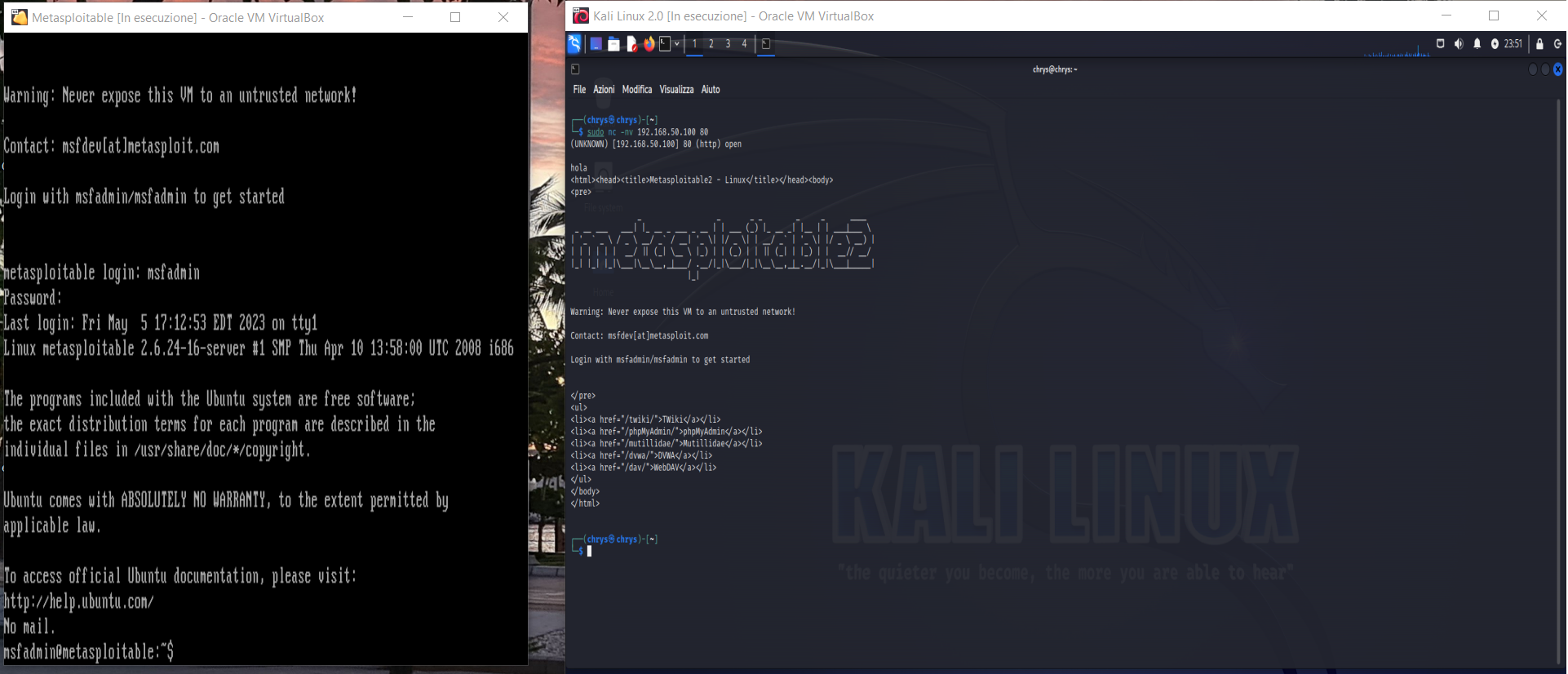
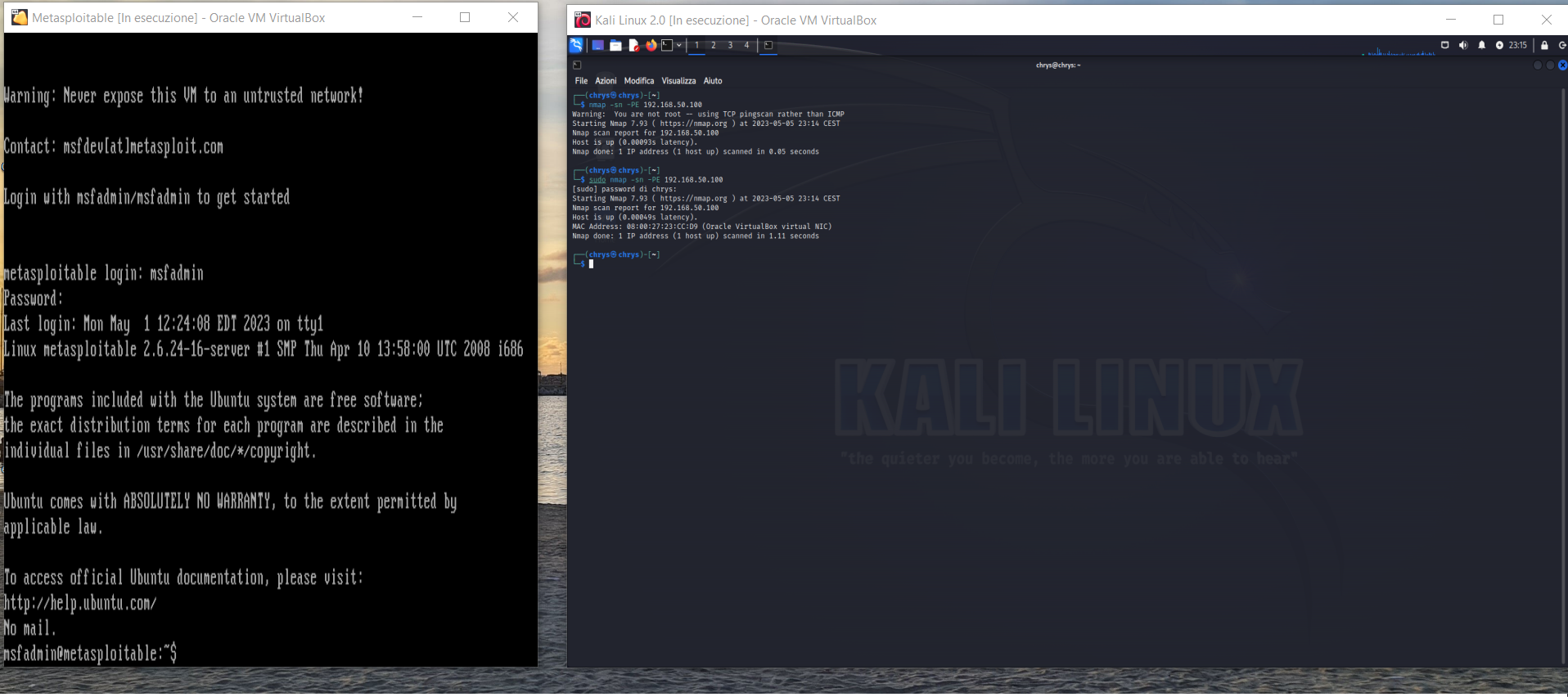
1) Comando netcat nc -nv con porta.

