**UNIVERSIDAD DON BOSCO**



**MANUAL SPP**

**Exploit EternalBlue.**

**INTEGRANTES:**

Manuel Alejandro Argueta Moreno AM180476

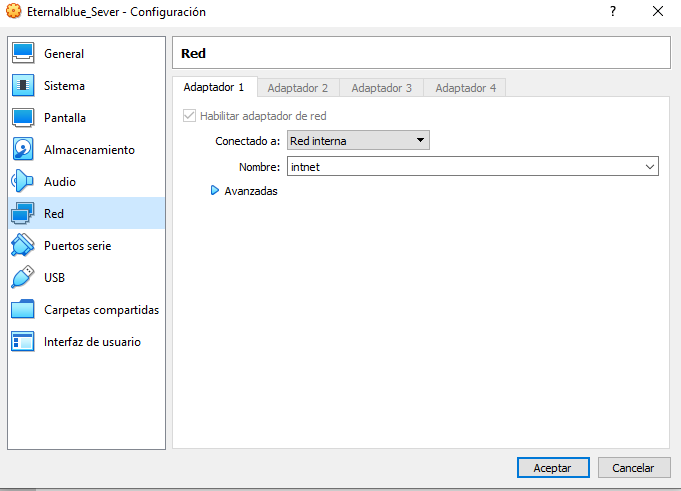
|  |  |
| --- | --- |
| Rodrigo Jesús Francia Quezada | FQ180616 |
| Alexis Rodrigo Molina Ruano | MR180477 |
| Elías Joel Munguía Vides | MV182041 |
| Edwin Antonio Rauda Vela | RV181969 |

# Preparación general de nuestras virtuales

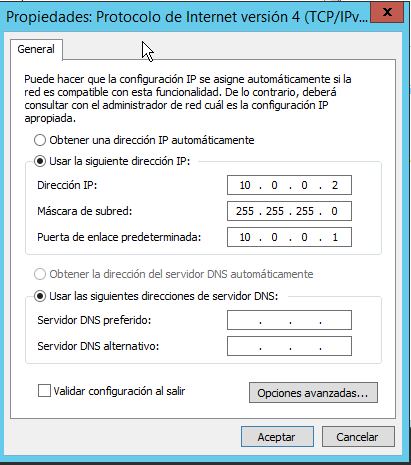
* Procedemos con la Instalación de Windows server 2012 y Kali Linux



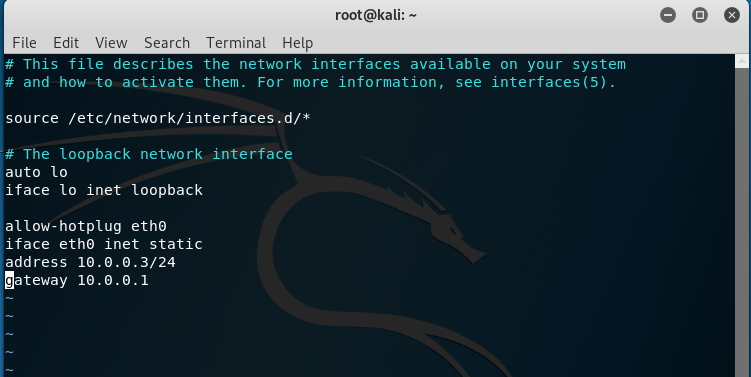
* Se configuran los adaptadores de red a red interna.
* En el caso de kali Linux se habiltan 2 uno de red interna y uno de adaptador puente.



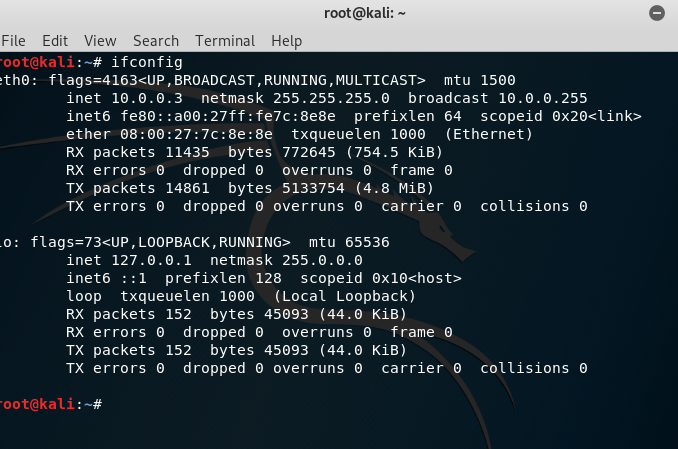
* Configuramos la ip de nuestro servidor (protocolo ipv4).

