#### Discovering Open Ports on Local Network using Nmap (Kali Linux) ~ BY Rishabh Kumar | rishabhcyy@gmail.com

#### ****Objective****

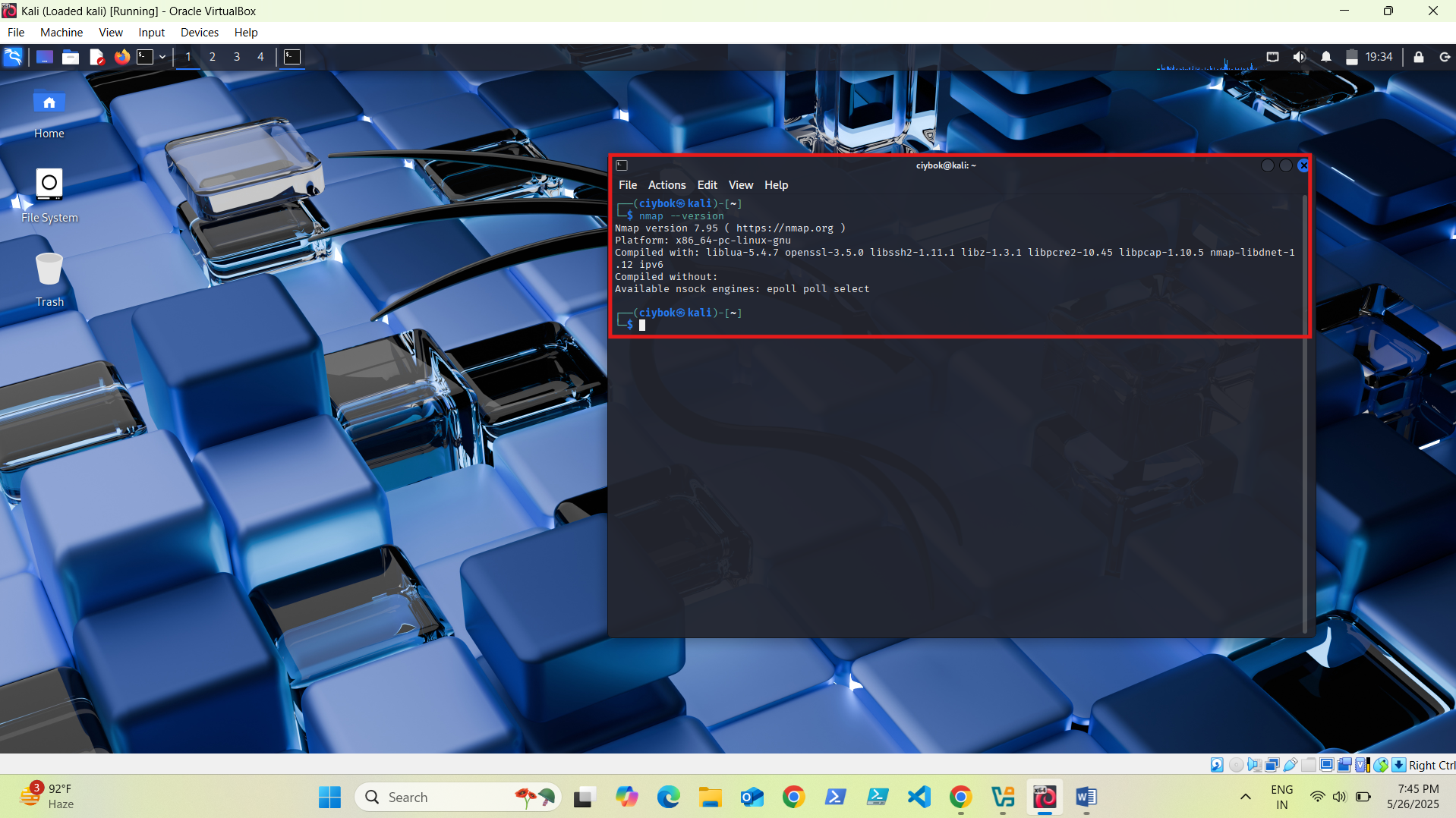
To discover open ports on devices in the local network using Nmap on Kali Linux and understand potential security risks.

