

Partiamo utilizzando nmap per fare una scansione dei servizi attivi con tanto di versioni del nostro target

```
(kali@kali)~$ nmap -sV 192.168.1.144
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 08:18 EST
Nmap scan report for 192.168.1.144
Host is up (0.0023s 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=1/23%Time=65AFBCA1%P=x86_64-pc-linux-gnu%r(NUL
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 64.59 seconds
```

una volta individuato il servizio al quale andremo ad applicare l’exploit, in questo caso telnet, possiamo ad utilizzare metasploit per trovare tutti gli exploit presenti in quel servizio

```
Matching Modules
--
#  Name                                     Disclosure Date  Rank  Check  Descripti
on
--  --
0  auxiliary/scanner/telnet/lantronix_telnet_version  normal  No  Lantronix
Telnet Service Banner Detection
1  auxiliary/scanner/telnet/telnet_version           normal  No  Telnet Se
rvice Banner Detection
```

scelto l’exploit che andremo ad applicare possiamo alla configurazione, impostando i dati necessari come l’IP del target

```

Name      Current Setting  Required  Description
--
PASSWORD  PASSWORD         no        The password for the specified username
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)
THREADS   THREADS          yes       The number of concurrent threads (max one per host)
TIMEOUT   TIMEOUT          yes       Timeout for the Telnet probe
USERNAME  USERNAME         no        The username to authenticate as

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

msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.144
rhosts => 192.168.1.144
```

per concludere diamo il via a l'exploit il quale come possiamo vedere ci dà con successo le credenziali di accesso (msfadmin/msfadmin)

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.1.144:23 - 192.168.1.144:23 TELNET
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login:
[*] 192.168.1.144:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```