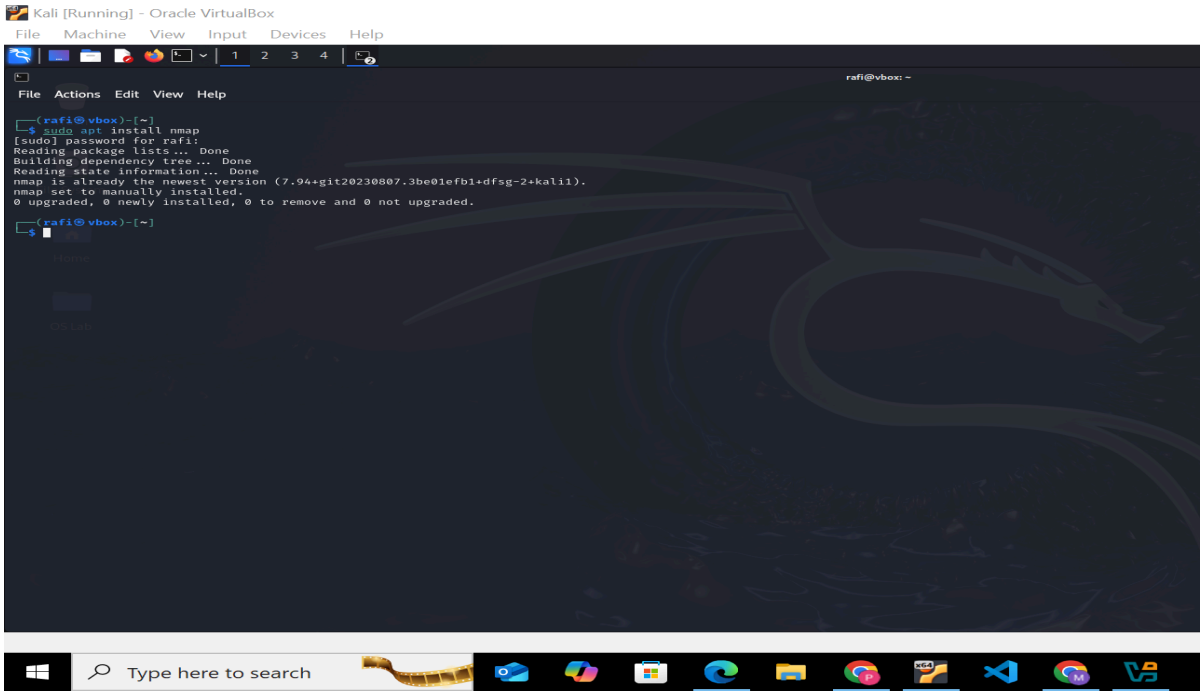
Basic Vulnerability Scan By nmap

Objective

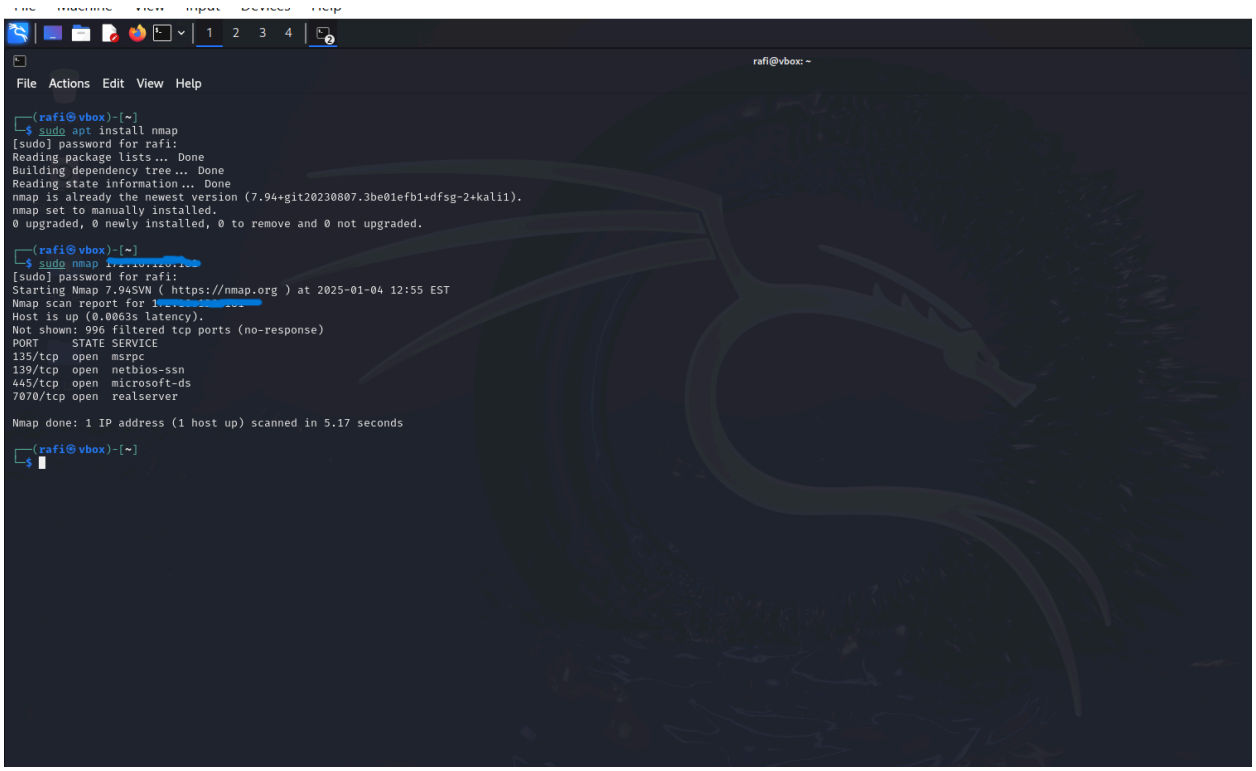
To perform a basic vulnerability scan on a target system to identify potential risks and vulnerabilities.

