EJERCICIOS METASPLOIT AVANZADO

Prerequisitos

Kali Linux

Windowsploitable

Metasploitable2

Ejercicio 1 - OSINT y Metasploit

Vulnerabilidad: CVE-2017-0144 (EternalBlue)

Ficha de la vulnerabilidad:

Descripción

permite a un atacante ejecutar código remoto en sistemas vulnerables

A que software afecta

microsoft windows

Utilidad del software

es un sistema operativo ampliamente utilizado tanto en entornos personales como empresariales

Versiones del software afectadas

varias versiones de windows y windows server

Puertos que lo utilizan

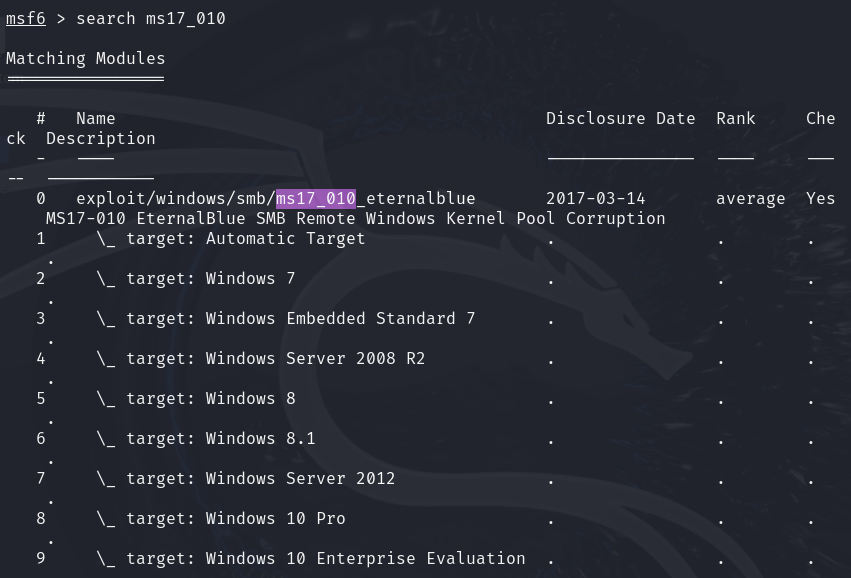
445

Módulos de metasploit relacionados

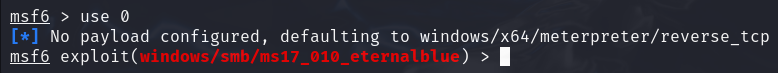
exploit/windows/smb/ms17\_010\_eternalblue

Explotar la vulnerabilidad:

