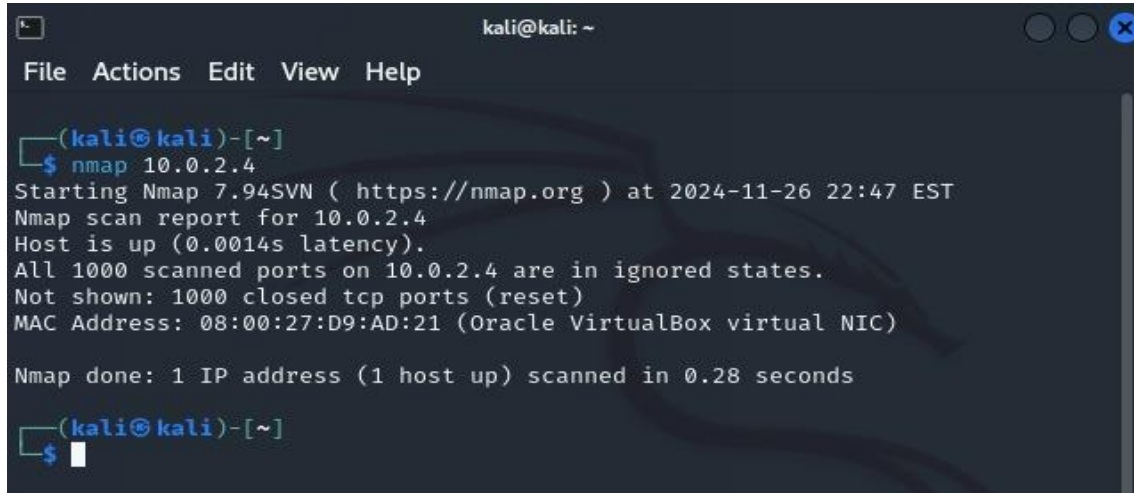


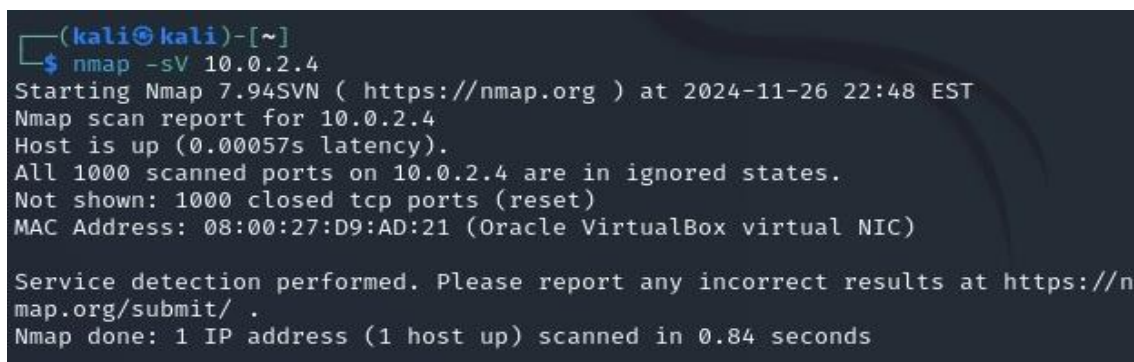
## PRÁCTICA DE ESCANEO CON NMAP

Se realizó un escaneo con nmap desde una máquina Kali Linux a una máquina Debian con IP 10.0.2.4 para descubrir hosts activos y puertos abiertos.

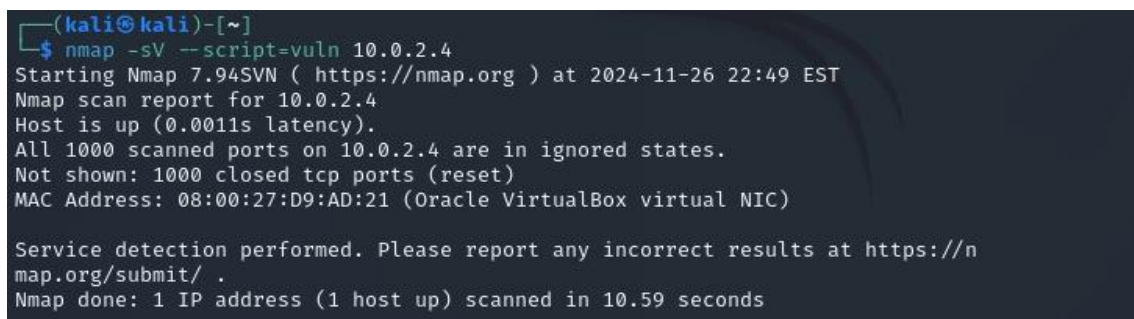
El primer escaneo simple (nmap 10.0.2.4) mostró los siguientes resultados:

A terminal window titled 'kali@kali: ~' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(kali@kali)-[~]'. The command '\$ nmap 10.0.2.4' is entered. The output shows: 'Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-26 22:47 EST', 'Nmap scan report for 10.0.2.4', 'Host is up (0.0014s latency).', 'All 1000 scanned ports on 10.0.2.4 are in ignored states.', 'Not shown: 1000 closed tcp ports (reset)', 'MAC Address: 08:00:27:D9:AD:21 (Oracle VirtualBox virtual NIC)', and 'Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds'. The prompt returns to '\$ '.

El segundo escaneo (nmap -sV 10.0.2.4) proporcionaría una lista de los puertos abiertos y servicios que operaran en dicha dirección IP. Los resultados fueron los siguientes:

A terminal window showing the command '\$ nmap -sV 10.0.2.4'. The output is similar to the first scan but includes 'Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .' and 'Nmap done: 1 IP address (1 host up) scanned in 0.84 seconds'.

El tercer escaneo que realicé ( nmap -sV --script=vuln 10.0.2.4) es un escaneo mucho más detallado y tiene como fin detectar vulnerabilidades. Los resultados son los siguientes:

A terminal window showing the command '\$ nmap -sV --script=vuln 10.0.2.4'. The output is similar to the previous scans but includes 'Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .' and 'Nmap done: 1 IP address (1 host up) scanned in 10.59 seconds'.

## RESULTADOS

En los tres tipos de escaneos, no se muestran puertos abiertos o servicios en ejecución y tampoco se han encontrado vulnerabilidades.