

## Traccia:

Sulla base di quanto visto, utilizzare Kali per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet\_version sulla macchina Metasploitable.

**Requisito:** Seguire gli step già visti. Prima, configurate l'IP della vostra Kali con 192.168.1.25 e l'IP della vostra Metasploitable con 192.168.1.40

## SVOLGIMENTO:

```
Session  Actions  Edit  View  Help
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Export your database results with db_export -f xml
<file>

IIIIII      dTb.dTb
 II      4'  v  'B
 II      6.    .P
 II      'T; . .;P'
 II      'T;  ;P'
IIIIII      'YvP'

I love shells --egypt

      =[ metasploit v6.4.94-dev ]
+ -- --=[ 2,564 exploits - 1,312 auxiliary - 1,683 payloads ]
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > █
```

ho avviato msfconsole

```
      =[ metasploit v6.4.94-dev ]
+ -- --=[ 2,564 exploits - 1,312 auxiliary - 1,683 payloads ]
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use auxiliary/scanner/tel
use auxiliary/scanner/telephony/wardial          use auxiliary/scanner/telnet/lantronix_telnet_version  use auxiliary/scanner/telnet/telnet_login
use auxiliary/scanner/telnet/brocade_enable_login use auxiliary/scanner/telnet/satel_cmd_exec             use auxiliary/scanner/telnet/telnet_ruggedcom
use auxiliary/scanner/telnet/lantronix_telnet_password use auxiliary/scanner/telnet/telnet_encrypt_overflow    use auxiliary/scanner/telnet/telnet_version
msf > use auxiliary/scanner/telnet/telnet_version
msf auxiliary(scanner/telnet/telnet_version) > █
```

```
msf > use auxiliary/scanner/telnet/telnet_version
msf 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.

msf auxiliary(scanner/telnet/telnet_version) > 
```

ho sfruttato il modulo auxiliary scanner/telnet/telnet\_version con il comando use

[illegible]

ho configurato Rhost con l'indirizzo della macchina meta e ho fatto partire l'exploit

```

PORT      STATE SERVICE
23/tcp    open  telnet
Linux telnetd
MAC Address: 08:00:27:9A:8B:1E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds

(kali㉿kali)-[~]
$ telnet 192.168.50.101
Trying 192.168.50.101...
Connected to 192.168.50.101.
Escape character is '^]'.

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: 
```

ho verificato la correttezza delle informazioni trovate dell'exploit provando l'accesso al servizio telnet con il comando telnet eseguito dalla kali.