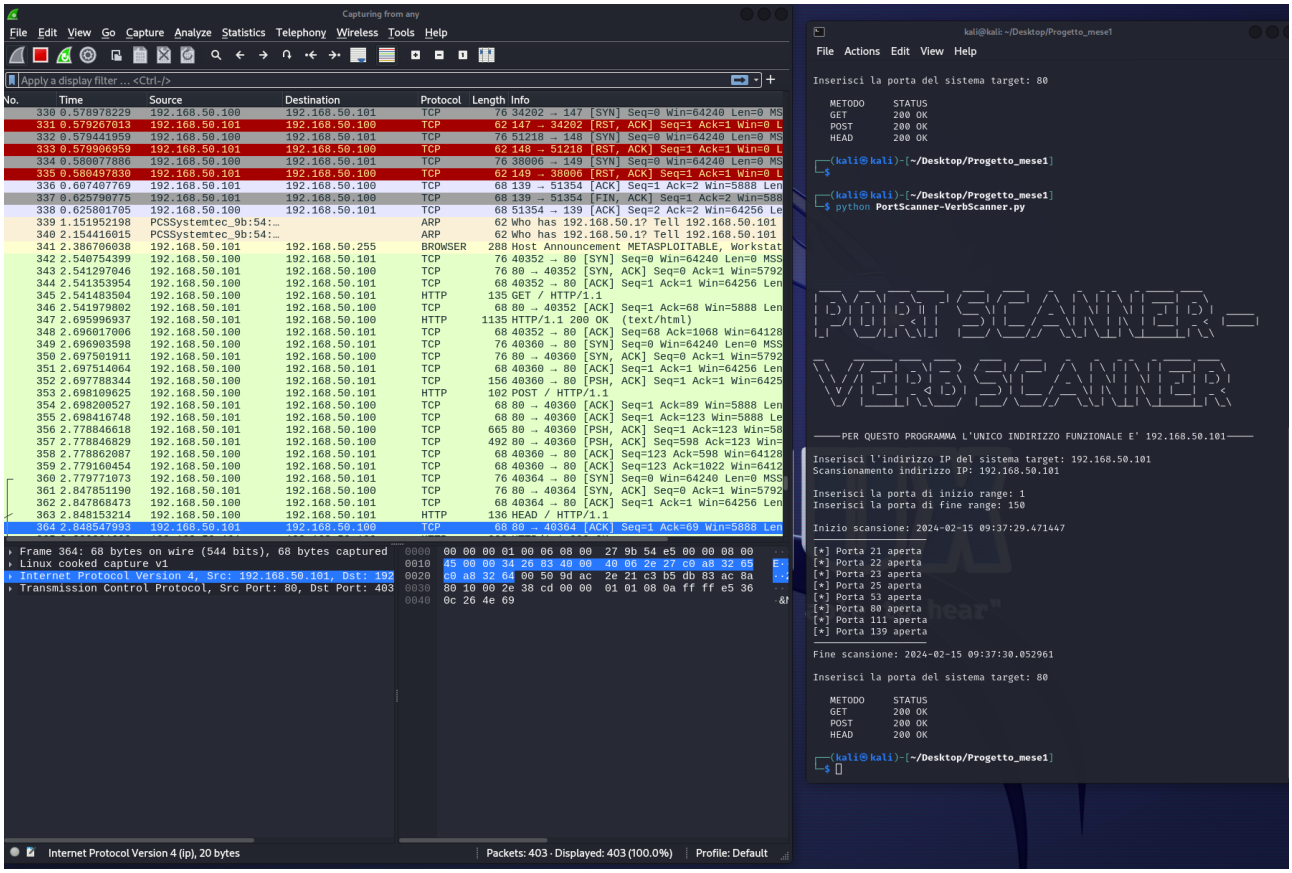
Port Scanner e Verb Scanner

(Schermata del codice in esecuzione)

