

Exploit Telnet con Metasploit

Descrizione dell'esercizio

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

Esecuzione

Avviamo Metasploit col comando **msfconsole**

```
(kali㉿kali)-[~]
$ msfconsole

https://metasploit.com

Metasploit v6.3.27-dev
+ -- --[ 2335 exploits - 1220 auxiliary - 413 post ]
+ -- --[ 1385 payloads - 46 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit tip: Set the current module's RHOSTS with
database values using hosts -R or services
-R
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

Cerchiamo il modulo richiesto tramite il comando **search**

```
msf6 > search auxiliary telnet_version

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -
0  auxiliary/scanner/telnet/lantronix_telnet_version  normal  No  Lantronix Telnet Service Banner Detection
1  auxiliary/scanner/telnet/telnet_version           normal  No  Telnet Service Banner Detection

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

```
msf6 > use 1
msf6 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 <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 RHOSTS 192.168.1.101
RHOSTS => 192.168.1.101
```

[illegible]

Dall'output possiamo vedere che l'exploit ha avuto successo perchè mostra dati sensibili sul servizio quali credenziali di accesso.