#### ****Tools Used****

* **Nmap** (Network Mapper)

**Step 1: Verify Nmap Installation (Kali)**

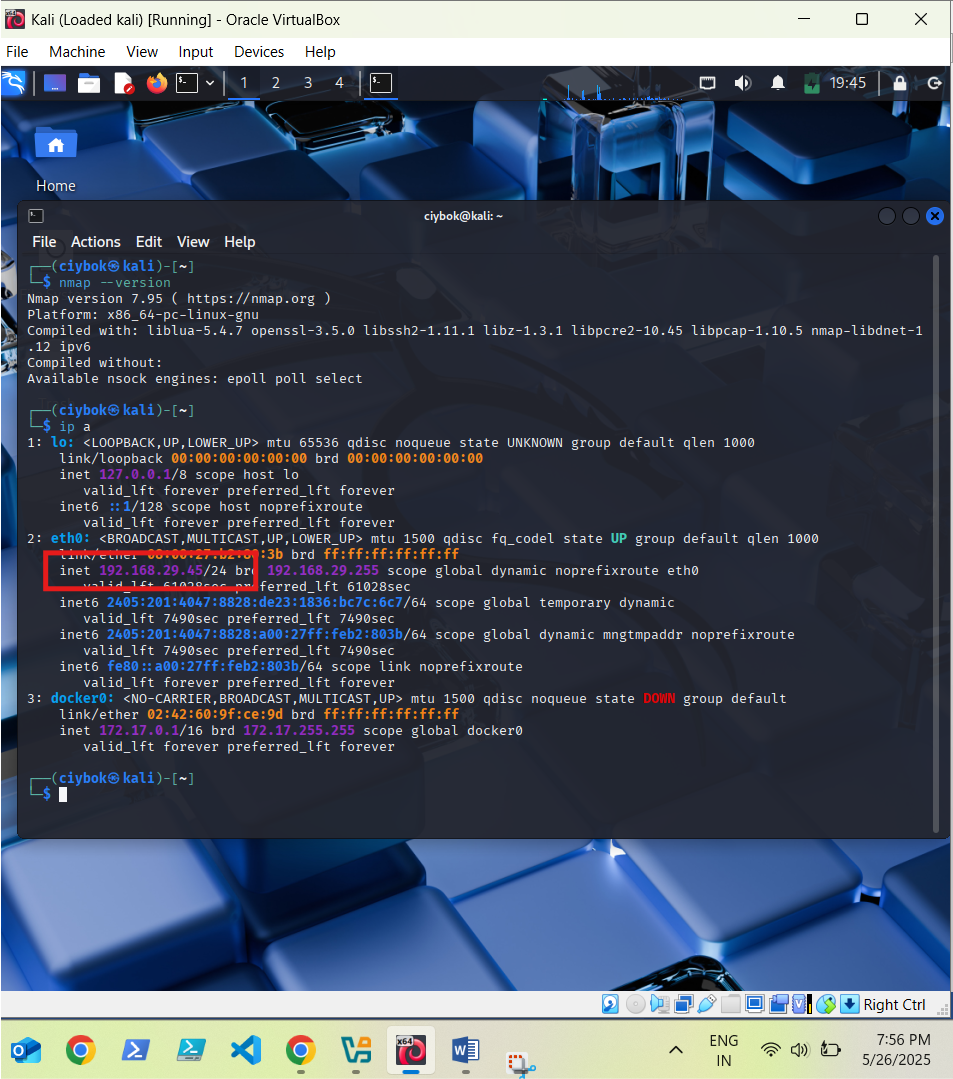
* Nmap is usually pre-installed on Kali.
* Run: nmap –version



