TASK 1: COMPREHENSIVE NETWORK VULNERABILITY ASSESSMENT

Introduction:

In the present era marked by rapid technological changes, the protection of the networks and the systems has become essential. As cyber threats become smarter, there is a need for organizations to perform network vulnerability assessments to find out any weaknesses in their networks and deal with them. This is the reason why the purpose of this work, which is to carry out a network assessment, arises.

The task at hand also pertains to the employment of the network security principles, which is the theoretical development, in the real life. By carrying out this assessment, you will gain experience in determination and evaluation of factors posing the threat to the network and in measures taken to improve its safety.

For the successful completion of this task, one should possess adequate knowledge on aspect of network vulnerability assessment and risk analysis. Furthermore, understanding how to operate Nmap to scan networks, OpenVAS to check for vulnerabilities, and Netcat for basic network troubleshooting will be required.

In this introduction, the aim is to give the reader a summary of the aim of carrying out a full network assessment as well as the abilities and gear needed for the successful performance of the assessment. You will gain practical knowledge in terms of learning how to deploy the defenses of a network in this particular project making such a project very worthwhile in terms of practical use.

Skills:

- Network Vulnerability Assessment
- Risk Analysis
- Remediation Strategies

Tools:

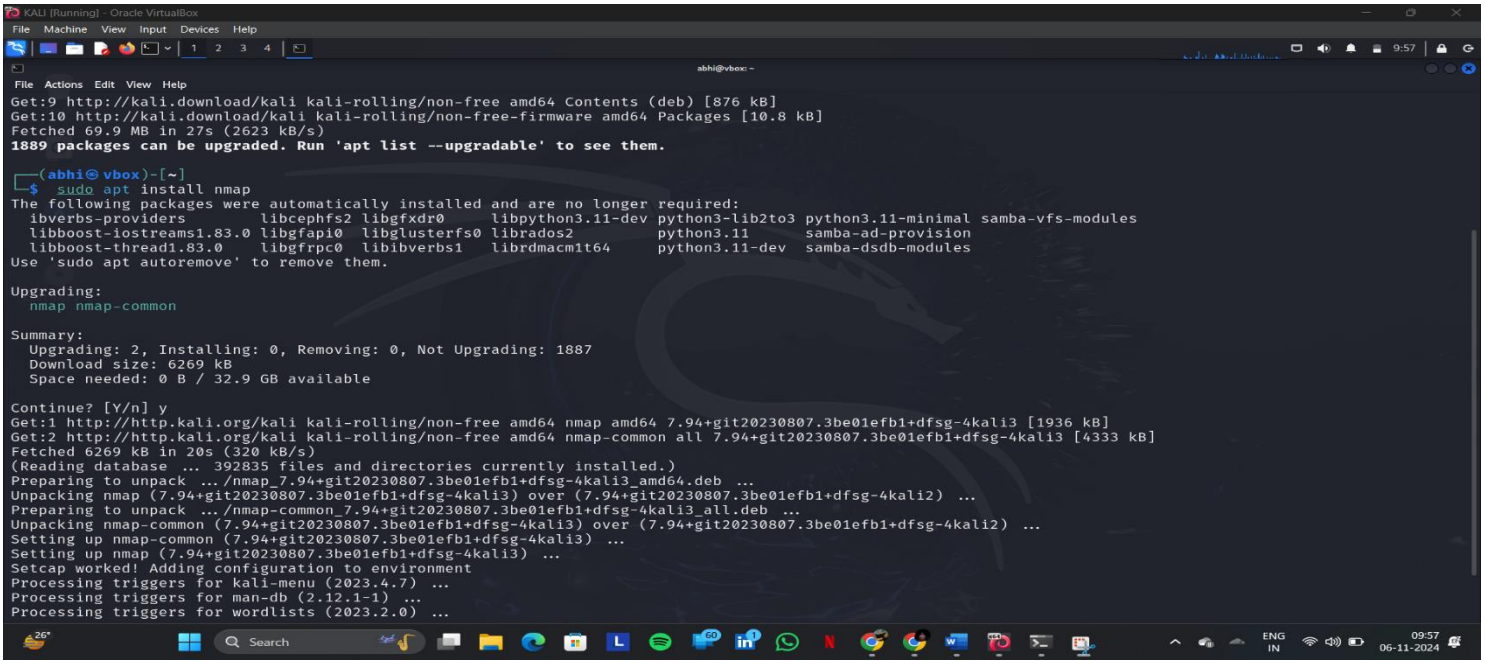
- Nmap (for network scanning)
- OpenVAS (for vulnerability scanning)
- Netcat (for network diagnostics)

