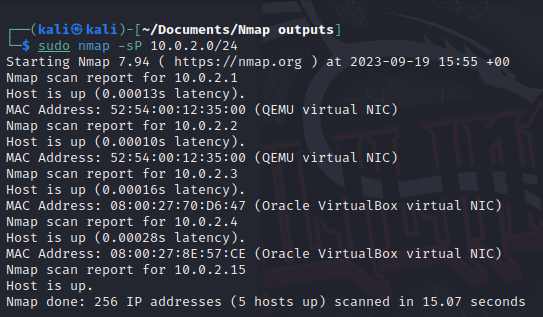
Rodrigo Brasil 09/2023

### **Part 2: Port Scanning with Nmap**

:

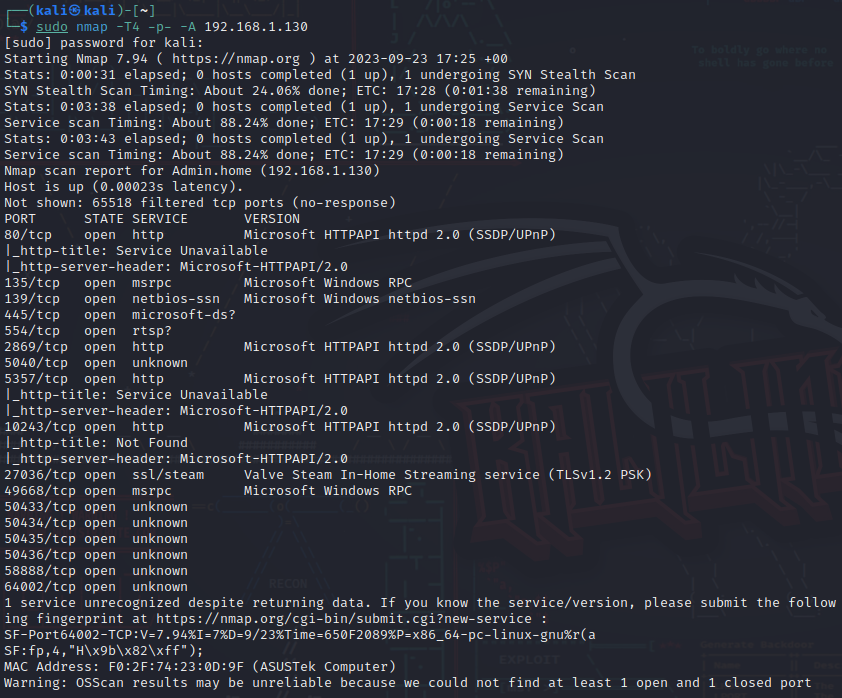
* Perform a scan to discover all hosts on , without scanning any ports.

sudo nmap -sP 10.0.2.0/24

This scan sends ping packets to all IP addresses within the specified network range (10.0.2.0/24). For each IP address in the range, it listens for responses. If it receives a ping from a host, it considers that host as online and available on the network.After scanning all IP addresses in the range, it generates a list of hosts that responded to the requests, indicating which hosts are currently active or reachable on the network.

The scan was correct because it shows all of the hosts on the network.

This type of scan is useful for quickly identifying which hosts are up on a local network segment without performing a more detailed and potentially time-consuming port scan.

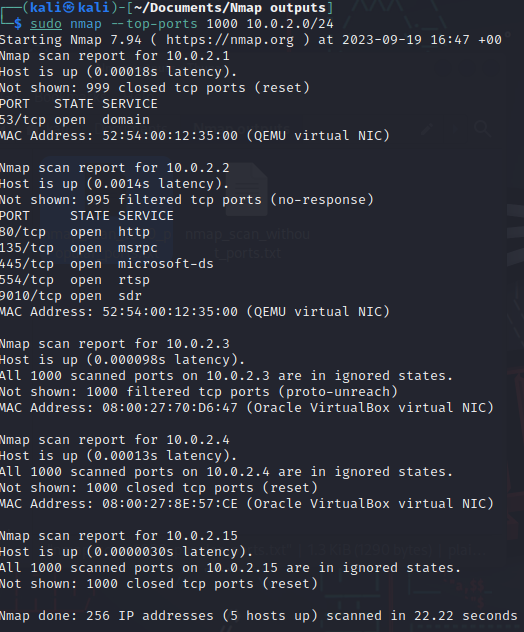
* Perform a fast, aggressive scan of the network.

