Logo, icon, company name

Description automatically generated

**Information Security**

**COMP-421**

**Section-B**

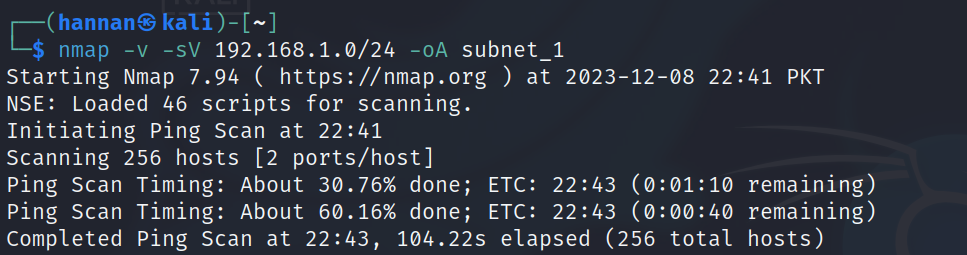
**Assignment - 1**

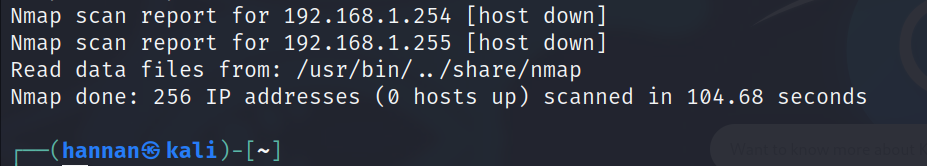
**Hannan Zahid**

**241545586**

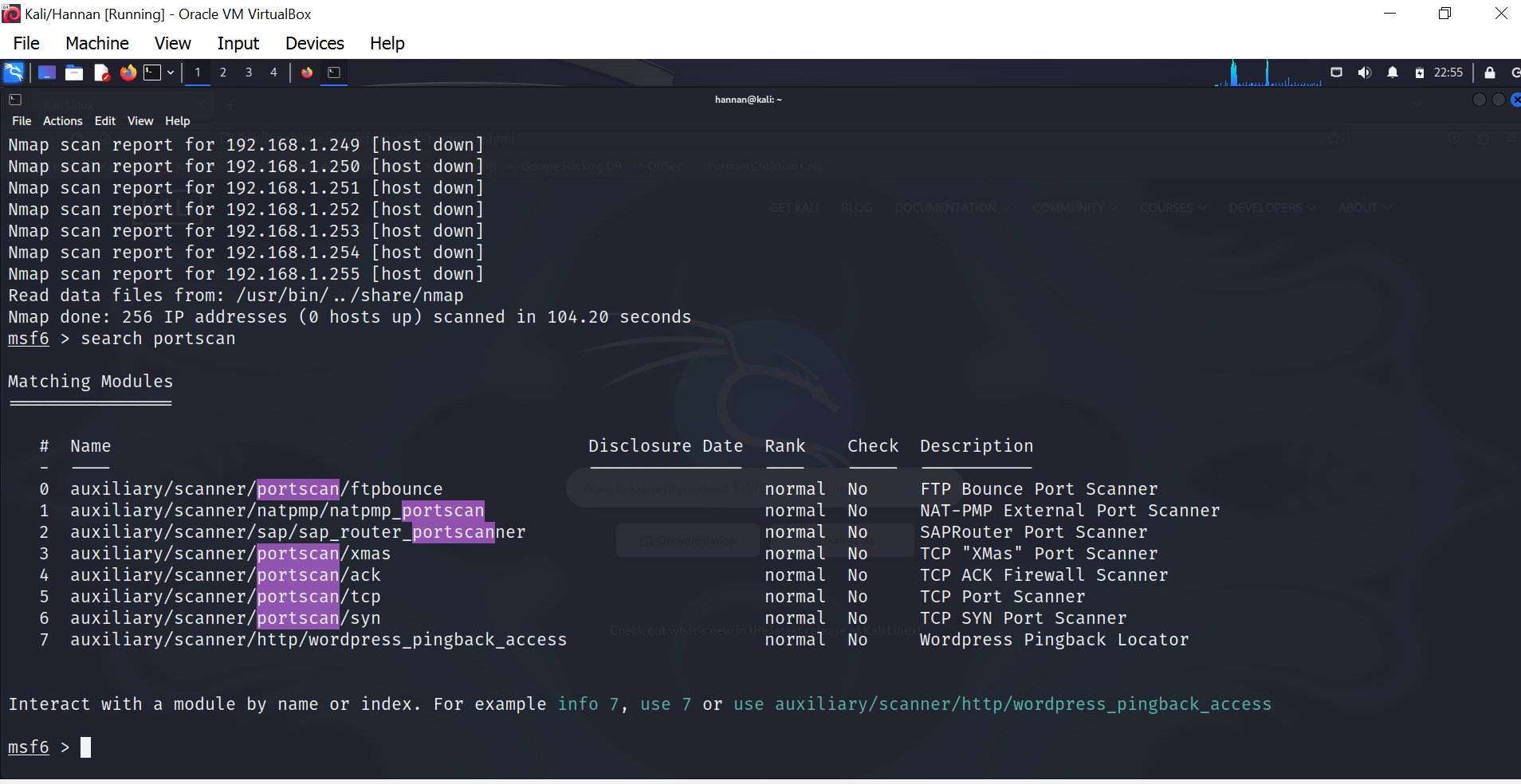
Link 1 Commands:  
<https://www.offsec.com/metasploit-unleashed/port-scanning/>

