Configurazione di un Server FTP e Cracking della Password con Hydra

1 Introduzione

Questo report descrive i passaggi effettuati per configurare un server FTP su Kali Linux e successivamente tentare di forzarne l'autenticazione utilizzando lo strumento Hydra. L'obiettivo era comprendere il processo di configurazione di un servizio di base ed esplorare le tecniche di cracking delle password.

2 Configurazione del Server FTP

Il primo passo ha riguardato l'installazione e l'avvio del servizio `vsftpd` (Very Secure FTP Daemon).

2.1 Installazione

È stato utilizzato il seguente comando per installare il pacchetto `vsftpd`:

```
sudo apt install vsftpd
```

La Figura1 mostra l'output del processo di installazione, indicando che il pacchetto `vsftpd` è stato installato con successo.

2.2 Avvio del Servizio

Dopo l'installazione, il servizio `vsftpd` è stato avviato utilizzando il seguente comando:

```
sudo service vsftpd start
```

3 Cracking della Password con Hydra

Con il server FTP in esecuzione, il passo successivo è stato tentare di forzare la password utilizzando lo strumento Hydra.

3.1 Attacco con Singola Password

Inizialmente, è stato effettuato un tentativo di prova con una singola password utilizzando l'opzione `-p`:

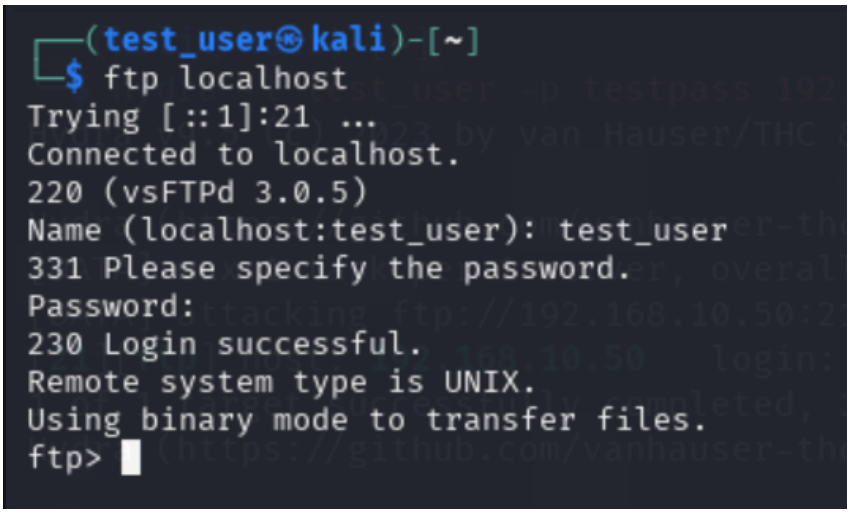
```
hydra -l test_user -p testpass 192.168.10.50 ftp
```

La Figura2 mostra che Hydra ha trovato con successo la password `testpass` per l'utente `test_user` sul server FTP all'indirizzo IP 192.168.10.50.

3.2 Test Locale

Per confermare che il server FTP fosse in esecuzione localmente, è stato effettuato un tentativo di connessione:

```
ftp localhost
```

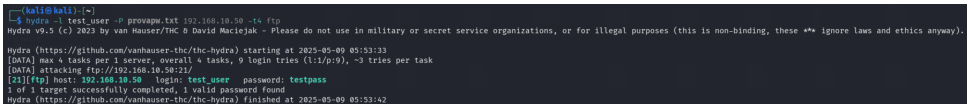


La Figura3 dimostra un login riuscito al server FTP locale utilizzando il nome utente `test_user` e la password testpass.

3.3 Attacco con Lista di Password

Successivamente, è stato tentato un attacco con una lista di password utilizzando l'opzione `-P` e un file denominato `provapw.txt`:

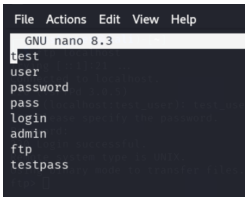
```
hydra -l test_user -P provapw.txt 192.168.10.50 ftp
```



La Figura4 mostra che, anche con una lista di password, Hydra ha identificato con successo la password corretta `testpass` (presente in `provapw.txt`).

3.4 Contenuto del File della Lista di Password

La Figura5 mostra il contenuto del file `provapw.txt`, che include la password `testpass` insieme ad altre potenziali password.



4 Sfide e Soluzioni Alternative

Come notato nella descrizione dell'esercizio, affidarsi esclusivamente a grandi elenchi di password come quelli presenti in SecLists può richiedere molto tempo. Ecco alcuni approcci alternativi da considerare per un cracking delle password o una valutazione della sicurezza più efficienti:

- **Generazione di Wordlist Mirate:** Invece di utilizzare elenchi di password generici, la creazione di wordlist personalizzate per l'obiettivo specifico può ridurre significativamente lo spazio di ricerca. Ciò comporta la raccolta di informazioni sull'organizzazione o sull'individuo target (se applicabile).
- **Attacchi Basati su Regole:** L' utilizzo di strumenti che consentono il cracking delle password basato su regole. Queste regole possono modificare le parole di una wordlist (ad esempio, aggiungendo numeri, caratteri speciali, maiuscole) per generare potenziali password basate su modelli comuni di creazione di password. Questo può essere più efficiente del semplice tentativo di ogni password in un grande elenco.
- **Sfruttamento di Vulnerabilità:** Invece di attaccare direttamente il meccanismo di autenticazione, l'identificazione e lo sfruttamento di altre vulnerabilità nel servizio FTP o nel sistema sottostante potrebbero fornire l'accesso senza la necessità di forzare la password. Ciò richiede una valutazione approfondita delle vulnerabilità.
- **Ingegneria Sociale:** In alcuni scenari (con la dovuta autorizzazione), è possibile impiegare tecniche di ingegneria sociale per ottenere le credenziali direttamente dagli utenti.

5 Conclusione

Questo esercizio ha dimostrato con successo la configurazione di base di un server FTP e l'uso di Hydra per il cracking delle password. Sebbene gli attacchi di forza bruta con grandi elenchi di password possano essere efficaci, sono spesso inefficienti. L'esplorazione di approcci più mirati e intelligenti, come la generazione di wordlist mirate e gli attacchi basati su regole, può migliorare significativamente l'efficienza dei tentativi di cracking delle password durante le valutazioni di sicurezza.