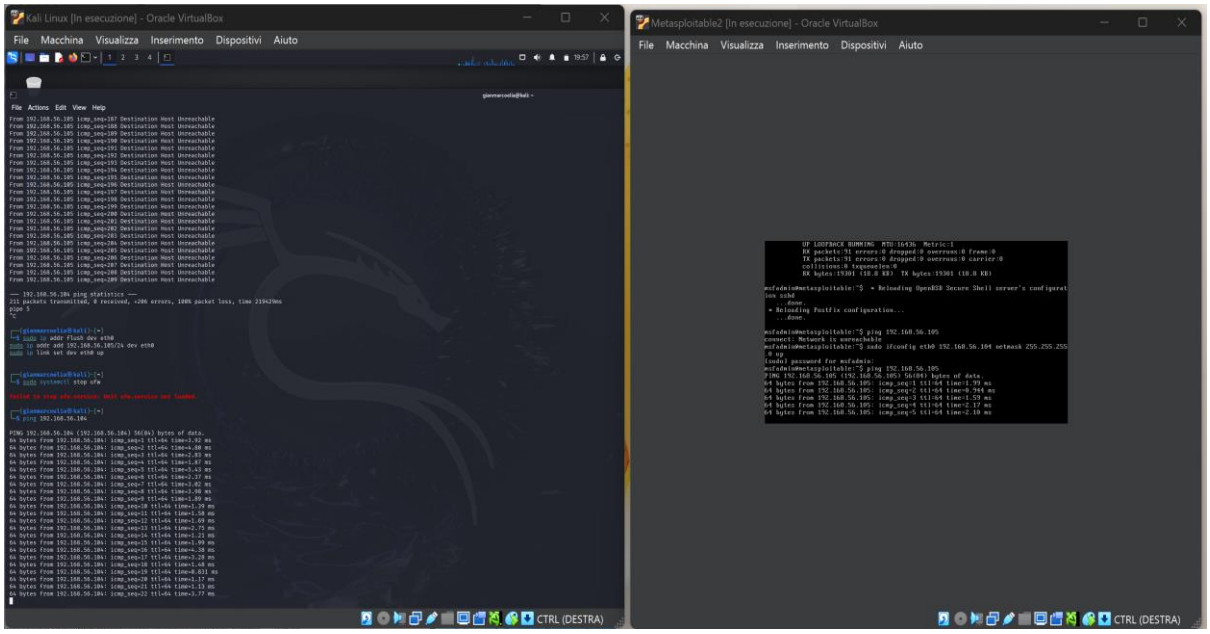
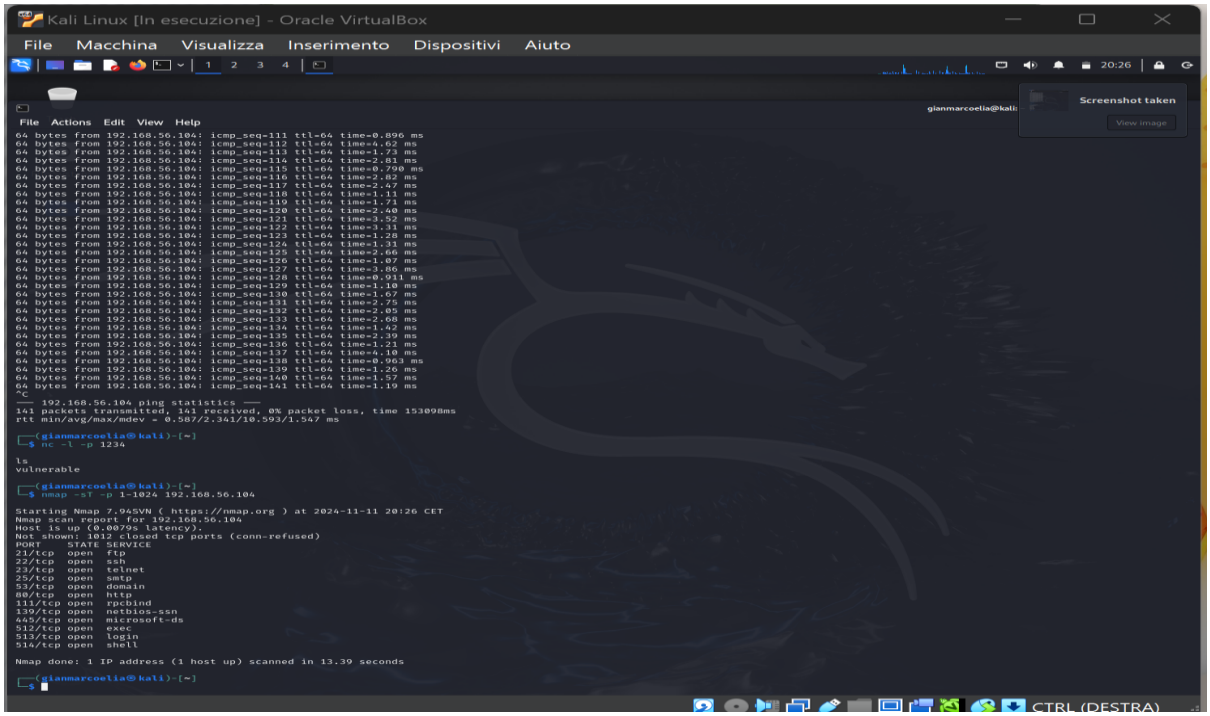
Gianmarco Elia – W9D1

