Network Port Scanning Report

# Objective

To scan the local network using Nmap from a Kali Linux VM running in VirtualBox, identify active hosts, and analyze potential risks based on open or closed ports.

# Tools Used

- Nmap (for port scanning)

- Kali Linux on VirtualBox

- Operating System: Kali Linux, Windows

# Network Scanning Details

IP Range Scanned: 192.168.211.0/24

Scan Command Used:

nmap -sS 192.168.211.0/24 -oN scan\_results.txt

# Scan Results Summary

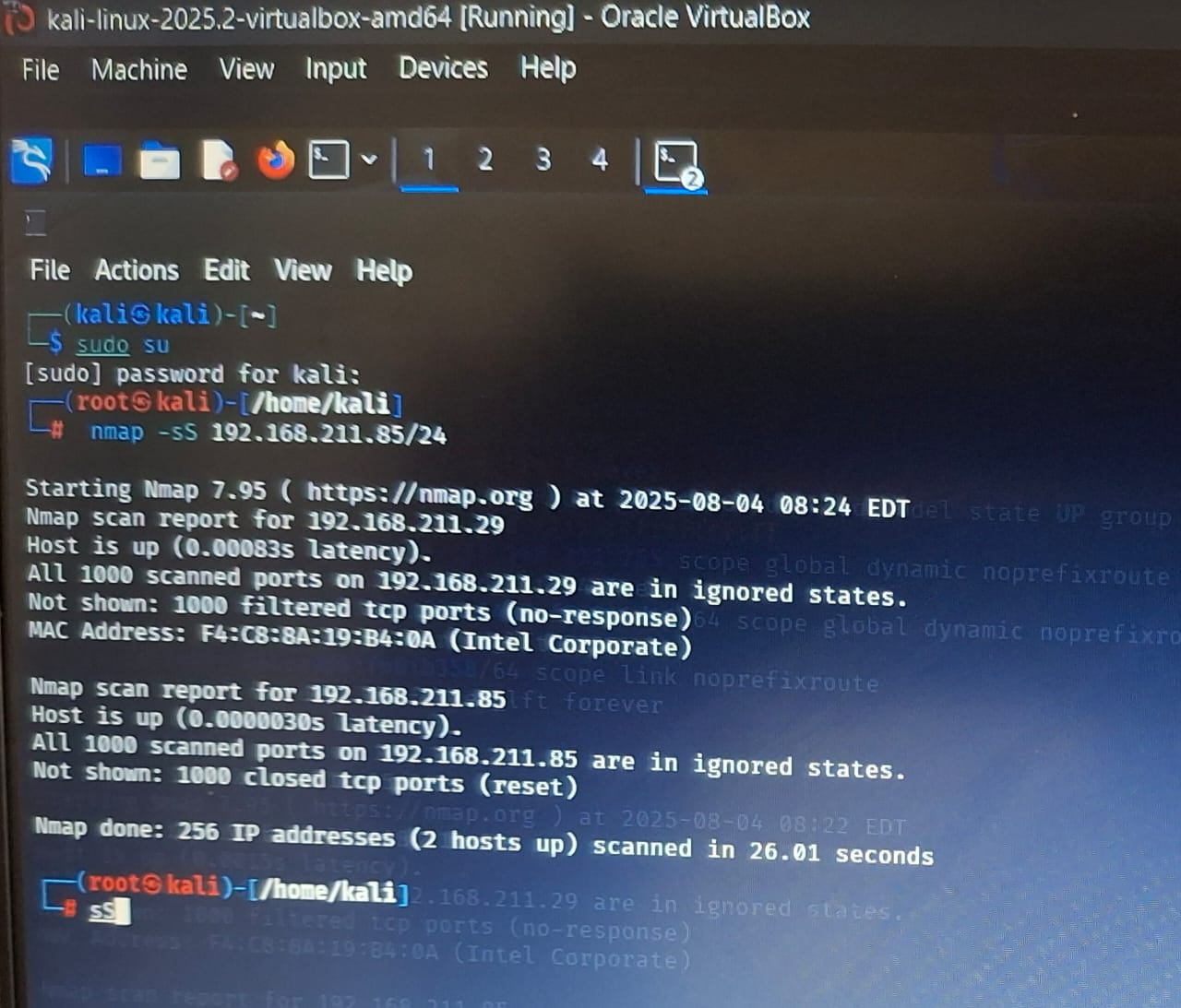
|  |  |  |  |
| --- | --- | --- | --- |
| IP Address | Status | Open Ports | Notes |
| 192.168.211.29 | Up | None | All ports filtered (likely firewall) |
| 192.168.211.85 | Up | None | All ports closed |

# Security Risk Analysis

|  |  |  |  |
| --- | --- | --- | --- |
| Host IP | Risk | Observation | Suggestion |
| 192.168.211.29 | Possible firewall detected | All ports filtered | Validate firewall configuration |
| 192.168.211.85 | No services exposed | All ports closed | No immediate risk, keep system updated |

# Attached Files

* scan\_results.txt – Output from Nmap
* README.md – Project overview and summary
* screenshots/ – Scan output screenshots



# Key Learnings

* Practiced using Nmap for network scanning in a virtual lab environment  
  - Identified that some hosts block or close all ports  
  - Understood how firewalls affect scanning results  
  - Gained knowledge of interpreting Nmap outputs

# Submission Checklist

* + Scan completed using Nmap
  + Results saved as scan\_results.txt
  + Report written and added to GitHub
  + Repo link submitted to the portal:- https://github.com/posurabari/nmap-network-scan-task

# Interview Questions & Answers

* Q: What is an open port?

A: An open port is a network port that is actively accepting connections.

* Q: How does Nmap perform a TCP SYN scan?

A: Nmap sends SYN packets to target ports and waits for a SYN-ACK to confirm if a port is open.

* Q: What risks are associated with open ports?

A: They can be exploited to gain unauthorized access, run vulnerable services, or leak information.

* Q: Explain the difference between TCP and UDP scanning.

A: TCP uses handshakes and is more reliable; UDP is connectionless and relies on lack of response.

* Q: How can open ports be secured?

A: Close unused ports, restrict access with firewalls, use secure protocols, and patch regularly.

* Q: What is a firewall's role regarding ports?

A: It blocks or allows network traffic based on rules, controlling access to specific ports.

* Q: What is a port scan and why do attackers perform it?

A: It detects open ports; attackers use it to find vulnerable entry points.

* Q: How does Wireshark complement port scanning?

A: It helps visualize traffic during scans, showing how packets move and how systems respond.