Detecting SYN Scan with Nmap & Wireshark

Name: Redjaimia Imad Eddine

Course: Network Security

Date: September 17, 2025

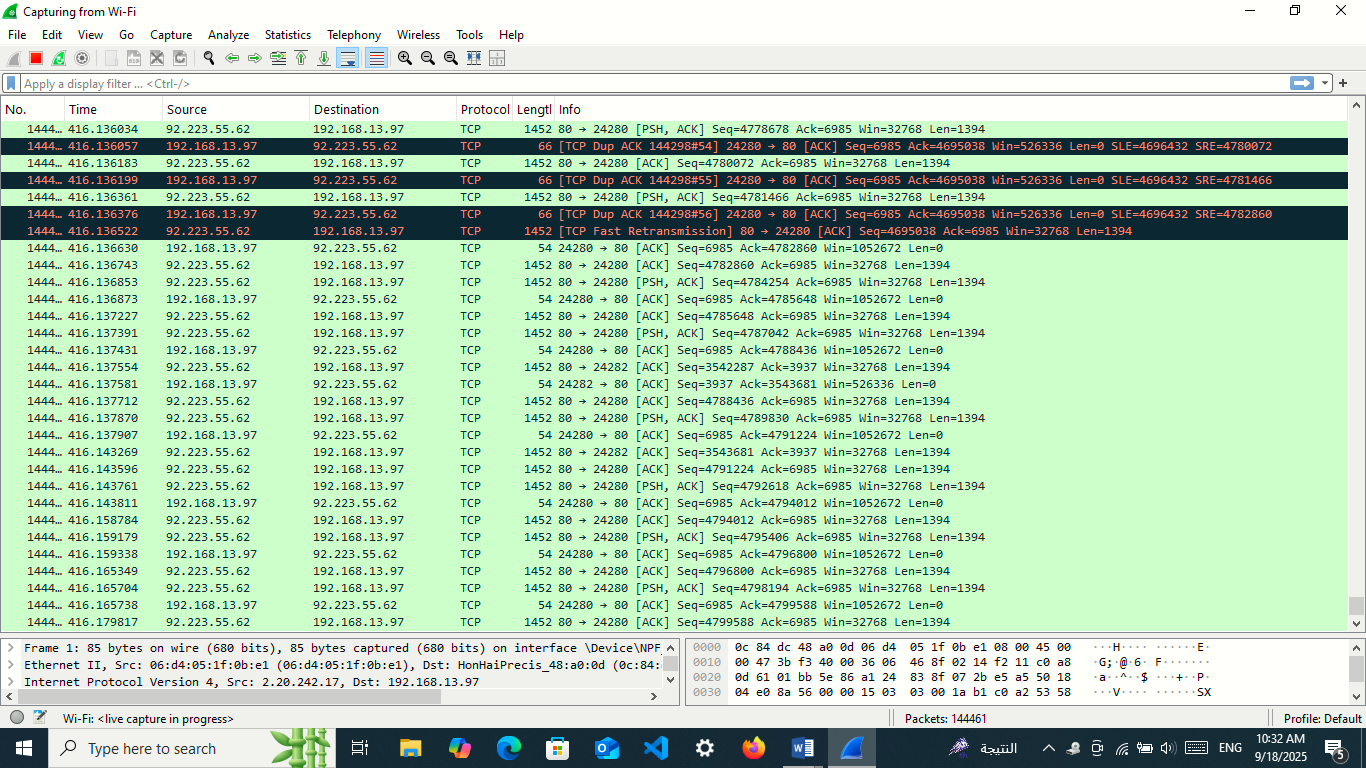
Objective: The objective of this project is to simulate a simple port scan attack using Nmap and detect it with Wireshark

Tools Used: Nmap (for syn scanning)

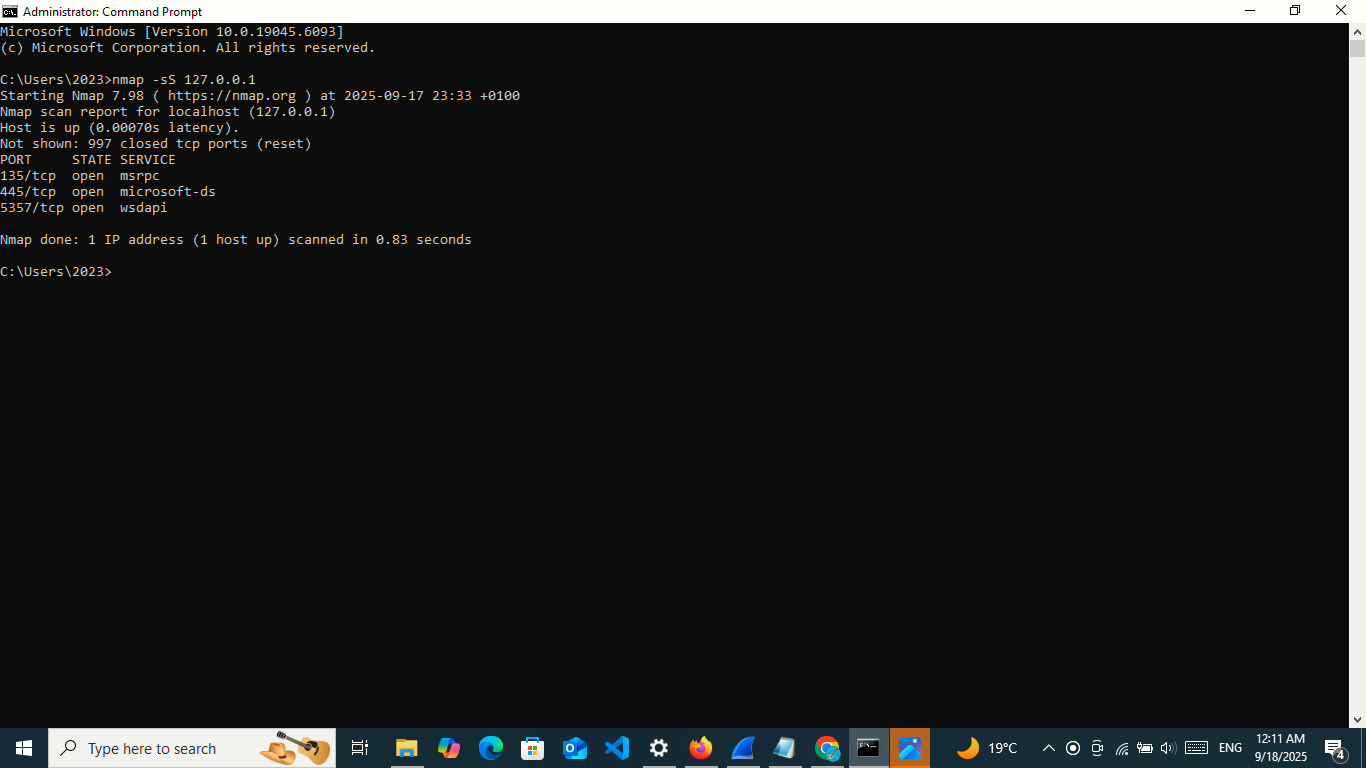
Wireshark (for traffic analysis)

