Lab 1: Network Scanning with Nmap

- **Performed network scanning to identify open ports and services on a target network.**
- **Analyzed the results to determine potential vulnerabilities.**

Author: Shashangka Upadhyaya

Provided a report which includes the following item.

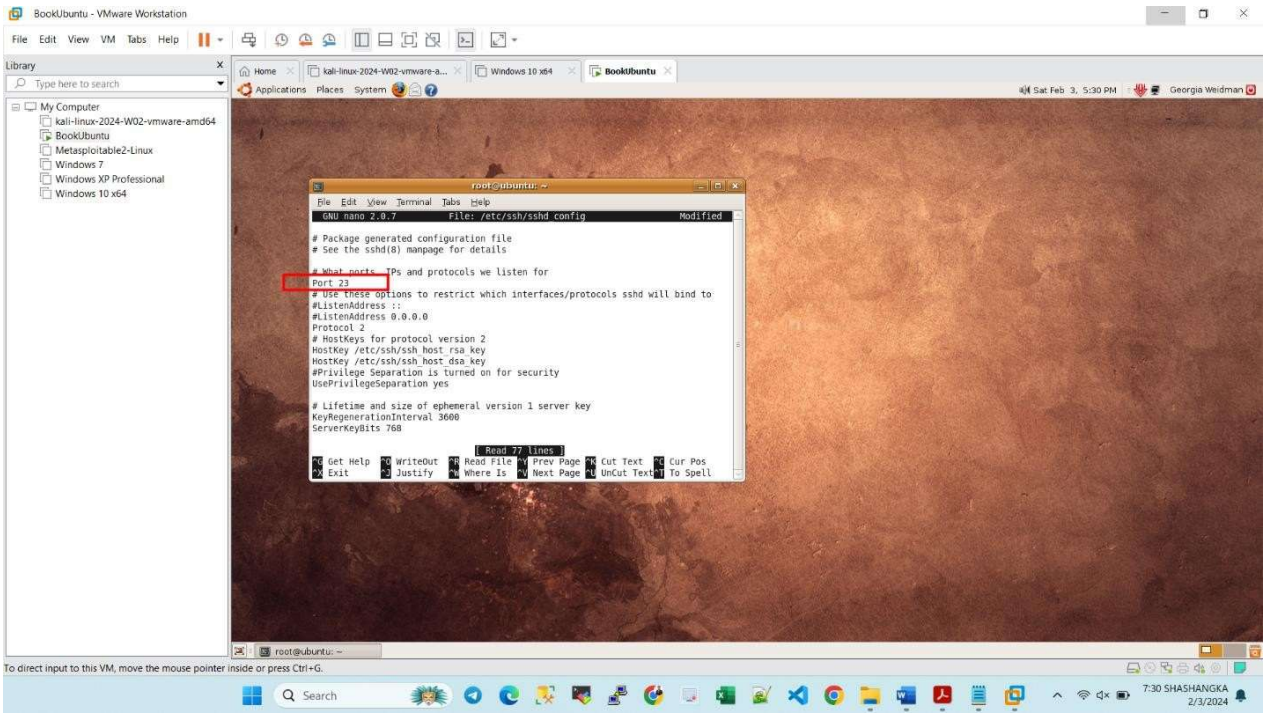
At first, I did all the necessary steps provided on the Lab Assignment 4. Let's have a look at the all the steps done on the Lab Assignment on windows ubuntu and kali Linux machine before doing task 1, task 2 and task 3

Step 1:

- Here I Open a terminal on Ubuntu Linux, switch to root, modify sshd config to change port 22 to 23, save changes, then instruct sshd to re-read config**.**

Command used to switch to root: **sudo su -**

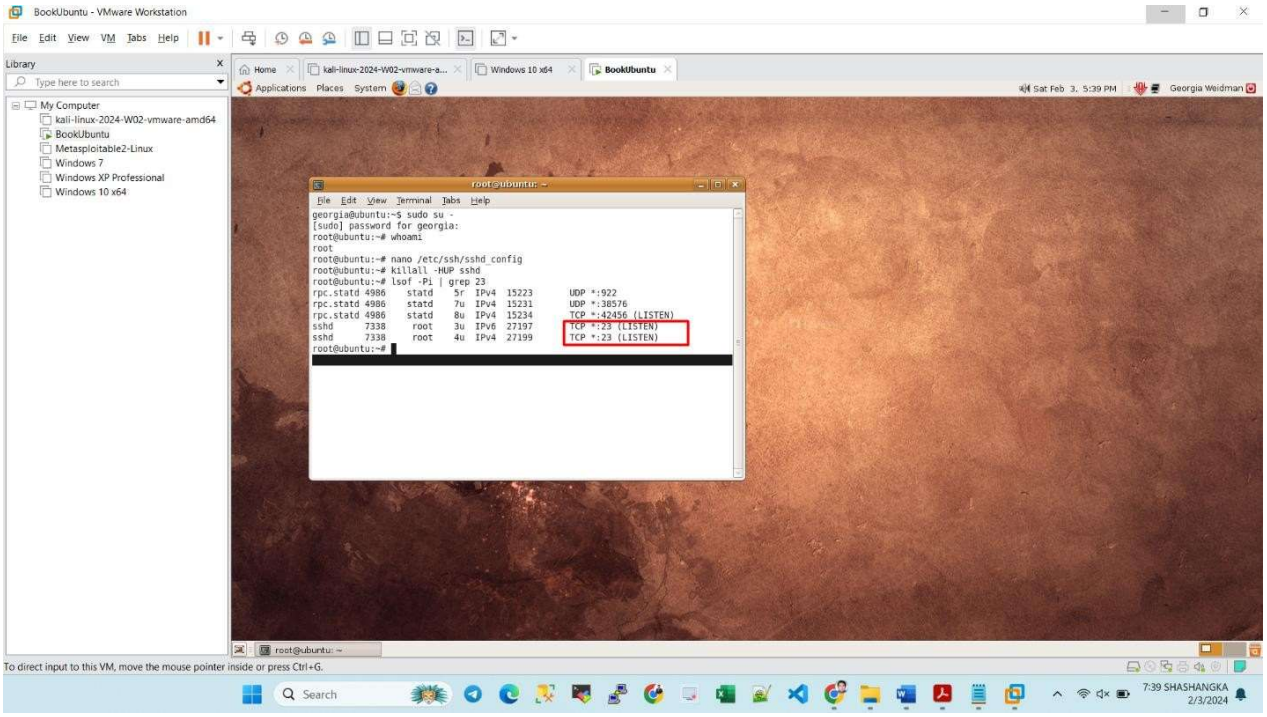
Command used to modify sshd config to change port 22 to 23.
nano /etc/ssh/sshd_config