1. Setting Up the Environment



Nmap, a powerful network scanning tool, is installed and configured on Kali Linux. This tool is essential for scanning and analyzing the target system.

2. Scanning the Target IP:

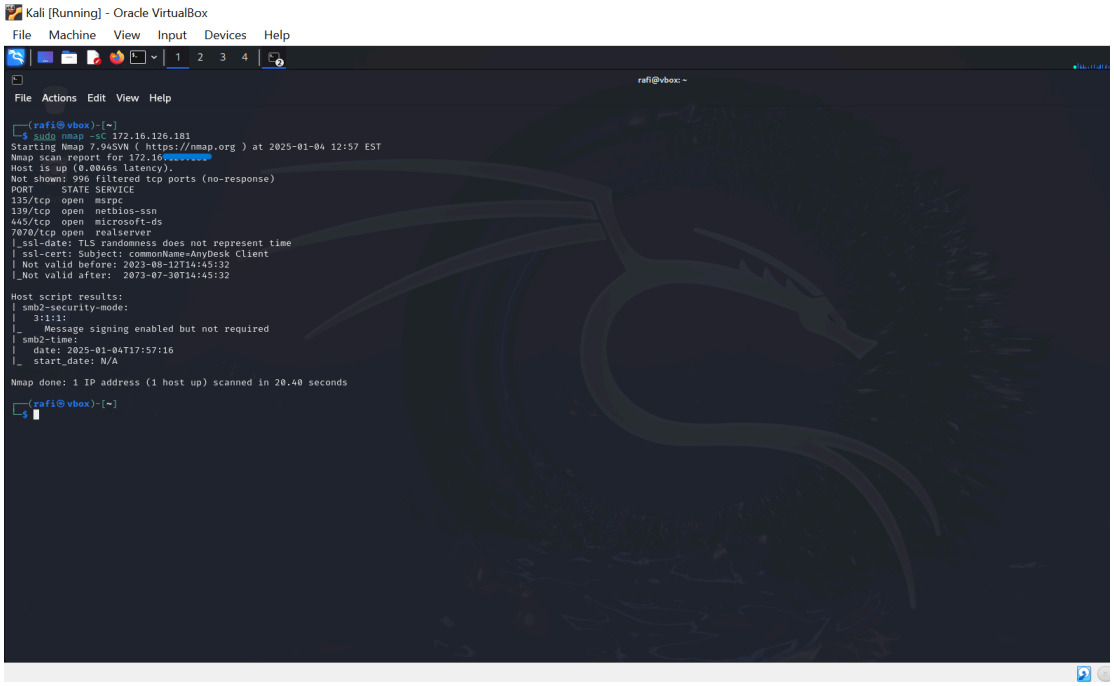


The target system is scanned to check if it is active and to identify any open ports. This provides an initial view of the system's exposure.