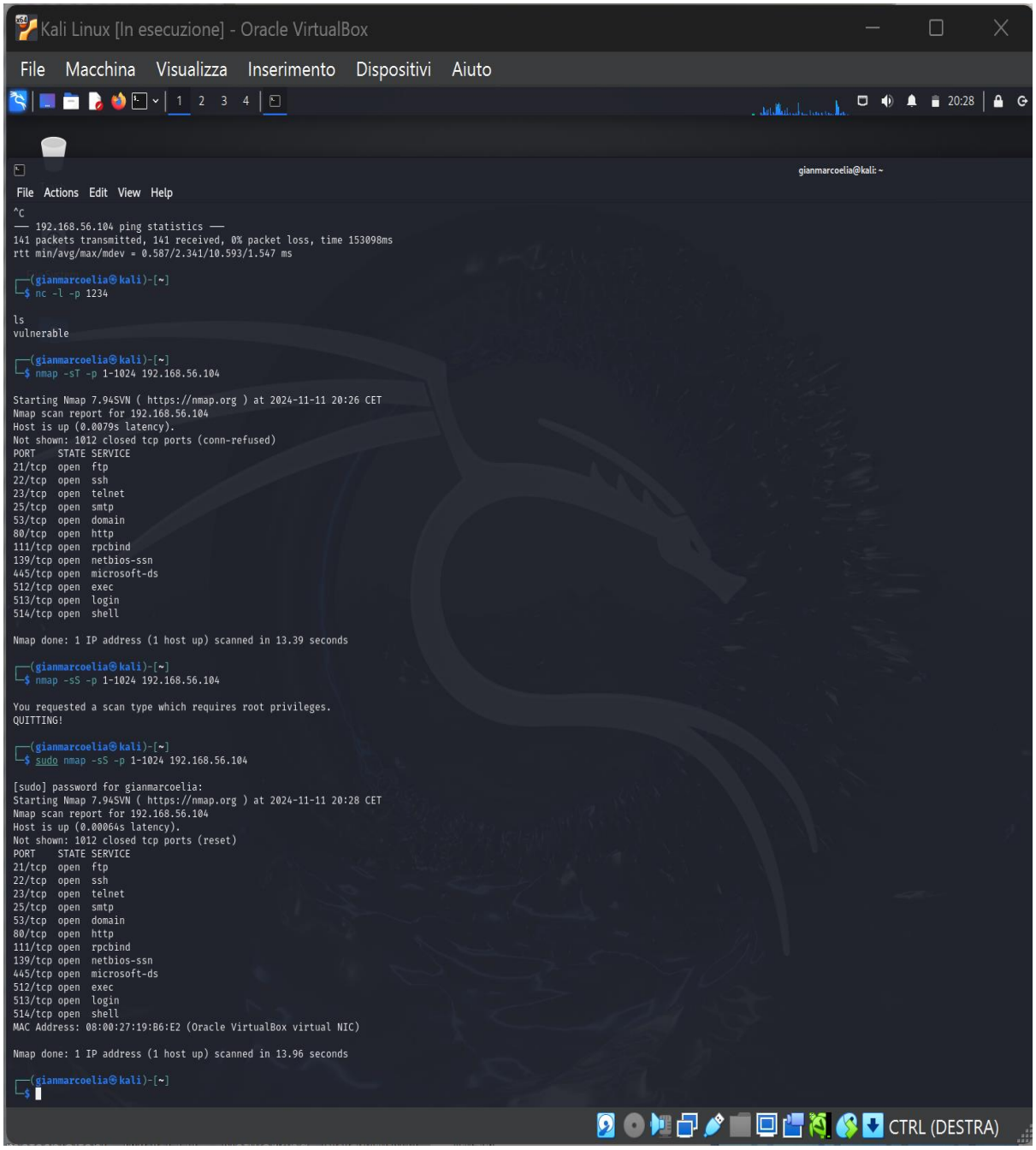
Innanzitutto si mette in comunicazione Kali Linux con Metasploitable2:



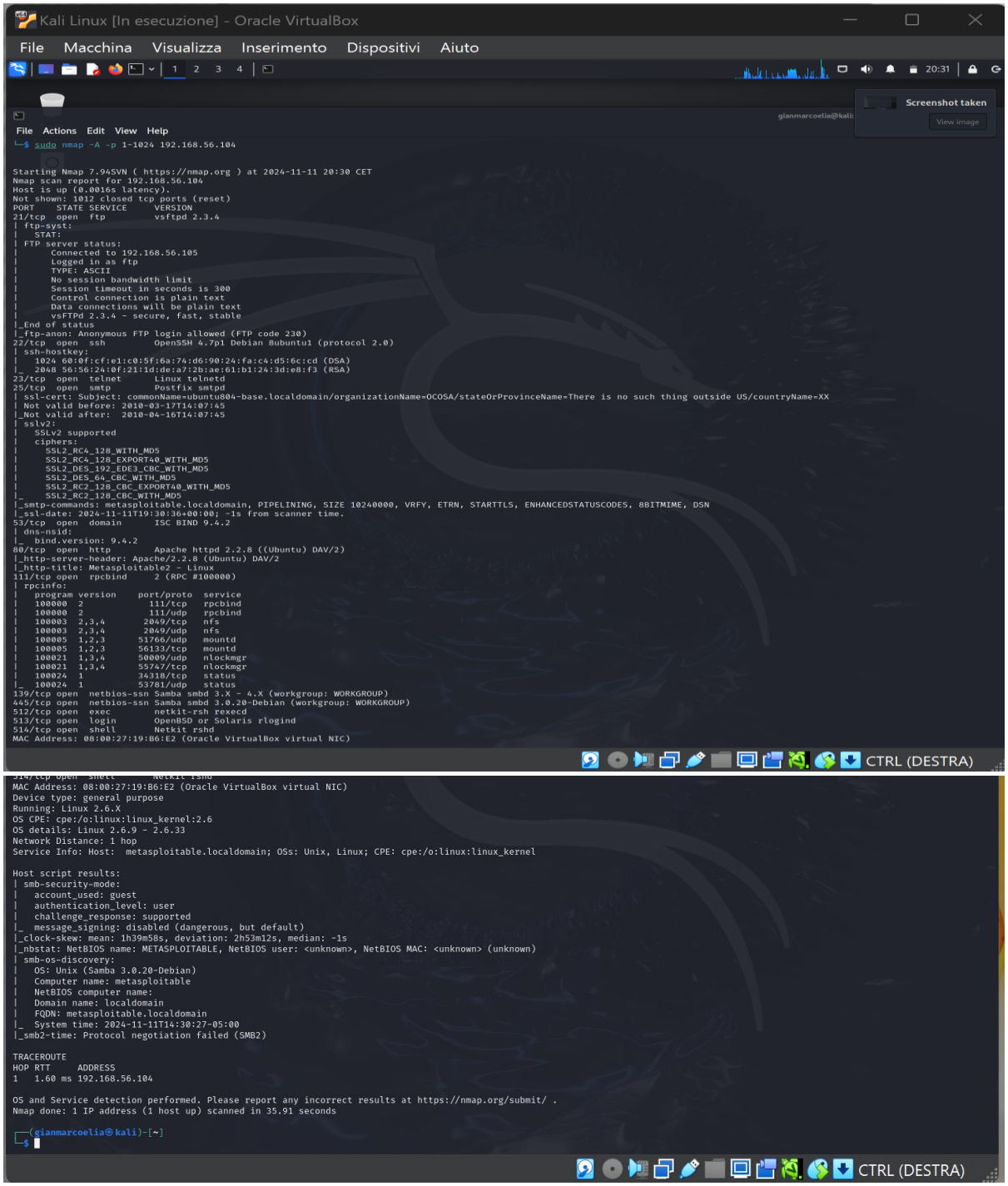
Scansione TCP sulle porte well-known:



Scansione SYN sulle porte well-known:



Scansione con switch –A sulle porte well-known:



Ho configurato una rete interna tra Kali Linux e Metasploitable2 su VirtualBox e verificato la connessione tramite ping. Successivamente, ho eseguito varie scansioni con nmap per rilevare le porte aperte su Metasploitable2. Ho iniziato con una scansione TCP completa (`nmap -sT`), identificando i servizi attivi sulle porte well-known. Poi, ho eseguito una scansione SYN (`nmap -sS`) per visualizzare le porte aperte senza stabilire una connessione completa. Infine, ho utilizzato Wireshark per confrontare i pacchetti catturati: nella scansione TCP completa si osserva il three-way handshake (SYN, SYN-ACK, ACK), mentre nella scansione SYN il processo si interrompe dopo il SYN-ACK. Tutte le scansioni sono andate a buon fine.