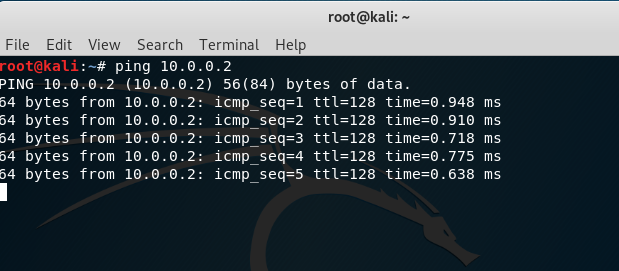


* Configuramos ip estática para kali Linux.



* Verificamos que la ip estática fue configurada correctamente.

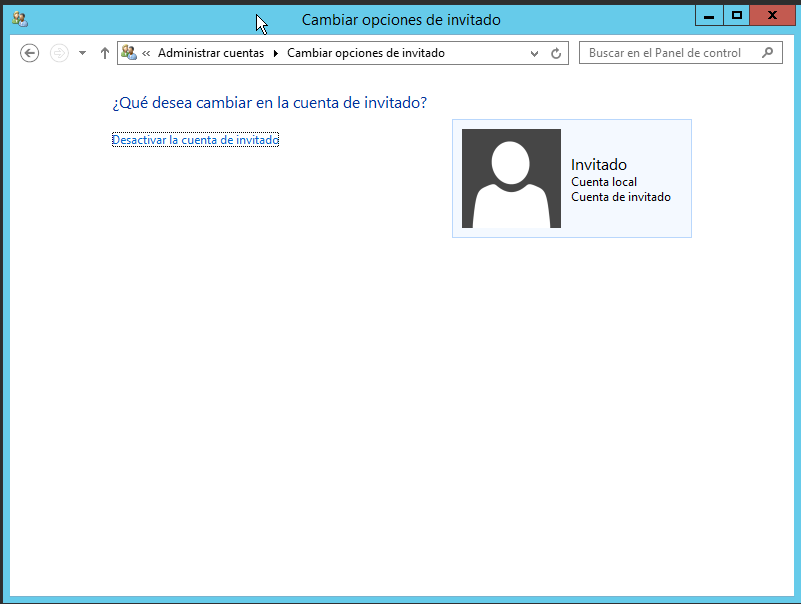


* Se hacen pruebas de comunicación entre Server y Kali Linux

# Preparación de entornos

preparación Windows server

* Habilitando usuario Invitado con fines de pruebas se habilito este usuario sin embargo no se usa en ningún momento ya que obtenemos la contraseña por medio de fuerza bruta.