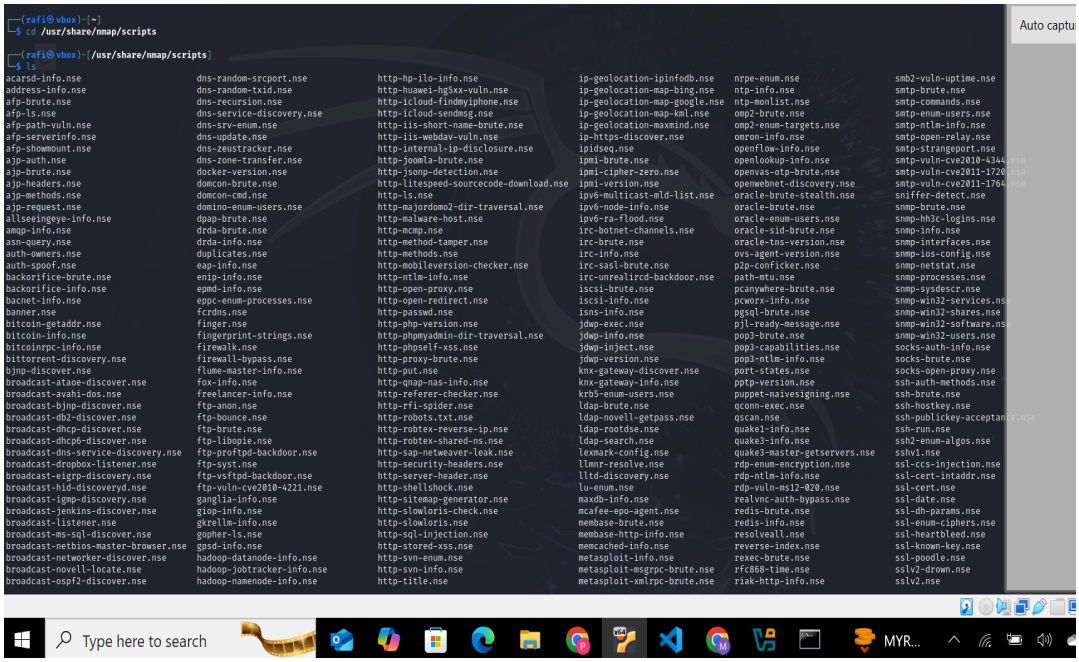
Here we can see several ports are open as 135,139,445

3. Testing for Vulnerabilities:

Using Nmap's built-in vulnerability scripts, the target system is analyzed for known vulnerabilities, including SMB-related issues.

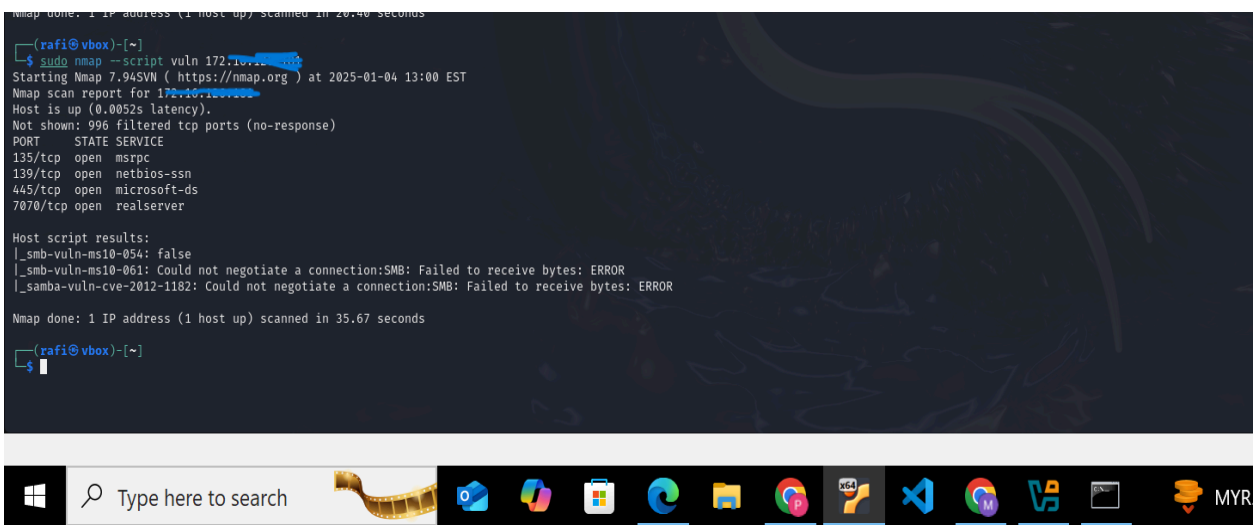


Also, there are a lot of built-in scripts available in Nmap that we can use specifically for specific vulnerability findings.