sudo nmap -T4 -p- -A 192.168.1.130

This scan sends various network packets to the IP address 10.0.2.4 to gather information about the open ports and services running on that host. The use of -T4 sets the scan timing to be more aggressive, meaning Nmap will send packets more quickly than in a standard scan. This can help speed up the scan but may be more conspicuous and may increase the risk of being detected by intrusion detection systems.

The scan was correct because it showed more open ports then the previous more stealthy commands

There are multiple reasons on why this particular scan would be used, one of them would be for security assessment It can help identify potential entry points for further vulnerability scanning or penetration testing.

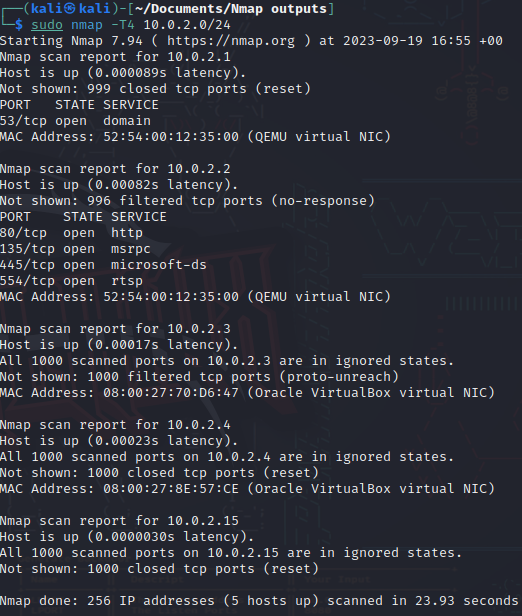
* Scan the 1000 most common ports on each host on the network.

sudo nmap –top-ports 1000 10.0.2.0/24

This command gives the top 1000 most common ports on all IP addresses within the 10.0.2.0/24 subnet. This scan aims to identify which services are running on these ports on the target hosts within the specified IP range.

The scan was correct because it gave me the top 1000 ports and what services are running in them.

This scan can be used for multiple purposes, like port Identification, security assessment, firewall testing and troubleshooting.

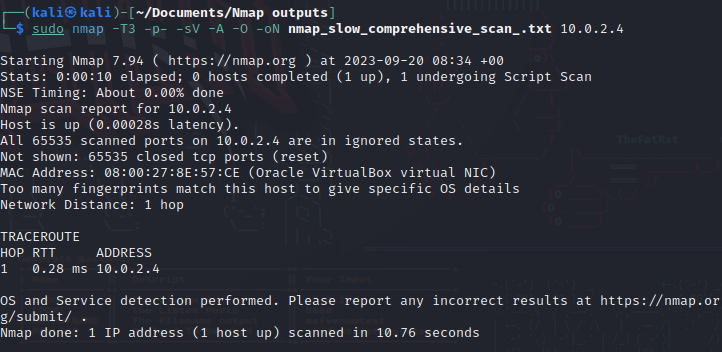
* Perform an intense scan on all hosts on the network.

sudo nmap -T4 10.0.2.0/24

In technical terms, this command performs an intense network scan on all hosts within the 10.0.2.0/24 subnet.

This scan was correct altho it was very similar to the other scan above

This scan is designed to gather detailed information about the target hosts, including their open ports, services, service versions, operating systems, and potential vulnerabilities.