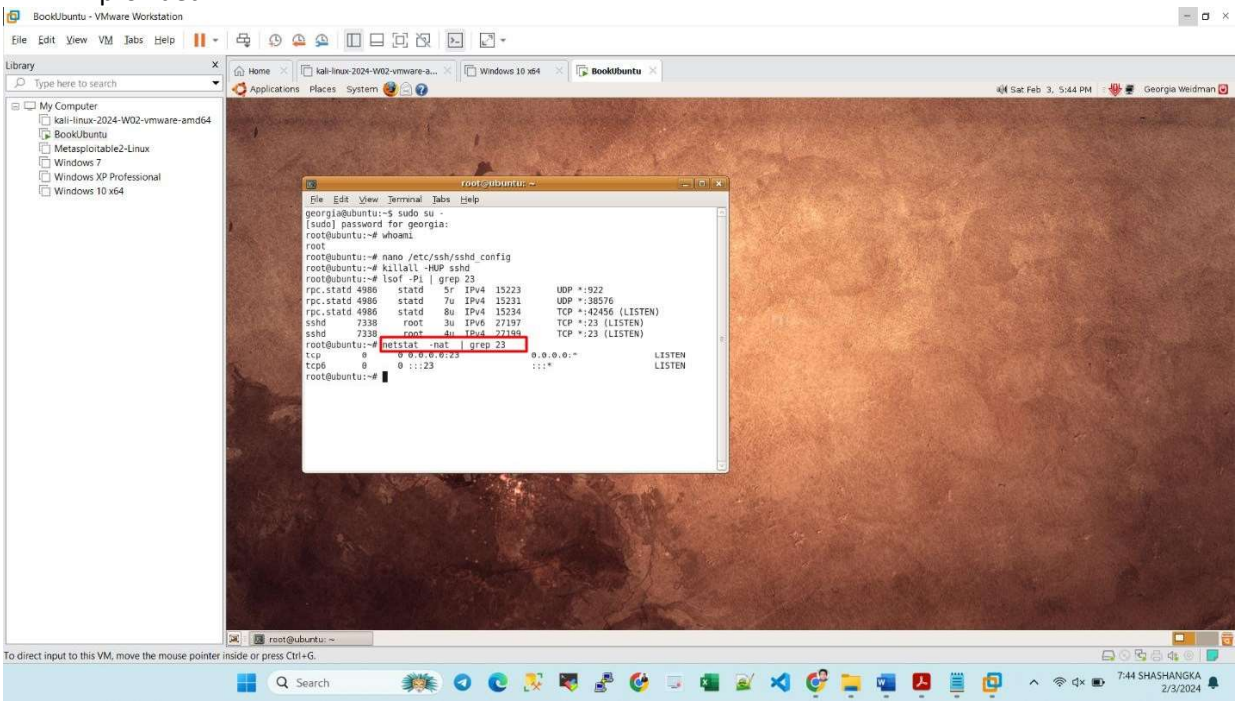
Step 2:

- Now, I made sshd reread its configuration file by sending it the HUP signal by using the command: **killall -HUP sshd**

- I Verify that my sshd is listening on TCP port 23 by typing **lsof -Pi | grep 23**

