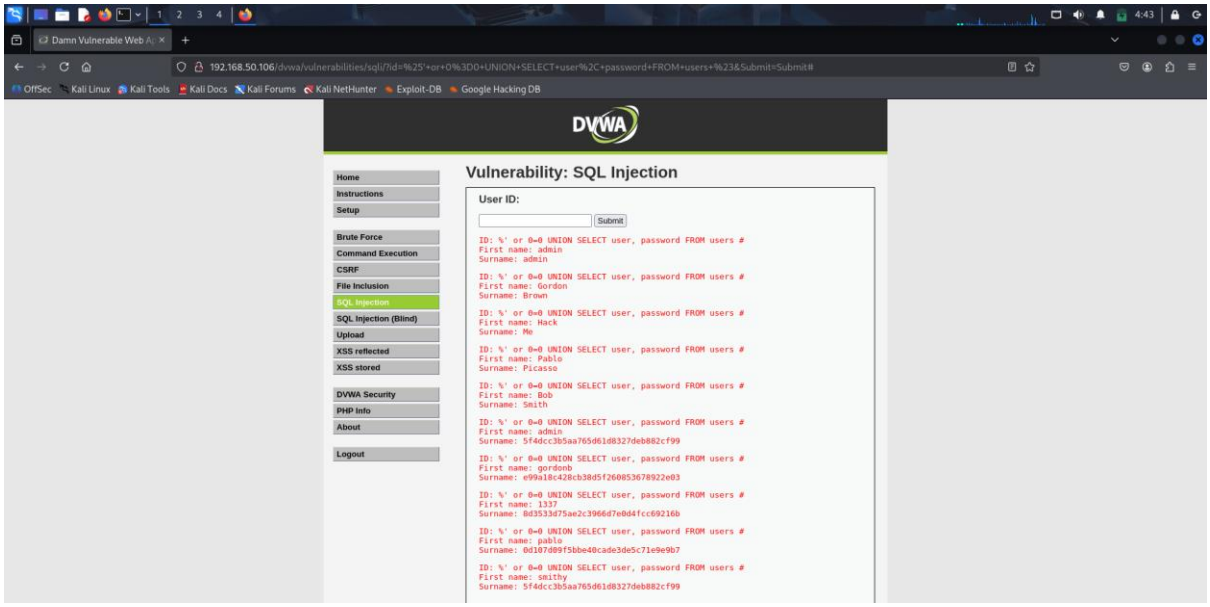
W14D1 – JOHN THE RIPPER

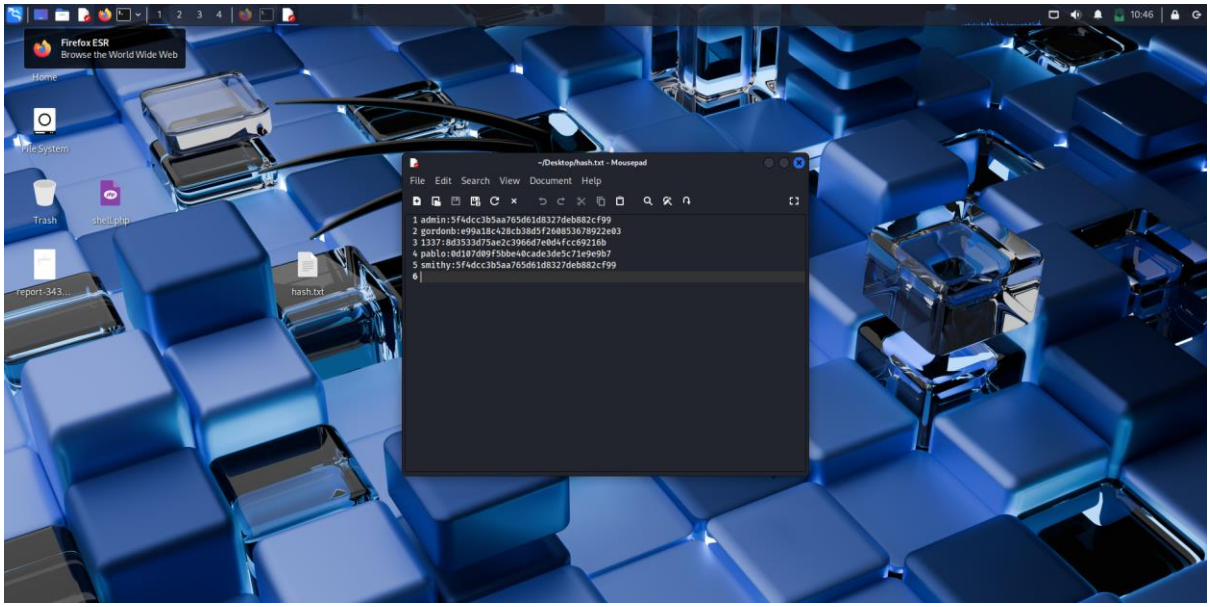
Con l'utilizzo della DVWA impostata su un livello low si effettua una SQL injection con l'uso del payload %' or 0=0 UNION SELELCT user, password FROM users#

