ESERCIZIO S6 L5

EPICODE | Progetto S6/L5 PDF | Esercizio — Traccia

Esercizio del Giorno

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

L'esercizio di oggi ha un duplice scopo:

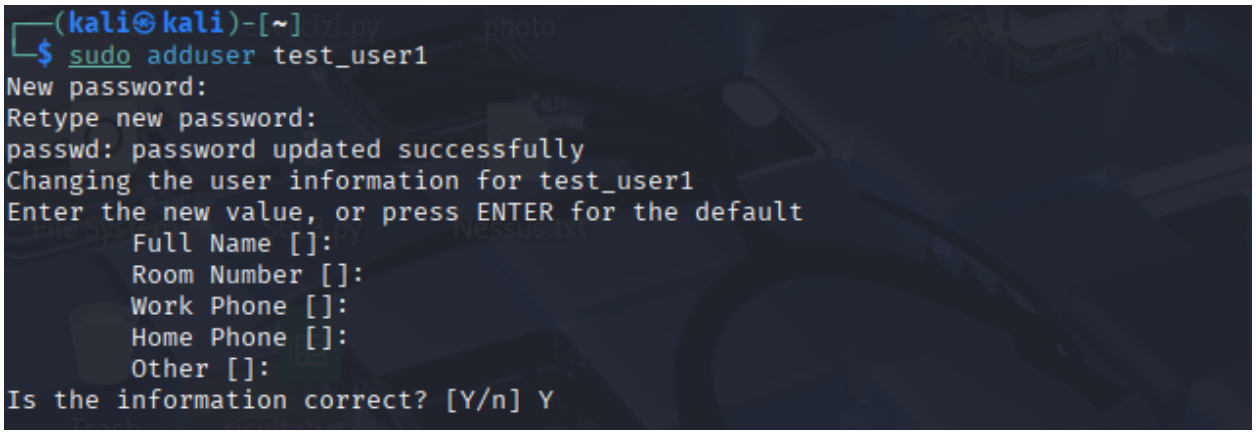
- Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete.
- Consolidare le conoscenze dei servizi stessi tramite la loro configurazione.

L'esercizio si svilupperà in due fasi:

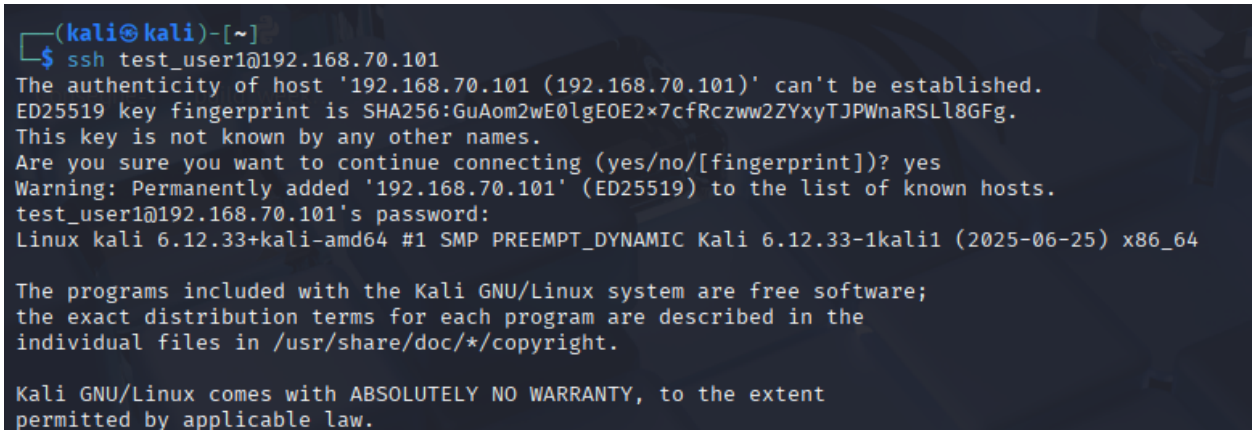
- Una prima fase dove insieme vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra.
- Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

RISPOSTA

Creo inizialmente un nuovo utente sulla VM Kali Linux: utilizzo sudo adduser test_user1 e configuro la nuova password : testpass



Ora testo la connessione SSH del nuovo utente creato utilizzando il comando : ssh test_user1@192.168.70.101