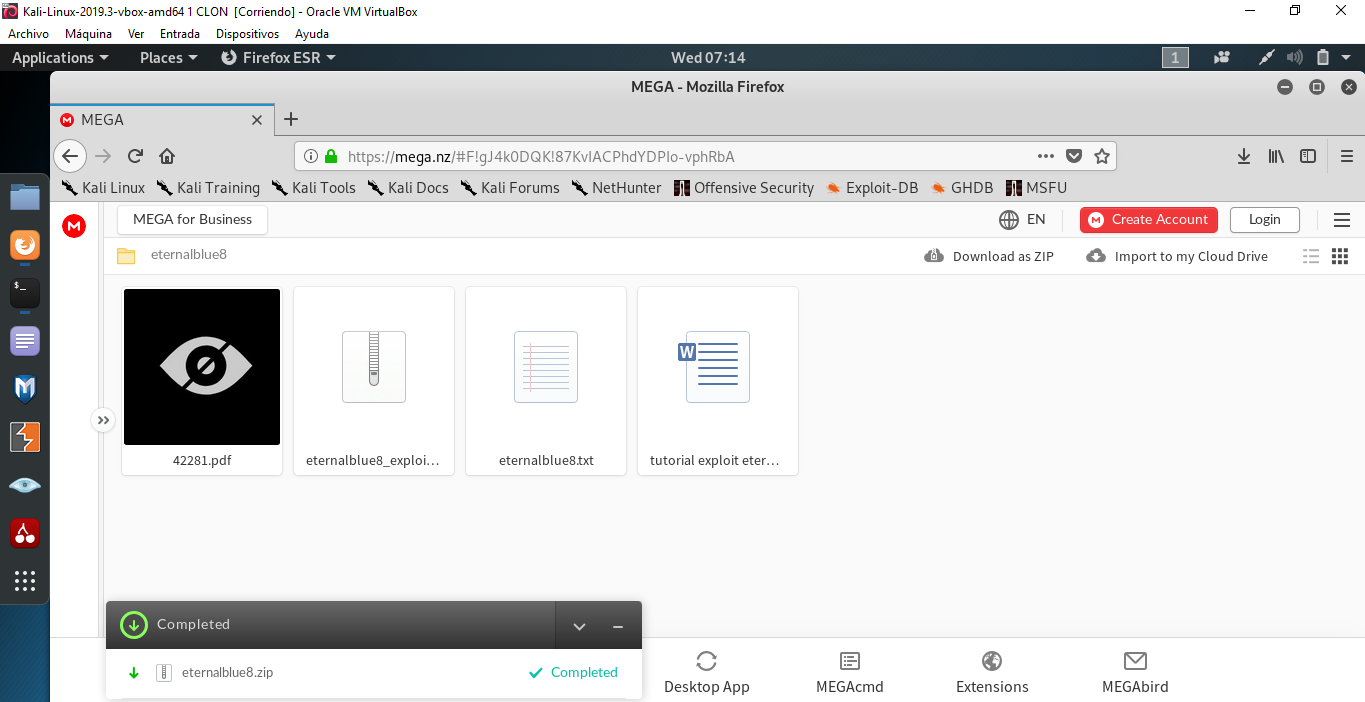


* Se desactiva el Firewall.

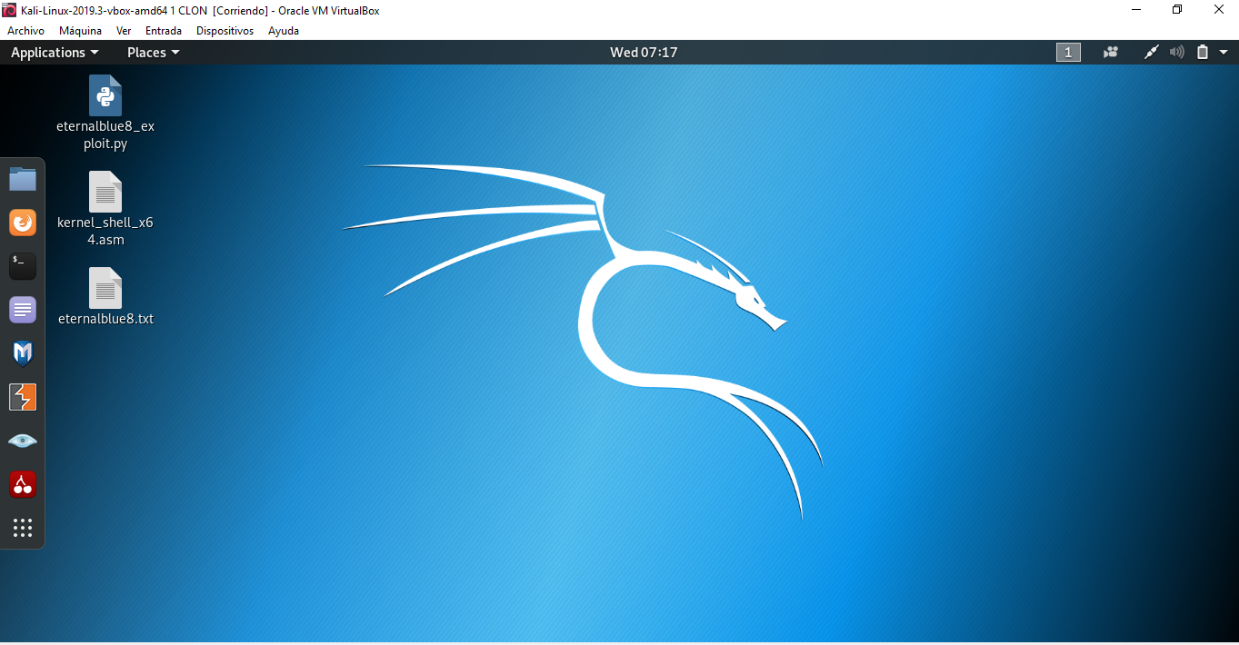


preparación kali Linux

* Se descargan los paquetes de EternalBlue Sleepya que se usaran para para poder hacer el ataque.