1.Network Scanning:

a.Install Nmap:

If you don't have Nmap installed, you can download and install it by using these commands.

- sudo apt update.
- sudo apt install nmap.

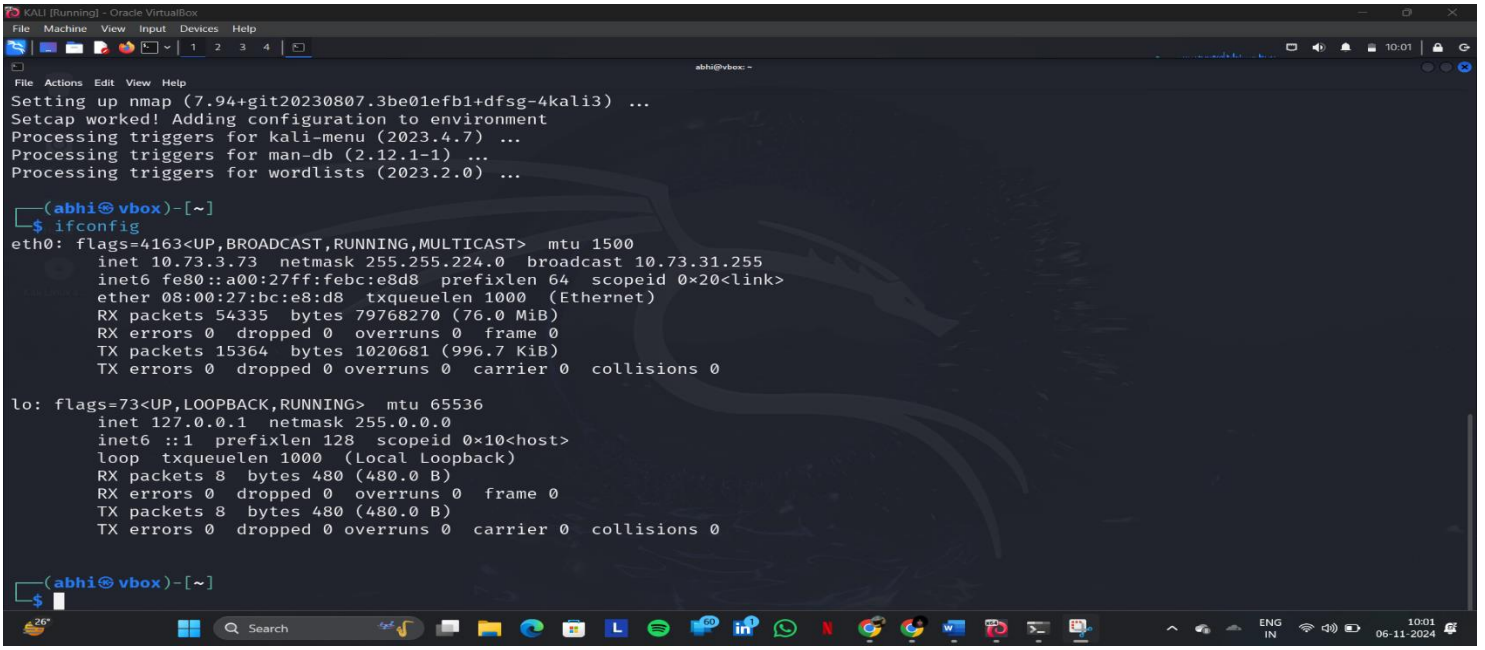


b.Identify Your Network Range:

Determine your local network range.

You can usually find this in your router settings or by checking your IP configuration by these commands.

- ifconfig .



