
EPICODE
Exploit Telnet con Metasploit

Traccia:

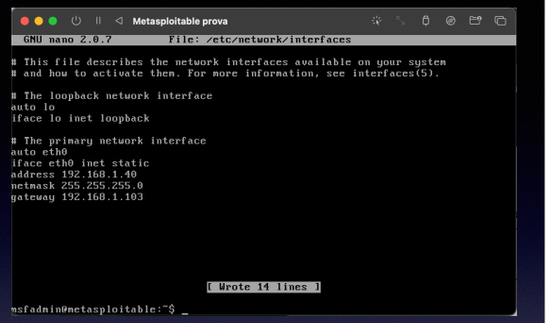
Sulla base dell'esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

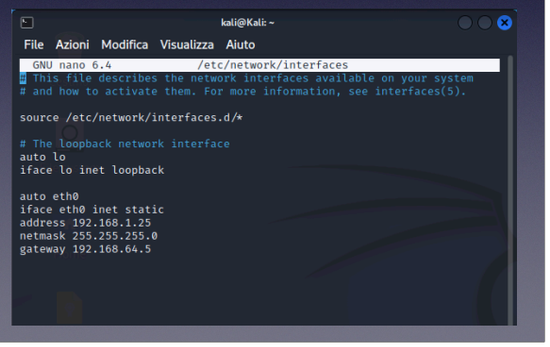
Requisito: Seguire gli step visti in lezione teorica. Prima, configurate l'ip della vostra Kali con 192.168.1.25 e l'ip della vostra Metasploitable con 192.168.1.40

Per prima cosa sono andato a configurare le due macchine con i seguenti indirizzi IP:

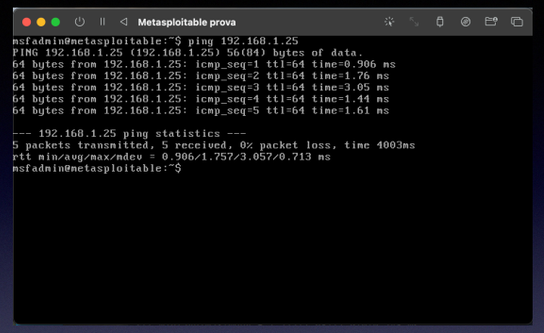
-Metasploitable 192.168.1.40

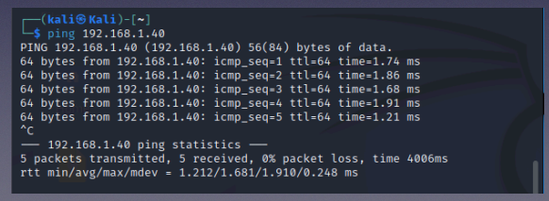
-Kali Linux 192.168.1.25





Poi mi sono assicurato che ci sia connessione fra entrambe le macchine per poter effettuare una scansione porte con nmap.

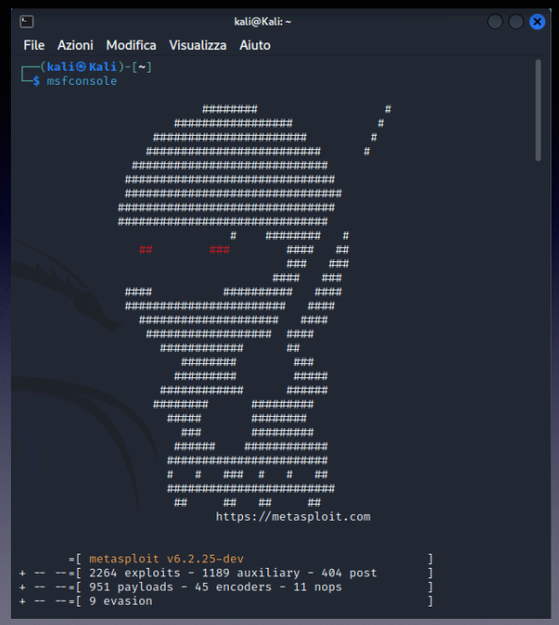




Connesse entrambe le macchine ho effettuato la scansione con comando:
“nmap -sV 192.168.1.40”,
ed ho ottenuto questo risultato.
In particolare la porta che a noi interessa ed andremo ad analizzare oggi è la 23 (telnet).

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.40
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-06 13:22 CET
Nmap scan report for 192.168.1.40
Host is up (0.0019s latency).
Not shown: 976 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?
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?
513/tcp   open  login?
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  unknown
32770/tcp open  status      1 (RPC #100024)
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 190.67 seconds
```

Nel frattempo sono andato ad avviare Metasploit Frame Work con comando: “msfconsole”



Una volta all'interno del programma sono andato a cercare col comando "search" il servizio telnet, ottenendo diversi risultati.

In particolare a noi interessa il servizio 35 (auxiliary/scanner/telnet/telnet_version) il quale lo andremo ad azionare con comando:
"use 35"

```
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 Ex
ecution
   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/ios_telnet_rocem
  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 Unauthenti
cated 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 Remo
te Command Execution
   9   exploit/unix/webapp/dogfood_spell_exec
  2009-03-03       excellent  Yes    Dogfood CRM spell.php Remote Comman
d Execution
   10  exploit/freebsd/telnet/telnet_encrypt_keyid
  2011-12-23       great      No     FreeBSD Telnet Service Encryption K
ey ID Buffer Overflow
   11  exploit/windows/telnet/gamsoft_telsrv_username
  2000-07-17       average    Yes    GAMSoft TelSrv 1.5 Username Buffer
Overflow
```

```
   35  auxiliary/scanner/telnet/telnet_version
                    normal     No     Telnet Service Banner Detection
```

```
msf6 > use 35
```

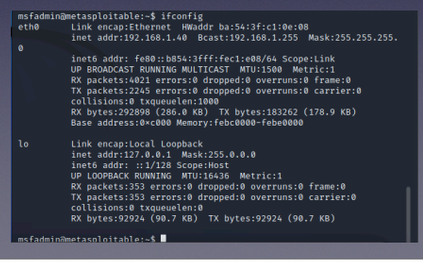
Fatto ciò sono andato ad impostare l'indirizzo della macchina che ho intenzione di attaccare, e non essendo necessario impostare alcun payload ho effettuato direttamente l'exploit.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.40
rhosts ⇒ 192.168.1.40
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    192.168.1.40     yes       The target host(s), see https:
                                        //github.com/rapid7/metasploit
                                        -framework/wiki/Using-Metasplo
                                        it
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threa
                                        ds (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate a
                                        s
```

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

[+] 192.168.1.40:23       - 192.168.1.40:23 TELNET _                  _
    _ _       _     _        ____    \x0a _ __ ___   ___| |_ __ _ ___ _ _
_ | | ___ (_) |_ __ _| |__ | | ___|____ \ \x0a| '_ ` _ \ / _ \ __/ _` / _
_| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_
| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\
__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\x0a
                |_|                                          \x0a\x0a\x0
aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact:
msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get star
ted\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Andato a buon fine l’exploit, non ci resta altro che avviare la macchina dal nostro programma con comando:
“telnet 192.168.1.40”

Dopo averci chiesto i dati per il login, ed aver fornito “msfadmin” sia per admin che per password, possiamo costare di essere all’interno della macchina con il comando:
“ifconfig”




EPICODE
GRAZIE
Epicode