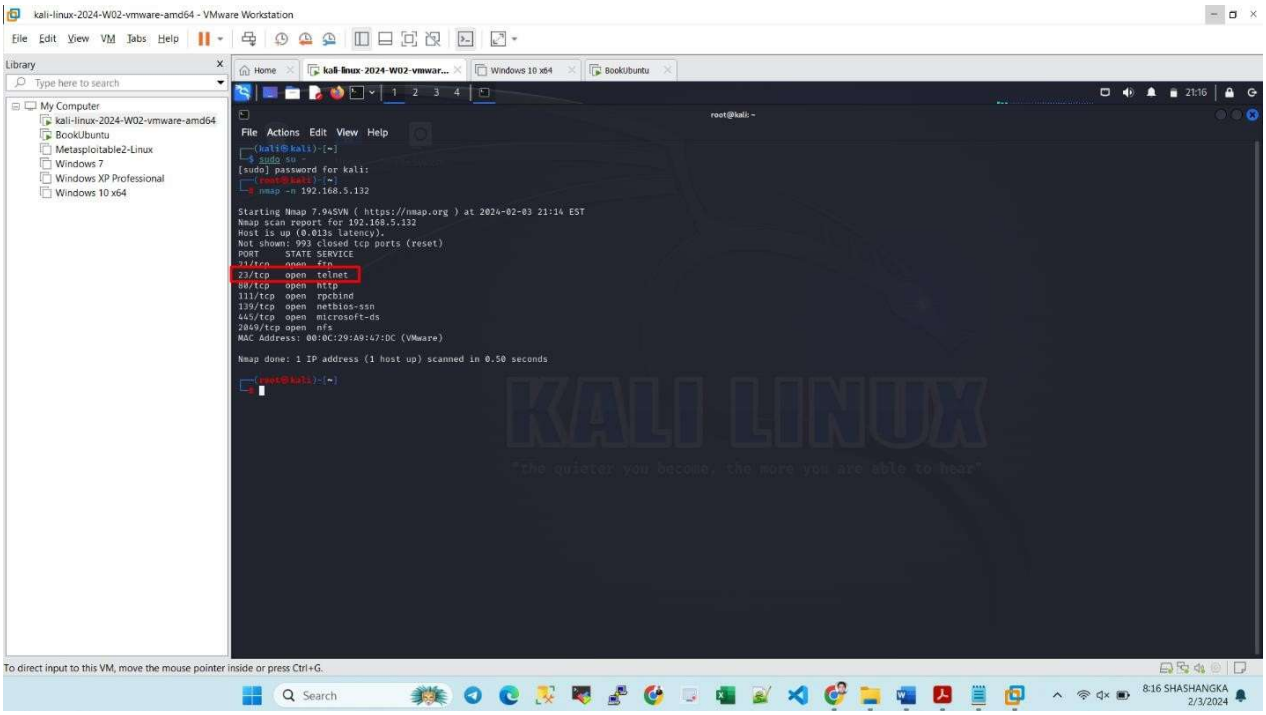


- Now I Try to use the netstat command to accomplish the same task Here is the screenshot provided.



Step 3:

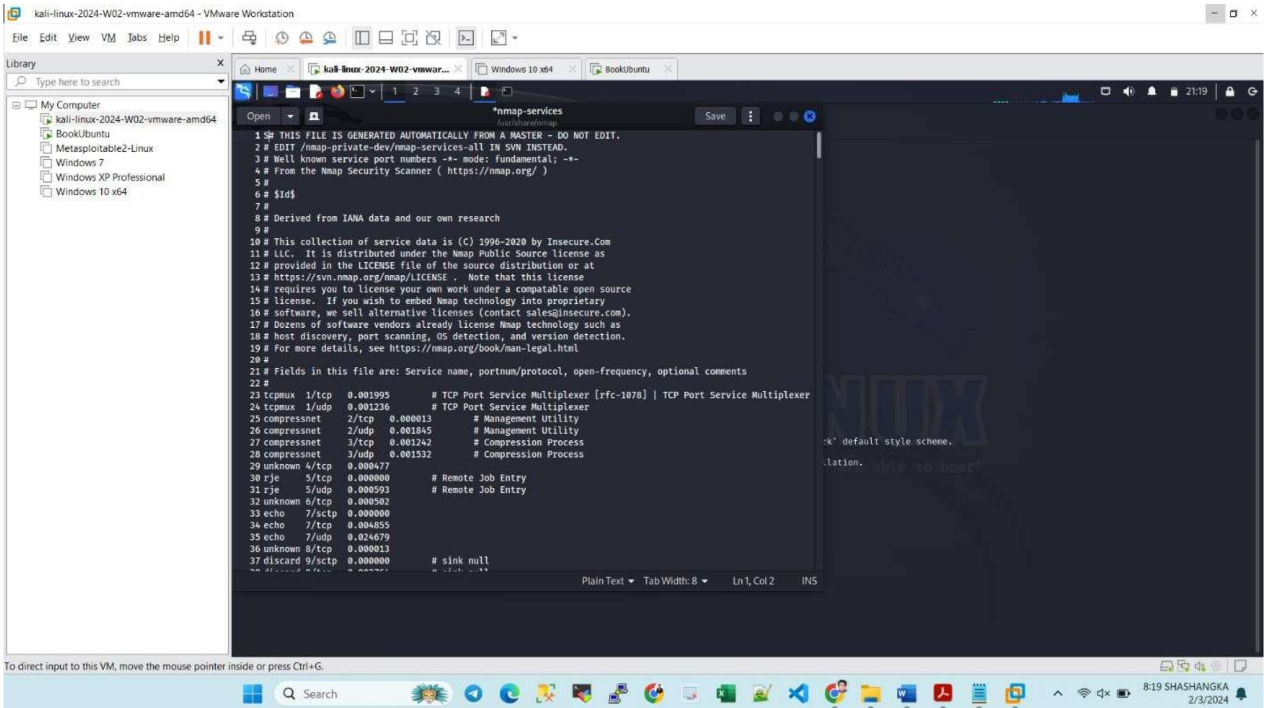
- **Now I** Move to Kali Linux machine and switch to the root account, and I run Nmap against the Ubuntu VM. I used the following command nmap **-n 192.168.5.132**