* Perform a slow, comprehensive scan on all hosts on the network.

sudo nmap -T3 -p- -sV -A -O -oN nmap\_slow\_comprehensive\_scan.txt 10.0.2.4

It initiates a thorough scan of the target host by scanning all 65,535 TCP ports. This allows it to identify any open ports where services may be running.

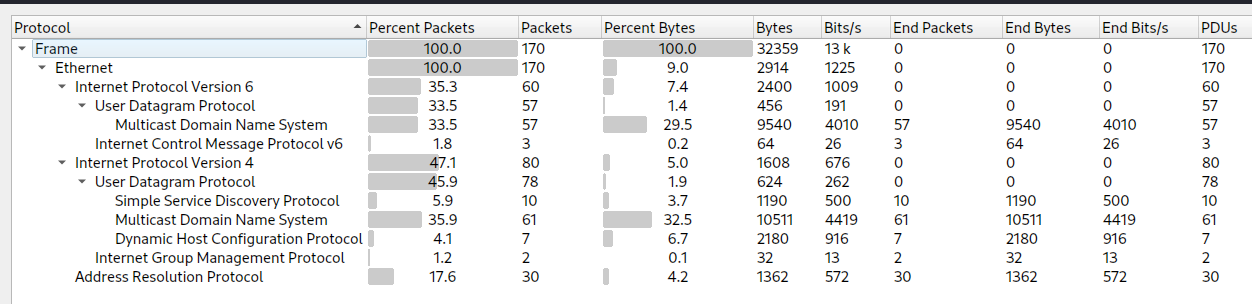
For each open port, it performs version detection to determine the specific service and version running on that port. This can help identify potential vulnerabilities associated with the running services.

### **Part 3: Reporting Nmap Findings**

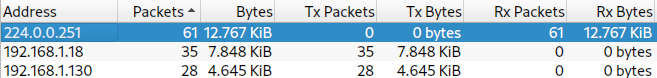
| **Scan Type** | **Scan Results** | **Actual** |
| --- | --- | --- |
| Port Scan | found 5 ip’s  10.0.2.1,10.0.2.2,10.0.2.3,10.0.2.4,10.0.2.15 | Found the IP´s of the virtual machines NIC’s |
| Aggressive Scan on a specific IP | Found a lot of ports open, OS detection, services version detection | Found OS version (win11), services running  port 135 / msrpc MW RPC  port 2896 / http HTTPAPI httpd 2.0 |
| Top Ports Scan | Scanned the top 1000 ports | Found ports 80,135,445,554,9010 open |
| Intensive Scan | Intensive scan on the whole network | Only showed ports and services from 1 host.  The rest were inconclusive |
| Slow Scan | Slow scan to get the most detailed info from a host | Was the least informative of them all |

| **Network Range** | **Server IP Address** | **Ports Open** | **Service/Banner** |
| --- | --- | --- | --- |
| 10.0.2.0/24 | 10.0.2.1 | 10.0.2.2 | 10.0.2.3 | 10.0.2.15 | no info | no info |
| 192.168.1.0/24 | 192.168.1.130 | 80 | 135 | 139 | 445 | 554 | 2869 | 5040 | 5357 | 27036 | 49668 | 50433 | 50434 | 50435 | 50436 | 58888 | 64002 | msrpc | netbios-ssn | microsoft-ds? | rtsp? | http | unknown | ssl/steam. |
| 10.0.2.0/24 | 10.0.2.1 | 10.0.2.2 | 10.0.2.3 | 10.0.2.15 | 80 | 135 | 445 | 554 | 9010 | http | msrpc | microsoft-ds | rtsp | sdr |
| 10.0.2.0/24 | 10.0.2.1 | 10.0.2.2 | 10.0.2.3| 10.0.2.4 | 10.0.2.15 | 80 | 135 | 445 | 554 | http | msrpc | microsoft-ds | rtsp |
| 10.0.2.0/24 | 10.0.2.4 | no info | no info |