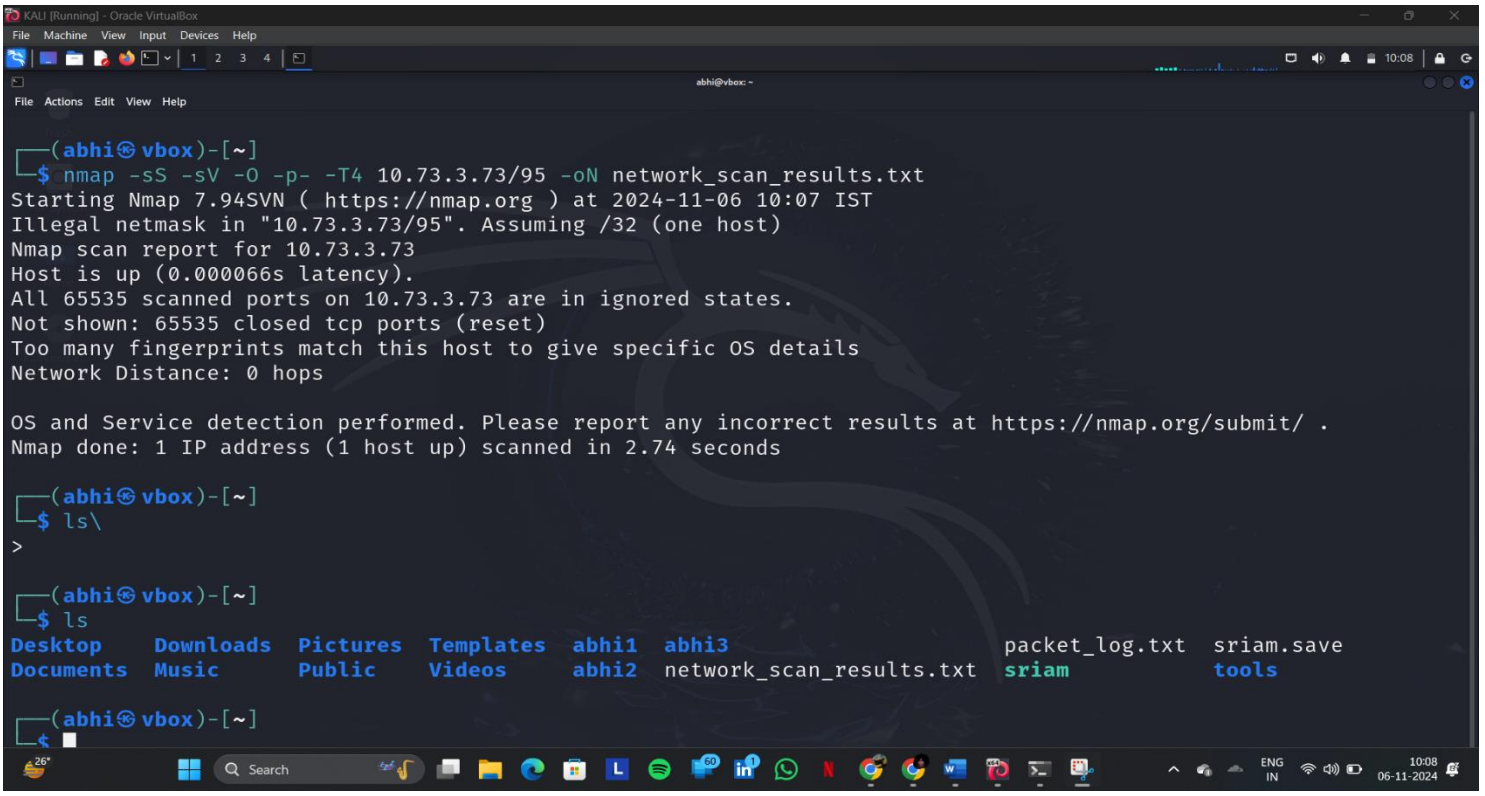
c.Perform the Scan:

use the following command to perform a comprehensive scan:

- nmap -sS -sV -O -p- -T4 10.73.3.73/95 -oN network_scan_results.txt.

