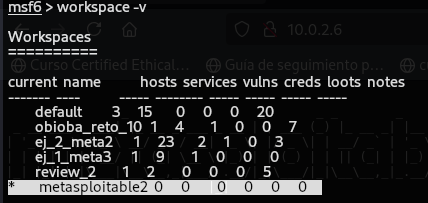


**EJERCICIO METAESPLOIT II**

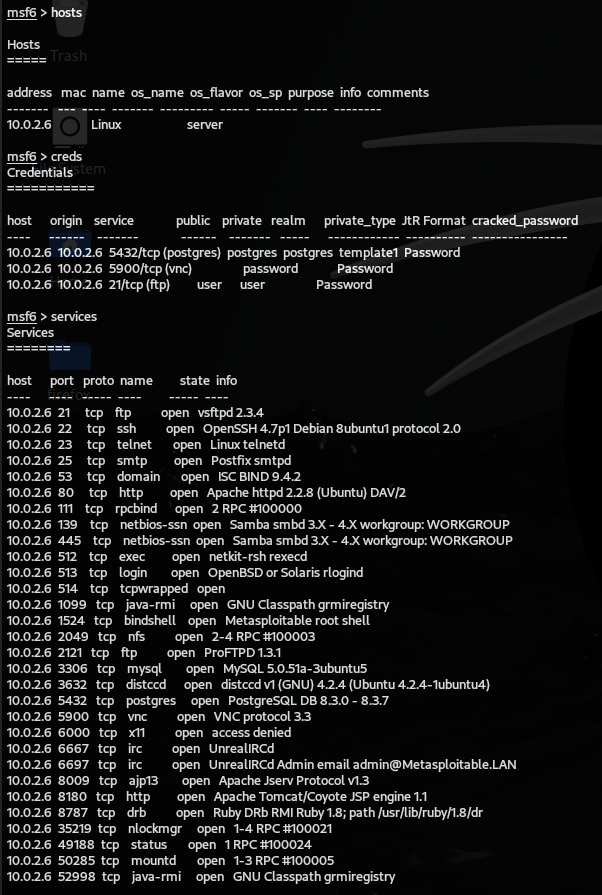
EJERCICIO 1 - METASPLOIT

1.- Crear un *workspace* de trabajo llamado *"metasploitable2"* y cambia al *workspace* de trabajo recién creado.



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

Se presenta un resumen de todo lo ejecutado (1-4) dentro del citado workspace:





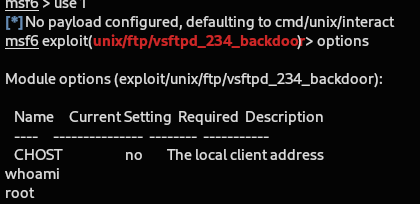
3.- Realizar un escaneo de puertos contra la máquina utilizando *db\_nmap.*



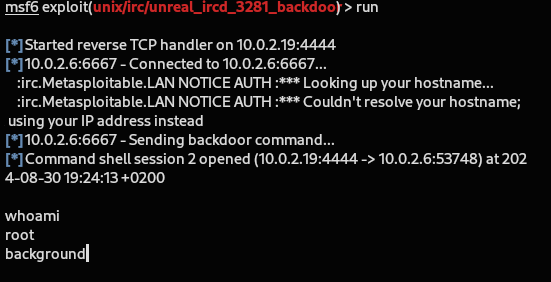
EJERCICIO 2 – METASPLOIT

1.- Explotar los *backdoors* de las versiones instaladas de *Vsftpd y UnrealIRCd.*