### **Part 4: Protocol Hierarchy Statistics with Wireshark**



Protocol hierarchy statistics report

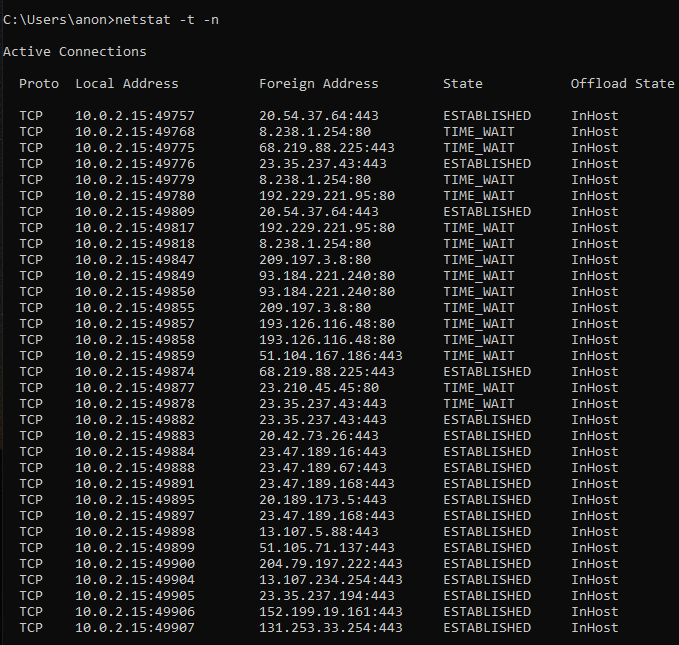


Top receivers and listeners

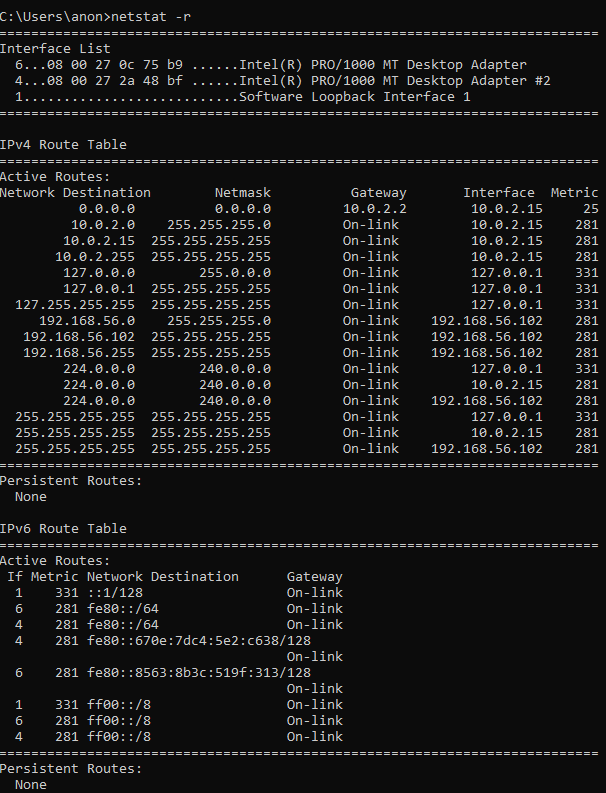
### Conversations sorted by session duration

### 

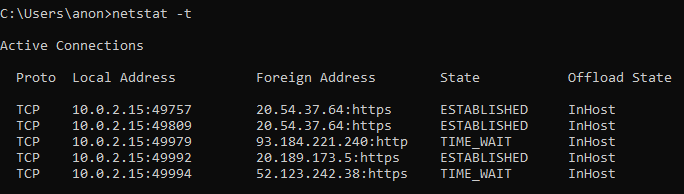
### **Part 5: Netstat**



all active ports



Routing Table



Only connections with the tcp protocol