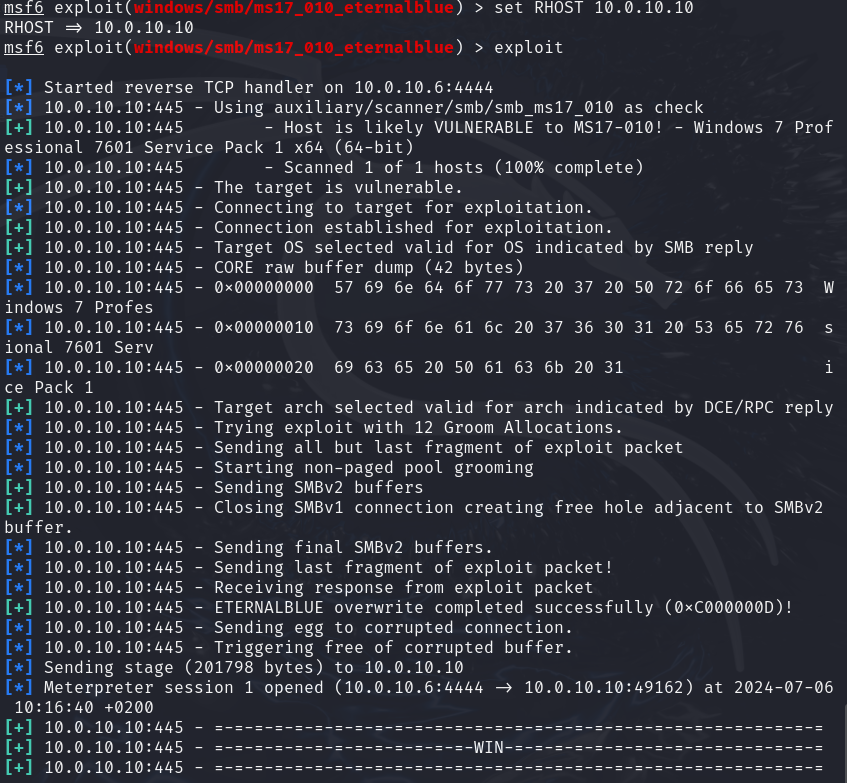
Buscar módulos de exploit en Metasploit



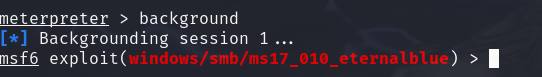
Elegir payload



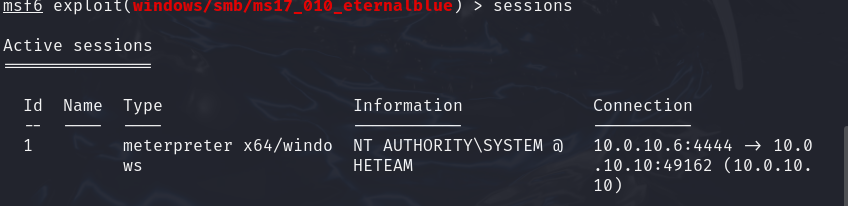
Configurar y explotar



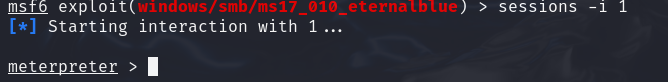
Dejar la sesión en background



Demostrar que la sesión esta en background

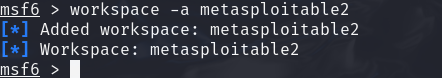


Recuperar la sesión



Ejercicio 2 - Metasploit

Crear un workspace de trabajo llamado "metasploitable2".

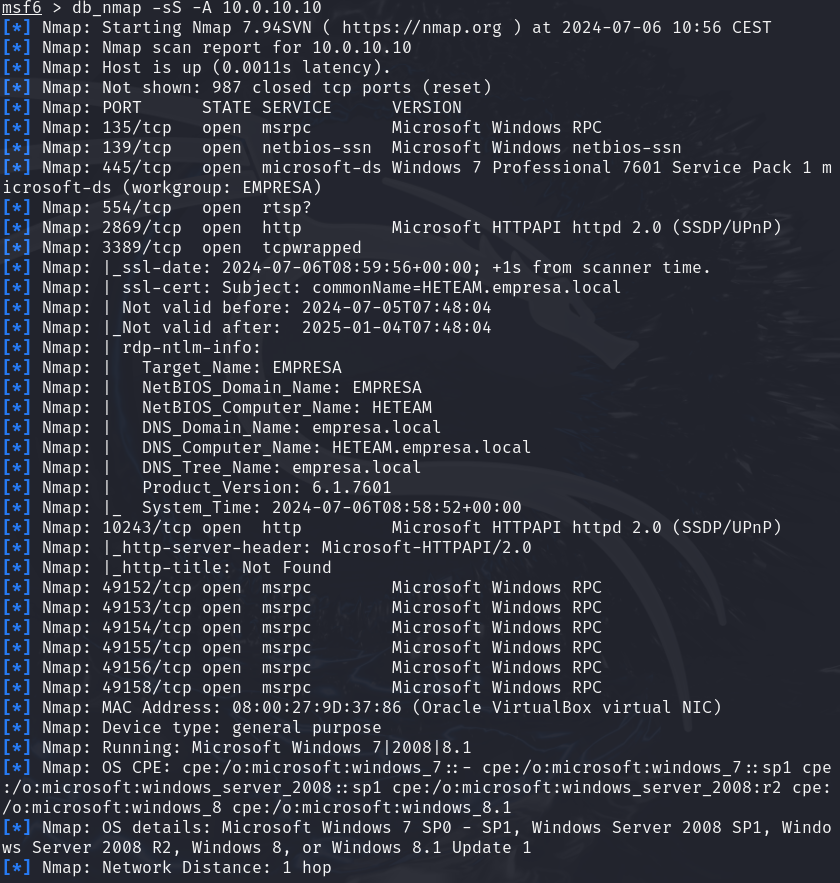


Cambiar al workspace de trabajo recién creado.

