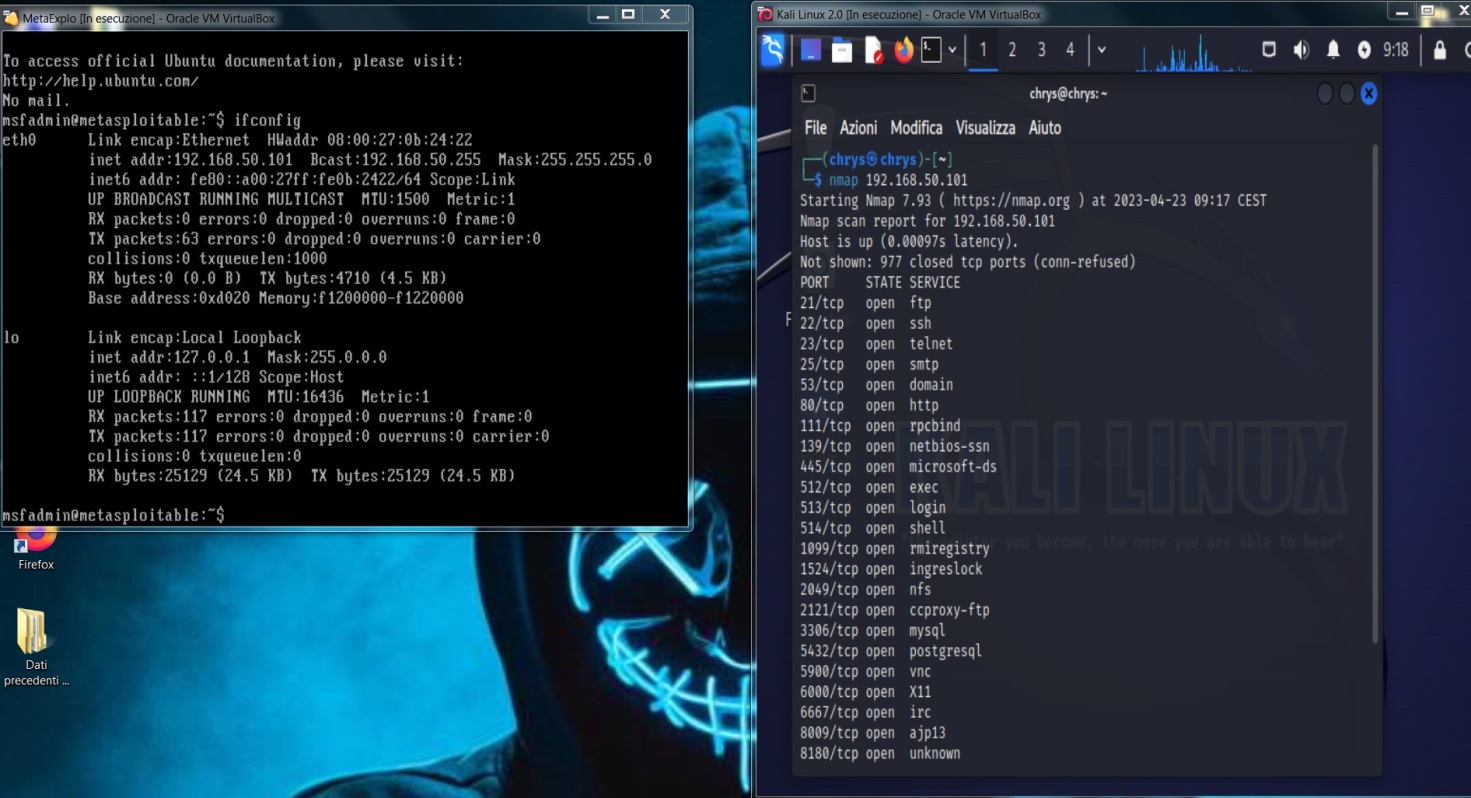
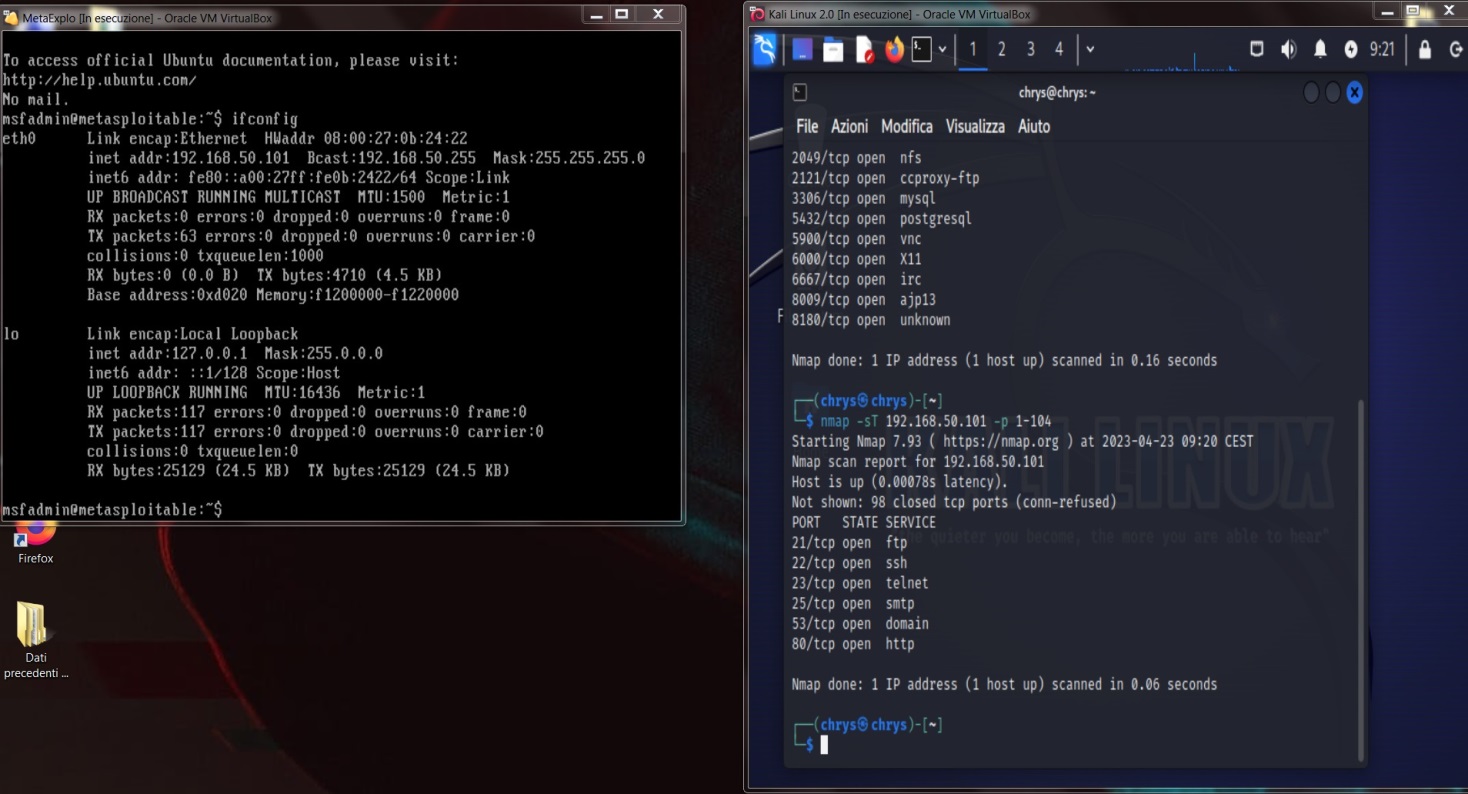
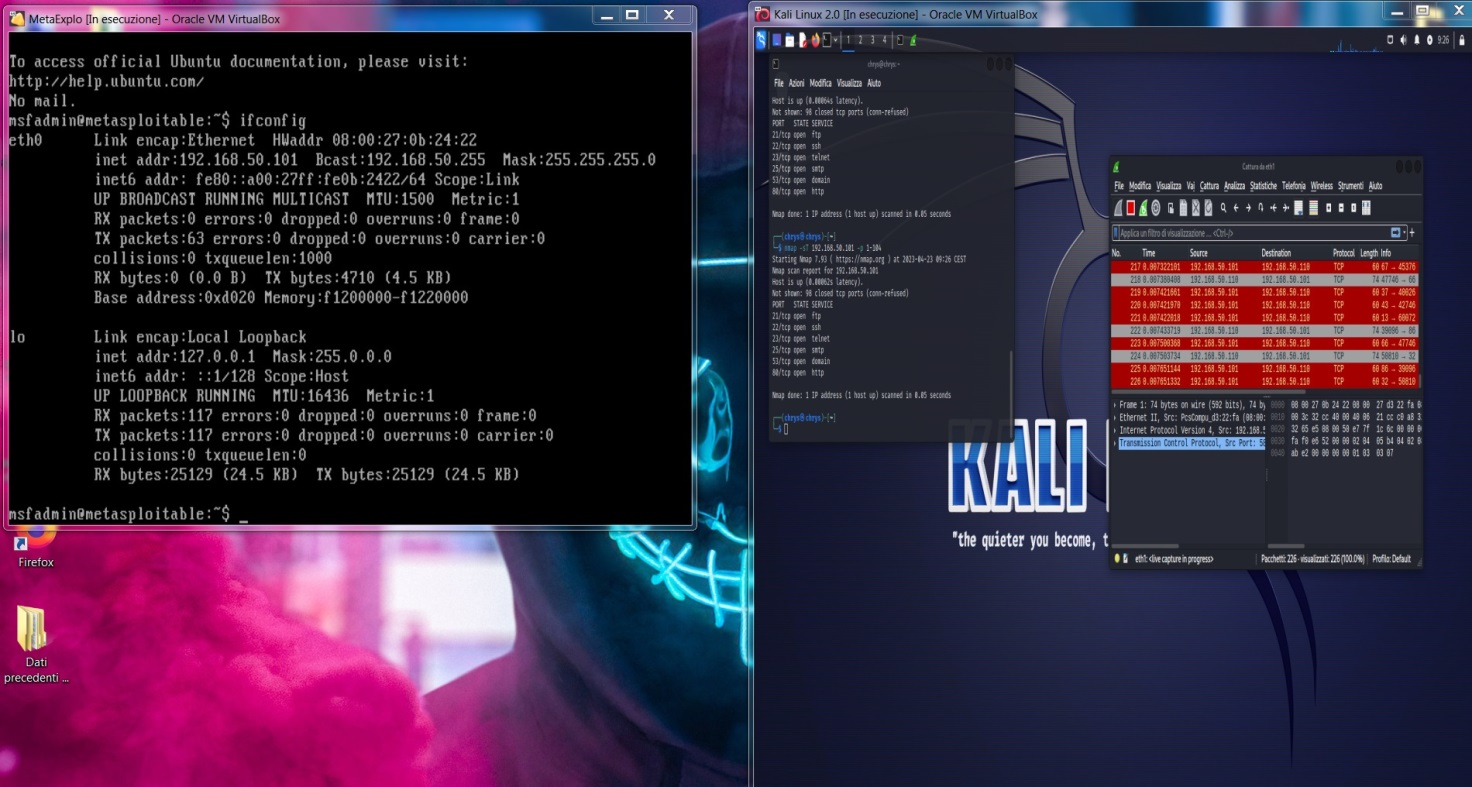
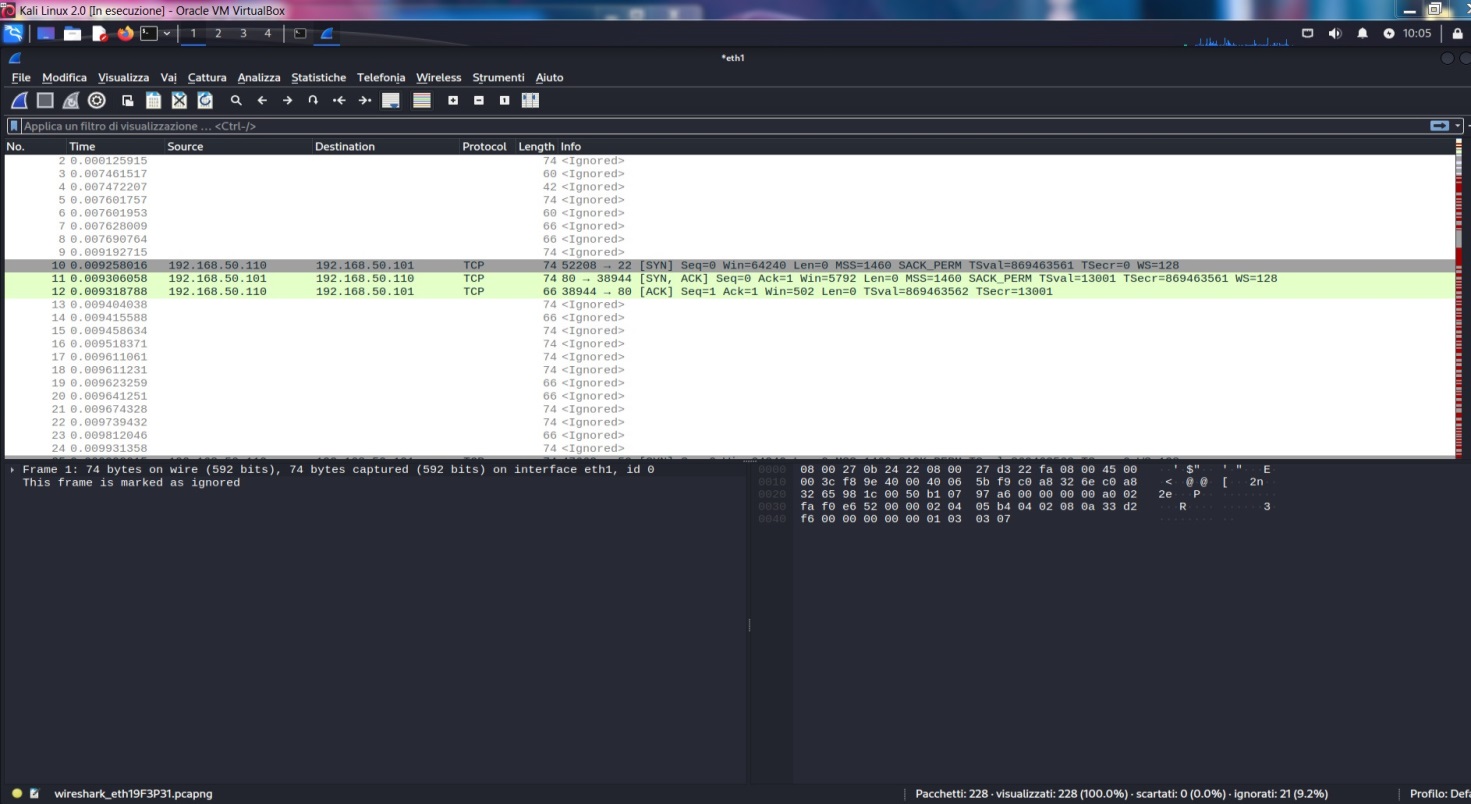
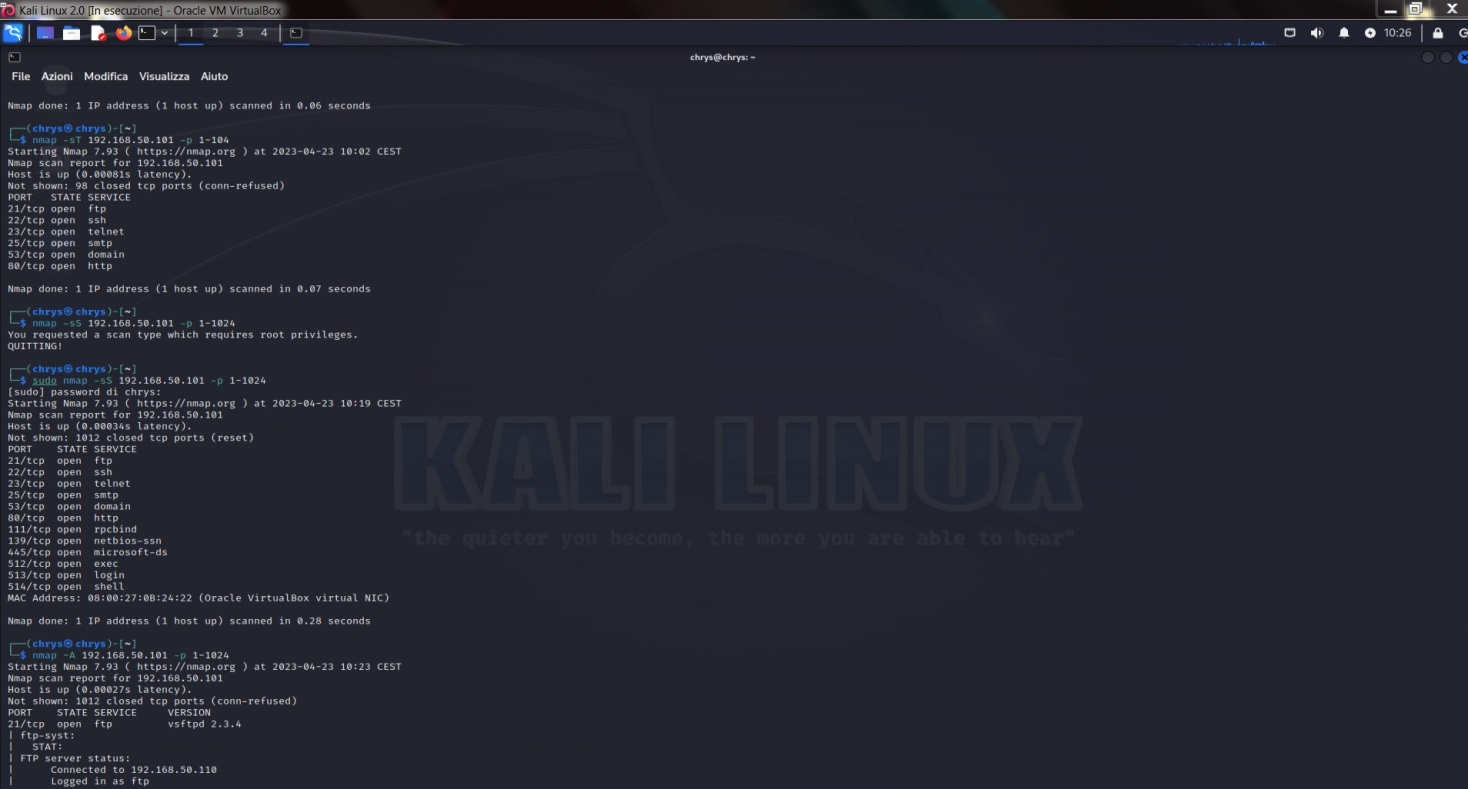
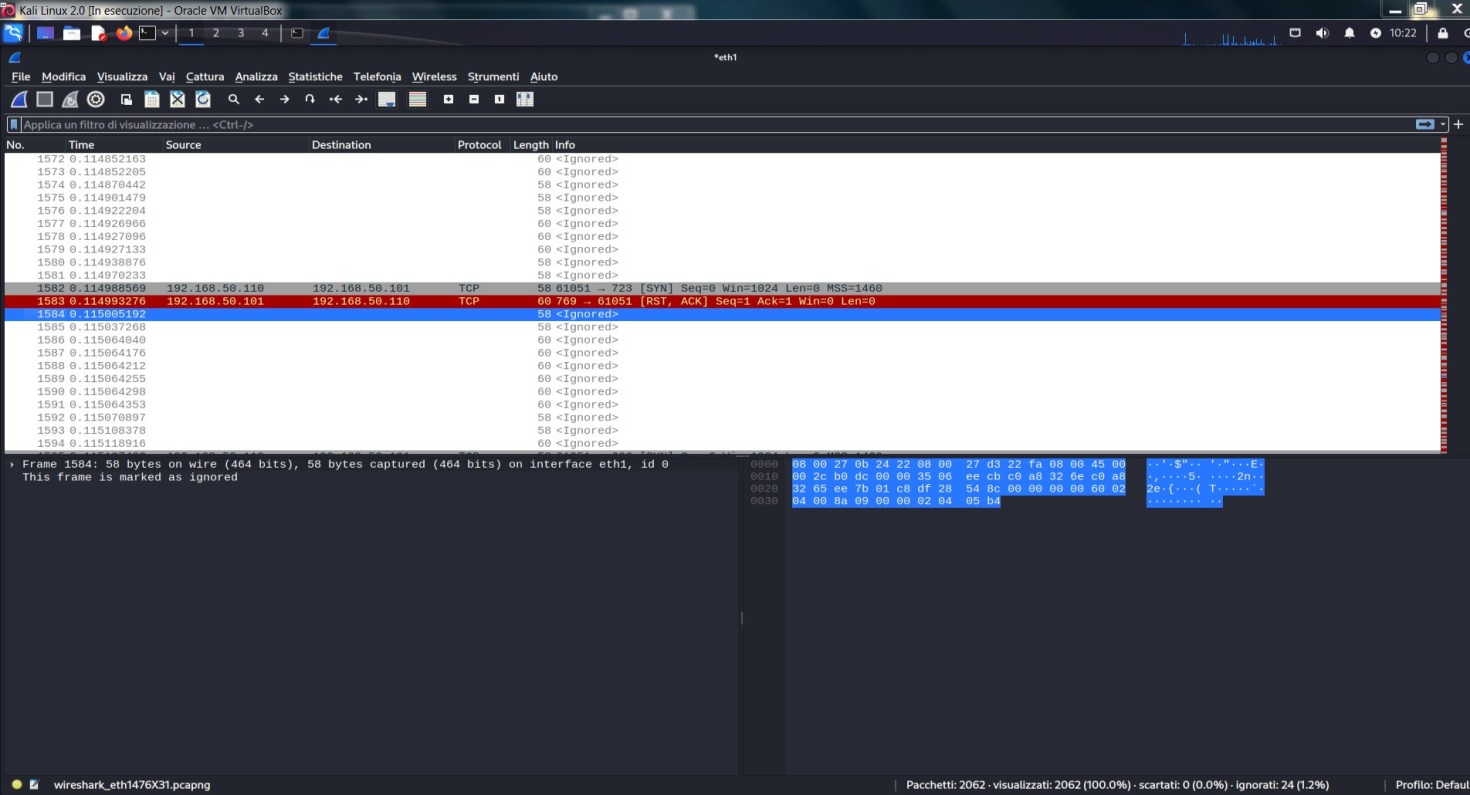
