Authentication cracking con Hydra

Nel lavoro di oggi andremo a craccare l'username e la password del nostro IP di loopback. Utilizzeremo **Hydra**, un password cracker veloce e flessibile, che supporta un'ampia gamma di protocolli di rete.
La traccia è la seguente:

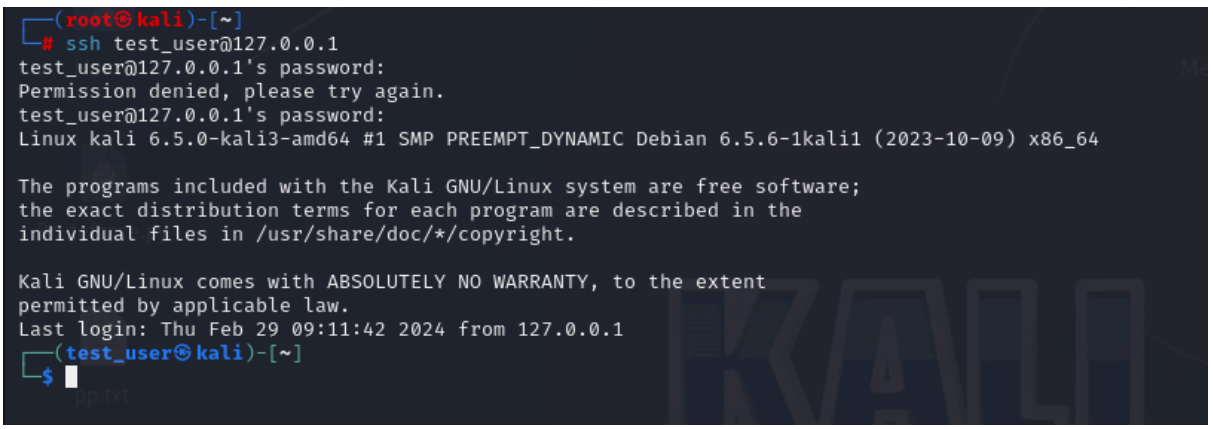
Si ricordi che la configurazione dei servizi costituisce essa stessa una parte integrante dell'esercizio.

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.

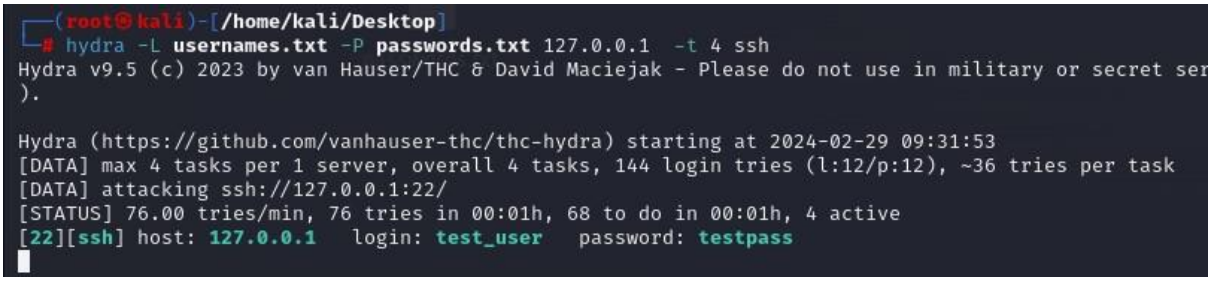
Creiamo un nuovo utente su Kali Linux, con il comando "adduser".
Chiamiamo l'utente **test_user**, e configuriamo una password iniziale come **testpass.**
Attiviamo il servizio ssh con il comando "**sudo service ssh start**".

Dopo aver seguito questi passaggi, scriviamo il comando **ssh test_user@127.0.0.1** per verificare se il secondo utente su kali è stato creato e raggiunto con successo.



Il secondo step da seguire prevede di eseguire hydra tramite codice per riuscire a craccare le credenziali corrette. In questo caso utilizzeremo **“hydra -L username_list -P password_list IP_KALI -t 4 ssh”**

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**.
Utilizziamo delle liste compilate con poche righe per evitare tempi eccessivi di cracking.



Installiamo il servizio ftp con il comando **“sudo apt-get install vsftpd”** e facciamolo partire.
Proviamo a craccare sul servizio ftp. Quindi riscriviamo il codice uguale cambiando ssh con ftp.