Step 4:

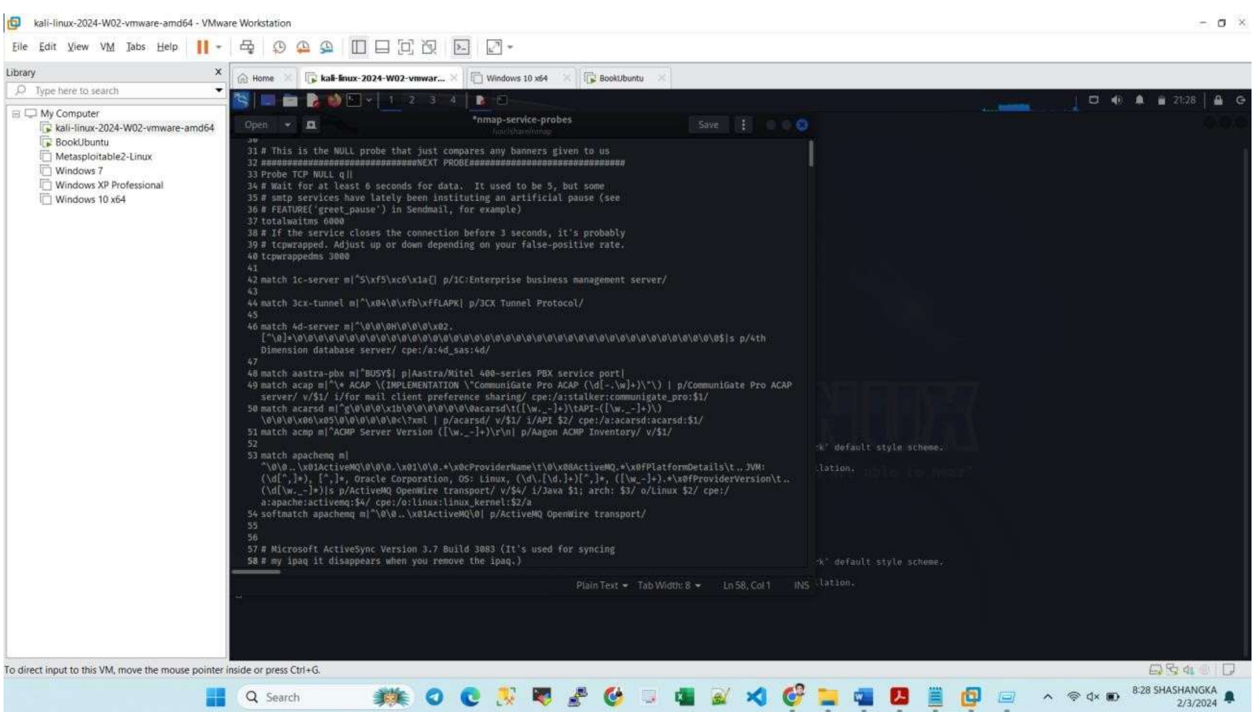
- At the Kali Linux command line, I ensure I execute gedit as a regular user, not as root, to avoid any issues with opening.

- Then I Use the following command: **sudo gedit /usr/share/nmap/nmap-services**



Step 5:

- At first, I see how Nmap conduct the version scan. At the Kali Linux terminal, run **sudo gedit /usr/share/nmap/nmap-service-probes**



Now we re-run the Nmap against the Ubuntu virtual machine with a version scan
nmap

1) Provide screenshots for the Task01~03 (3 screenshots are needed)

Task 01

Step 1:

- I tried to re-run the Nmap against the Ubuntu virtual machine with a version scan.