.

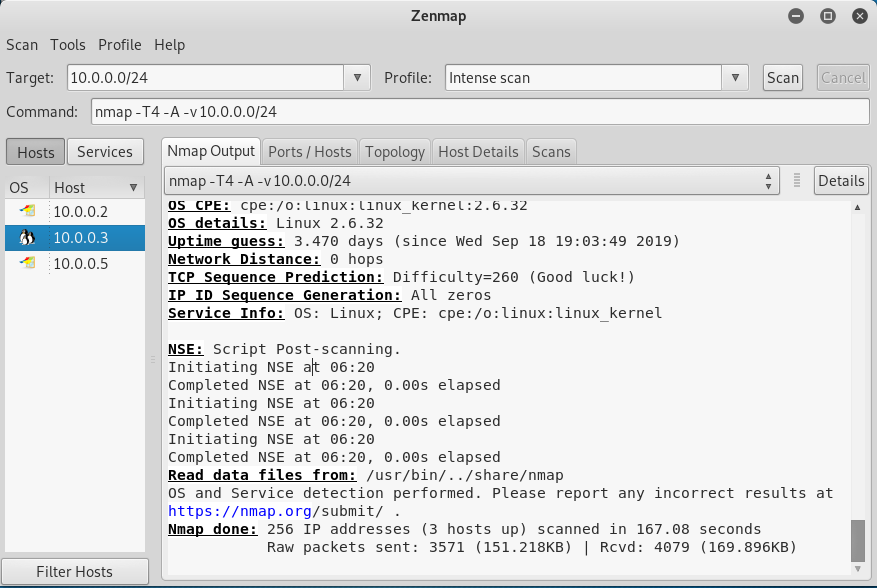
* Extraemos los archivos y copiamos los archivos al escritorio que es donde estaremos trabajando el ataque.

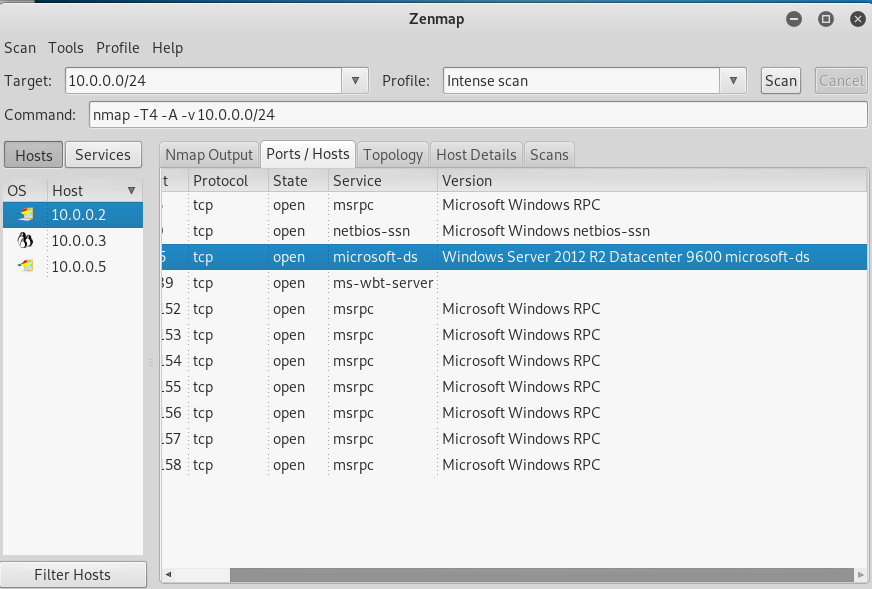


# Inicialización de ataque

escaneo de red para ver vulnerabilidades

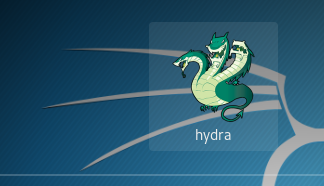
* Se realiza un escaneo de red con Zenmap para ver si podemos realizar nuestro ataque.