che restituisce l'elenco di users e password criptate di determinati utenti.

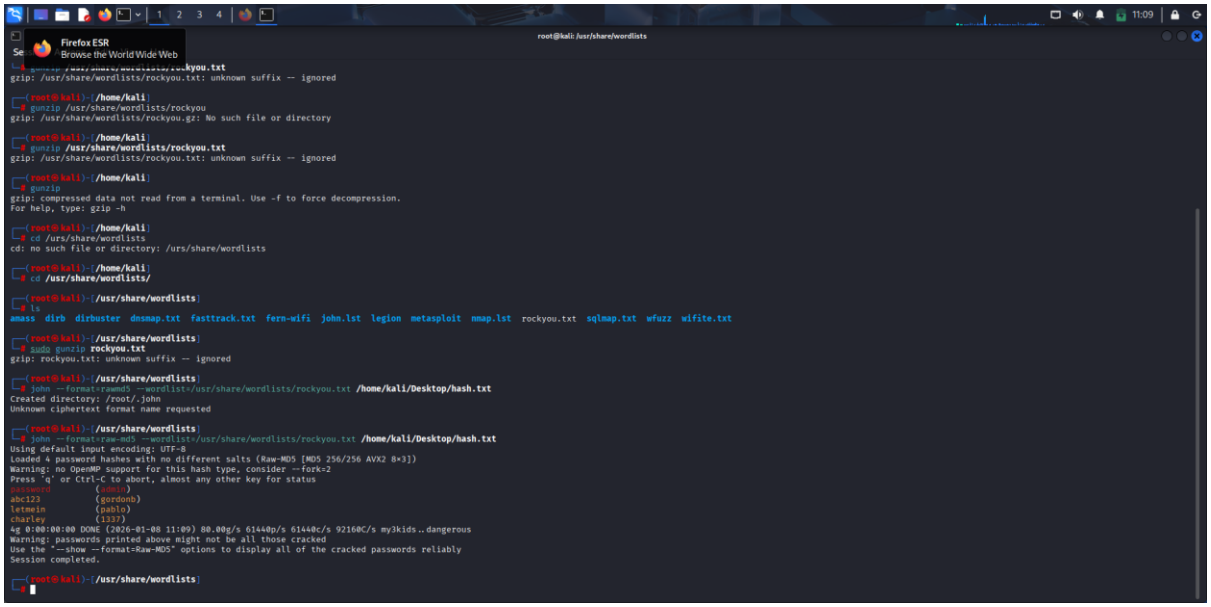


Come è facile notare le password non sono in chiaro bensì risultati di hash di password.

Si va successivamente a creare un file .txt in cui si inseriscono admin e password ottenuti che servirà per utilizzare il tool John the Ripper e Per recuperare le versioni in chiaro delle passwords.



john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Desktop/hash.txt



Completata la sessione dopo l'attivazione del tool e la creazione del file contenente gli hash delle password in md5, otteniamo come risultato le password in chiaro. John the ripper utilizza la wordlist rockyou contente un elenco di password note e per ogni parola contenuta nella wordlist il tool effettua la trasformazione in hash poi fa il paragone con l'hash che gli è stato passato dall'utente per verificare il match.