Breakdown of the Command:

- -sS: SYN scan, stealthy and fast.
- -sV: Service version detection.
- -O: Operating system detection.
- -p-: Scans all ports (1-65535).
- -T4: Increases speed; use cautiously.
- 192.168.1.0/24: Your network range.
- -oN network_scan_results.txt: Saves the results to a file named network_scan_results.txt.



d. Review the Results:

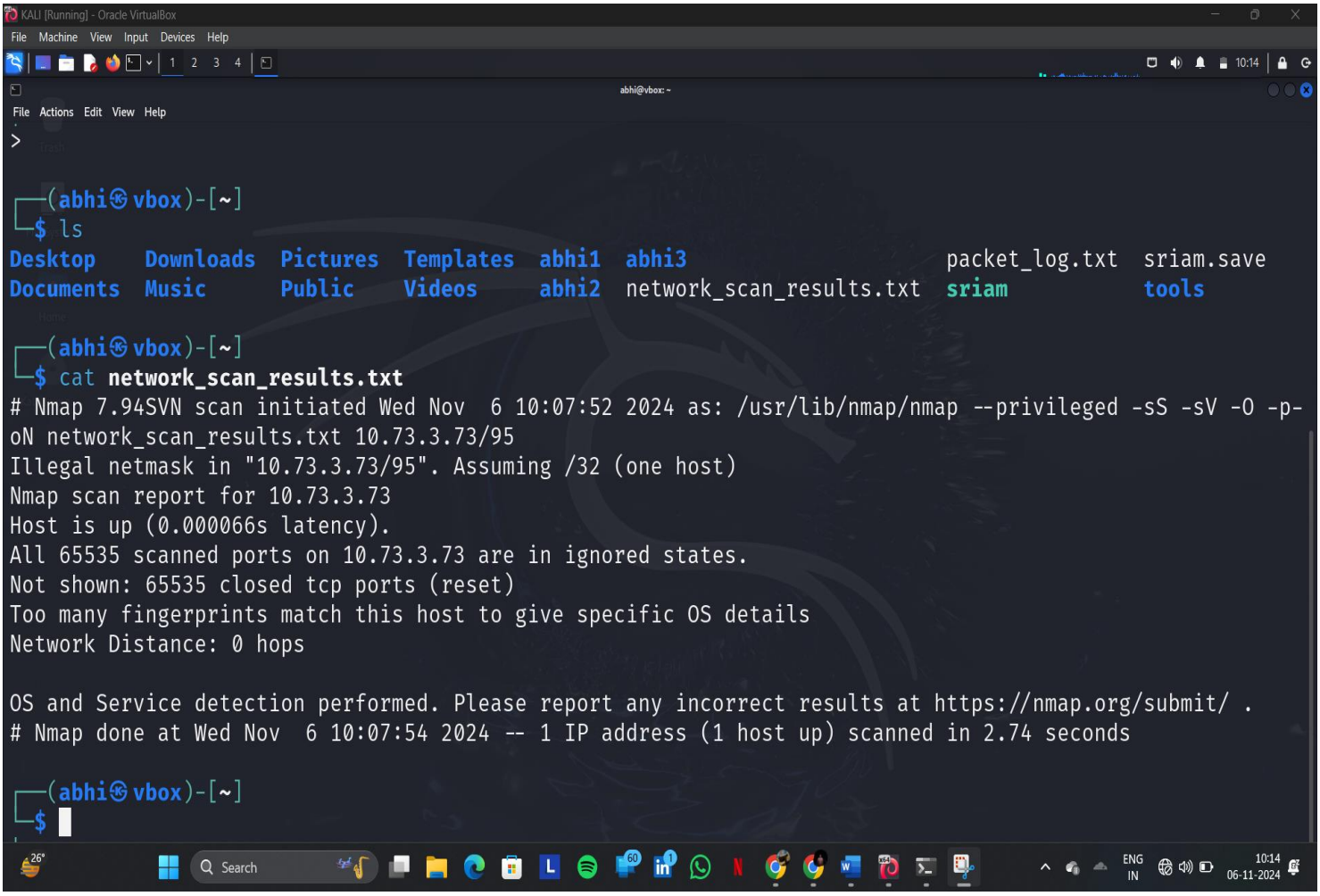
Once the scan completes, we can open the output file with any text editor:

- cat network_scan_results.txt.

e. Analyze the Output;

In the results, we'll find:

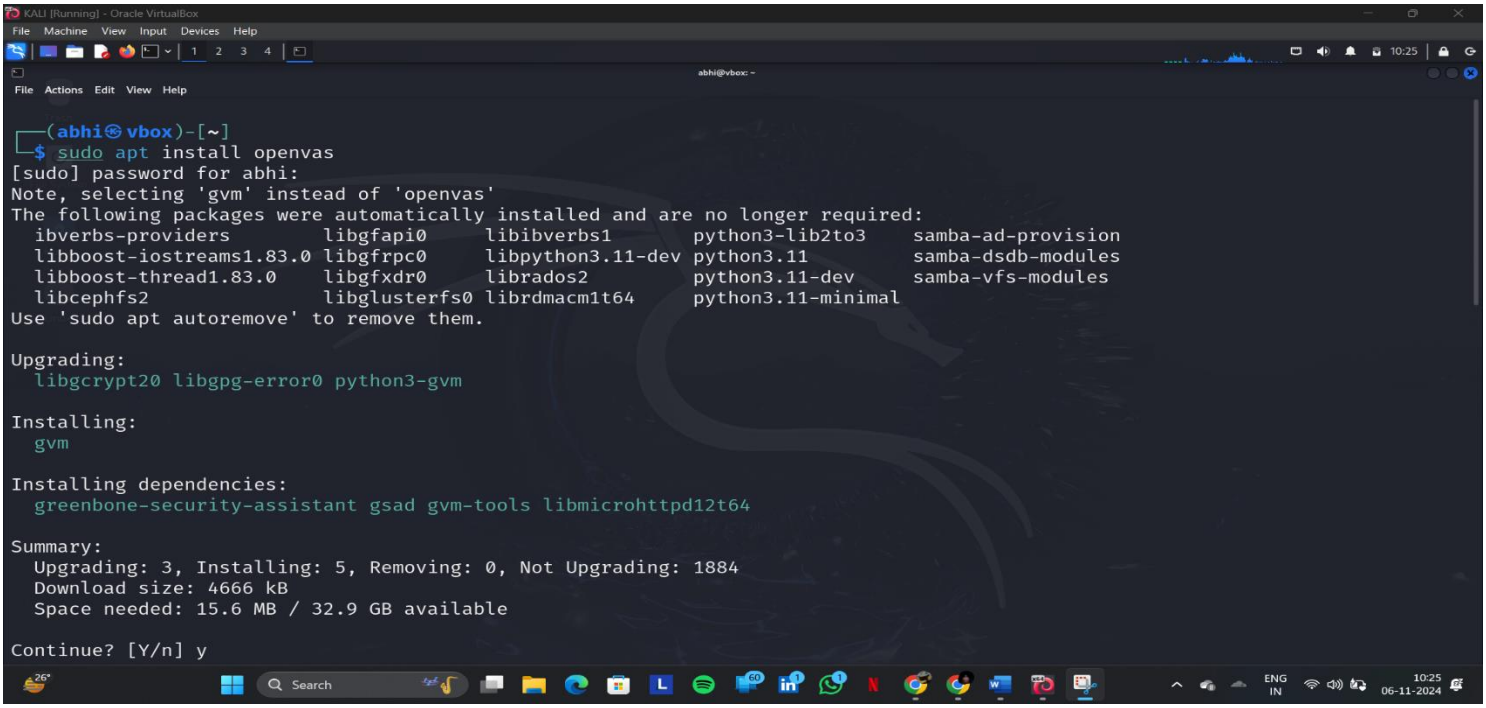
- **Active devices**: Listed with their IP addresses and MAC addresses.
- **Open ports**: A list of ports detected as open on each device.
- **Services**: Information about the services running on those ports.
- **Operating systems**: The estimated OS for each device (if detectable).