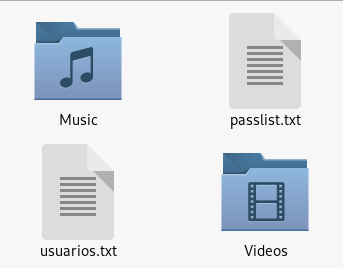
* Se analizan todas las ips que encuentran y verificamos por medio la información del escaneo quien es el servidor de todas las ips y se verifican los puertos en especial el puerto 445 que es por donde haremos nuestro ataque.

obtener contraseña administrador por fuerza bruta

* Iniciamos la herramienta Hydra que nos ayudara a hacer nuestro ataque de fuerza bruta.



* Procedemos a crear nuestra lista de usuarios y nuestro diccionario de contraseñas que ocupara nuestro ataque de fuerza bruta.

****

* Procedemos a ejecutar nuestro ataque de fuerza bruta.

-t 1 – número de tareas en paralelo. Por defecto 16.

-V – verbose, muestra usuario y contraseña usados en cada intento.

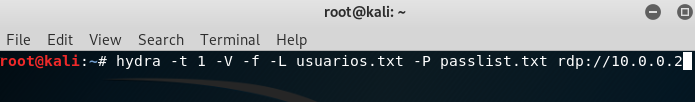
-f – finalizar proceso al encontrar el primer usuario y password válidos.

-L usuarios.txt – archivo que contiene los nombres de usuario a probar. Un nombre por línea.

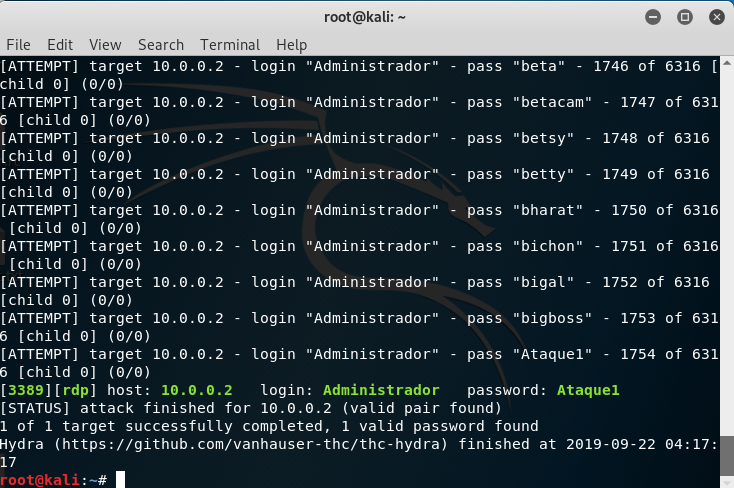
-P passlist.txt – archivo que contiene los passwords a probar. Un password por línea.

rdp:// - le decimos que vamos a atacar un RDP.

10.0.0.2– IP del objetivo.

****

* Ver resultados de nuestro ataque de fuerza bruta.