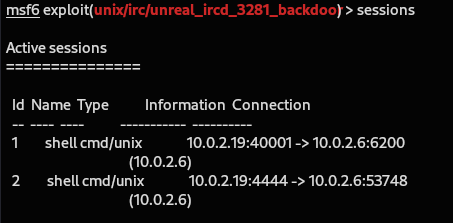
*VsFTPd*



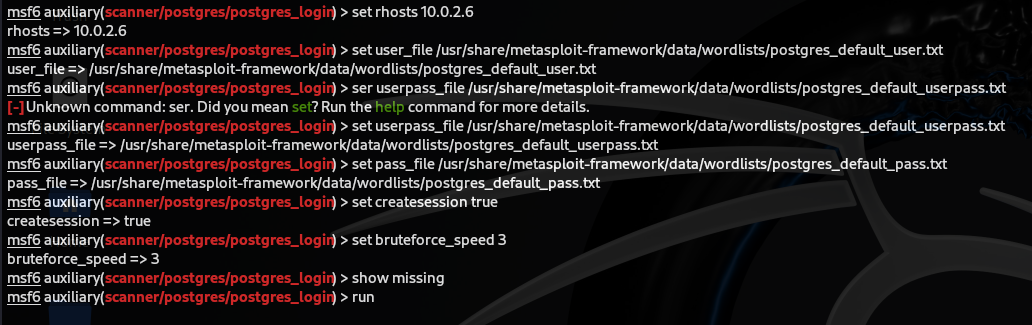
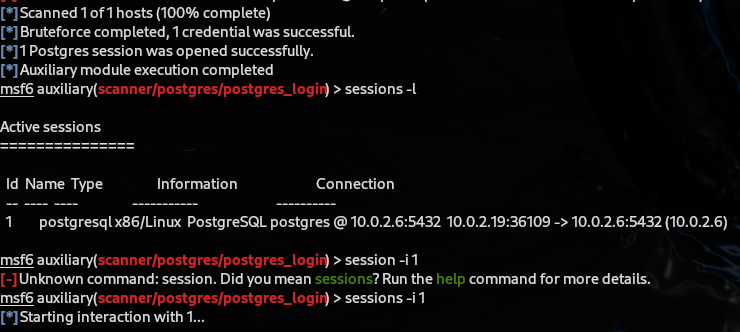
UnrealIRCd

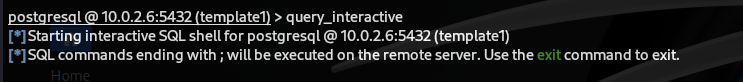
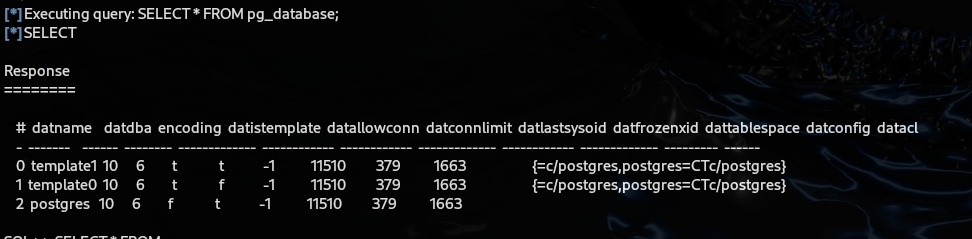


Sesiones explotadas



EJERCICIO 3 - METASPLOIT

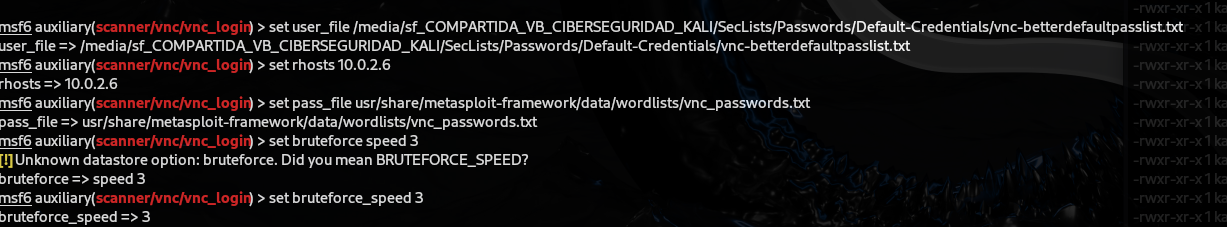
1.- Realizar un ataque de fuerza bruta con los módulos auxiliares correspondientes para conseguir las credenciales de acceso de PostgreSQL y explotarlo para conseguir acceso a la máquina.



EJERCICIO 4 - METASPLOIT

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

VNC



FTP