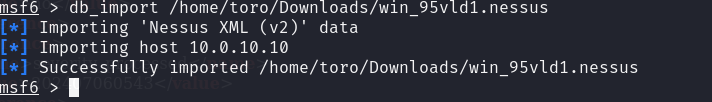


Realizar las siguientes operaciones en el workspace, comprobando las entradas en la base de datos del Workspace (comandos hosts, services, vulns, notes, creds...).

1.Realizar un escaneo de puertos contra la máquina utilizando db\_nmap.

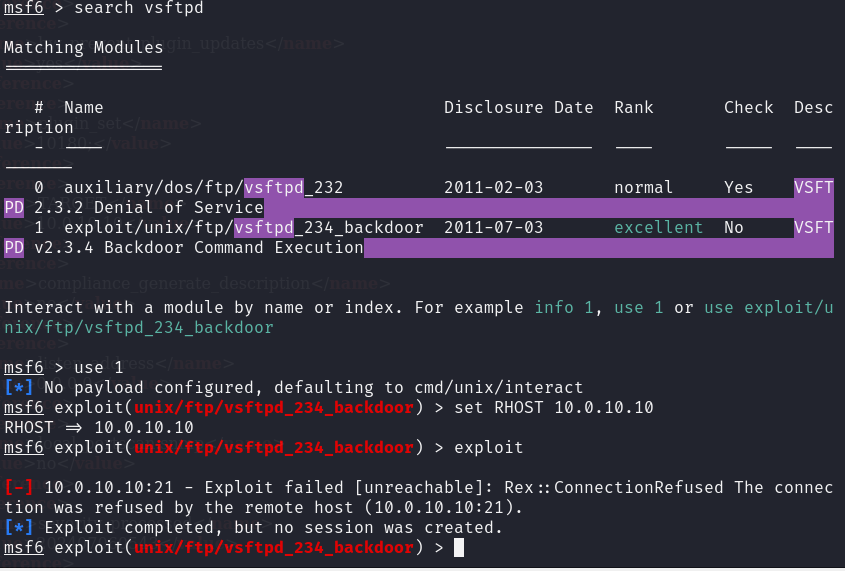


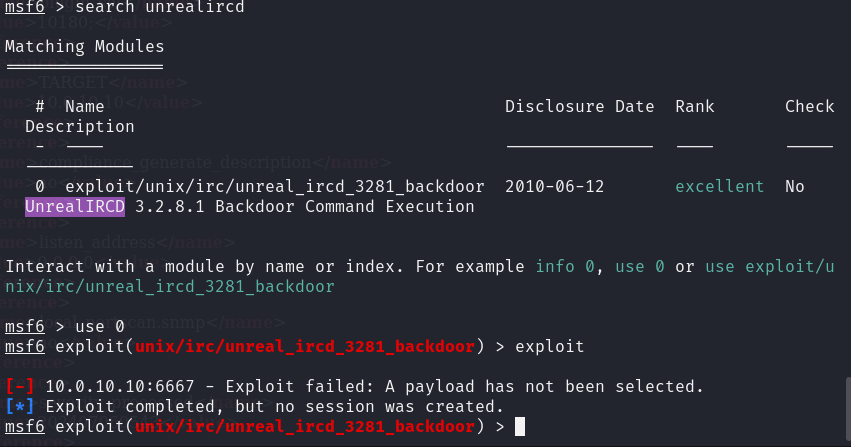
2.Importar un informe Nessus de la máquina en Metasploit.



