

Hacking con Metasploitable verso Telnet

Cambiamo l'indirizzo di Metasploitable tramite il comando "sudo nano /etc/network/interfaces" e impostiamo così il file.

```
auto eth0
iface eth0 inet static
address 192.168.1.40
netmask 255.255.255.0
gateway 192.168.1.1
dns-nameservers 8.8.8.8 8.8.4.4
```

Per riavviare scheda rete da terminale eseguire "sudo systemctl restart networking", se non funziona riavviare la macchina virtuale.

stessa procedura su kali:

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.25 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 2001:b07:646a:e2c6:a00:27ff:fe0a:d9c6 prefixlen 64 scopeid 0<global>
    inet6 fe80::a00:27ff:fe0a:d9c6 prefixlen 64 scopeid 0<link>
    ether 08:00:27:0a:d9:c6 txqueuelen 1000 (Ethernet)
    RX packets 7144 bytes 519684 (507.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1410 bytes 117723 (114.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Avviamo nmap -sV IP_TARGET e vi mostrerà tutte le porte aperte.

```
(kali@kali)-[~]
└─$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-12 09:13 EST
Nmap scan report for 192.168.1.149
Host is up (0.0016s 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        netkit-rsh rexecd
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 https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.32 seconds

(kali@kali)-[~]
└─$ msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple authentication-capturing and poisoning services
```

Avviamo msfconsole per entrare nei comandi che si agganceranno al target.

Cerchiamo con “search nome_del_protocollo_vulnerabile”
avviamo con “use Numero_o_path”

```
msf6 > search telnet_version

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
--  --                                     -
0  auxiliary/scanner/telnet/lantronix_telnet_version .          normal No  Lantronix Telnet Service Banner Detection
1  auxiliary/scanner/telnet/telnet_version .          normal No  Telnet Service Banner Detection

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_version

msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

Name      Current Setting  Required  Description
--      -
PASSWORD  no              no       The password for the specified username
RHOSTS    yes            yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     23             yes       The target port (TCP)
THREADS   1              yes       The number of concurrent threads (max one per host)
TIMEOUT   30             yes       Timeout for the Telnet probe
USERNAME  no              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 192.168.1.149
rhosts => 192.168.1.149
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

Name      Current Setting  Required  Description
--      -
PASSWORD  no              no       The password for the specified username
RHOSTS    192.168.1.149   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     23             yes       The target port (TCP)
THREADS   1              yes       The number of concurrent threads (max one per host)
TIMEOUT   30             yes       Timeout for the Telnet probe
USERNAME  no              no       The username to authenticate as
```

set rhosts IP_TARGET per impostare la connessione

e infine “run” per confermare l’exploit e “ifconfig” per controllare di essere entrati.

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

[*] 192.168.1.149:23 - 192.168.1.149:23 TELNET
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
[*] 192.168.1.149:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.9 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 2001:b07:646a:e2c6:a00:27ff:fe0a:d9c6 prefixlen 64 scopeid 0<global>
    inet6 fe80::a00:27ff:fe0a:d9c6 prefixlen 64 scopeid 0<20<link>
    ether 08:00:27:0a:d9:c6 txqueuelen 1000 (Ethernet)
    RX packets 6992 bytes 509806 (497.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1401 bytes 116957 (114.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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