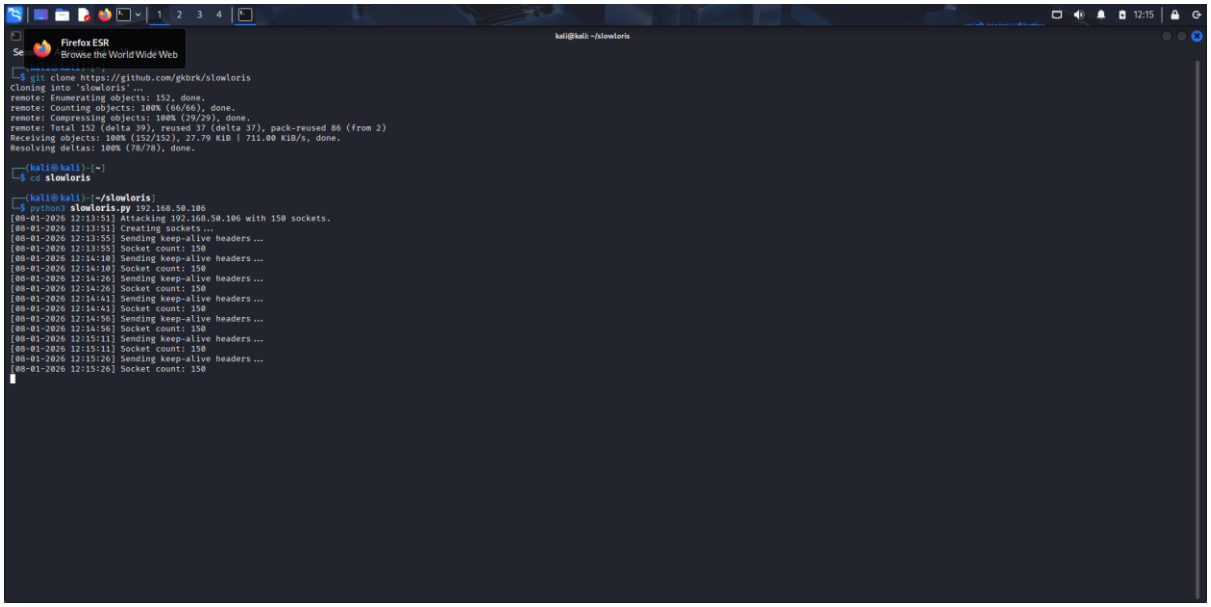
ESERCIZIO EXTRA: slowloris

git clone https://github.com/gkbrk/slowloris

Si procede ad avviare il tool e a lanciare l'attacco DOS sulla meta con il comando

