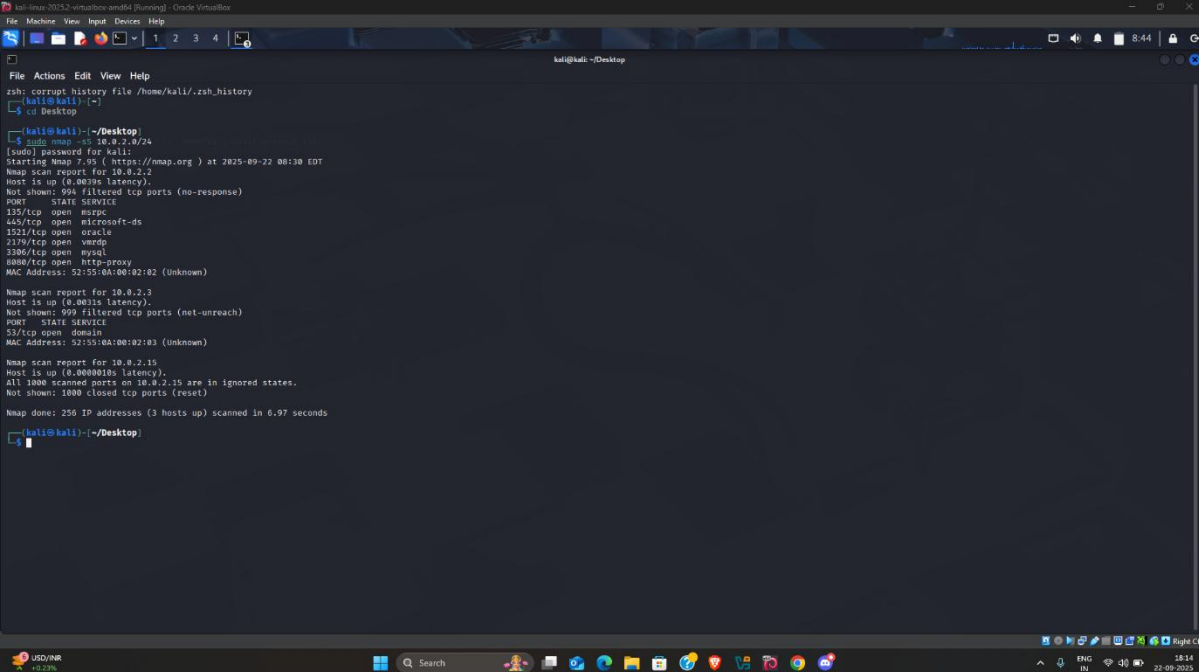


❖ **Run: `nmap -sS 192.168.1.0/24` to perform TCP SYN scan.**



```
kali@kali:~$ sudo nmap -sS 192.168.1.0/24
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 08:38 EDT
Nmap scan report for 10.0.2.2
Host is up (0.0039s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
1521/tcp  open  oracle
2179/tcp  open  vmrpd
3306/tcp  open  mysql
8080/tcp  open  http-proxy
MAC Address: 52:55:0A:00:02:02 (Unknown)

Nmap scan report for 10.0.2.3
Host is up (0.0031s latency).
Not shown: 999 filtered tcp ports (net-unreach)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 52:55:0A:00:02:03 (Unknown)

Nmap scan report for 10.0.2.15
Host is up (0.0000014s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

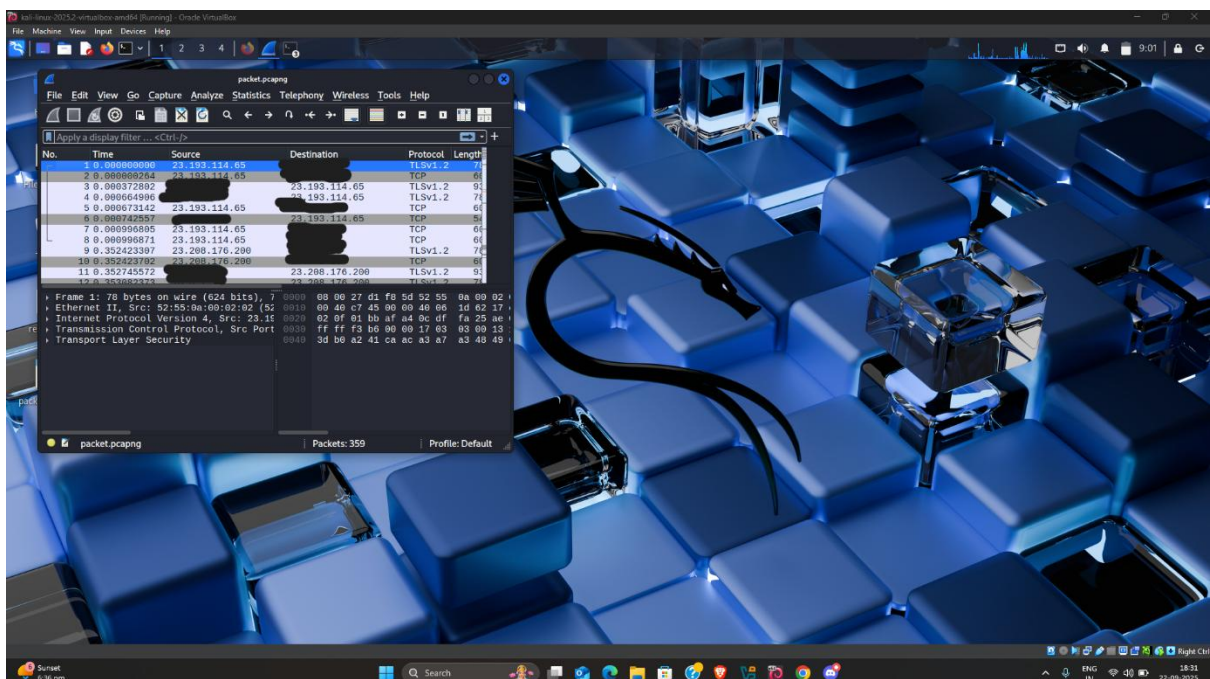
Nmap done: 256 IP addresses (3 hosts up) scanned in 6.97 seconds
kali@kali:~$
```

❖ **Research common services running on those ports.**

- **135/tcp (msrpc):** This port is used by Microsoft Remote Procedure Call (MSRPC), which allows distributed applications to communicate with each other.
- **445/tcp (microsoft-ds):** This port is for Microsoft-DS (Directory Service), which is used by Server Message Block (SMB) for file sharing and printer access on Windows networks.
- **1521/tcp (oracle):** This is the default port for the Oracle Database listener service.
- **2179/tcp (vmrpd):** This port is associated with VMware VirtualCenter Agent and is used for its Remote Desktop Protocol (RDP).