- **Code is executed on kali Linux machine from root user.**

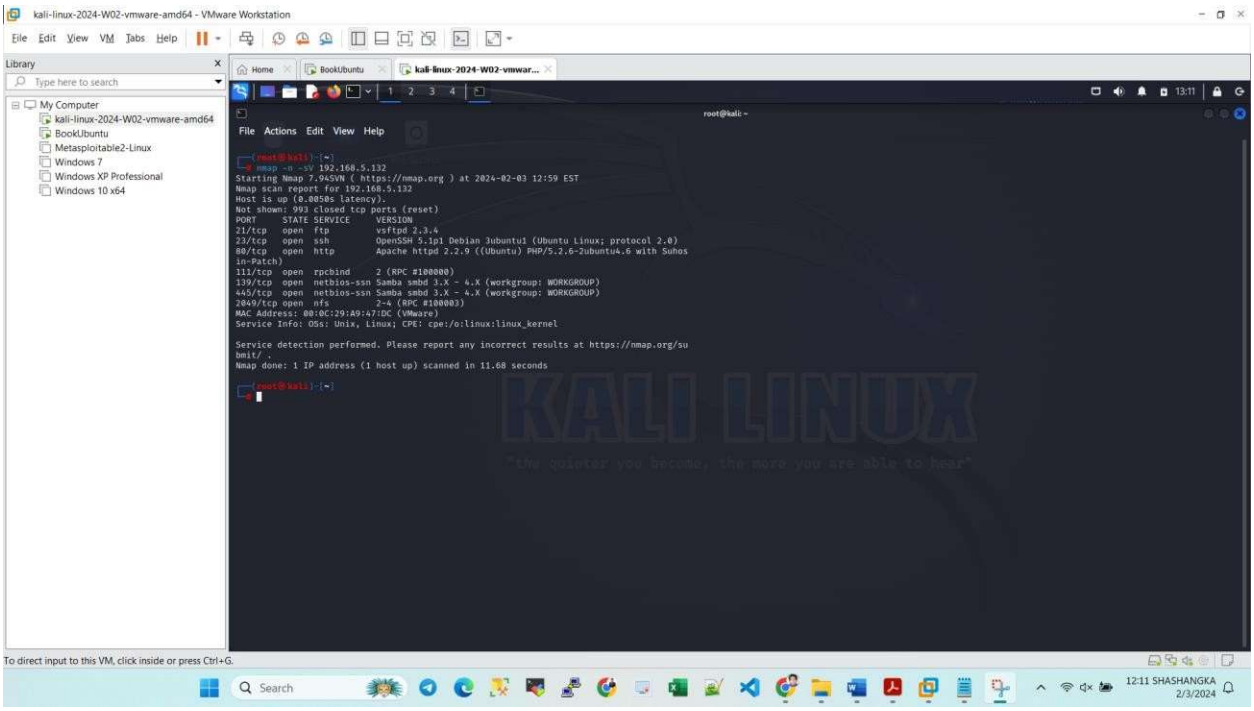
  nmap -n -sV 192.168.5.132

  where 192.168.5.132 is my ubuntu IP Address.

Step 2:

- This helped me to find the version of each running services in an extra column called Version as shown below on the screenshot.

Screenshot Task 1:



- This information would be used to conduct vulnerability research to find out the potential exploits of the Target System.

Task 02

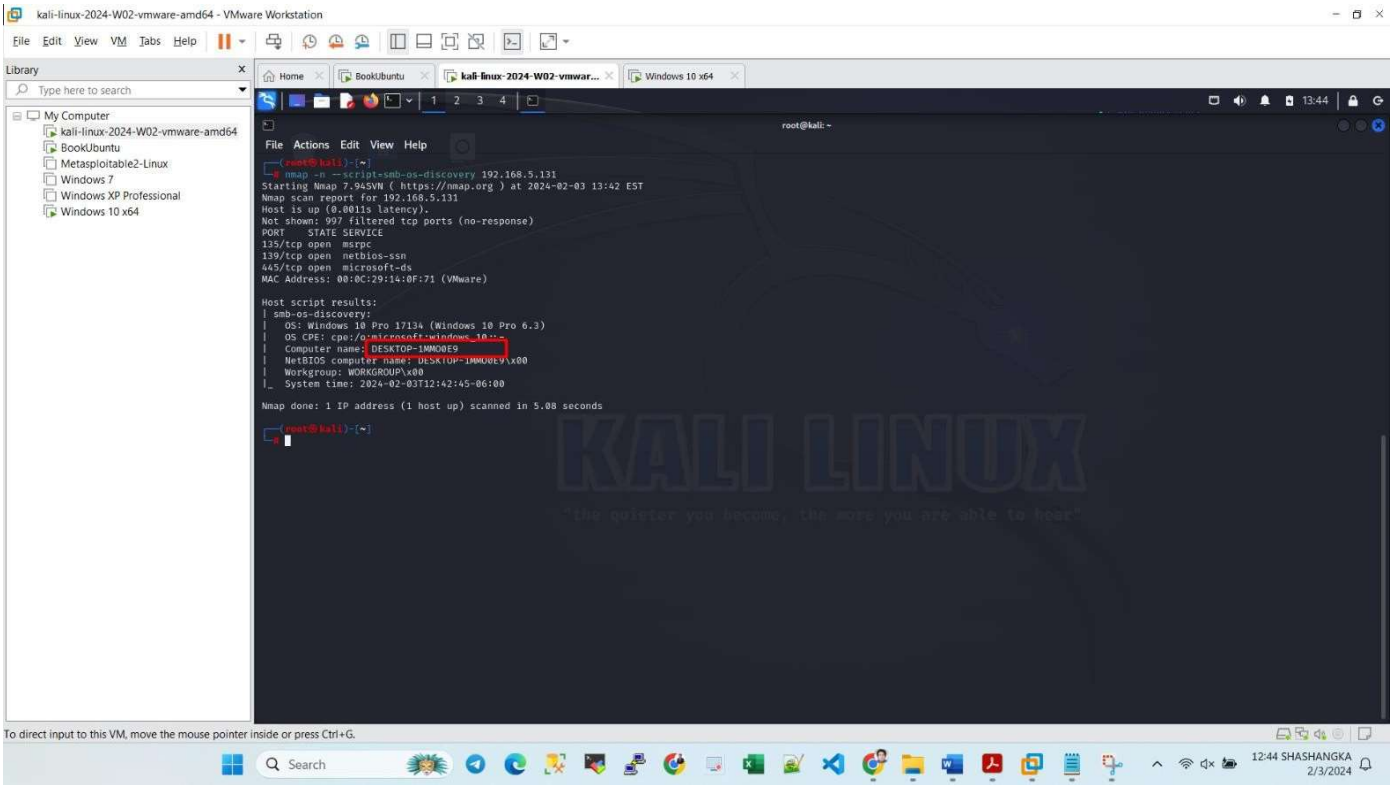
Step 1:

- I attempted to execute the Nmap smb-os-discovery.nse script, which provides information about the operating system of the target machine, including machine names. This data could be valuable for user enumeration processes, such as utilizing tools like sid2user.