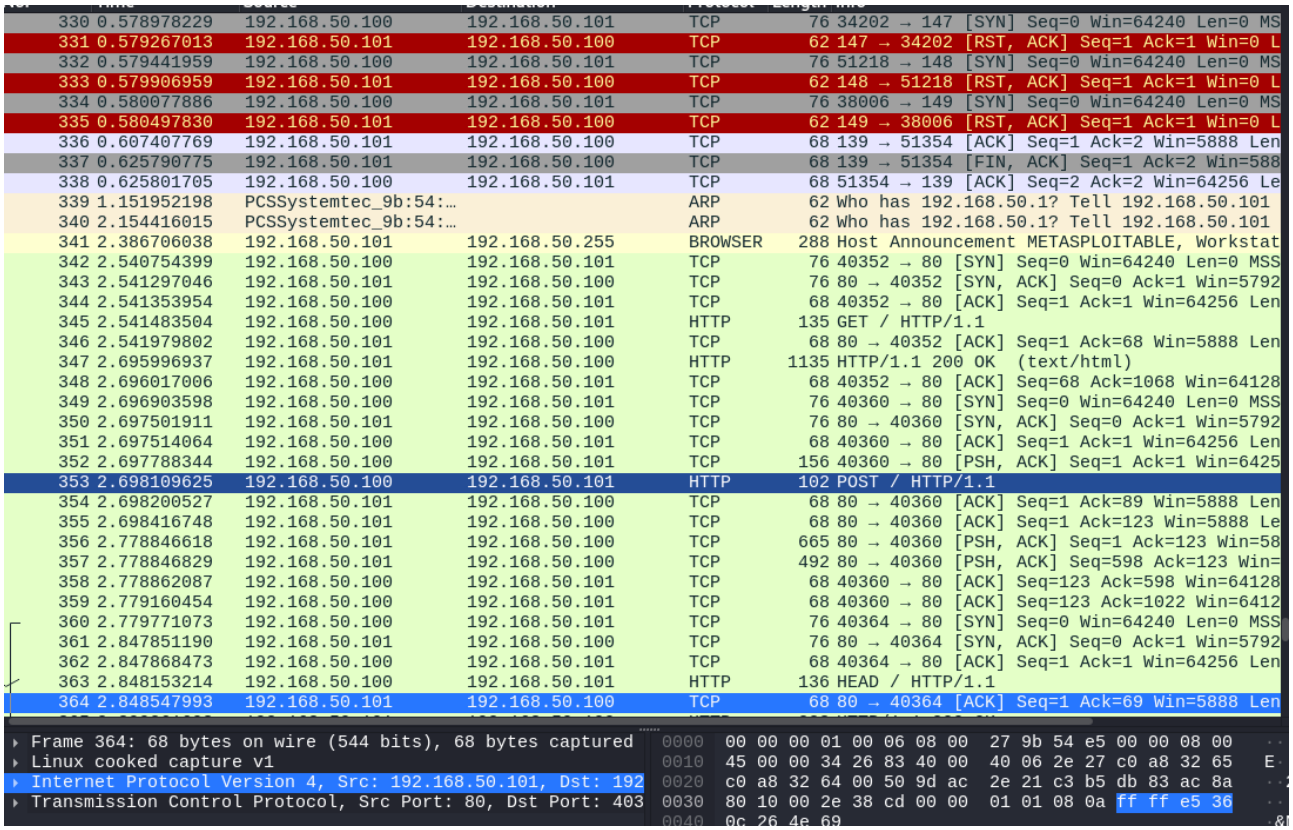
Una funzione avanzata alla quale abbiamo pensato e sviluppato è stata semplicemente pensare alla user experience. Abbiamo lavorato seguendo questo modello per facilitarne l'utilizzo. I codici sviluppati singolarmente ""Scanner delle porte" e "Enumerazione dei metodi HTTP" sono stati quindi uniti per migliorarne l'esperienza d'uso.

Il codice inizia chiedendo all'utente di inserire un indirizzo IP (che in questo specifico caso è solo quello specificato a inizio del programma, in quanto viene indicato per la macchina di Metasploitable) e quale range di porte vuole scansionare. Una volta trovate le porte aperte selezioniamo quella su cui vogliamo lavorare (che nel nostro caso specifico è la porta 80) per poi lanciare una serie di richieste di GET, POST e HEAD, facendoci visualizzare se la connessione è andata a buon fine e il relativo status. Questo poi ci permetterà di concentrarci sull'attacco Brute Force da eseguire nella fase successiva essendo già a

conoscenza dei metodi che possiamo utilizzare per comunicare con la porta aperta precedentemente rilevata.



(Nella parte sinistra della foto sopra Wireshark che ci conferma l'invio dei pacchetti lanciati dal programma che possiamo vedere in esecuzione nella parte destra della foto)



(Nella foto sopra Wireshark che conferma l’invio dei pacchetti con relativo metodo GET, POST ed HEAD verso la porta 80)