

Week 7 Lesson 2

- 1. Introduzione**
- 2. Configurazione e Connettività**
- 3. Analisi del Servizio Telnet su Metasploitable**
- 4. Accesso a Metasploit ricerca ed Utilizzo del Modulo Telnet**
- 5. Recupero delle Credenziali Telnet**
- 6. Accesso Effettivo a Metasploitable tramite Telnet**
- 7. Conclusioni**

Traccia dell'Esercizio

Sulla base dell'esercizio visto in lezione teorica, l'obiettivo era utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable. Il requisito preliminare consisteva nel configurare l'IP della Kali con 192.168.1.25 e l'IP di Metasploitable con 192.168.1.40.

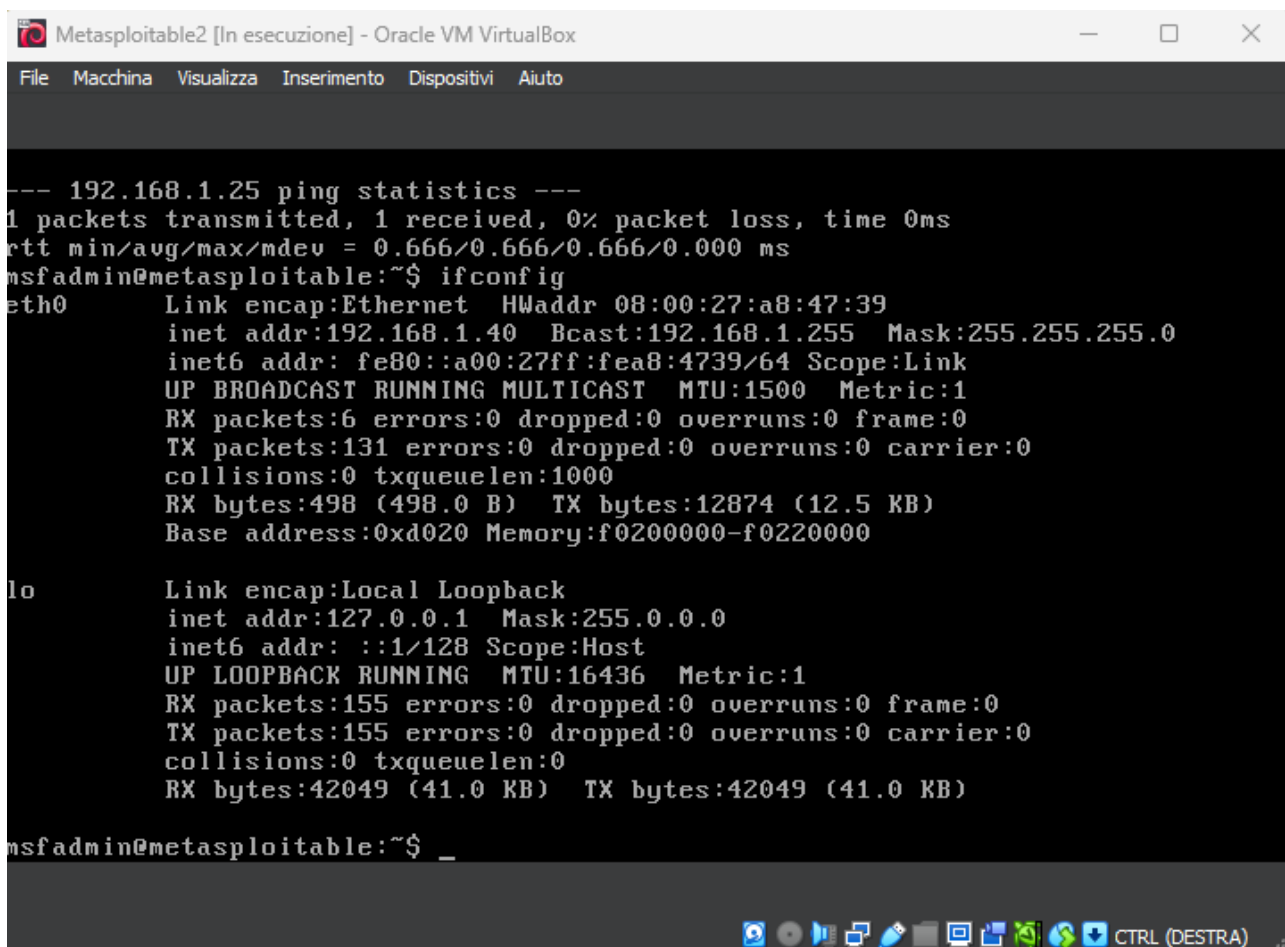
Introduzione

Nel contesto dell'apprendimento pratico della sicurezza informatica, ho seguito la traccia per sfruttare la vulnerabilità Telnet su Metasploitable utilizzando Metasploit. Questo report dettaglia ogni passo compiuto per ottenere accesso non autorizzato alla macchina bersaglio.

