EXPLOIT TELNET CON METASPLOIT

FRANCESCO PERSICHETTI

L'esercizio consiste nel:

1. Cambiare indirizzo IP della macchina Kali e Metasploitable, inserire rispettivamente i nuovi indirizzi "192.168.1.25" e "192.168.1.40"
2. Utilizzare Metasploit per sfruttare la vulnerabilità di Telnet con il modulo "auxiliary telnet_version" sulla macchina Metasploitable

1.

Per iniziare l'esercitazione devo prima mettere la macchina attaccante(kali) e la macchina vittima(metasploitable) sulla stessa rete per poter comunicare tra di loro andando a cambiare il loro indirizzo IP

```
auto eth0
iface eth0 inet loopback

auto eth0
iface eth0 inet static
address 192.168.1.25/24
gateway 192.168.1.103
```

IP Kali

```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.40
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.104
```

IP Metasploitable

2.

Prima di iniziare la sessione di hacking sul servizio telnet vedo se il servizio in questione è attivo sulla macchina vittima attraverso una scansione

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV  192.168.1.40
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 03:38 EST
Nmap scan report for 192.168.1.40
Host is up (0.00059s latency).
Not shown: 979 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?
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  rmiregistry?
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql?
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
Service Info: Host: 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 187.04 seconds
```

Una volta appurato che il servizio c'è ed è attivo, apro "msfconsole" da kali e vado a cercare il modulo "auxiliary/scanner/telnet/telnet_version" che mi servirà per l'exploit

```
msf6 > search telnet

Matching Modules
================

   #   Name                                                     Disclosure Date
   -   ----                                                     ---------------
   0   exploit/linux/misc/asus_infosvr_auth_bypass_exec         2015-01-04
   1   exploit/linux/http/asuswrt_lan_rce                       2018-01-22
   2   auxiliary/server/capture/telnet
   3   auxiliary/scanner/telnet/brocade_enable_login
   4   exploit/windows/proxy/ccproxy_telnet_ping                2004-11-11
   5   auxiliary/dos/cisco/ios_telnet_rocem                     2017-03-17
   6   auxiliary/admin/http/dlink_dir_300_600_exec_noauth       2013-02-04
   7   exploit/linux/http/dlink_diagnostic_exec_noauth          2013-03-05
   8   exploit/linux/http/dlink_dir300_exec_telnet              2013-04-22
   9   exploit/unix/webapp/dogfood_spell_exec                   2009-03-03
   10  exploit/freebsd/telnet/telnet_encrypt_keyid              2011-12-23
   11  exploit/windows/telnet/gamsoft_telsrv_username           2000-07-17
   12  exploit/windows/telnet/goodtech_telnet                   2005-03-15
   13  exploit/linux/misc/hp_jetdirect_path_traversal           2017-04-05
   14  exploit/linux/http/huawei_hg532n_cmdinject               2017-04-15
   15  exploit/linux/misc/igel_command_injection                2021-02-25
   16  auxiliary/scanner/ssh/juniper_backdoor                   2015-12-20
   17  auxiliary/scanner/telnet/lantronix_telnet_password
   18  auxiliary/scanner/telnet/lantronix_telnet_version
   19  exploit/linux/telnet/telnet_encrypt_keyid                2011-12-23
   20  auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof             2010-12-21
   21  exploit/linux/telnet/netgear_telnetenable                2009-10-30
   22  auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass  2021-09-06
   23  auxiliary/admin/http/netgear_r6700_pass_reset            2020-06-15
   24  auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce  2021-04-21
   25  exploit/unix/misc/polycom_hdx_auth_bypass                2013-01-18
   26  exploit/unix/misc/polycom_hdx_traceroute_exec            2017-11-12
   27  exploit/freebsd/ftp/proftp_telnet_iac                    2010-11-01
   28  exploit/linux/ftp/proftp_telnet_iac                      2010-11-01
   29  auxiliary/scanner/telnet/telnet_ruggedcom
   30  auxiliary/scanner/telnet/satel_cmd_exec                  2017-04-07
   31  exploit/solaris/telnet/ttyprompt                         2002-01-18
   32  exploit/solaris/telnet/fuser                             2007-02-12
   33  exploit/linux/http/tp_link_sc2020n_authenticated_telnet_injection  2015-12-20
   34  auxiliary/scanner/telnet/telnet_login
   35  auxiliary/scanner/telnet/telnet_version
```

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

       Name: Telnet Service Banner Detection
     Module: auxiliary/scanner/telnet/telnet_version
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  hdm <x@hdm.io>

Check supported:
  No

Basic options:
  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  PASSWORD                   no        The password for the specified username
  RHOSTS                     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  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

Description:
  Detect telnet services
```

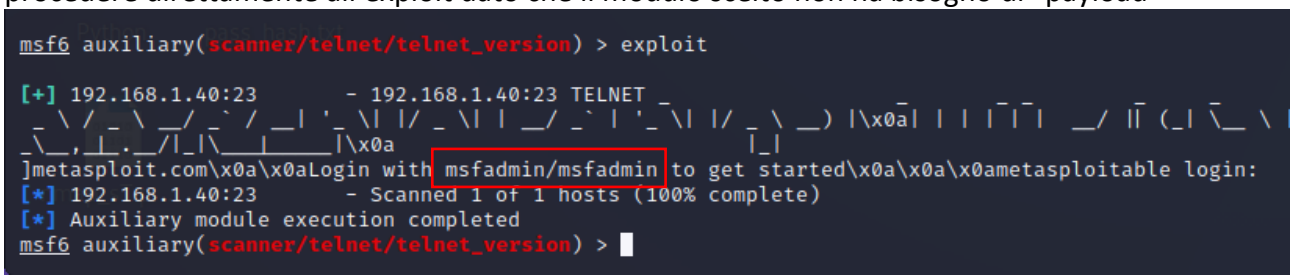
Dalle info posso notare i parametri da configurare richiesti per l'exploit come "RHOSTS", dove vado a mettere l'indirizzo IP della macchina Metasploitable con il comando "set RHOSTS"

```
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-Metasploit
   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
```

Dopo aver fatto un nuovo “show options” vedo che il parametro configurato è stato preso e posso procedere direttamente all’exploit dato che il modulo scelto non ha bisogno di “payload”



L’exploit mi restituirà le credenziali di accesso alla macchina metasploitable.
Infatti, se dal terminale lancio il comando telnet più l’indirizzo IP di meta (“telnet 192.168.1.40”), mi verrà restituito il login di meta in cui posso accedere con le credenziali appena trovate per testare la buona riuscita dell’exploit