

05 MARZO 2024

REPORT - EPICODE

S7L2

PRESENTED BY

Alessandro Marasca



EXPLOIT TELNET CON METASPLOIT

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.

Requisito: Seguire gli step visti in lezione teorica. Prima, configurate l'ip della vostra Kali con 192.168.1.25 e l'ip della vostra Metasploitable con 192.168.1.40

02 - EXPLOIT TELNET CON METASPLOIT

```
(kali@kali)-[~]
$ msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor
```

```
Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready ...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
```

```

    = [ metasploit v6.3.43-dev ]
+ -- -- [ 2376 exploits - 1232 auxiliary - 416 post ]
+ -- -- [ 1391 payloads - 46 encoders - 11 nops ]
+ -- -- [ 9 evasion ]
```

Metasploit Documentation: <https://docs.metasploit.com/>

```
msf6 > auxiliary/scanner/telnet/telnet_version
[-] Unknown command: auxiliary/scanner/telnet/telnet_version
This is a module we can load. Do you want to use auxiliary/scanner/telnet/telnet_version? [y/N] y
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.

View the full module info with the `info`, or `info -d` command.

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit
[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40
[*] exec: telnet 192.168.1.40
```

```
Trying 192.168.1.40 ...
Connected to 192.168.1.40.
Escape character is '^['.
```



Warning: Never expose this VM to an untrusted network!

Contact: [msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

Login with `msfadmin/msfadmin` to get started

```
metasploitable login: msfadmin
Password:
Last login: Tue Mar 5 06:10:41 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:~$ |
```



Alessandro Marasca

Epicode

S7L2- CS0124

05 MARZO 2024