**Nmap & db\_nmap:**

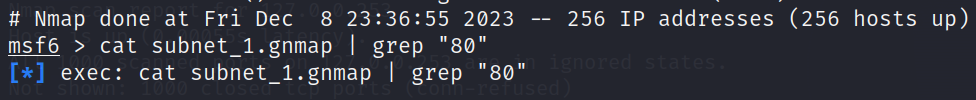


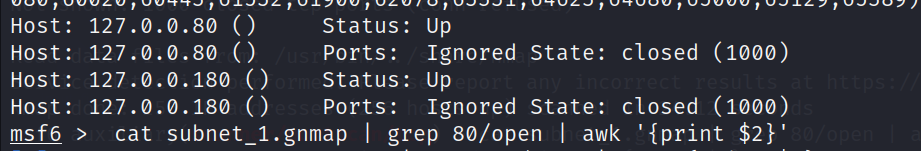


**Port Scanning:**

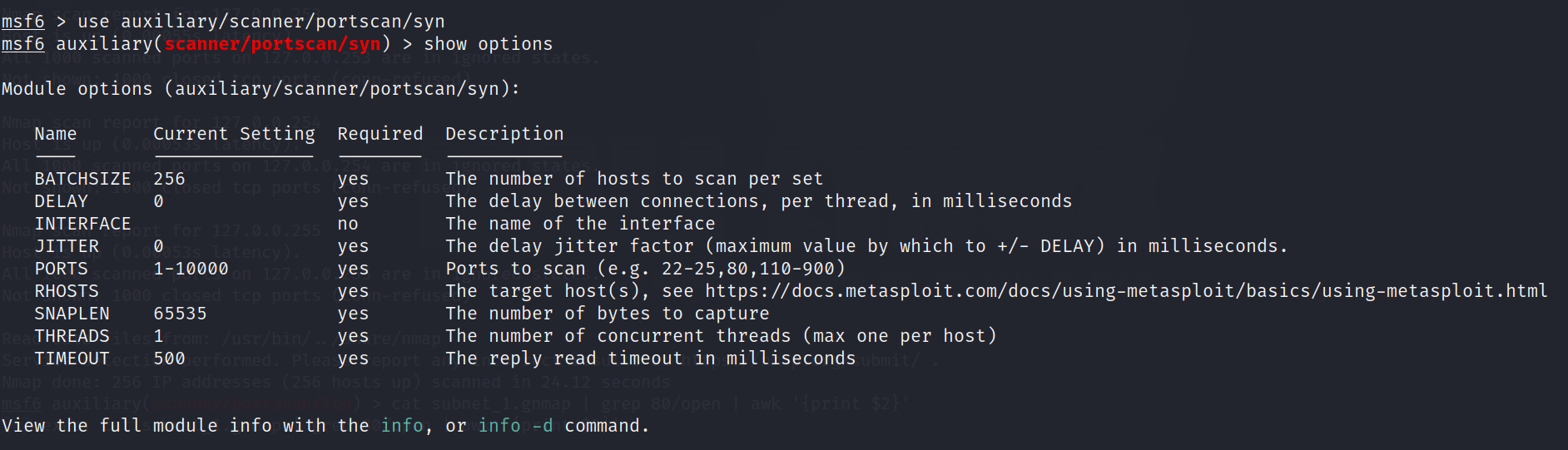