Configurazione e Connettività

Per iniziare, ho configurato gli indirizzi IP come richiesto nella traccia (192.168.1.25 per Kali e 192.168.1.40 per Metasploitable). Il successivo ping tra le macchine ha confermato una connessione operativa.

```
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:fe21:b1d0 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)  
    RX packets 63 bytes 5458 (5.3 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 26 bytes 3220 (3.1 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 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~]  
$ ping 192.168.1.40  
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.  
64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=1.84 ms  
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.959 ms  
^C  
— 192.168.1.40 ping statistics —  
2 packets transmitted, 2 received, 0% packet loss, time 1002ms  
rtt min/avg/max/mdev = 0.959/1.400/1.842/0.441 ms  
  
(kali@kali)-[~]  
$
```



```
Metasploitable2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

--- 192.168.1.25 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.666/0.666/0.666/0.000 ms
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a8:47:39
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea8:4739/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:131 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:498 (498.0 B)  TX bytes:12874 (12.5 KB)
          Base address:0xd020 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:155 errors:0 dropped:0 overruns:0 frame:0
          TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:42049 (41.0 KB)  TX bytes:42049 (41.0 KB)

msfadmin@metasploitable:~$ _
```

Analisi del Servizio Telnet su Metasploitable

Utilizzando il comando `nmap -sV`, ho identificato la presenza del servizio Telnet sulla porta 23 di Metasploitable. Questa informazione è stata fondamentale per l'attività successiva.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -sV 192.168.1.40  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-05 10:03 CET  
Nmap scan report for 192.168.1.40  
Host is up (0.00062s 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?  
514/tcp   open  shell        Netkit rshd  
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
```

Accesso a Metasploitn ricerca ed Utilizzo del Modulo Telnet

Avviando la console Metasploit con il comando "msfconsole", ho cercato il modulo auxiliary relativo a Telnet utilizzando il comando "search". Successivamente, ho impostato l'indirizzo host con il comando "set RHOSTS" seguito dall'indirizzo IP di Metasploitable. Infine, ho eseguito il modulo con il comando "exploit".

```
kali@kali: ~  
File Actions Edit View Help  
~ /// omh // dMMMMMMMMMMMMMMMMN / ::::: /+ooso- /ydh//+s+/osssso: - syN///os:  
/MMMMMMMMMMMMMMMMMMMMd. ' /++-.-yy/ ... esydh/-+oo:-`o// ... oyodh+  
-hMMmsddd+:dMMmNMMh. ' .-mmk.//^^^\\'.^^':++:^o: //^^^\\'::  
.sMMmo. -dMd--:mN/` ||-X-|| ||-X-||  
...../yddy/: ... +hmo- ... hdd:.....\\=v=//.....\\=v=//.....  
+-----+  
+-----+  
+ | Session one died of dysentery. | +  
+-----+  
+-----+  
  
Press ENTER to size up the situation  
  
%%%%%%%%%%%%%%  
%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%  
%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%%%  
%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%  
%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%  
%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%  
%%%%%%%%%%%%%%  
  
Press SPACE BAR to continue  
  
+ -- --=[ metasploit v6.3.55-dev ]  
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post ]  
+ -- --=[ 1391 payloads - 46 encoders - 11 nops ]  
+ -- --=[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > |
```

