Metasploit v5.0.49-dev

Este comando va a activar la base de datos de postgresql

root@computaxion:~# service postgresql start

nota: si no les carga postgresql pueden actualizar la base de datos con este comando

root@computaxion:~# msfdb reinit

Con el siguiente comando vamos a llamar a metasploit

root@computaxion:~# msfconsole

Metasploit v5.0.49-dev]

+ -- --=[1926 exploits - 1076 auxiliary - 330 post]

+ -- --=[556 payloads - 45 encoders - 10 nops]

+ -- --=[7 evasion

Con este comando verificamos que metasploit esté conectado a la base de datos de postgresql y así poder guardar los registros de los análisis realizados

msf5 > db_status

[*] Connected to msf. Connection type: postgresql.

Este comando aparte d cambiarnos el banner, nos muestra el listado de artillería que trae metasploit, más abajo les comparto el significado de cada uno de ellos.

msf5 > banner

1926 exploits

1076 auxiliary

330 post

556 payloads

45 encoders

10 nops

7 evasion

En este comando vamos a ver los host que tenemos en la base de datos.

msf5 > hosts

Hosts

=====

address mac name os_name os_flavor os_sp purpose info comments

------- --- ---- ------- --------- ----- ------- ---- --------

Como se ve en los resultados no tenemos ningún hosts en la bd.

msf5 > services

Services

========

Host port proto name state info

---- ---- ----- ---- ----- ----

Como se ve en los resultados no tenemos ningún servicio en la bd.

El siguiente comando nos muestra las credenciales que tenemos en la bd.

msf5 > creds

Credentials

===========

host origin service public private realm private_type JtR Format

---- ------ ------- ------ ------- ----- ------------ ----------

Como se ve en los resultados no tenemos ninguna credencial en la bd.

Bien ahora vamos a ver dónde podemos encontrar toda la artillería que contiene metasploit, tanto como en consola come en directorios.

Para saber dónde encontrar los diferentes módulos en consola vamos a la siguiente dirección.

root@computaxion: cd/usr/share/metasploit-framework/modules# ls

auxiliary encoders evasion exploits nops payloads post

Bien en esta ruta podemos encontrar todos los módulos de metasploit

exploit: un exploit es un conjunto de datos o secuencia de comandos que se utiliza para aprovecharse de una vulnerabilidad o una brecha de seguridad, en un sistema de cómputo, el objetivo del mismo es conseguir un comportamiento no deseado en la victima, obtener un acceso no autorizado y tomar el control del mismo. Los exploit se pueden convertir en diferentes tipos de software por ejemplo en un script, virus o gusano.