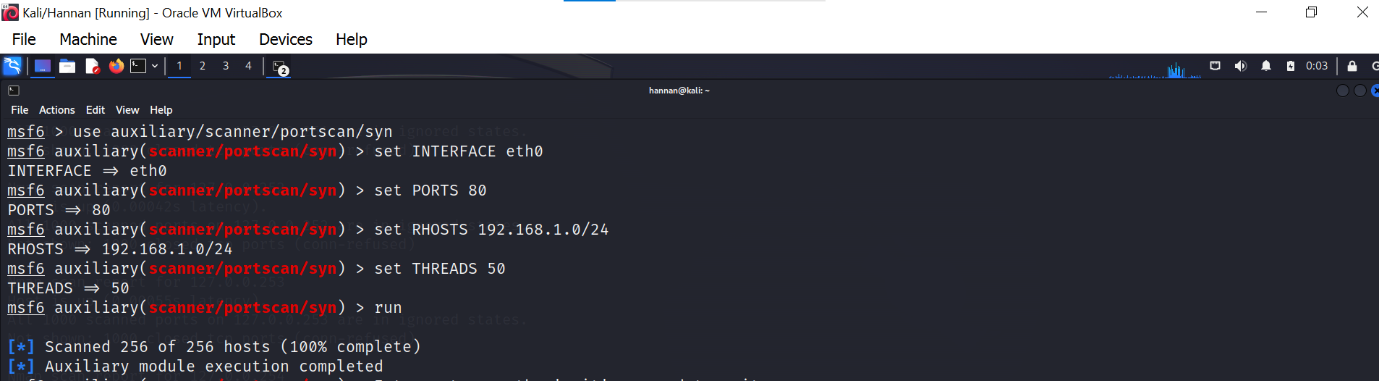
**Cat Subnet:**

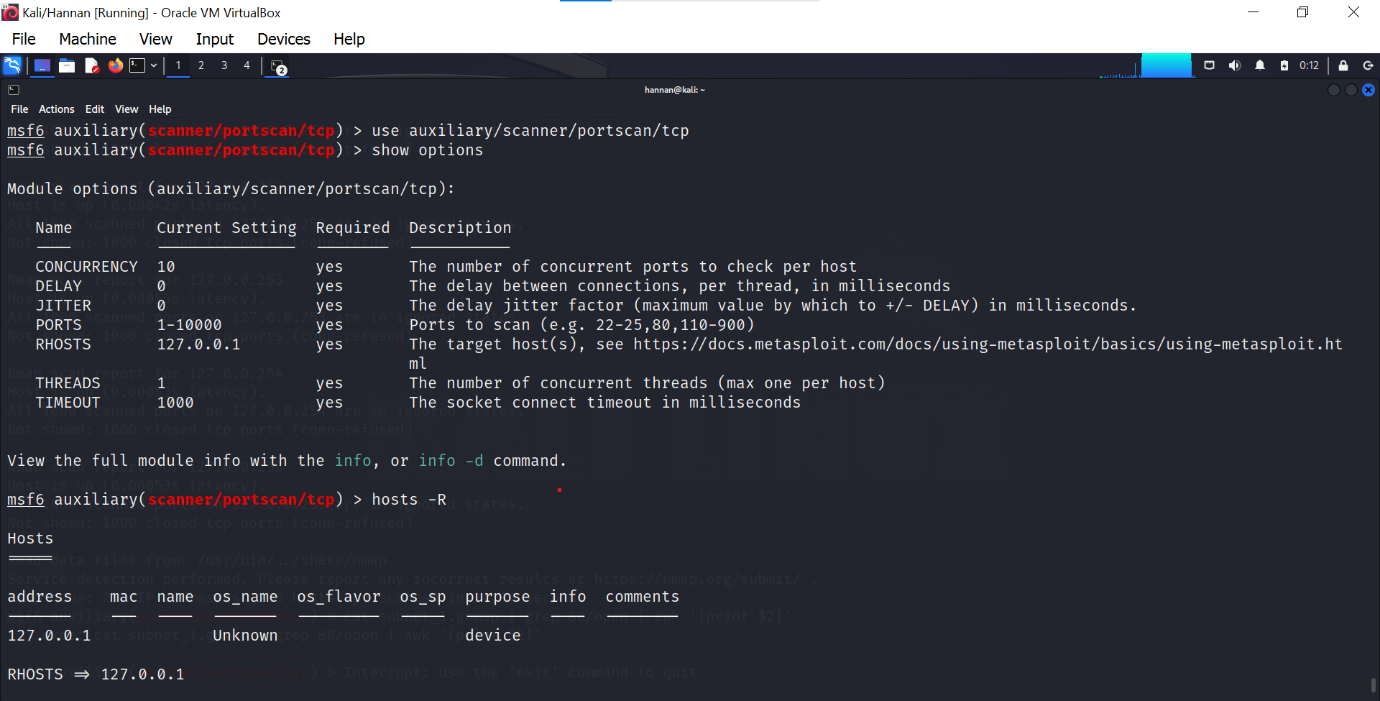


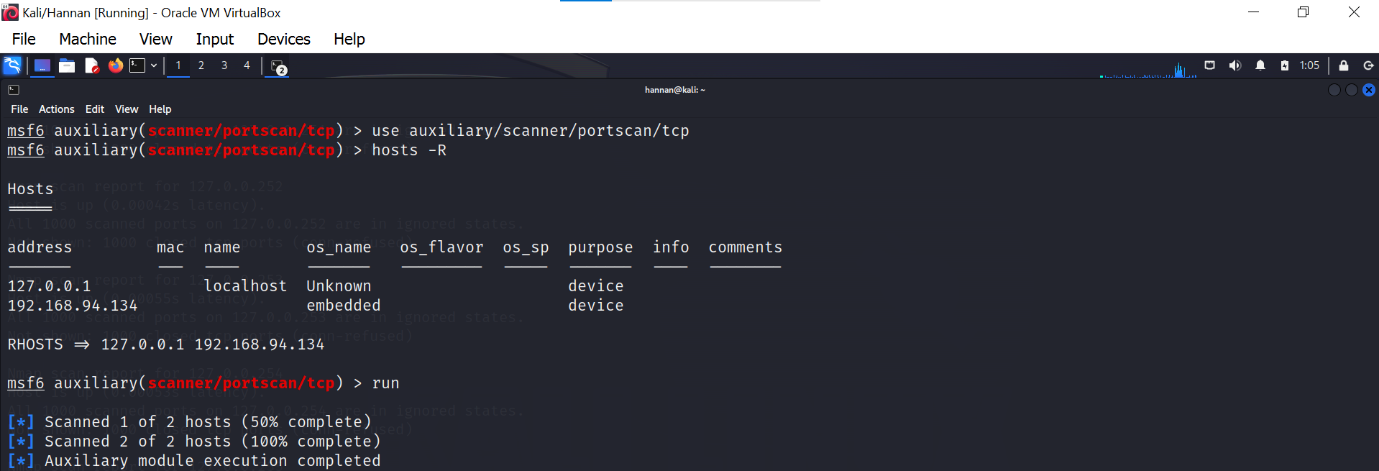


**SYN Scan:**

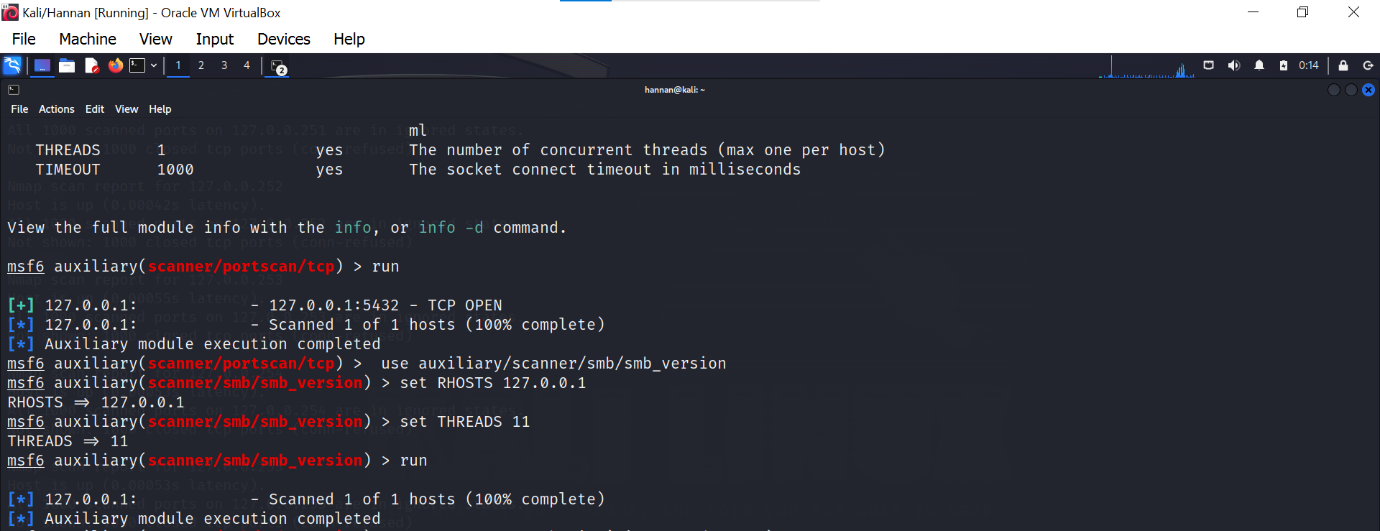