**Terminal output showing the Nmap version.**

**Step 2: Identify Local Network Range**

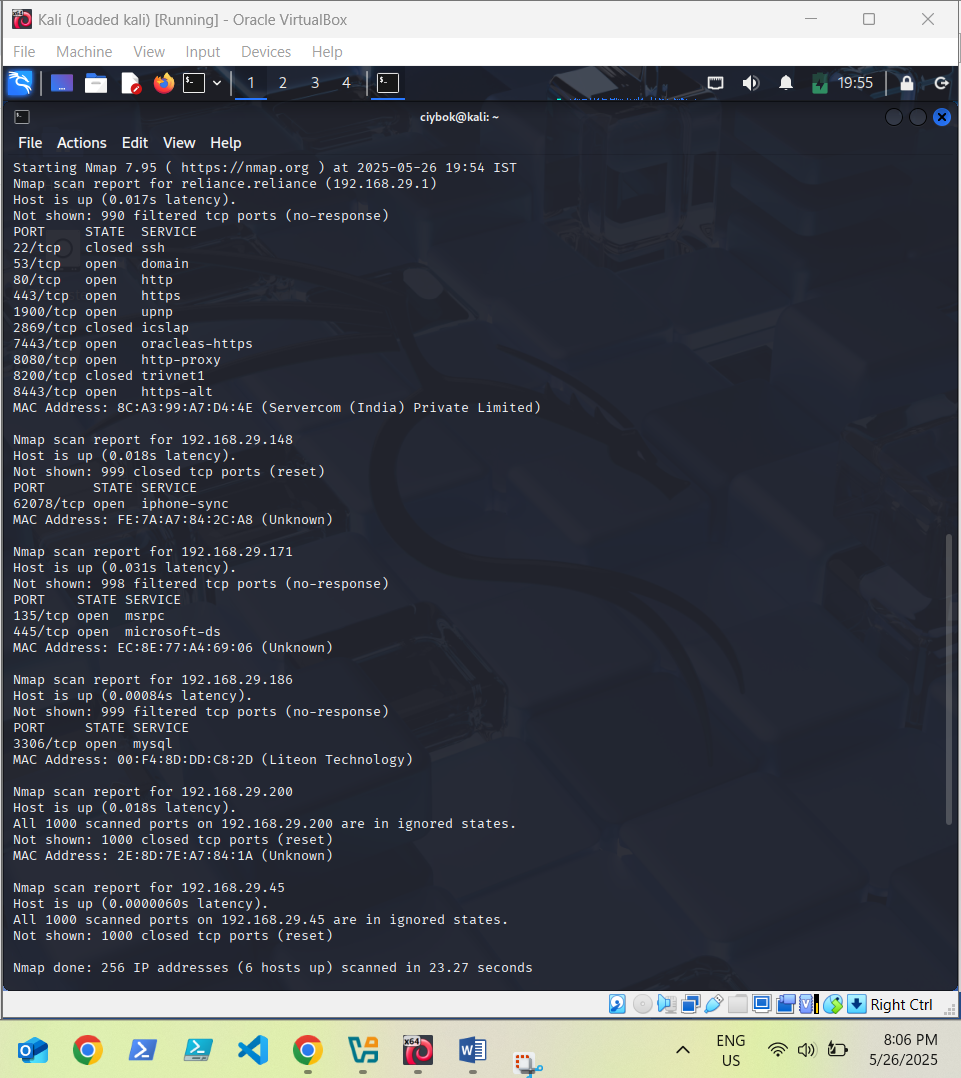
* Run : ip a



**Terminal output showing your IP address and subnet.**

**Step 3: Perform a TCP SYN Scan**

* Run command : sudo nmap -sS 192.168.1.0/24 (This scans all 256 IPs in your subnet.)



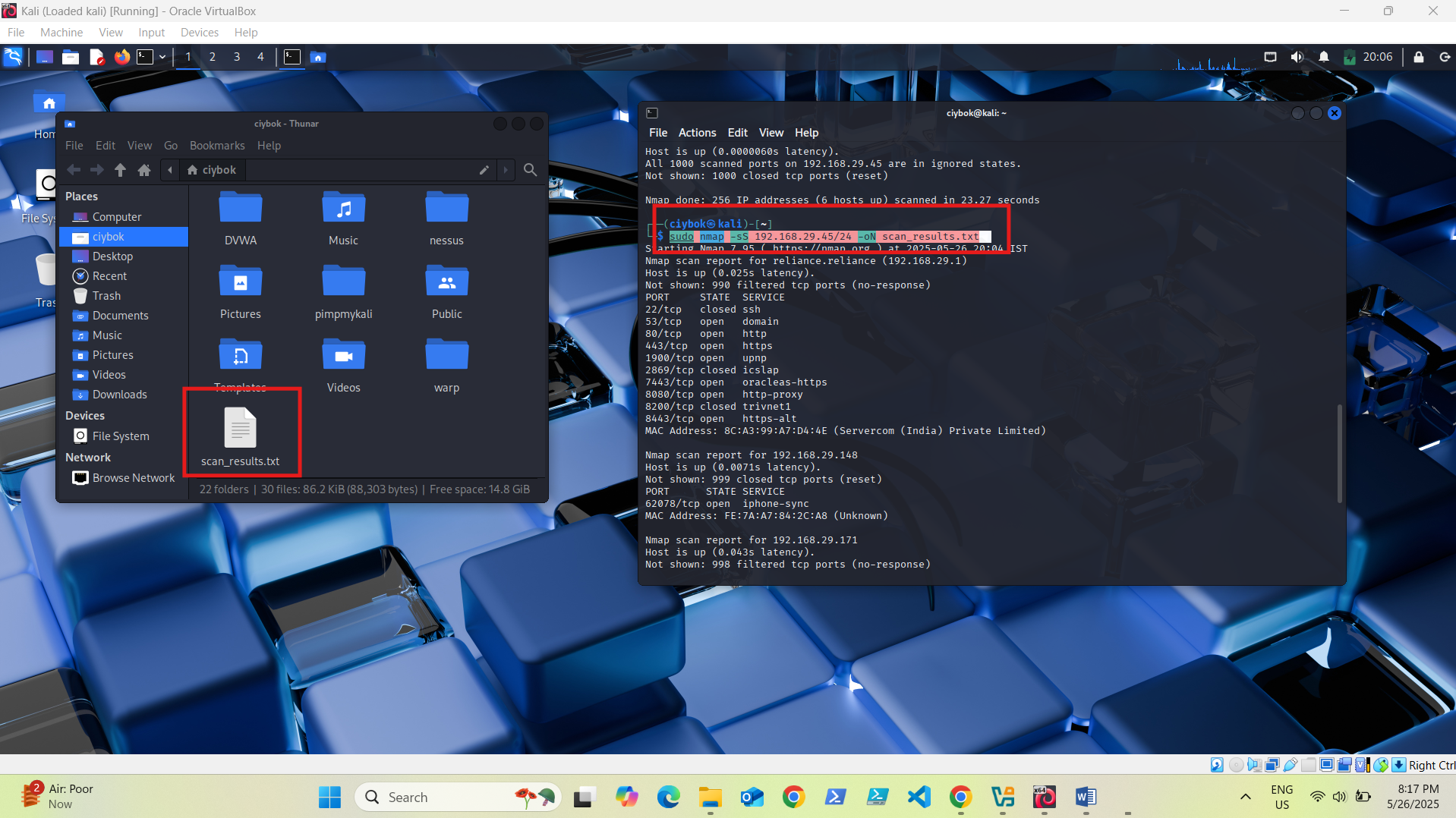
**Terminal showing discovered hosts and open ports**