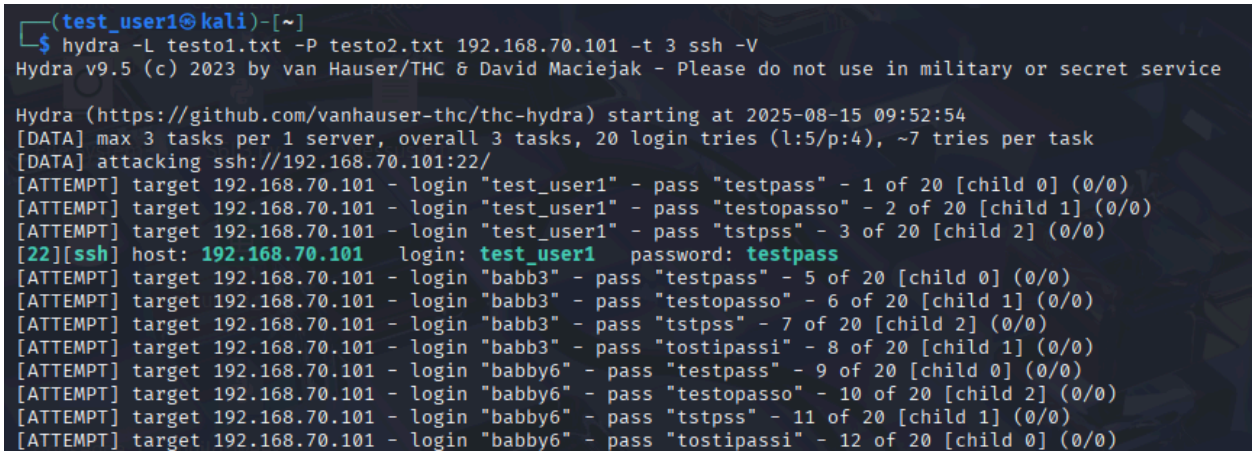
Avendo inserito le credenziali corrette ho ricevuto il prompt dei comandi dell'utente test_user1 sulla mia Kali.

A questo punto non mi resta che utilizzare **Hydra** per la sessione di cracking, ma prima, dato che andrò ad utilizzare delle liste per l'attacco a dizionario, credo due file.txt (**testo1.txt** e **testo2.txt**) dove inserisco rispettivamente una lista di nomi utente con all'interno il nome utente corretto e una lista di password con quella corretta all'interno.

Ora utilizzo Hydra, potrei attaccare l'autenticazione SSH con il seguente comando, dove –l, e –p minuscole si usano se vogliamo utilizzare un singolo username ed una singola password. Ipotizzo in questo caso, di **non conoscere username e password** ed utilizzo invece delle liste per l'attacco a dizionario. Uso quindi –L, -P (entrambe in maiuscolo). con il comando:

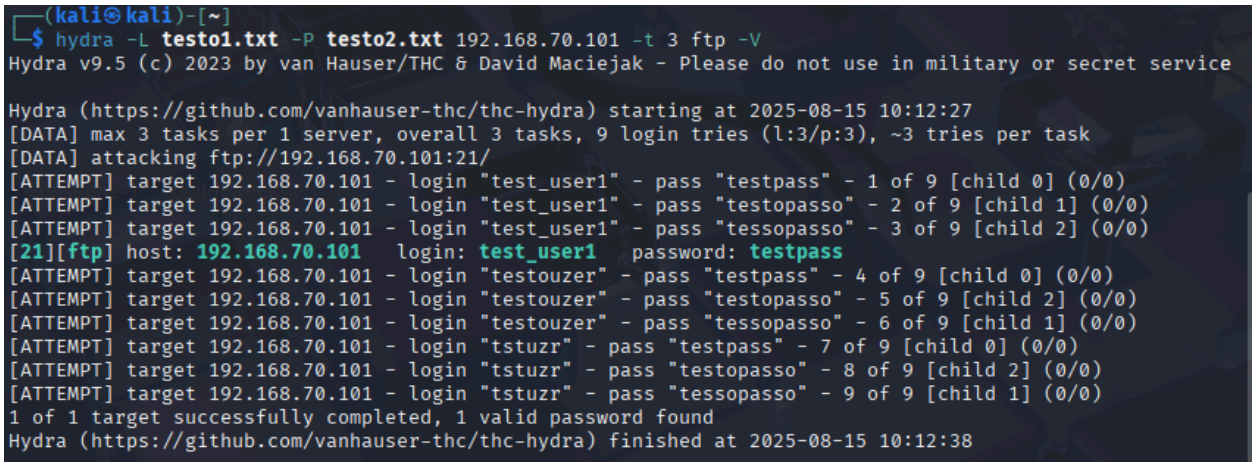
hydra -L testo1.txt -P testo2.txt 192.168.70.101 -t 3 ssh -V

Ho aggiunto -V per poter controllare “live” i tentativi di cracking di Hydra.



Possiamo notare che username e password corrette vengono trovate e sottolineate dal colore diverso e dal grassetto.

Ho eseguito lo stesso attacco per un altro servizio, per questo esercizio ho scelto **FTP**



CONCLUSIONE

Con questo esercizio ho potuto simulare un attacco di cracking utilizzando Hydra e alcune delle sue funzionalità. In particolare ho eseguito degli attacchi a dizionario sui servizi ssh e ftp con lo scopo di ottenere le credenziali di accesso dell’utente (creao in precedenza per lo svolgimento dell’esercizio). Per entrambi in servizi l’attacco è avvenuto con successo. Grazie a questo esercizio ho compreso come la complessità

delle password che scegliamo ha una forte valenza ai fini di proteggersi da queste tipologie di attacchi.