Step 2:

- **Code is executed on kali Linux machine from root user.**
- **nmap -n --script=smb-os-discovery 192.168.5.131**
- **where 192.168.5.131 is windows 10 IP Address.**

Screenshot Task 2:



Step 3:

- The output reveals that the name of the Windows 10 system is DESKTOP-1MMO0E9.

- The reason Nmap performed a port scan in addition to running the smb-os-discovery.nse script is to ascertain which ports are open. This information is crucial for determining the availability of the service being tested by the script.

Task 03

Step 1:

- I tried to run the script below and found out that the directories that are listed in the robots.txt file of the UCM website. Also notice that both ports 80 and 433 are open.

Step 2:

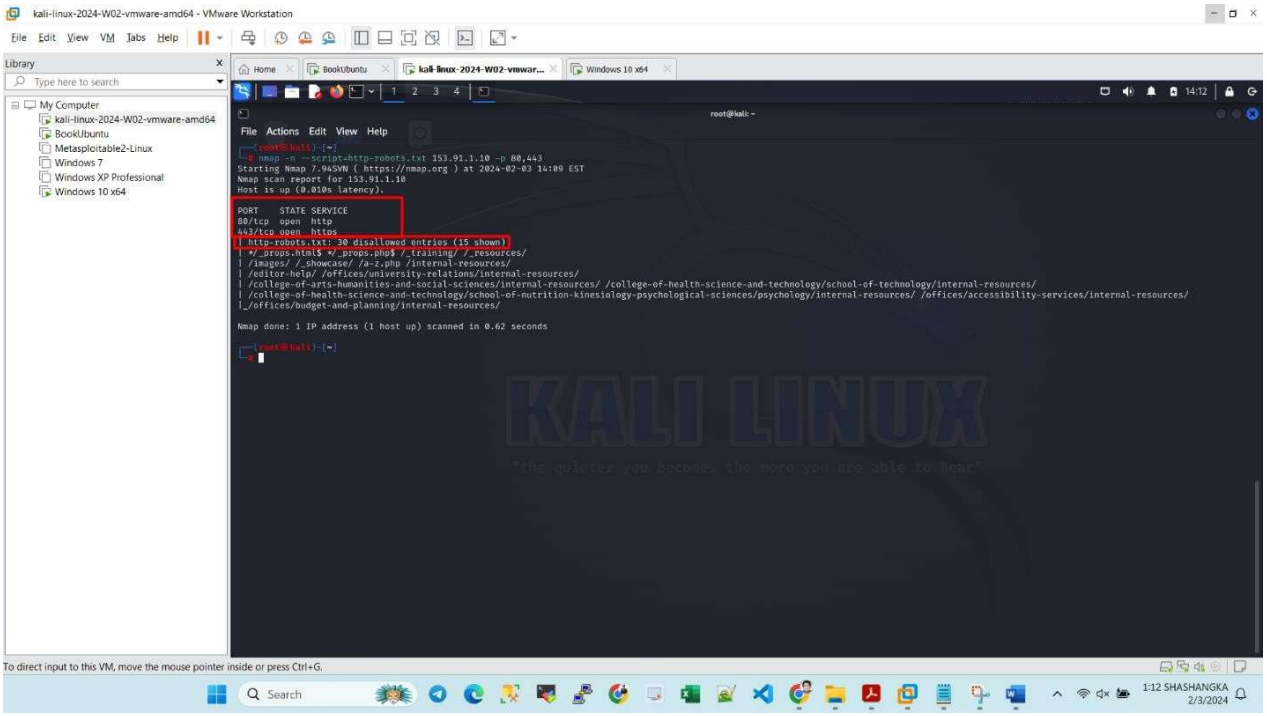
- **Code is executed on kali Linux machine from root user.**

- **nmap -n --script=http-robots.txt 153.91.1.10 -p 80,443**

- **where 153.91.1.10 is UCM IP Address and 80 and 443 are port numbers**

Screenshot Task 3: Finally, I came to know that NMAP not only helps to view us open port of the target It also helps to find robots.txt file and its directory too.

We now see all the directories that are listed in the robots.txt file of the UCM website. Also notice that both ports 80 and 433 are open**.**



Task 2

Review the information about the whois-ip script at https://nmap.org/nsedoc/scripts/whoisip.html

Now I Run the script against an UCM Provide a screenshot showing the output of the script.

I review the information from the given website and came to know these things that are listed in points.