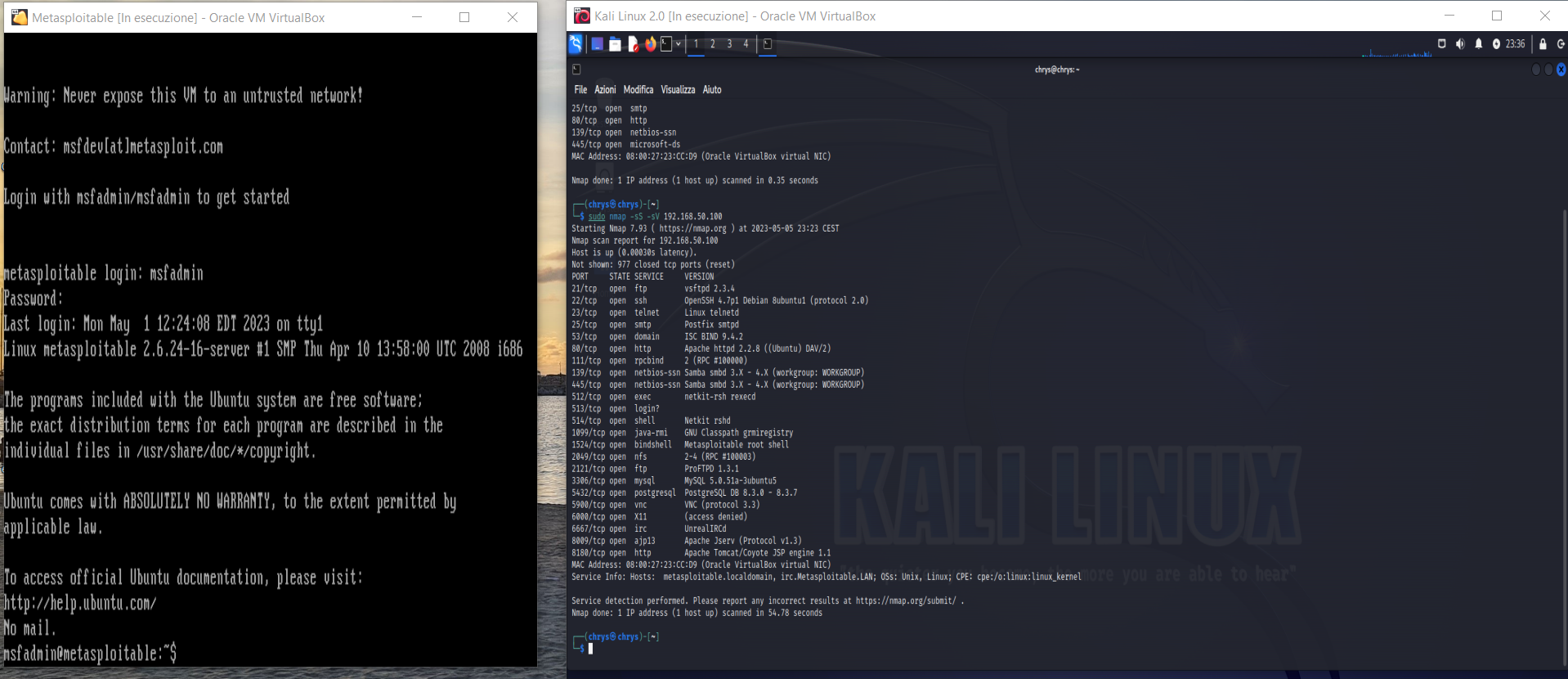
Il comando ci mostra lo stato della porta selezionata + il fingerprinting della macchina e la versione.