2. Vulnerability Identification:

1. Install OpenVAS:

- sudo apt install openvas.

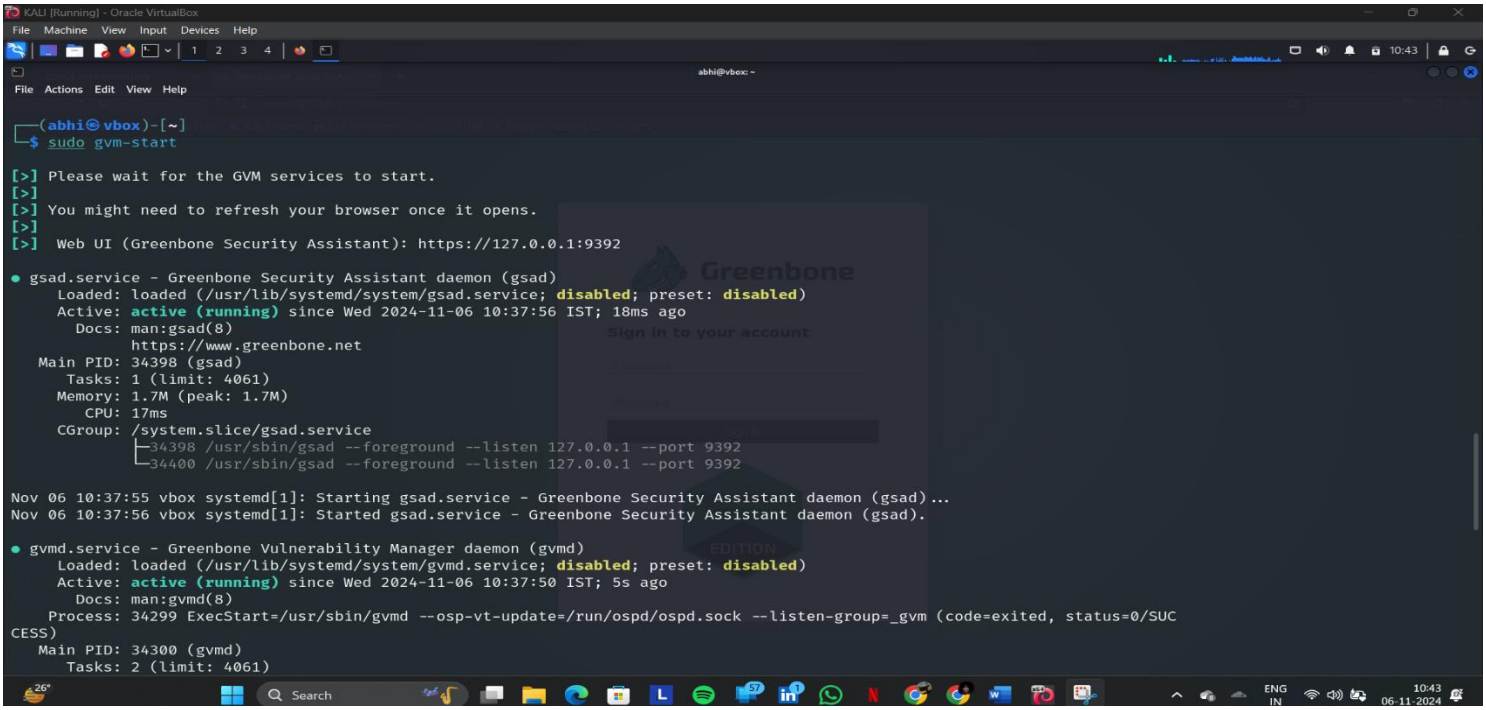


a.This command will set up OpenVAS, downloading necessary components and creating a default user.

- sudo openvas-setup.

b.Start OpenVAS Services:

- sudo openvas-start.



c.Access the Web Interface: Open a web browser and go to:

- https://127.0.0.1:9392

Log in with the credentials created during setup.

2.Configure OpenVAS:

a.Update NVTs: After logging in, update the Network Vulnerability Tests (NVTs) database. This can usually be done from the "Administration" tab.