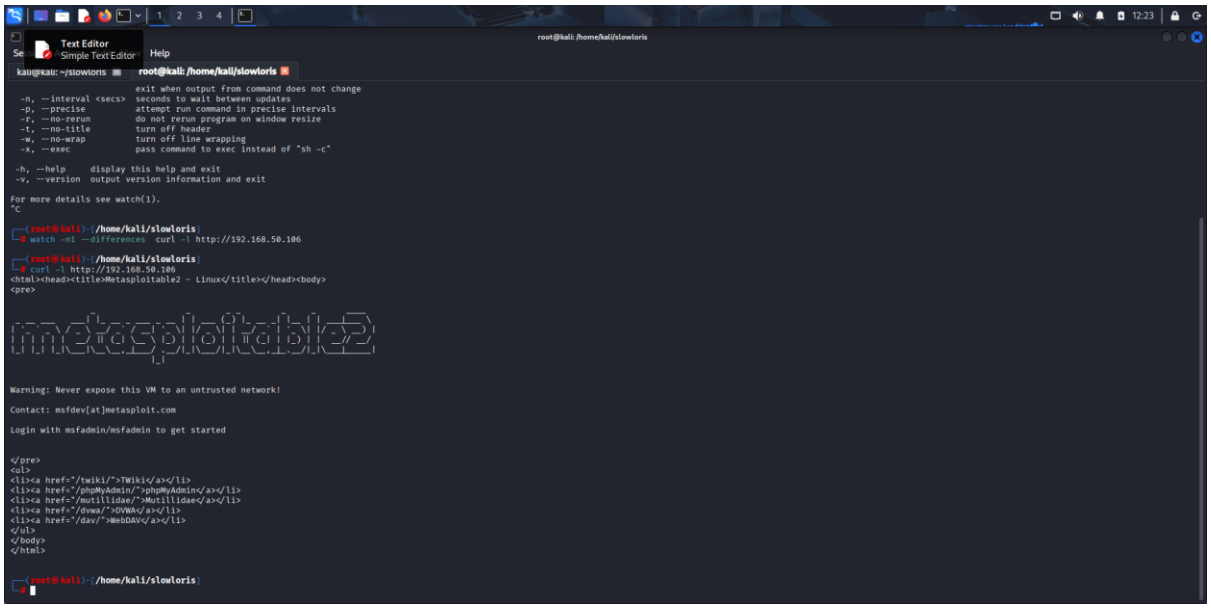
python3 slowloris.py 192.168.50.106

Si può testare l'attacco andando su un altro tab e lasciando in esecuzione il comando appena avviato.



Per vedere le risposte in tempo reale e la connettività http si utilizza il comando

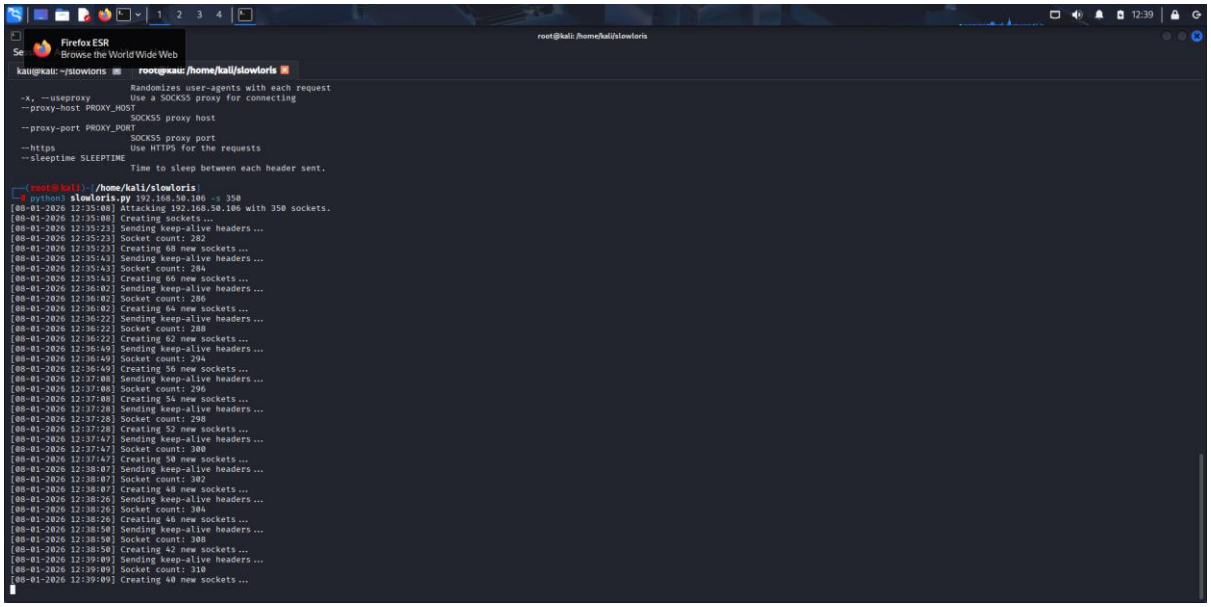
watch -n1 --differences | curl -l http://192.168.50.106; allo stesso tempo interrompendo il dos in esecuzione sull'altro tab si ha come risultato la risposta attesa.