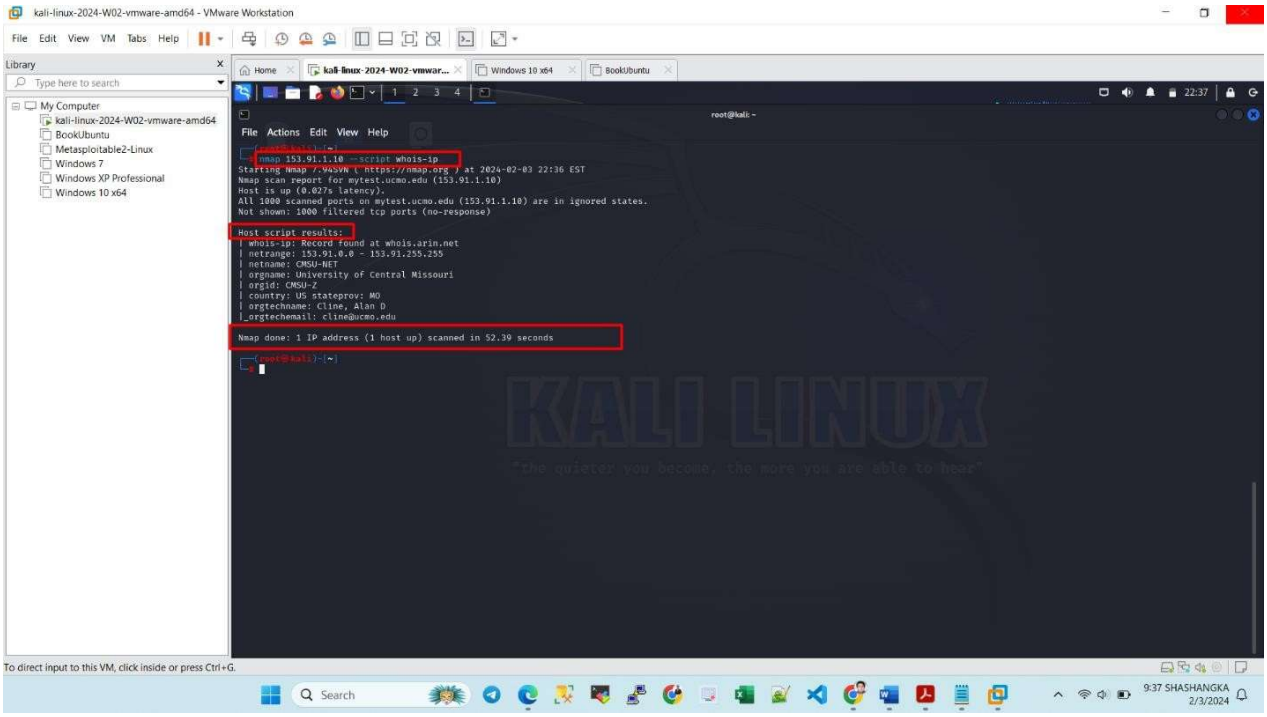
- The “ whois-ip ”script in Nmap sends a WHOIS query to the relevant WHOIS server for the provided IP address.
- The server responds with registration details, including the owning organization, registrant contact information, registration, and expiration dates.

- Additional technical information about the **IP address range** might also be included in the response.

- **Command for this is: nmap 153.91.1.10 --script whois-ip**

- **where 153.91.1.10 is UCM IP address my target system**

Target System: 153.91.1.10 (UCM IP Address)



About the output:

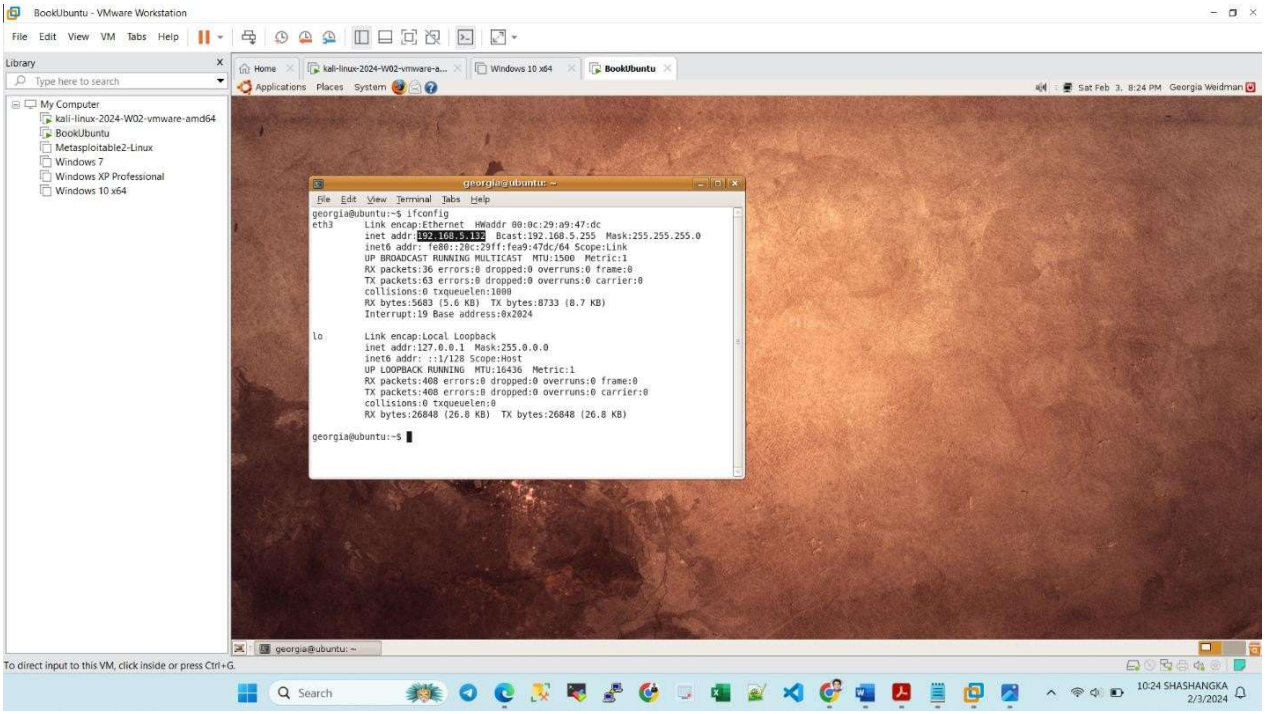
- Network administrators and security professionals benefit from the information provided by the “whois-ip” script output.