2) Comando nmap -sn –PE.



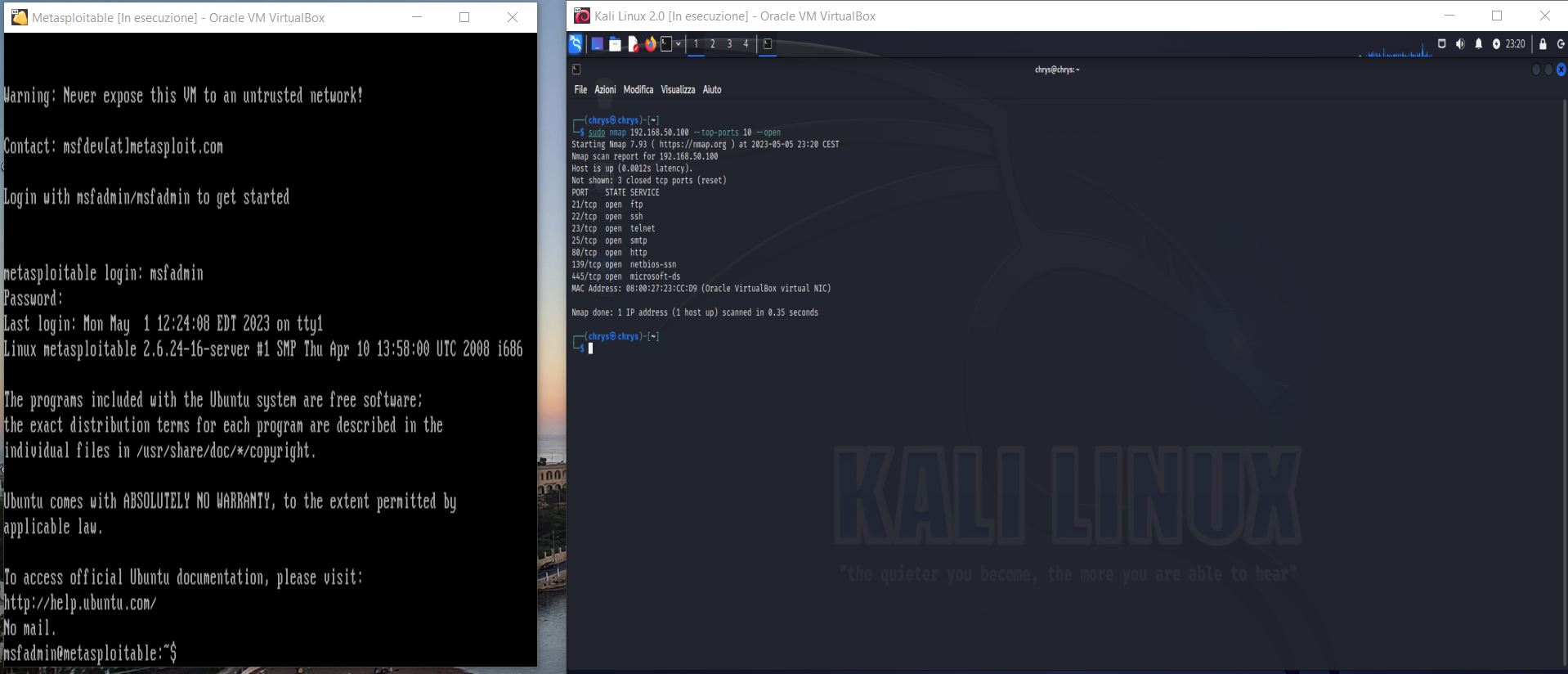
* L'opzione "-sn" indica a Nmap di effettuare una scansione ping sweep, cioè di inviare un pacchetto ICMP echo request a tutti gli host nella rete specificata per determinare quali host sono attivi.
* L'opzione "-PE" indica a Nmap di utilizzare il metodo di sondaggio di tipo Ping ICMP Echo per determinare se un host remoto è raggiungibile.

3)Comando nmap –sS –sV.



* L'opzione "-sS" indica a Nmap di effettuare una scansione TCP SYN, cioè di inviare un pacchetto TCP SYN a una porta specifica dell'host remoto per determinare se la porta è aperta, chiusa o filtrata dal firewall.
* L'opzione "-sV" indica a Nmap di eseguire la rilevazione della versione del servizio, cioè di identificare il servizio e la versione del software in esecuzione su ogni porta aperta.

4)Comando nmap –top –ports 10 –open.

Il comando ci restituisce le prime 10 porte aperte.