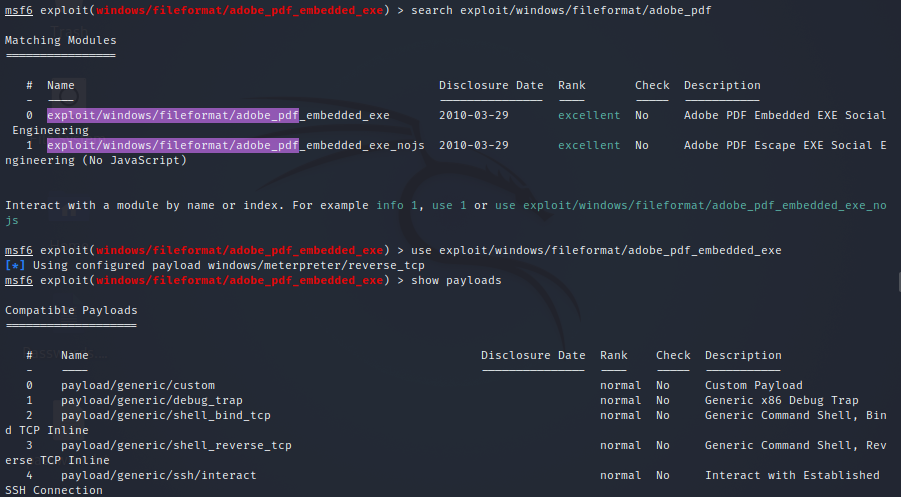
use auxiliary/scanner/ftp/Anonymous

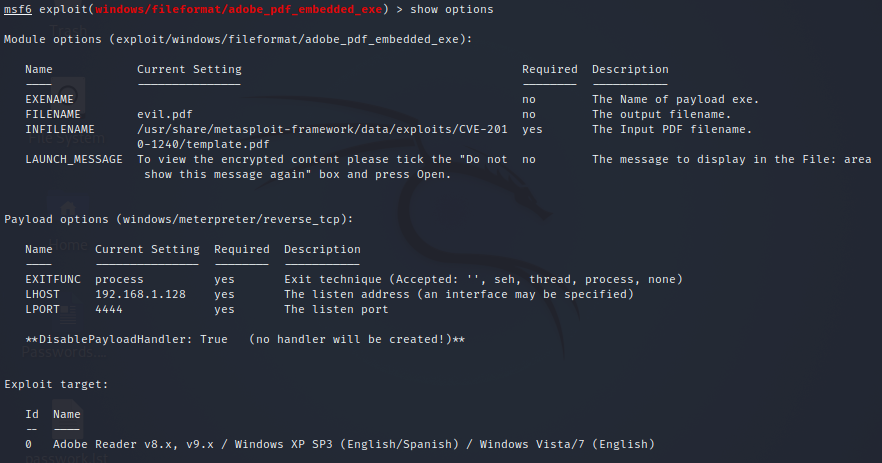
y ver las opciones del módulo con: show options



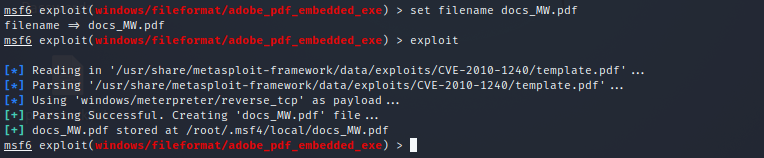
### **2.6 Explotar vulnerabilidades Client-side**

Empleamos el exploit con: use exploit/windows/fileformat/adobe\_pdf\_embedded\_exe, mostramos los payloads disponibles y escogemos windows/meterpreter/reverse\_tcp

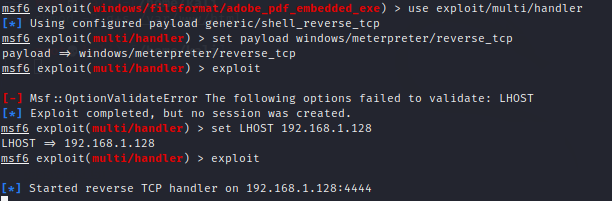




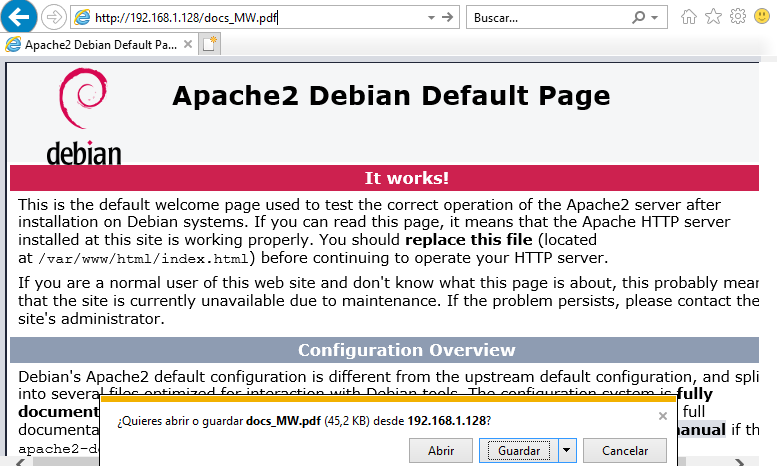
El siguiente paso es personalizar el fichero y generarlo: set FILENAME y activar el exploit luego para generarlo con run o exploit… y fijarse en la ruta donde se va a guardar el fichero.



Ahora vamos a crear un HANDLER o CONTROLADOR para gestionar la conexión inversa con el comando siguiente: use exploit/multi/handler volvemos a cargar el mismo payload set payload windows/meterpreter/reverse\_tcp



Accéder la máquina Windows y descargar el fichero .pdf malicioso y abrirlo con Adobe reader 9.3 para infectar la máquina y observar que responde el controlador remoto del exploit y atrapa la máquina del cliente



Se acepta todo lo que nos pide el adobe acrobat y elegimos abrirlo