- Let’s see in the context of UCM just knowing its IP address and Nmap tool we came up with all the net range of University of Central Missouri IP address, also the country United States and the state name information. Nmap scan report is very useful both for attackers and security professionals.
- It assists in getting the ownership and registration details associated with a given IP address.
- This information serves various functions, including troubleshooting network issues, examining potential security vulnerabilities, and gathering intelligence on target networks.

3. Review the information about the banner script at https://nmap.org/nsedoc/scripts/banner.html.
Run the script against Ubuntu IP address. Provide a screenshot showing the output of the script.

Step 1:

At first, I found the ubuntu ip address (my target) IP and then I Run the script against Ubuntu IP address

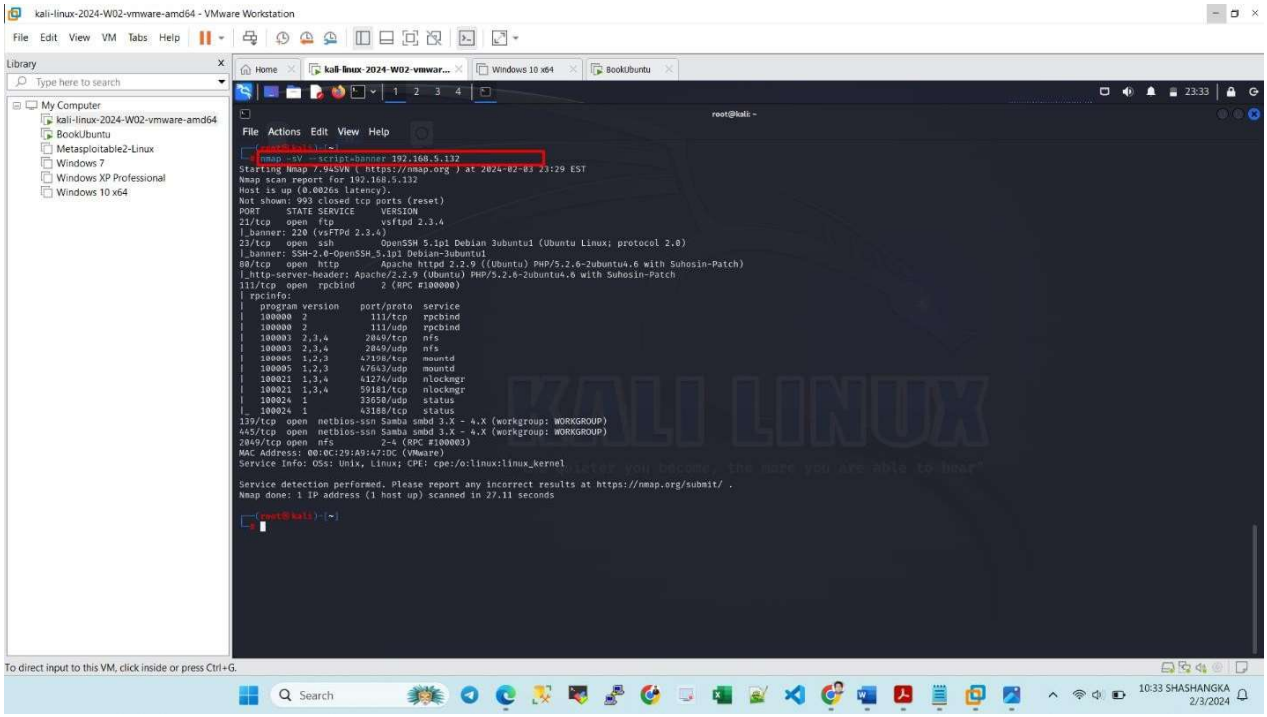


Step 2:

- My script:

nmap -sV --script=banner 192.168.5.132

- I run the banner script from my kali Linux machine to my target machine (Ubuntu). Then I Provide a screenshot showing the output of the script.



Conclusion:

I review the information from the given website and came to know these things that are listed in points.

- **A banner grabber is a tool that connects to an open TCP port** and retrieves information sent by the listening service **within a five-second time frame**.
- This tool aids in network reconnaissance, providing initial insights into running services and applications on target systems.
- It assists in assessing security posture, identifying outdated or vulnerable software versions, and supporting vulnerability assessment and penetration testing endeavors.