Steps:

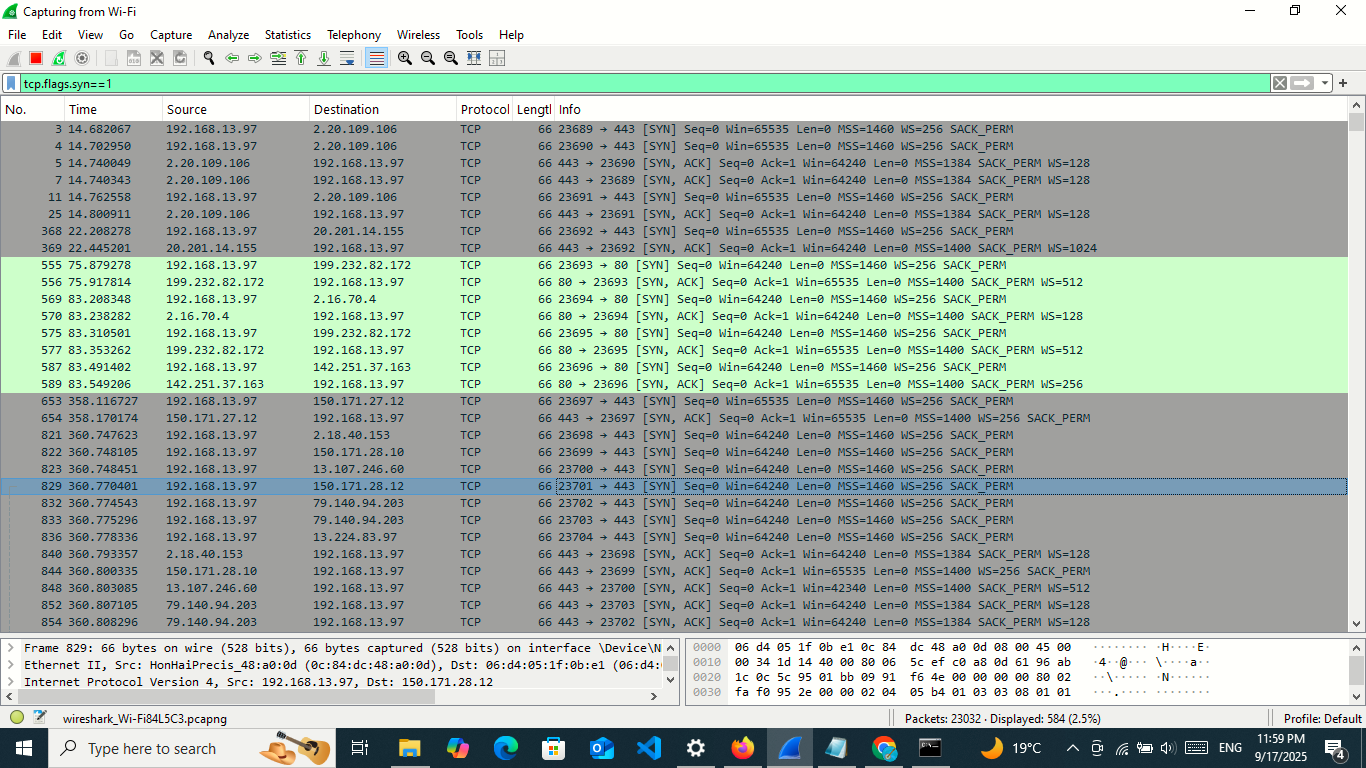
1. Wireshark was started to capture traffic on the Wi-Fi interface.



1. A port scan was executed using the command: nmap -sS [127.0.0.1](http://127.0.0.1/?fbclid=IwZXh0bgNhZW0CMTAAYnJpZBExVm1yblhzaVJwc0xkRWJyQQEeWn_eNnEO2Iu-QRMQEWaqreEnwCIc-Vcft5m-mJ1qcbM1aqN2jLwXx5mYst0_aem__vKg7s__ib4X2kPOz1OJ8A)



1. In Wireshark, multiple TCP SYN packets were observed, which is a typical pattern of a port scan.



Conclusion: The experiment shows how a port scan generates detectable traffic. Such activity can be identified by defensive teams and prevented using firewalls or intrusion detection systems (IDS).