Esercizio

Sulla base dell'esercizio visto in lezione teorica, utilizzare Kali per sfruttare la vulnerabilità relativa a TWiki con la tecnica che meglio preferite, sulla macchina Metasploitable.

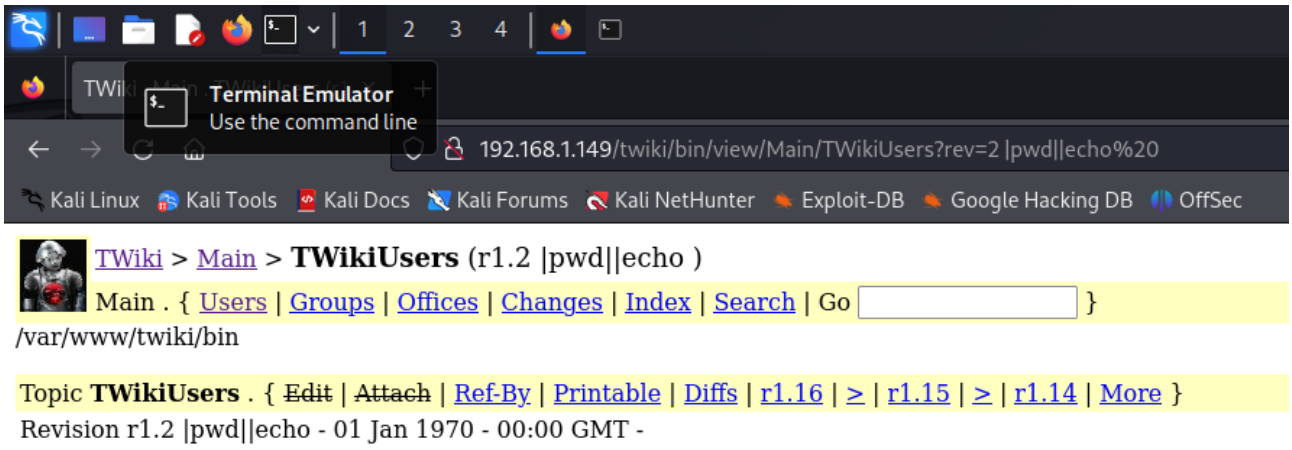
Dettagli dell'Attività

TWiki presenta una vulnerabilità nel parametro "rev" che permette l'inserimento di codice arbitrario. Questa vulnerabilità può essere sfruttata inserendo un parametro specifico nell'URL in questo modo:

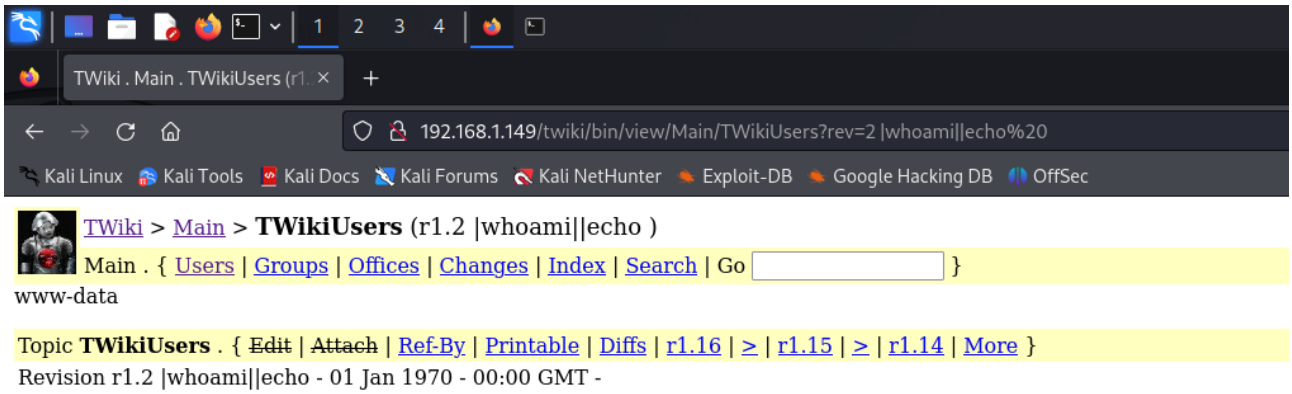
- ?rev=2|comando||echo%20.

