S7 – L3 BONUS

Post-Exploitation: Privilege Escalation e Analisi di Backdoor Persistente con Metasploit

Introduzione

In questa fase bonus ho eseguito un'**attività di post-exploitation finalizzata all'analisi di possibili vettori di privilege escalation e alla valutazione dell'installazione di una backdoor persistente**, utilizzando esclusivamente msfconsole.

L'obiettivo è stato verificare l'impatto reale della compromissione e la possibilità di mantenere l'accesso al sistema nel tempo.

BONUS FASE 1 — Identificazione vulnerabilità locali (modulo post)

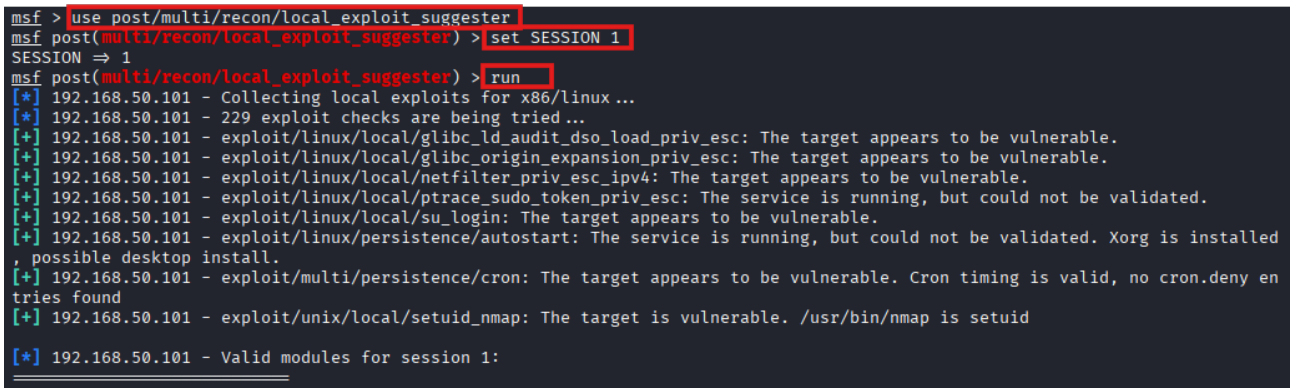
Obiettivo

Identificare potenziali vulnerabilità locali sfruttabili per l'escalation di privilegi utilizzando un **modulo post di msfconsole**.

Attività svolta (msfconsole)

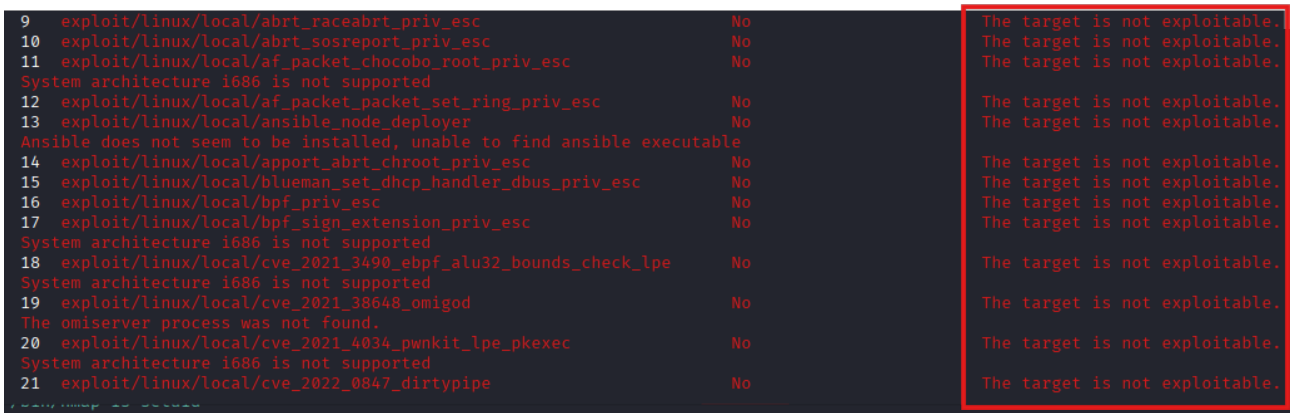
Ho messo in background la sessione Meterpreter ottenuta in precedenza e ho caricato un modulo post di msfconsole dedicato all'individuazione di vulnerabilità locali. Ho associato il modulo alla sessione attiva e ne ho eseguito l'analisi.

```
use post/multi/recon/local_exploit_suggester
set SESSION 1 (ID_SESSIONE)
run
```



Cosa ottengo

- Un elenco di vulnerabilità/exploit locali suggeriti in base a:
    - versione del kernel
    - architettura del sistema
    - configurazione del target



- Output completo del modulo post con la lista dei risultati

BONUS FASE 2 — Selezione degli exploit suggeriti

Obiettivo

Selezionare uno o più exploit tra quelli individuati dal modulo post come **potenzialmente applicabili**.

Attività svolta

Ho analizzato i risultati restituiti dal modulo post e ho selezionato uno degli exploit suggeriti, valutandone la coerenza con:

- sistema operativo
- versione del kernel
- architettura del target
- contesto dell’utente corrente

Cosa ottengo

- Un exploit selezionato (o più, se applicabile) da testare per l’escalation dei privilegi
- Evidenza dell’exploit selezionato nell’output del suggeritore

---

BONUS FASE 3 — Esecuzione exploit locali suggeriti

Obiettivo

Eseguire gli exploit locali selezionati utilizzando esclusivamente msfconsole.