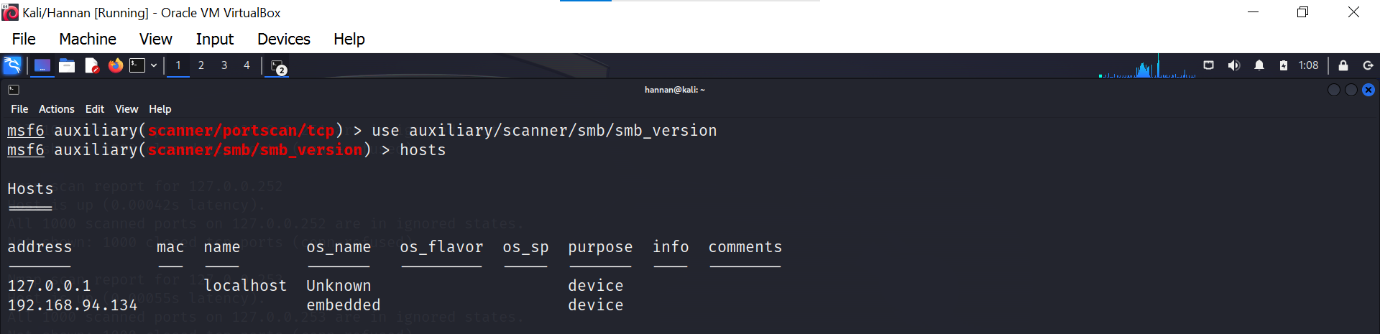




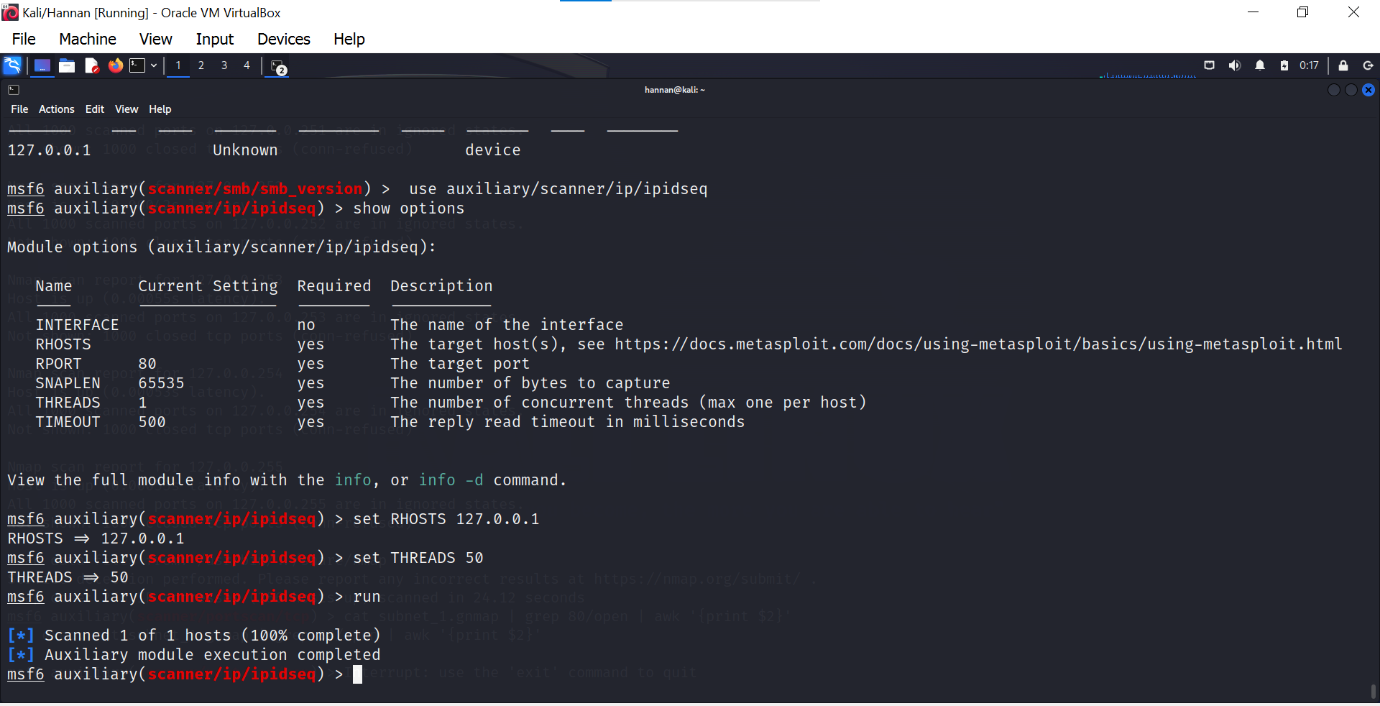
**Run Command:**  
****

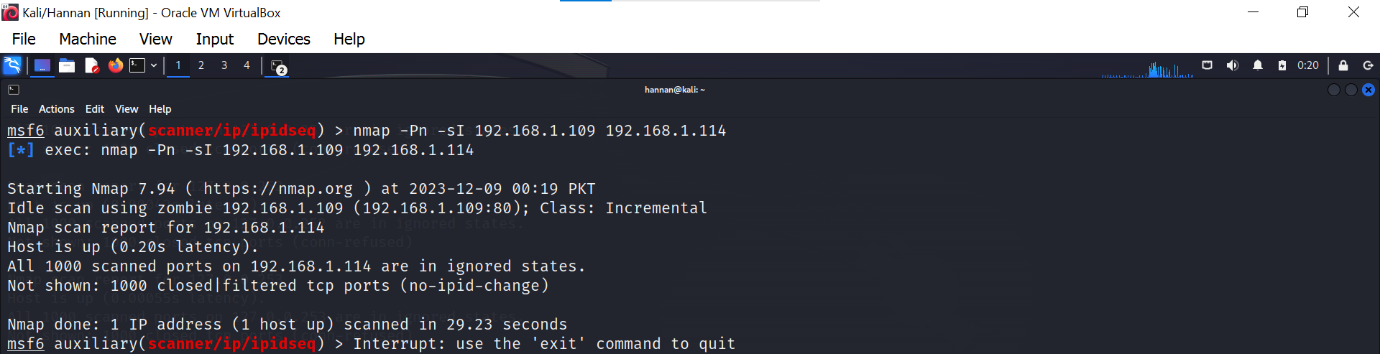
**SMB Version Scanning:**





**IDLE