Otteniamo l'interfaccia che si otterrebbe da browser perchè l'attacco è stato lanciato con una CURL (call url).

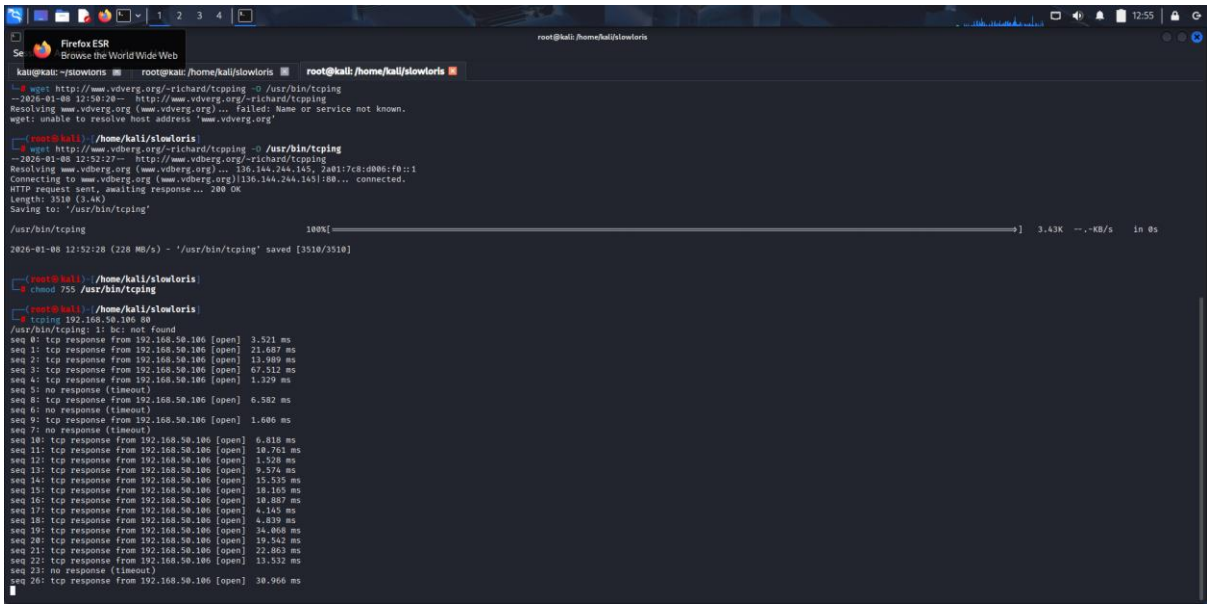
Per andare a stressare ancora di più la macchina utilizziamo il seguente comando per l'invio di 350 socket.

