

## Pratica S7L2

Per prima cosa andiamo a scansionare il sistema Meta alla ricerca di vulnerabilità:

```
(luca@kali)~$ nmap -sV 192.168.1.149
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-06 14:43 CET
Nmap scan report for 192.168.1.149
Host is up (0.0048s 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         OpenBSD or Solaris rlogind
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 12.04 seconds
```

In questo caso il nostro obiettivo è il servizio telnet, in ascolto sulla porta 23. Avviamo quindi il framework metasploit alla ricerca di exploit per questo protocollo. Nell'esercizio andremo ad usare il modulo ausiliario, non necessitante di payload, al percorso **auxiliary/scanner/telnet/telnet\_version**. Utilizzo il comando `use auxiliary/scanner/telnet/telnet_version` per avviarlo. Utilizzo quindi **show options** per controllare se tutti i parametri necessari per l'esecuzione del modulo sono presenti:

```
root@kali: /home/luca
File Actions Edit View Help

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

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

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



| Name     | Current Setting | Required | Description                                                                                                                                                                                       |
|----------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PASSWORD |                 | no       | The password for the specified username                                                                                                                                                           |
| RHOSTS   |                 | yes      | The target host(s), see <a href="http://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">http://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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       | The username to authenticate as                                                                                                                                                                   |



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

Noto che manca la configurazione del parametro rhosts, in quanto gli altri parametri richiesti (colonna yes) hanno già un valore di default configurato. Imposto quindi tale parametro attraverso il comando **set rhosts 192.168.1.149** andando ad inserire come ip quello della macchina Metasploitable su cui stiamo lanciando l'attacco:

```
Warning: Never expose this VM to an untrusted network!\nContact: msfdev[at]metasploit.com\nLogin with msfadmin/msfadmin to get started\nmetasploitable login:\n[*] 192.168.1.149:23 - Scanned 1 of 1 hosts (100% complete)\n[*] Auxiliary module execution completed\nmsf6 auxiliary(scanner/telnet/telnet_version) >
```

L'exploit ha avuto successo, come possiamo vedere abbiamo recuperato login/password per il servizio telnet che in questo caso corrispondono a **msfadmin/msfadmin** come da figura sopra. Vado quindi a testare le credenziali provando una connessione su telnet:

```
root@kali: /home/luca\nFile Actions Edit View Help\nWarning: Never expose this VM to an untrusted network!\nContact: msfdev[at]metasploit.com\nLogin with msfadmin/msfadmin to get started\n\nmetasploitable login: msfadmin\nPassword:\nLast login: Tue Nov 7 03:25:09 EST 2023 on tty1\nLinux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686\n\nThe programs included with the Ubuntu system are free software;\nthe exact distribution terms for each program are described in the\nindividual files in /usr/share/doc/*/copyright.\n\nUbuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by\napplicable law.\n\nTo access official Ubuntu documentation, please visit:\nhttp://help.ubuntu.com/\nNo mail.\nmsfadmin@metasploitable:~$ ifconfig\neth0      Link encap:Ethernet  HWaddr 08:00:27:72:f6:3c\n          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0\n          inet6 addr: 2001:b07:aac:7465:a00:27ff:fe72:f63c/64 Scope:Global\n          inet6 addr: fe80::a00:27ff:fe72:f63c/64 Scope:Link\n          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1\n          RX packets:9437 errors:0 dropped:0 overruns:0 frame:0\n          TX packets:266 errors:0 dropped:0 overruns:0 carrier:0\n          collisions:0 txqueuelen:1000\n          RX bytes:635515 (620.6 KB)  TX bytes:29035 (28.3 KB)
```

L'obiettivo è stato raggiunto, e come dimostrato dal comando ifconfig ci troviamo sull'host 192.168.1.149, ossia quello che volevamo attaccare