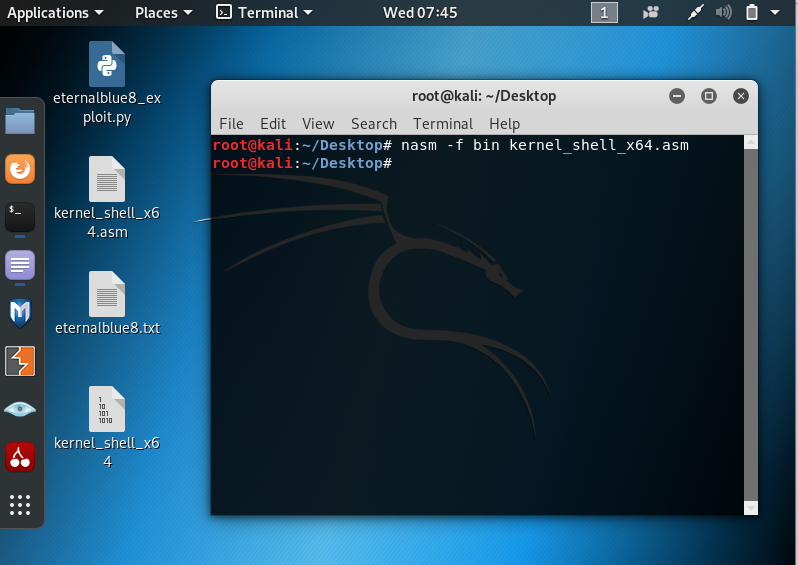


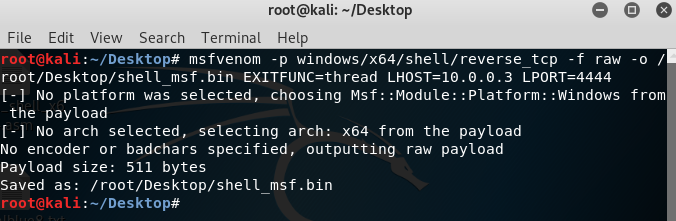
inicio de ataque

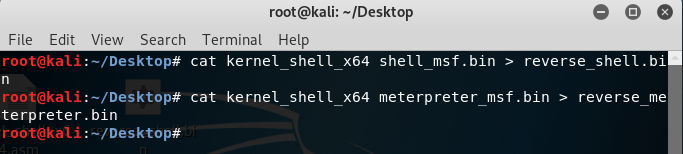
* Ingresamos a la ruta donde tenemos todos nuestros archivos para el ataque.



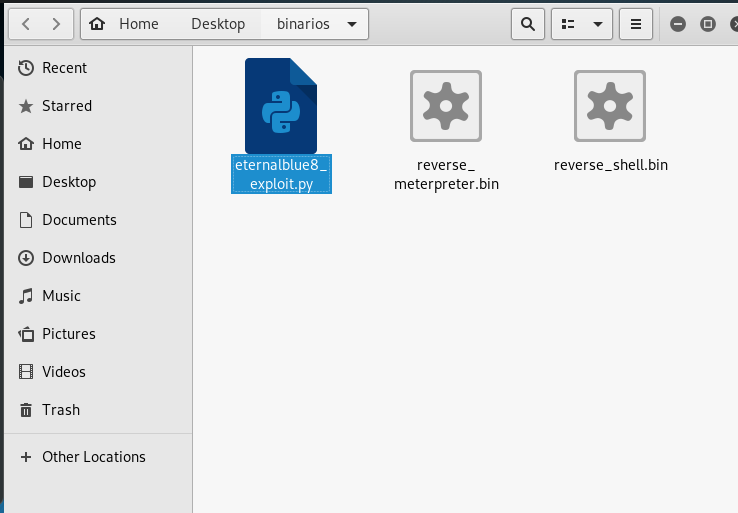
* Lo primero que deberemos hacer es ensamblar el Kernel Shellcode que creo Sleepya.



* Se crea nuestro Userland Shellcode es un archivo binario el cual contendrá nuestro payload.
* Lo siguiente que deberemos hacer es concatenar el payload con el kernel\_shell\_x64, de esta manera generaremos nuevos binarios, los cuales utilizaremos en la última etapa.



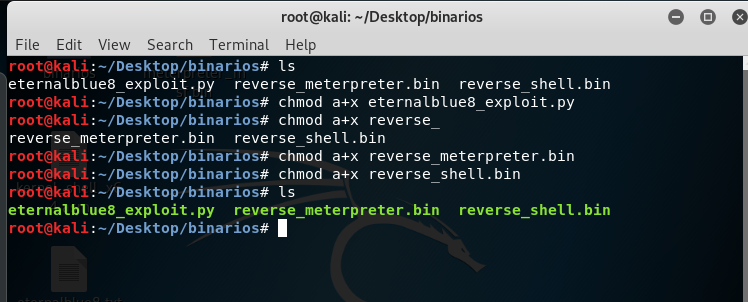
* Creamos una carpeta llamada binarios en la cual vamos a copiar los archivos meterpreter.bin y reverse\_shell.bin y nuestro eternalblue8 que será el ejecutable para nuestro ataque.



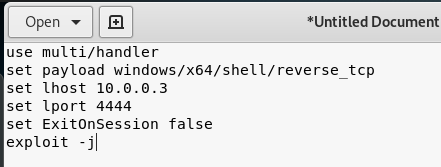
* Se edita el archivo eternalblue8.py donde lo que haremos es agregar nuestro usuario de autenticación en el server en este caso es el Administrador con su respectiva contraseña.



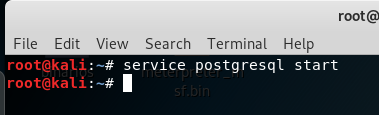
* Accedemos a la carpeta binarios y procedemos a darle los permisos necesarios.

