

Login Metasploitable

Traccia:

Sulla base dell'esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

msfconsole e auxiliary telnet_version

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)~  
$ msfconsole  
Metasploit tip: View advanced module options with advanced  
  
Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f  
EFLAGS: 00010046  
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001  
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60  
ds: 0018  es: 0018  ss: 0018  
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)  
  
Stack: 90909090909090909090909090909090  
90909090909090909090909090909090  
90909090.90909090.90909090  
90909090.90909090.90909090  
90909090.90909090.09090900  
90909090.90909090.09090900  
.....  
cccccccccccccccccccccccccccccccc  
cccccccccccccccccccccccccccccccc  
cccccccc.....  
cccccccccccccccccccccccccccccccc  
cccccccccccccccccccccccccccccccc  
.....cccccccccc  
cccccccccccccccccccccccccccccccc  
cccccccccccccccccccccccccccccccc  
.....  
ffffffffffffffffffffffffffff  
ffffffff.....  
ffffffffffffffffffffffffffff  
ffffffff.....  
ffffffff.....  
ffffffff.....  
.....  
  
Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00  
Alee, Killing Interrupt handler  
Kernel panic: Attempted to kill the idle task!  
In swapper task - not syncing  
  
=[ metasploit v6.4.18-dev ]  
+ --=[ 2437 exploits - 1255 auxiliary - 429 post ]  
+ --=[ 1471 payloads - 47 encoders - 11 nops ]  
+ --=[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > use auxiliary/scanner/telnet/telnet_version  
  
Matching Modules  
  
# Name Disclosure Date Rank Check Description  
- - - - -  
0 auxiliary/scanner/telnet/telnet_version . normal No Telnet Service Banner Detection  
  
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/telnet/telnet_version  
[*] Using 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://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.
```

User/Password e Login

```
[*] Using auxiliary/scanner/telnet/telnet_version
msf5 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.

msf5 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.149
rhosts => 192.168.1.149
msf5 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   | 192.168.1.149   | 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.

msf5 auxiliary(scanner/telnet/telnet_version) > exploit

[*] 192.168.1.149:23 - 192.168.1.149:23 TELNET
fdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: ms
[*] 192.168.1.149:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.149 23
[*] exec: telnet 192.168.1.149 23

Trying 192.168.1.149...
Connected to 192.168.1.149.
Escape character is '^['.

Metasploit

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: Mon Nov 11 08:23:30 EST 2024 from kali.wind3.hub on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 1686

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:~$
```

Relazione

Il compito di oggi prevedeva di effettuare un attacco alla macchina Metasploitable sfruttando la vulnerabilità del servizio Telnet sulla porta 23.

1. Ho avviato Metasploit con il comando: `msfconsole`.
2. Successivamente, ho utilizzato il modulo `use auxiliary/scanner/telnet/telnet_version` per scansionare il servizio Telnet.
3. Ho impostato il target con il comando `set RHOSTS 192.168.1.149`.
4. Dopo aver trovato un nome utente e una password validi, ho aperto una connessione Telnet per verificare le credenziali con il comando: `telnet 192.168.1.149 23` (inserendo l'IP e la porta).
5. Inserendo il nome utente e la password recuperati, sono riuscito ad accedere al sistema.

Questo mi ha permesso di confermare l'efficacia dell'attacco e dimostrare la vulnerabilità di Telnet a un attacco di brute-force, consentendo un accesso non autorizzato alla macchina Metasploitable.