python3 slowloris.py 192.168.50.106 -s 350

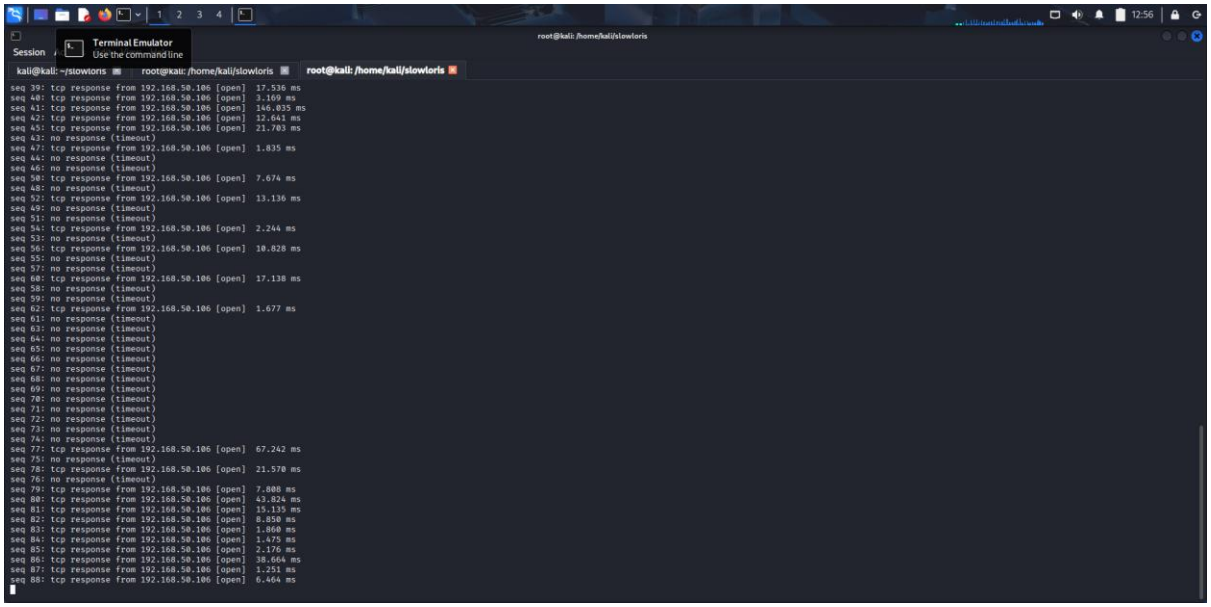


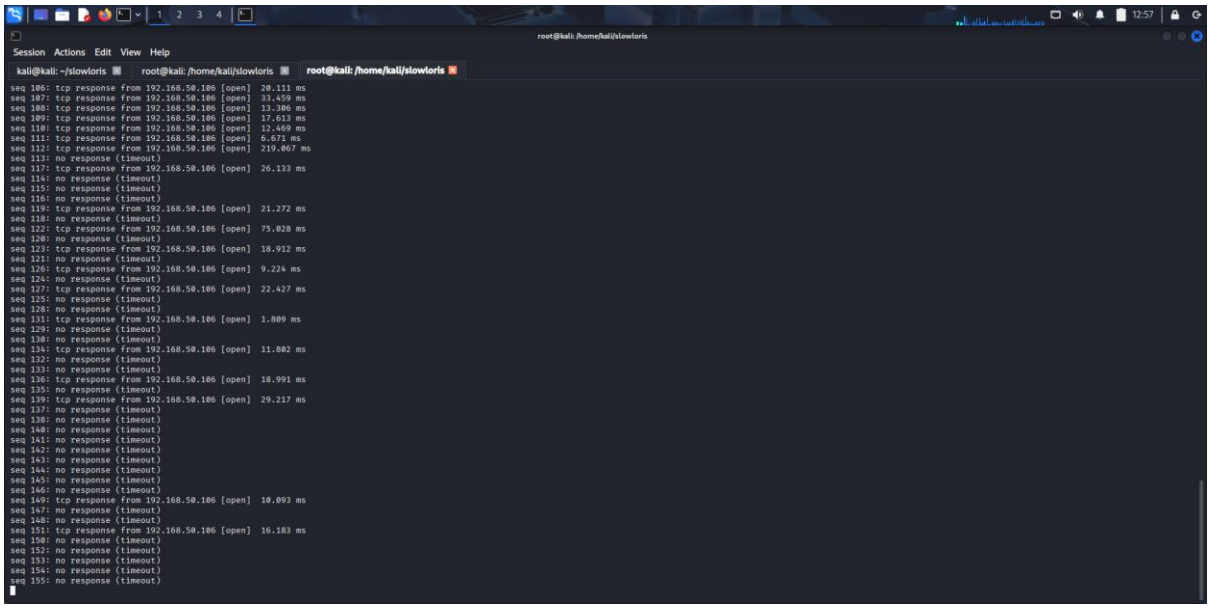
Come attività finale si effettua il controllo della connettività tcp sulla porta 80 con il tool tcping

Tcping 192.168.50.106 80



Le risposte iniziano ad arrivare in leggero ritardo





Fino ad arrivare ad un timeout della meta.