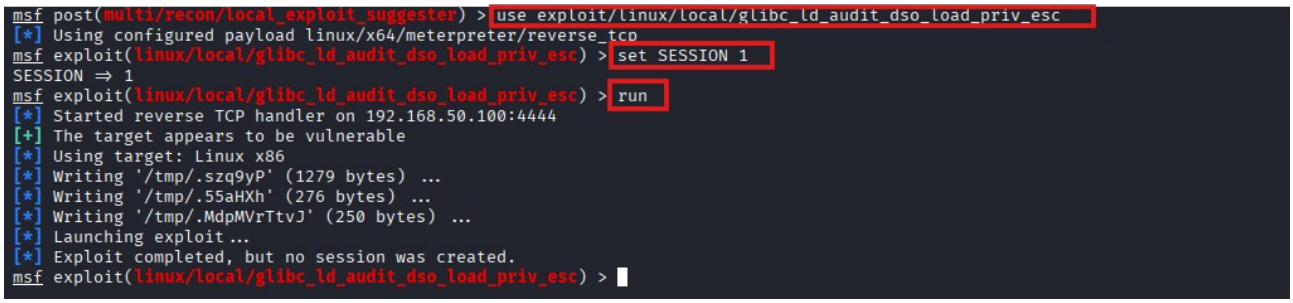
Attività svolta (msfconsole)

Ho caricato l'exploit locale selezionato e l'ho associato alla sessione Meterpreter ottenuta in precedenza, quindi ne ho avviato l'esecuzione.

```
use exploit/linux/local/glibc_ld_audit_dso_load_priv_esc
set SESSION 1 (ID_SESSIONE)
run
```

Cosa ottengo

- Output dell'esecuzione dell'exploit con indicazione dell'esito (successo o fallimento)



- Avvio dell'exploit
- Output finale con l'esito dell'esecuzione

BONUS FASE 4 — Verifica escalation dei privilegi

Obiettivo

Verificare se l'esecuzione degli exploit ha comportato un'elevazione dei privilegi.

Attività svolta (Meterpreter)

Dopo ogni tentativo di exploit, sono rientrato nella sessione Meterpreter e ho verificato l'identità dell'utente corrente.

```
getuid
```

(in alternativa, ho tentato l'esecuzione di un'azione che richiede privilegi di root per confermare l'esito)

Cosa ottengo

- Conferma dell'utente corrente: utente limitato (es. `postgres`) in caso di fallimento

- Output di `getuid` dopo ciascun exploit testato

BONUS FASE 5 — Installazione backdoor / persistenza (msfconsole)

Obiettivo

Valutare la possibilità di installare una backdoor persistente utilizzando esclusivamente funzionalità di msfconsole.

Attività svolta

Ho valutato le funzionalità di persistenza disponibili in Metasploit verificandone la fattibilità nel contesto della sessione ottenuta.
Prima di procedere, ho controllato il livello di privilegi dell'utente corrente per determinare se fossero sufficienti all'installazione di una persistenza di sistema.

Verifica privilegi (Meterpreter)

```
getuid
```

Cosa ottengo

La sessione risulta associata all'utente `postgres`, account di servizio con privilegi limitati.
In assenza di privilegi root, non è stato possibile installare una backdoor persistente di sistema utilizzando esclusivamente msfconsole.

BONUS FASE 6 — Dimostrazione accesso in un momento successivo

Obiettivo

Valutare la possibilità di riaccedere al sistema target in un momento successivo senza ripetere la fase di exploit iniziale.

Attività svolta
Ho analizzato la possibilità di ristabilire una sessione sul sistema target senza rieseguire l’exploit iniziale, verificando la presenza di meccanismi di persistenza configurati durante le fasi precedenti.

Cosa ottengo
Poiché non è stato possibile ottenere privilegi di root e non è stata configurata una backdoor persistente di sistema, non è risultato tecnicamente possibile dimostrare un accesso successivo al target senza ripetere la fase di exploit iniziale.

BONUS FASE 7 — Conclusione del BONUS

Obiettivo

Documentare l’esito complessivo delle attività di privilege escalation e di valutazione della persistenza.

Cosa documento

- Le vulnerabilità locali individuate tramite modulo post di msfconsole
- Gli exploit locali testati
- L’esito della verifica dei privilegi dopo ciascun tentativo
- La fattibilità o meno dell’installazione di una backdoor persistente nel contesto analizzato

Testo di chiusura

> Le attività di post-exploitation mi hanno consentito di individuare e testare potenziali vulnerabilità locali utilizzando esclusivamente msfconsole.
>
> Nonostante i tentativi effettuati, **l’escalation dei privilegi a root non è stata ottenuta e, di conseguenza, non è stato possibile dimostrare l’installazione di una backdoor persistente stabile nel contesto del sistema analizzato.**

Conclusioni:

Le attività di post-exploitation hanno permesso di individuare e testare potenziali vulnerabilità locali utilizzando esclusivamente msfconsole.

Nel contesto analizzato l’escalation dei privilegi a root non è stata ottenuta e, di conseguenza, non è risultata fattibile l’installazione di una backdoor persistente, evidenziando l’importanza del contesto e dei privilegi nell’impatto di una compromissione.