Scanning:**





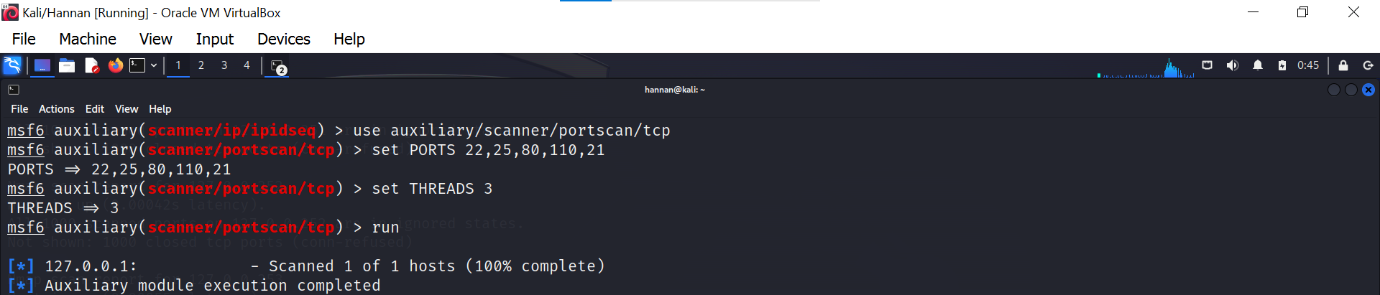
**Link 2:**

<https://www.cm-alliance.com/cybersecurity-blog/using-metasploit-and-nmap-to-scan-for-vulnerabilities>