Ejercicio 3 - Metasploit

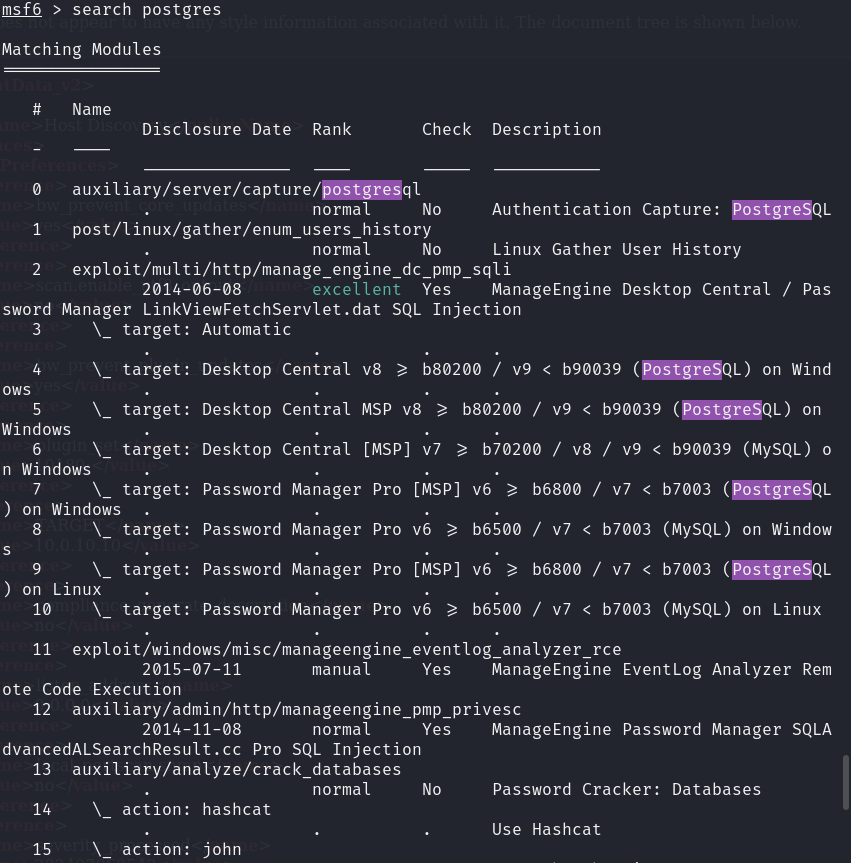
Explotar los backdoors de las versiones instaladas de Vsftpd y UnrealIRCd.

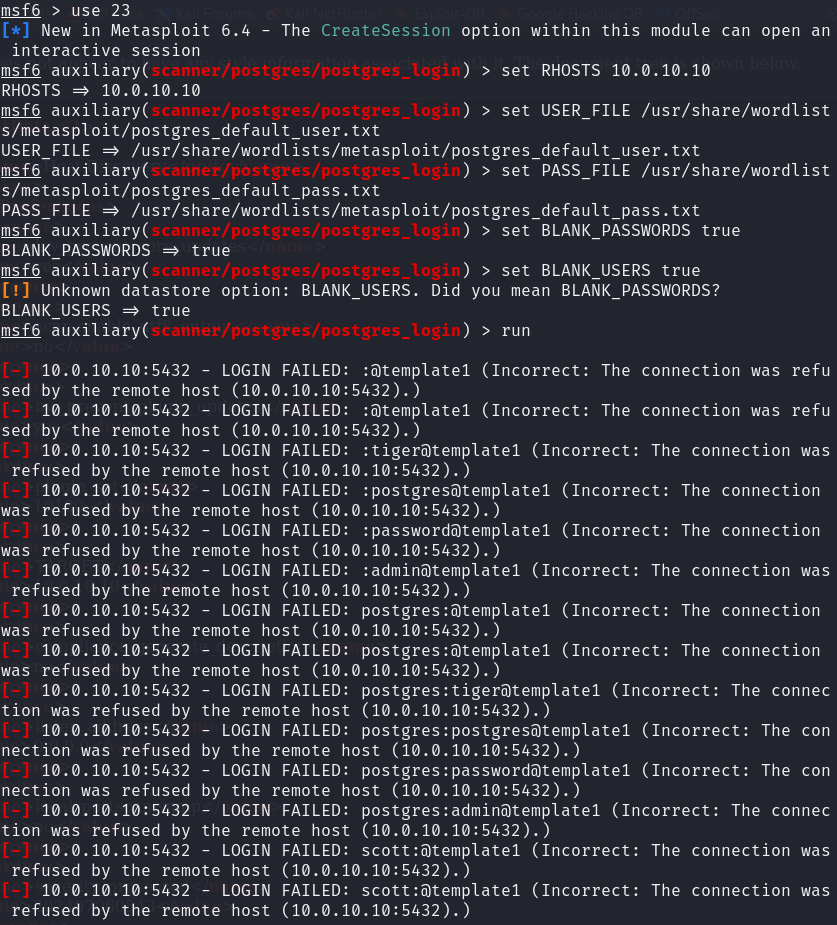


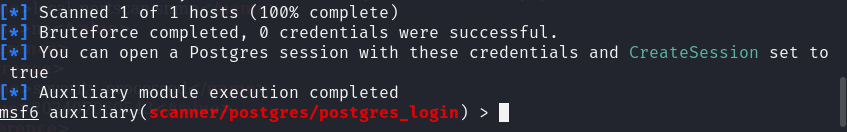


Ejercicio 4 - Metasploit

Realizar un ataque de fuerza bruta con los módulos auxiliares correspondientes para conseguir las credenciales de acceso de PostgreSQL y explotarlo para conseguir acceso a la máquina con meterpreter, ¿qué usuario tenemos?