Esercizio all utilizzo del tool Nmap di Kali attraverso la comunicazione fra la macchin Kali e Meta con i flag: -sT, -sS”default” e –A.

1. Avvio ricerca porte attive su Meta attraverso “Nmap” di Kali.
2. Avvio scansione sull IP della macchina Meta con l utilizzo del flag ‘ –sT’ per effettuare una ricerca invasiva con il metodo 3 Way Handshake.
3. Controllo della trasmissione tra le 2 macchine attraverso la verifica dell ‘ invio/ricezione’ pacchetti con l utilizzo del tool WireShark.



1. Ricerca della trasmissione 3 Way Handshake tra i pacchetti inviati attraverso le sigle: SYN, SYN ACK, ACK.
2. Avvio scansione sull IP della macchina Meta con l utilizzo del flag: -sS “di base è di default”, questa tipologia di ricerca sarà meno invasiva e meno dettagliata.
3. In questo caso la macchina attaccante interrompe la comunicazione con il target dopo aver ricevuto una risposta.
4. Scansione sull IP della Macchina Target con l utilizzo del flag: -A. Questo tipo di scansione ci permette di ottenere più informazioni sulla MT quali “ versione del sistema operativo e servizi aperti disponibili”. Con questo flag la scansione risulta puù produttiva ma più lenta e con una comunicazione più lunga con la MT.