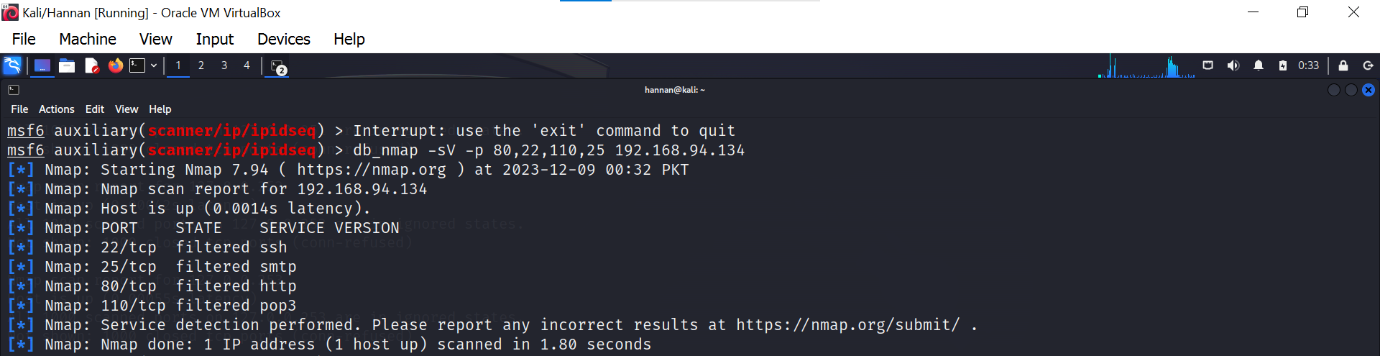
**Using Metasploit and Nmap to scan for vulnerabilities:**

use auxiliary/scanner/portscan/tcp

set PORTS 22,25,80,110,21

****

**Combining Nmap with Metasploit for a more detailed and in-depth scan on the client machine:**

****

## ****Scanning for vulnerabilities with Nmap and Metasploit:****

## C:\Users\Hi\Desktop\scanning vuln with ms and nmap.png