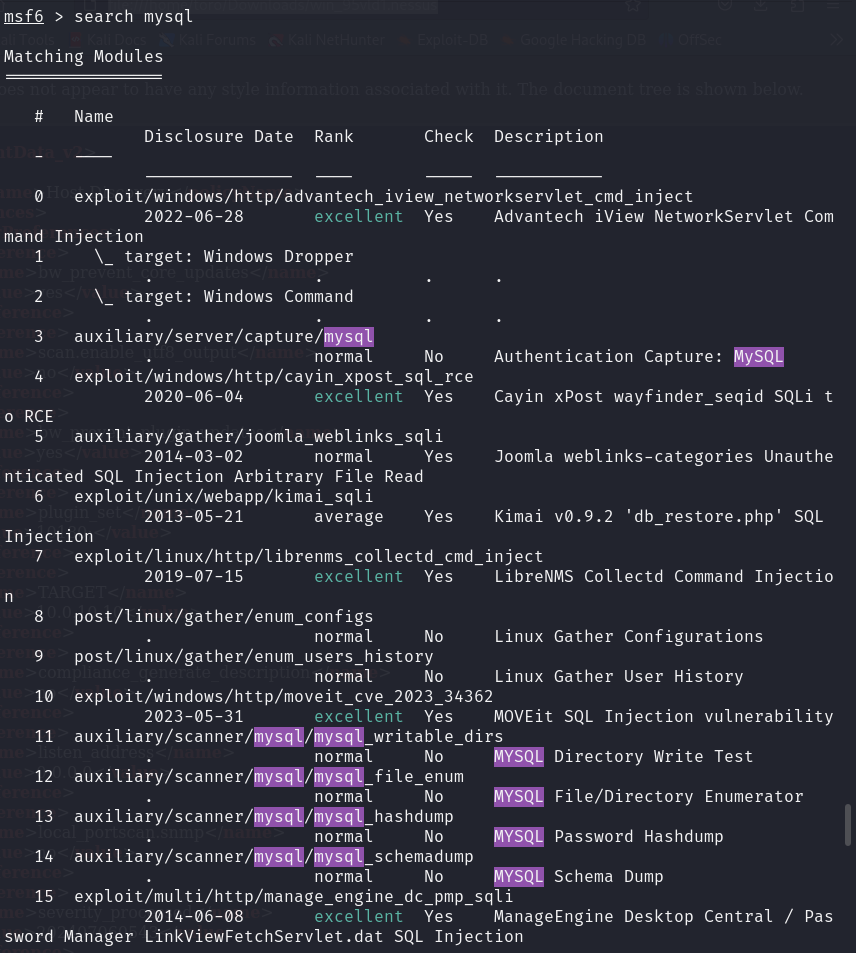


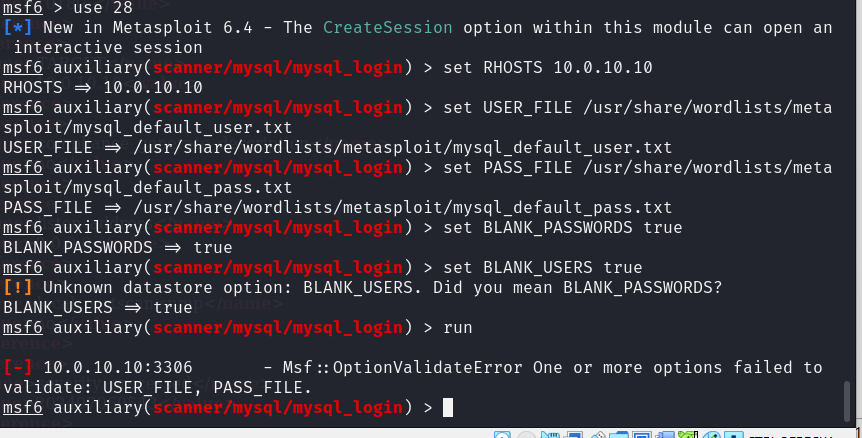


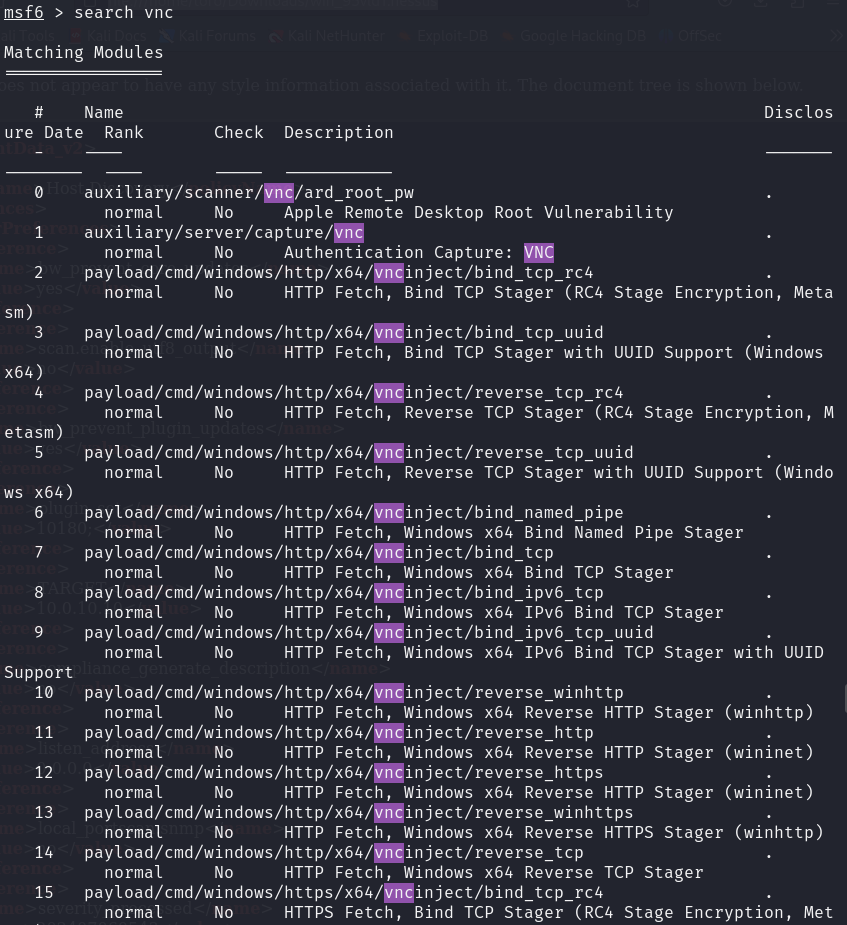
NOTA: Utilizar los diccionarios disponibles en Kali en la ruta /usr/share/wordlists/metasploit/ y tened en cuenta en las opciones que tanto usuario como contraseña pueden estar en blanco.

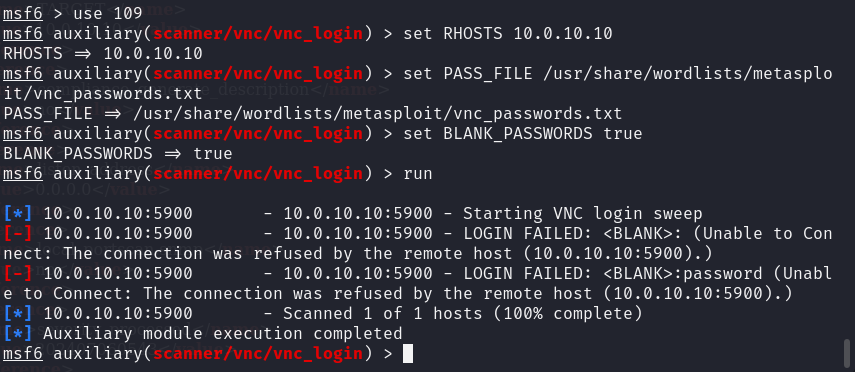
Ejercicio 5 - Metasploit

Realizar un ataque de fuerza bruta con los módulos auxiliares correspondientes para conseguir las credenciales de acceso de MySQL y VNC Server.









NOTA: Utilizar los diccionarios disponibles en Kali en la ruta /usr/share/wordlists/metasploit/ y tened en cuenta en las opciones que tanto usuario como contraseña pueden estar en blanco.