4. Findings and Analysis:

Here we perform a vulnerability by a script:



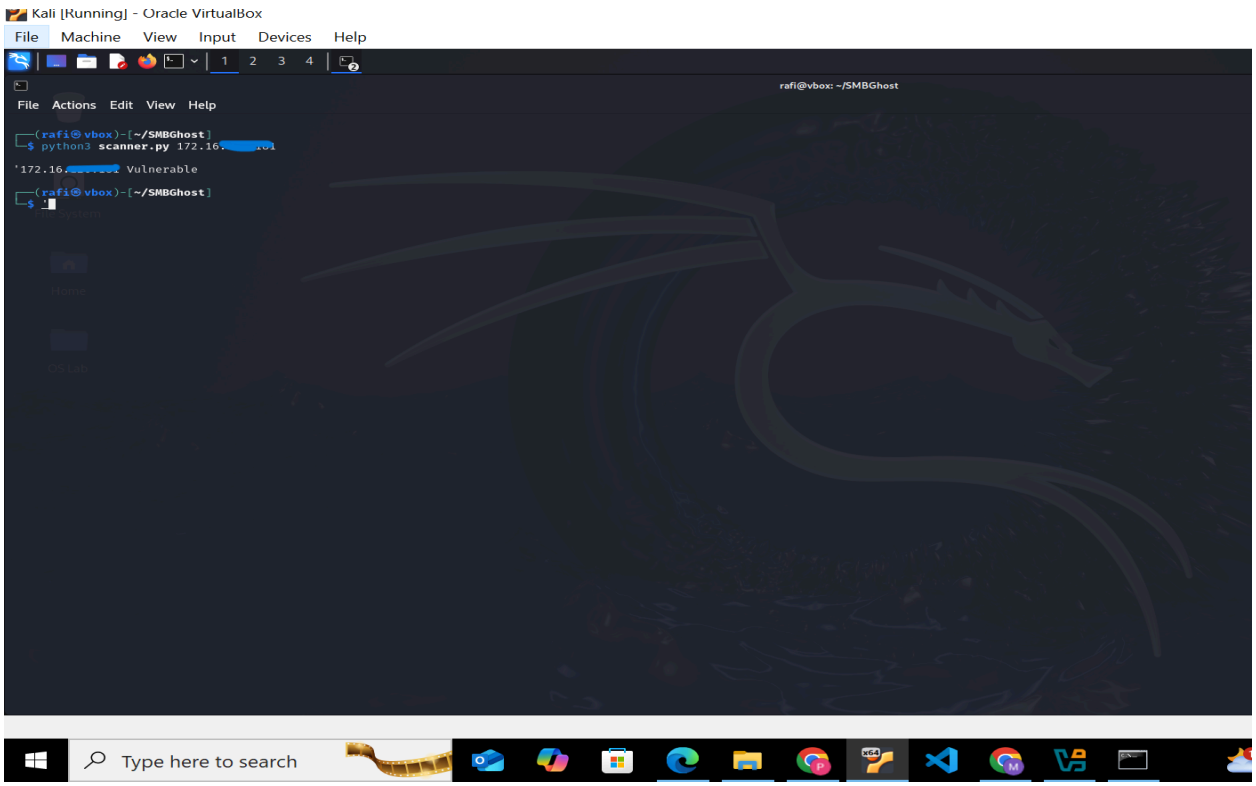
`vuln`	Scans for specific vulnerabilities.	`nmap --script vuln 10.10.10.0/24`

4.1 Summary of Open Ports

The scan reveals the following open ports, which provide insights into the services running on the target system:

- **Port 135:** Microsoft RPC
- **Port 139:** NetBIOS-SSN
- **Port 445:** SMB

4.2 Vulnerability Findings:



- **SMBGhost (CVE-2020-0796):**
  - A critical vulnerability in SMBv3 that could allow remote code execution or denial of service.
  - This issue has a high impact and requires immediate attention.

5. Recommendations;

1. **Apply Security Patches:** Ensure that all critical updates are applied to mitigate vulnerabilities like SMBGhost.
2. **Restrict Access:** Limit access to sensitive ports, especially from untrusted networks.
3. **Monitor SMB Traffic:** Use appropriate tools to detect and respond to suspicious activities.

6. Conclusion

The vulnerability scan highlights potential risks, including open ports and SMBGhost. Immediate remediation steps are recommended to secure the target system.