

Esercitazione W14D4

Authentication Cracking - Hydra

Fabio Benevento - 08/02/2024

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

Ricordate che 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.

Implementazione

Fase 1 - Cracking SSH

Per questa esercitazione ho in primo luogo creato un nuovo utente con credenziali username: `test_user` e password: `testpass` mediante il comando `sudo adduser testuser`.

Ho avviato quindi il servizio con il comando `sudo service ssh start` e verificato la correttezza delle credenziali accedendo in maniera canonica con il comando `ssh`.

```
(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 []: utente_test
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' ...

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

```
(kali@kali)-[~]
$ ssh test_user@127.0.0.1
test_user@127.0.0.1'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.
Last login: Tue Feb 13 09:21:06 2024 from 127.0.0.1
(test_user@kali)-[~]
$
```

Ho lanciato quindi l'esecuzione di Hydra utilizzando come dizionario le password salvate nel file `xato-net-10-million-passwords.txt`. Dopo svariati tentativi Hydra è riuscito ad individuare la password impostata in precedenza come mostrato in figura.

```
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "9562876" - 5191 of 5189454 [child 2] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "5656" - 5192 of 5189454 [child 3] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "1945" - 5193 of 5189454 [child 0] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "159632" - 5194 of 5189454 [child 2] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "15151515" - 5195 of 5189454 [child 0] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "123456qw" - 5196 of 5189454 [child 2] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "1234567891" - 5197 of 5189454 [child 0] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "02051983" - 5198 of 5189454 [child 2] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "02041983" - 5199 of 5189454 [child 2] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "02031987" - 5200 of 5189454 [child 1] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "02021989" - 5201 of 5189454 [child 1] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "z1x2c3v4" - 5202 of 5189454 [child 1] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "xing" - 5203 of 5189454 [child 1] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "vSjasmel12" - 5204 of 5189454 [child 1] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "twenty" - 5205 of 5189454 [child 3] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "toolman" - 5206 of 5189454 [child 3] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "thing" - 5207 of 5189454 [child 3] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "testpass" - 5208 of 5189454 [child 0] (0/0)
[22][ssh] host: 192.168.40.100 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 2024-02-13 14:00:10
```

Fase 2 - Cracking FTP

Per questa esercitazione ho in primo luogo creato un nuovo utente con credenziali username: ftp_user e password: peanut mediante il comando `sudo adduser ftp_user`.

Ho avviato quindi il servizio con il comando `sudo service vsftpd start` e verificato la correttezza delle credenziali accedendo in maniera canonica con il comando `ftp`.

```
File Actions Edit View Help
(kali@kali)-[~]
$ ftp 127.0.0.1
Connected to 127.0.0.1.
220 (vsFTPd 3.0.3)
Name (127.0.0.1:kali): ftp_user
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Ho lanciato quindi l'esecuzione di Hydra utilizzando come dizionario le password salvate nel file `xato-net-10-million-passwords.txt`. Dopo svariati tentativi Hydra è riuscito ad individuare la password impostata in precedenza come mostrato in figura.

```
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "fucker" - 108 of 1000 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "merlin" - 109 of 1000 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "diamond" - 110 of 1000 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "1234qwer" - 111 of 1000 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "gfhjkm" - 112 of 1000 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "hammer" - 113 of 1000 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "silver" - 114 of 1000 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "222222" - 115 of 1000 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "88888888" - 116 of 1000 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "anthony" - 117 of 1000 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "justin" - 118 of 1000 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "test" - 119 of 1000 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "bailey" - 120 of 1000 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "q1w2e3r4t5" - 121 of 1000 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "patrick" - 122 of 1000 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "internet" - 123 of 1000 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "scooter" - 124 of 1000 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "orange" - 125 of 1000 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "11111" - 126 of 1000 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "golfer" - 127 of 1000 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "cookie" - 128 of 1000 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "richard" - 129 of 1000 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "samantha" - 130 of 1000 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "bigdog" - 131 of 1000 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "guitar" - 132 of 1000 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "jackson" - 133 of 1000 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "whatever" - 134 of 1000 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "mickey" - 135 of 1000 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "chicken" - 136 of 1000 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "sparky" - 137 of 1000 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "snoopy" - 138 of 1000 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "maverick" - 139 of 1000 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "phoenix" - 140 of 1000 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "camaro" - 141 of 1000 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "sexy" - 142 of 1000 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "peanut" - 143 of 1000 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ftp_user" - pass "morgan" - 144 of 1000 [child 0] (0/0)
[22][ssh] host: 127.0.0.1 login: ftp_user password: peanut
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-15 05:52:18
```