Questo permette di ottenere informazioni dal sistema target. Ad esempio:

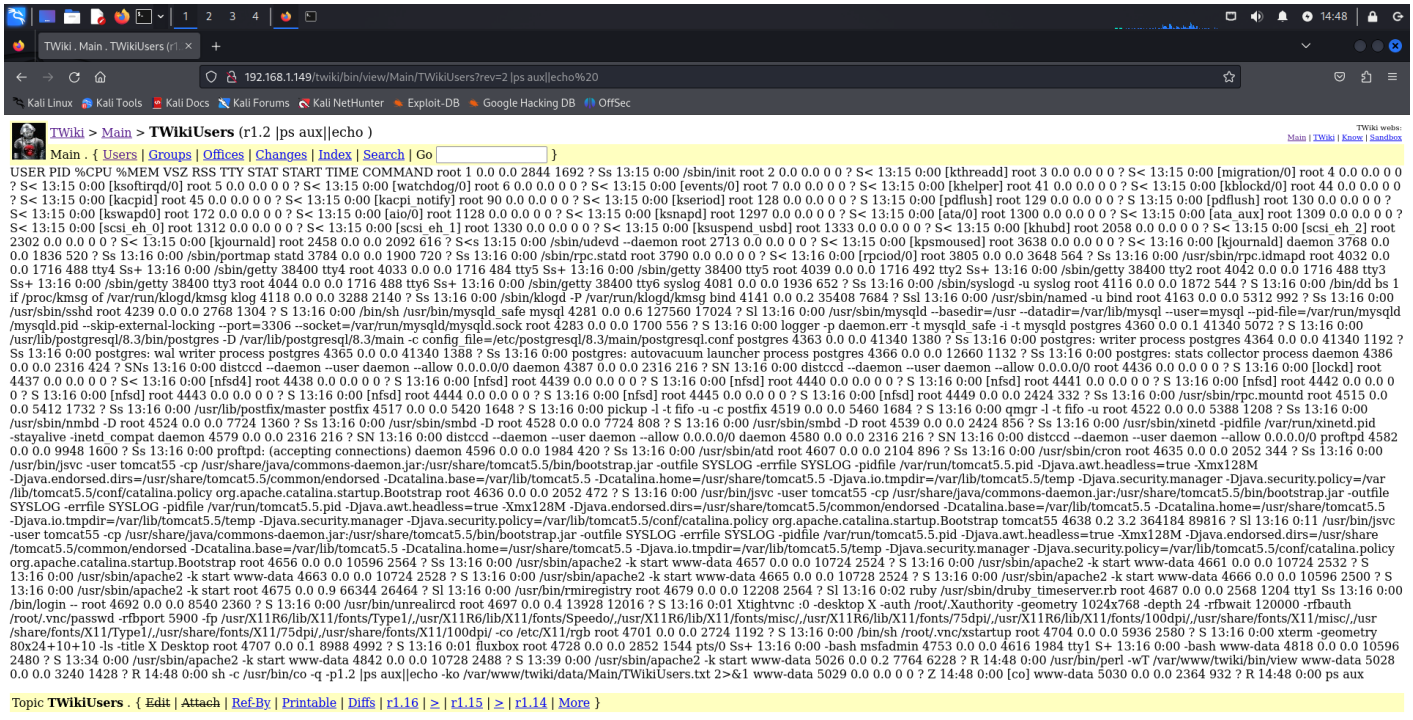
- Per visualizzare la directory corrente, si utilizza il comando pwd.



- Per identificare l'utente attualmente loggato, si utilizza il comando whoami.



- Per vedere i processi attivi, si utilizza il comando ps aux.



Esempio di Utilizzo

Modificando l'URL con il parametro vulnerabile, possiamo eseguire diversi comandi sul sistema target e ottenere informazioni preziose che possono aiutare nel proseguimento dell'attacco o nell'analisi della vulnerabilità.