- **3306/tcp (mysql):** This is the default port for the MySQL database system.
- **8080/tcp (http-proxy):** This is a common alternate port for HTTP, often used for web proxies or as a secondary web server.

❖ *Identify potential security risks from open ports.*

- ❖ **Port 135 (MSRPC):** This Windows service has been historically vulnerable to exploits that can allow an attacker to take over the system.
 - ❖ **Port 445 (Microsoft-DS):** Used for file sharing, this port is a common target for ransomware and malware, notably exploited by the WannaCry and NotPetya attacks.
 - ❖ **Port 1521 (Oracle):** This is the default port for Oracle databases and can be vulnerable to attacks like SQL injection and buffer overflows, which could lead to data theft.
 - ❖ **Port 2179 (VMware RDP):** This remote access service can be susceptible to brute-force attacks and has had known vulnerabilities that could allow an attacker to gain control of the virtual machine.
 - ❖ **Port 3306 (MySQL):** The default port for MySQL databases is often targeted with brute-force attacks and SQL injection attempts to steal or corrupt data.
 - ❖ **Port 8080 (HTTP-Proxy):** This port, often used for web services, is a target for general web attacks like cross-site scripting (XSS) and denial-of-service (DoS) attacks.
- ❖ *Optionally analyze packet capture with Wireshark.*



=====***=====