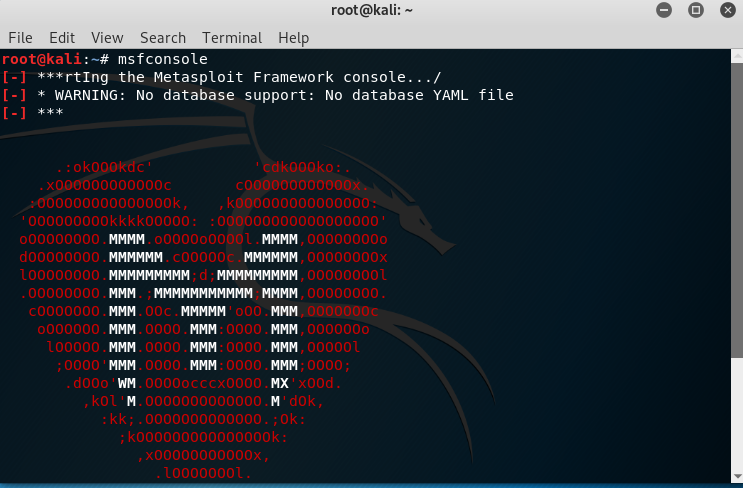


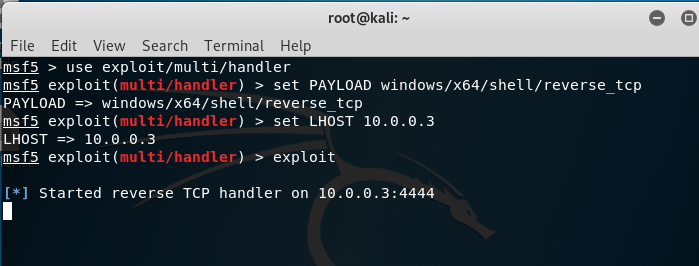
* Lo siguiente es crear nuestro archivo handler.rc que es el que se encargara de nuestra escucha.



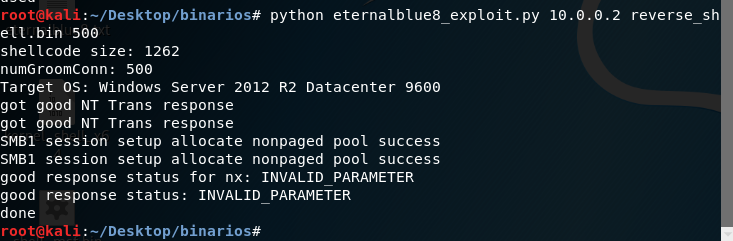
* Se procede a abrir 2 terminales en la primera inicializaremos el servicio Postgresql.



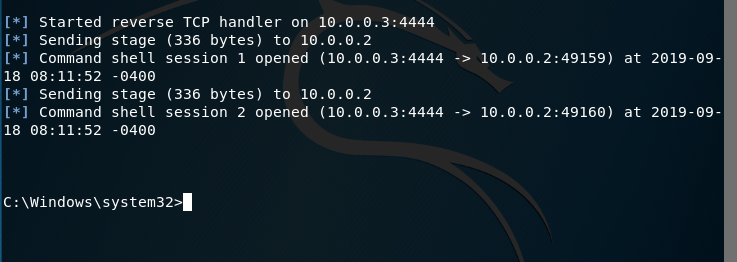
* En la segunda consola ejecutamos msconsole para cargar nuestro Payloads
* Procedemos a setear nuestro escucha y ejecutamos nuestro exploit.



* En la primer terminal donde iniciamos postgresql procemos a lanzar el ataque con el exploit.py y el binario que contendrá el payload de la shell reversa o bien el de la sesión de meterpreter.

 El parámetro con valor “500” corresponde al “numGroomConn”. El ajustar la cantidad de conexiones “Groom” ayuda a alcanzar un pool de memoria contigua en el kernel para que la sobreescritura del buffer termine en la ubicación que deseamos y lograr ejecutar la shellcode correctamente.

* Una vez ejecutado todo podremos tener el control del server.



pruebas adentro del server

* Este punto se desarrollará el día de la defensa.
* Conectar a rdp rdesktop 10.0.0.2
* Crear keylogger java -jar sAINT.jar

<https://learn-hackbase.blogspot.com/2017/12/como-crear-un-spyware-para-robar-la.html>