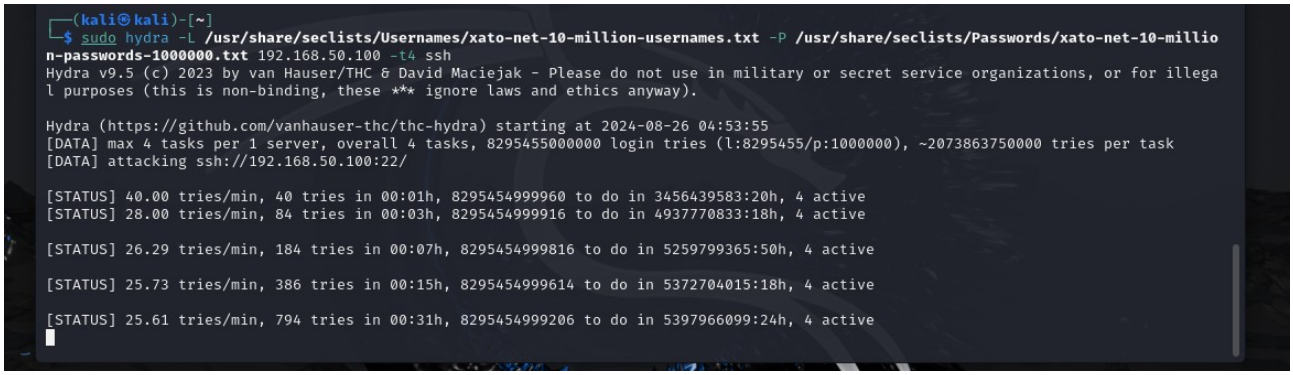
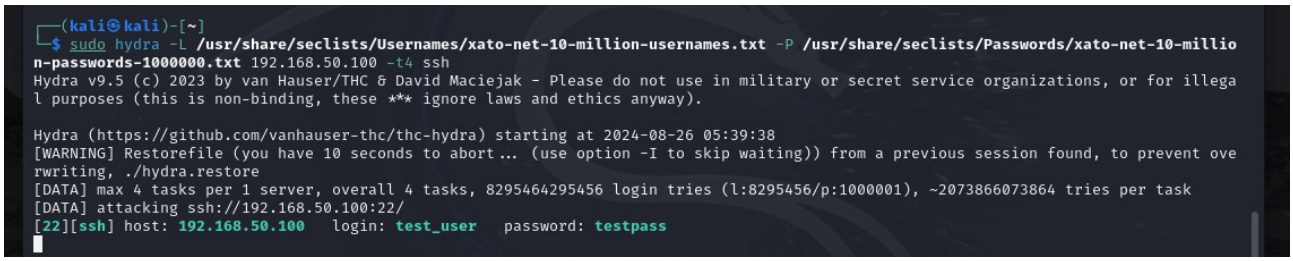
Consegna week 14 day 4 – Daniele Rufo

HYDRA

Ho seguito la parte guidata dell'esercizio configurando il server ssh e connettendomi con il nuovo utente creato su kali (test_user).
Ho quindi lanciato l'attacco con hydra. Ad un certo punto l'ho interrotto (dopo oltre 30 minuti) perché il processo era lunghissimo. Anche se c'era da aspettarselo ho modificato i due file inserendo username e password del server ssh per facilitare l'azione di cracking e renderla breve ai fini dell'esercizio.



Si vede chiaramente dai vari STATUS che il processo completo avrebbe preso molto tempo.
Dopo la modifica invece restituisce i valori quasi immediatamente come si evince dallo screen sottostante.



Ho poi proseguito con il resto dell'esercizio configurando il servizio ftp. Come avvenuto per l'ssh ho usato hydra per il password cracking. Le credenziali sono state trovate subito perché ho scelto i file già usati in precedenza. È naturale pensare che in un ambiente reale il processo impieghi molto tempo. La rapidità con cui hydra lavora in questo caso è frutto dell'artificio che ho creato modificando i file degli user e delle password usati per questo attacco.
Questo procedimento può essere usando per tentare un password cracking su diversi servizi. Cambia leggermente la sintassi di hydra(già dagli screen notiamo la differenza tra un attacco rivolto a ssh o ftp), ma il ragionamento generale dietro gli attacchi rimane lo stesso.

Grazie