**Step 4: Analyze the Results**

* **Which IPs responded :** 192.168.29.1, 192.168.29.45, 192.168.29.148, 192.168.29.171, 192.168.29.186, 192.168.29.200
* **Which Ports are open :** 
  + 192.168.29.1: 53, 80, 443, 1900, 7443, 8080, 8443
  + 192.168.29.148: 62078
  + 192.168.29.171: 135, 445
  + 192.168.29.186: 3306
  + Others (192.168.29.45, 192.168.29.200): No open ports

**Step 5: Save the scan results**

* Run : sudo nmap -sS 192.168.29.45/24 -oN scan\_results.txt



**Scan results saved**

**Research on Common Ports & common services that run on them (Based on my scan results) :**

| **Port** | **Service** | **Common Use** |
| --- | --- | --- |
| **53** | **DNS (Domain Name System)** | Resolves domain names (like google.com) to IP addresses. |
| **80** | **HTTP (HyperText Transfer Protocol)** | Standard web traffic; sends websites over the internet (not secure). |
| **443** | **HTTPS (HTTP Secure)** | Secure version of HTTP using encryption (SSL/TLS). |
| **1900** | **UPnP (Universal Plug and Play)** | Auto-discovers devices on local network; often used by smart devices. |
| **7443** | **OracleAS / HTTPS-Alt** | Alternative secure web services, sometimes admin panels. |
| **8080** | **HTTP Proxy / Alt HTTP** | Used for web services, test environments, or proxies. |
| **8443** | **HTTPS-Alt** | Another common alternative port for secure web interfaces. |
| **62078** | **iPhone Sync** | Used by Apple devices to sync data with iTunes or Finder. |
| **135** | **MSRPC (Microsoft RPC)** | Remote Procedure Call for Windows networking and DCOM functions. |
| **445** | **Microsoft-DS / SMB** | File sharing, network browsing, and printer sharing on Windows networks. |
| **3306** | **MySQL Database** | Used to connect to MySQL databases, usually for websites or apps. |

**Identification of Potential Security Risks (based on my scan results) :**

**Risky Ports :**

* **135/445 (Windows SMB):** Often targeted by malware (e.g., WannaCry).
* **UPnP (1900):** Can expose internal devices if misconfigured.
* **MySQL (3306):** Should not be exposed without authentication/firewall rules.
* **HTTP (80):** Unencrypted web traffic can leak sensitive info.
* **8080/8443/7443:** Often used for admin panels; risky if unprotected.

**Conclusion**

#### ****What did I learn?****

* Several devices run potentially vulnerable or unnecessary services.
* Some common ports expose services that could be exploited.
* Scanning helps uncover hidden risks in a network.

#### ****How can scanning help in cybersecurity?****

* **Identifies open ports/services** that attackers could use.
* Helps detect misconfigurations or unintentional exposures.
* Allows proactive security measures like firewall rules or patching.