```
kali@kali: ~  
File Actions Edit View Help  
dows/gather/credentials/mremote  
msf6 > search auxiliary telnet  
Matching Modules  


| #  | Name                                                            | Check      | Description                                                     | Disclosure |
|----|-----------------------------------------------------------------|------------|-----------------------------------------------------------------|------------|
| 0  | auxiliary/server/capture/telnet                                 | normal No  | Authentication Capture: Telnet                                  |            |
| 1  | auxiliary/scanner/telnet/brocade_enable_login                   | normal No  | Brocade Enable Login Check Scanner                              |            |
| 2  | auxiliary/dos/cisco/ios_telnet_rocem                            | normal No  | Cisco IOS Telnet Denial of Service                              | 2017-03-17 |
| 3  | auxiliary/admin/http/dlink_dir_300_600_exec_noauth              | normal No  | D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Executi | 2013-02-04 |
| 4  | auxiliary/scanner/ssh/juniper_backdoor                          | normal No  | Juniper SSH Backdoor Scanner                                    | 2015-12-20 |
| 5  | auxiliary/scanner/telnet/lantronix_telnet_password              | normal No  | Lantronix Telnet Password Recovery                              |            |
| 6  | auxiliary/scanner/telnet/lantronix_telnet_version               | normal No  | Lantronix Telnet Service Banner Detection                       |            |
| 7  | auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof                    | normal No  | Microsoft IIS FTP Server Encoded Response Overflow Trigger      | 2010-12-21 |
| 8  | auxiliary/admin/http/netgear_pnp_getsharefolderlist_auth_bypass | normal Yes | Netgear PNPX_GetShareFolderList Authentication Bypass           | 2021-09-06 |
| 9  | auxiliary/admin/http/netgear_r6700_pass_reset                   | normal Yes | Netgear R6700v3 Unauthenticated LAN Admin Password Reset        | 2020-06-15 |
| 10 | auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce |            |                                                                 | 2021-04-21 |


```



```
kali@kali: ~  
File Actions Edit View Help  
Injection Vulnerability  
13 auxiliary/scanner/telnet/telnet_login  
normal No Telnet Login Check Scanner  
14 auxiliary/scanner/telnet/telnet_version  
normal No Telnet Service Banner Detection  
15 auxiliary/scanner/telnet/telnet_encrypt_overflow  
normal No Telnet Service Encryption Key ID Overflow Detection  
  
Interact with a module by name or index. For example info 15, use 15 or use auxiliary/scanner/telnet/telnet_encrypt_overflow  
  
msf6 > use 14  
msf6 auxiliary(scanner/telnet/telnet_version) > show options  
  
Module options (auxiliary/scanner/telnet/telnet_version):  
  
Name          Current Setting  Required  Description  
-----  
PASSWORD        
RHOSTS          
  
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.  
  
msf6 auxiliary(scanner/telnet/telnet_version) > |
```

```
kali@kali: ~  
File Actions Edit View Help  
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.  
  
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40  
RHOSTS => 192.168.1.40  
msf6 auxiliary(scanner/telnet/telnet_version) > shot options  
[-] Unknown command: shot  
msf6 auxiliary(scanner/telnet/telnet_version) > show options  
  
Module options (auxiliary/scanner/telnet/telnet_version):  
  
  Name      Current Setting  Required  Description  
  ---      -  
  PASSWORD  192.168.1.40    no        The password for the specified username  
  RHOSTS    192.168.1.40    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              The username to authenticate as  
  
View the full module info with the info, or info -d command.  
  
msf6 auxiliary(scanner/telnet/telnet_version) > |
```

Recupero delle Credenziali Telnet

L'esecuzione del modulo ha fornito le credenziali Telnet della macchina Metasploitable, consentendomi di accedere non autorizzato al sistema.


```
kali@kali: ~  
File Actions Edit View Help  
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://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       | The username to authenticate as                                                                        |

  
View the full module info with the info, or info -d command.  
msf6 auxiliary(scanner/telnet/telnet_version) > exploit  
[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET  
aWarning: Never expose this VM to an untrusted network!\nContact: msfdev[at]metasploit.com\nLogin with msfadmin/msfadmin to get started\natable login:  
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Accesso Effettivo a Metasploitable tramite Telnet

Ho utilizzato il comando "telnet" seguito dall'indirizzo IP di Metasploitable per accedere al sistema. Le credenziali recuperate in precedenza sono state utilizzate con successo per autenticarmi.

```
kali@kali: ~  
File Actions Edit View Help  
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40  
[*] exec: telnet 192.168.1.40  
  
Trying 192.168.1.40 ...  
Connected to 192.168.1.40.  
Escape character is '^]'.  
  
Metasploit 6.0.0-dev  
  
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 Mar 5 03:52:26 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:~$
```

Conclusioni

L'esercizio ha raggiunto con successo l'obiettivo di sfruttare la vulnerabilità Telnet su Metasploitable utilizzando Metasploit.