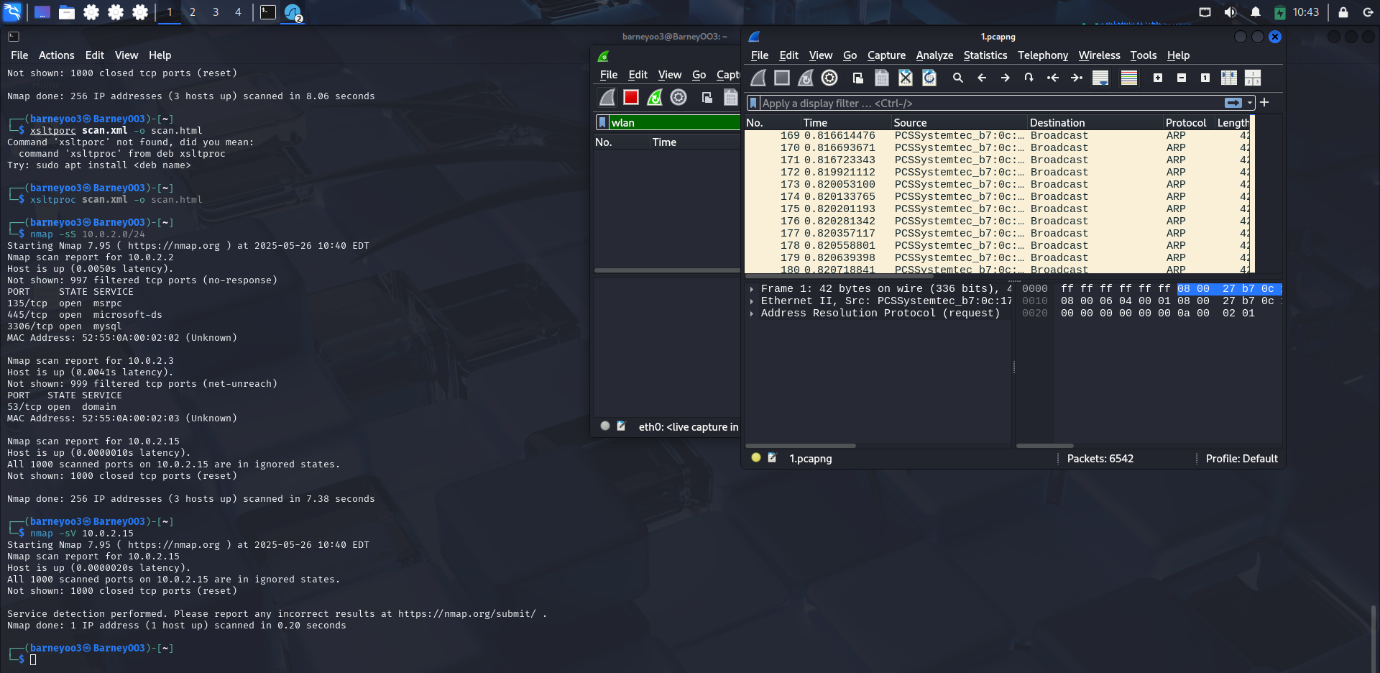
**Task 1 : Scanning Local Network for Open Ports**



In this task, I learned how to perform basic **network reconnaissance** by scanning my local network to identify **active devices and open ports**. Here's what I did and learned:

1. **Identified My IP and Subnet**
   * Used the ifconfig command to find my IPv4 address: 10.0.2.15
   * Determined my subnet range as 10.0.2.0/24
2. **Scanned the Local Network with Nmap**
   * Used the command: nmap -sS 10.0.2.0/24 to perform a TCP SYN scan.
   * This helped me detect live hosts and their open TCP ports.
   * Learned how to interpret common open ports (e.g., 22 for SSH, 80 for HTTP).
3. **Analyzed Live Network Traffic with Wireshark**
   * Captured network packets during the Nmap scan using Wireshark.
   * Filtered for TCP SYN and SYN-ACK packets to see the actual scan behavior.
   * Understood how Nmap communicates stealthily using TCP flags.
4. **Understood Security Exposure**
   * Realized how open ports represent potential attack surfaces.
   * Observed how unused or unnecessary services (like Telnet, RDP) could be security risks if left open.