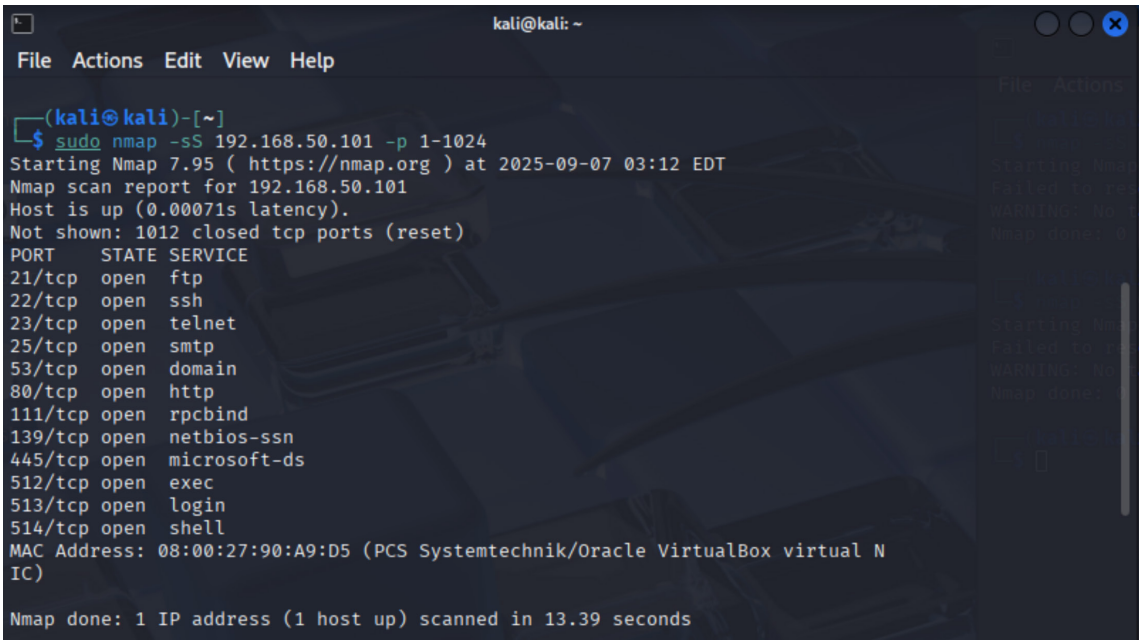
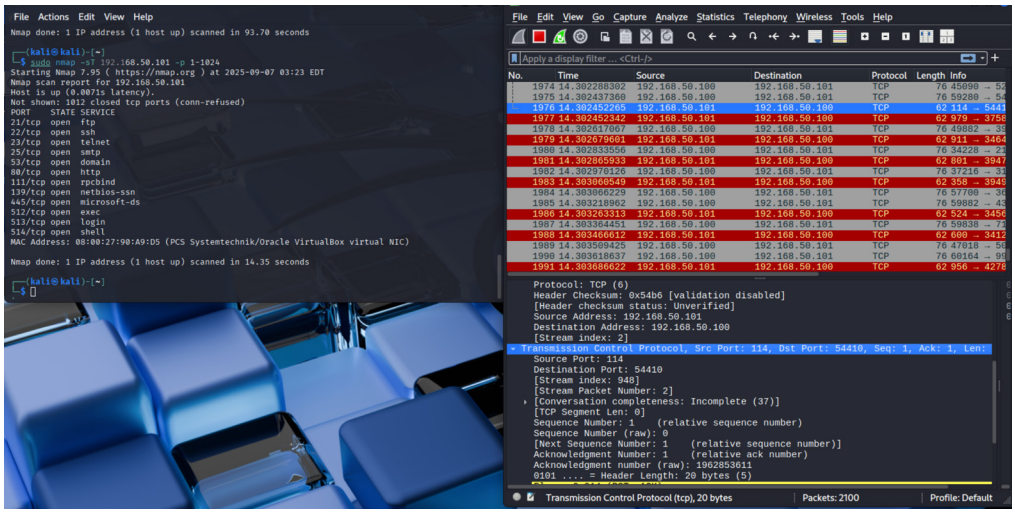
W9D1

Scanzione della rete di un IP tramite nmap.
La scanzione con nmap fornisce numerose informazione iniziali per individuare potenziali vulnerabilità.

nmap -sS
Metodo di scansione che permete di vedere le porte e il tipo. Si può vedere che le porte sono aperte in questo caso per cui potenzialmente vulnerabili



Con Wireshark è possibile vedere le richieste e le risposte e catturarne il traffico



nmap -A

Metodo di scansione che permete di vedere molte informazioni e potenziali vulnerabilità, il sistema operativo, servizi (ssh, https, http, mysql..), traceroute (tracciamento rotte) e script