

ETHICAL HACKING

ASSIGNMENT-4

Name: Dasari Sanath Kumar

CRN:22285

ID: 700760349

- In this lab we are going to Use Nmap to perform various scan such as TCP, UDP, version and OS fingerprinting.
- Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.
- OS fingerprinting is the process a hacker goes through to determine the type of operating system being used on a targeted computer.

apt-get install nmap - This command is used install nmap packages.

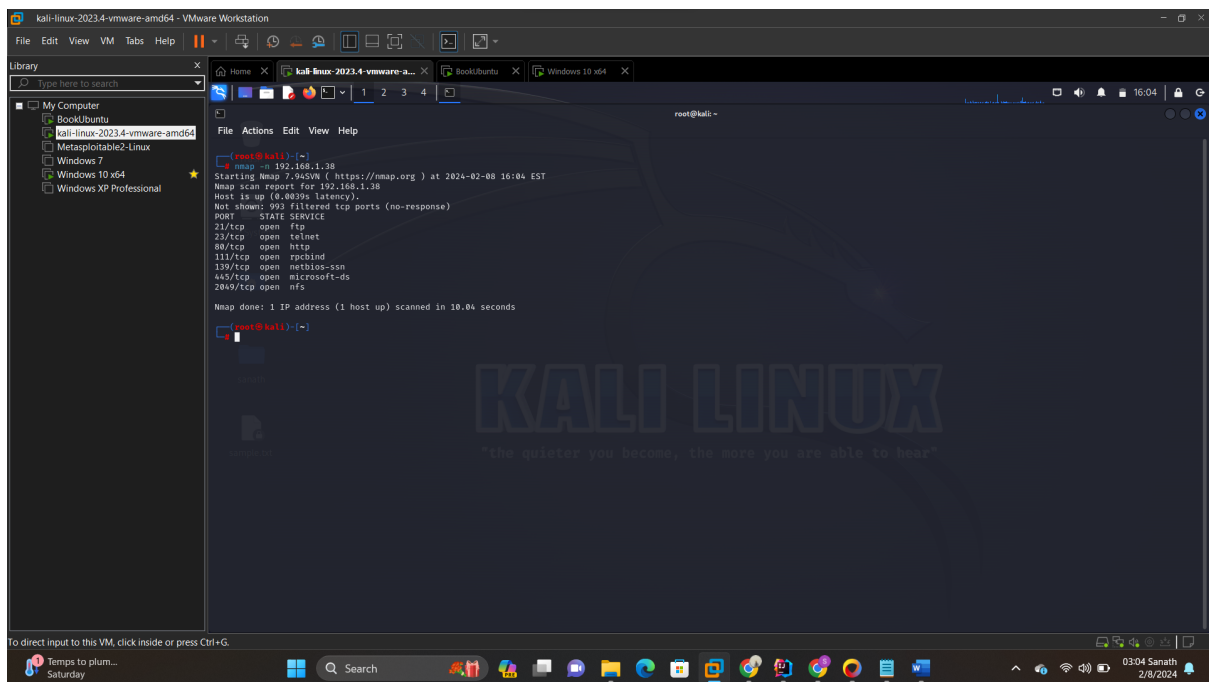
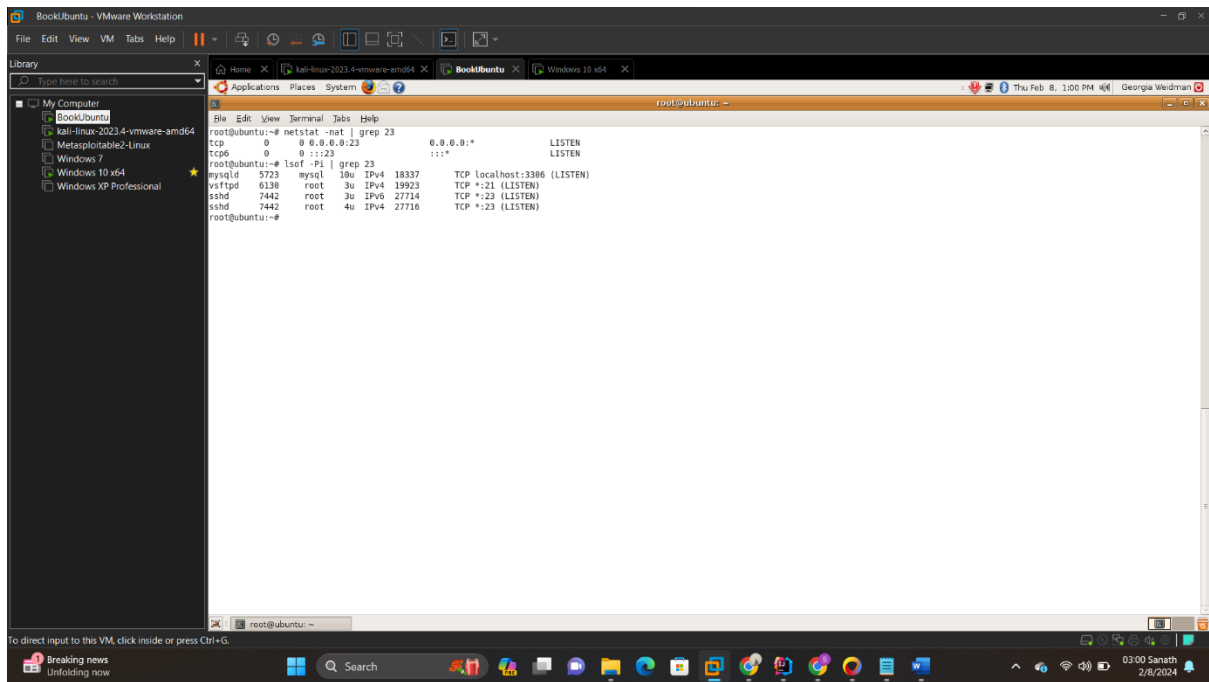
Nmap Scripting Engine:

One of the most potent and adaptable aspects of Nmap is the Nmap Scripting Engine (NSE). It enables users to automate a wide range of networking functions by writing (and sharing) straightforward scripts in the Lua computer language. These scripts run concurrently and with the efficiency and speed you would expect from Nmap. When using Nmap, users have access to an expanding and varied collection of scripts, or they can create their own to suit specific requirements.

Here we need to change the port number of ubuntu linux machine from 22 – 23 by executing following commands.

nano /etc/ssh/sshd_config in ubuntu

The service operating at port 23 is accurately reported as ssh by Nmap, this output displays an additional column named Version. Each active service's version is shown. This information could be used to carry out vulnerability research and allow us to get access to the target machine.

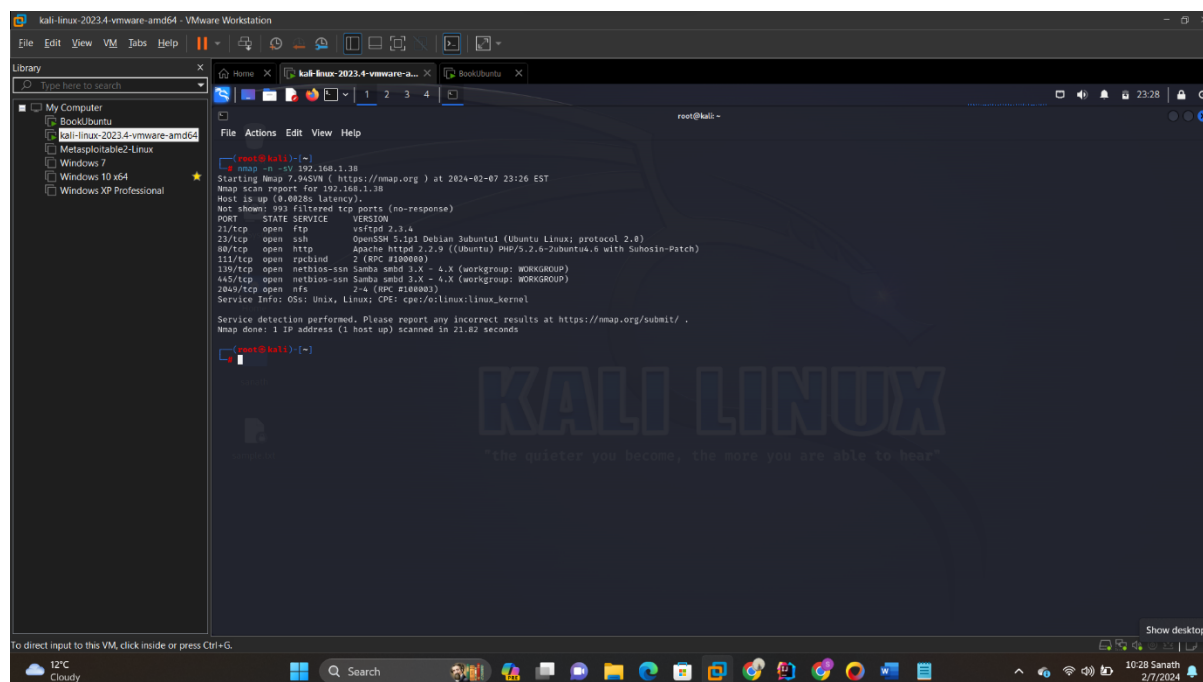


This NMAP is done against my ubuntu server having Ip address – 192.168.1.38

In the above screenshot we can clearly see that on different ports different services are established which includes (Http, Telnet, ftp, nfs, rpcbind, netbios-ssn, Microsoft-ds)

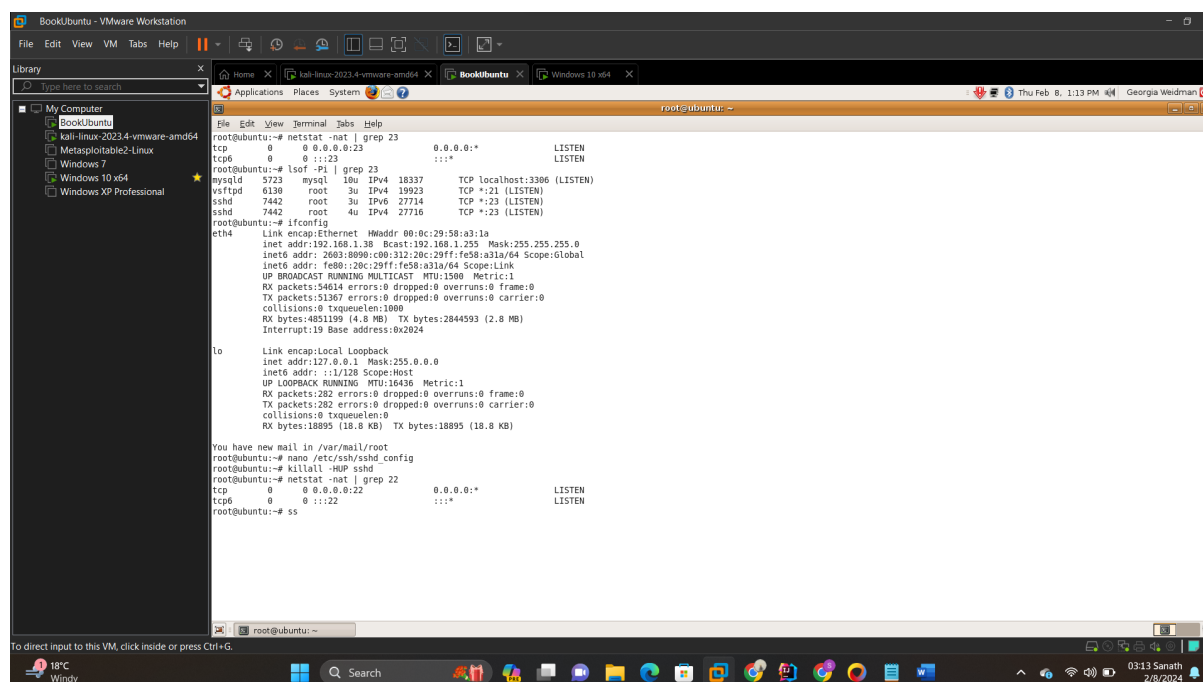
1. Provide screenshots for the Task01~03 (3 screenshots are needed)

Task 1:



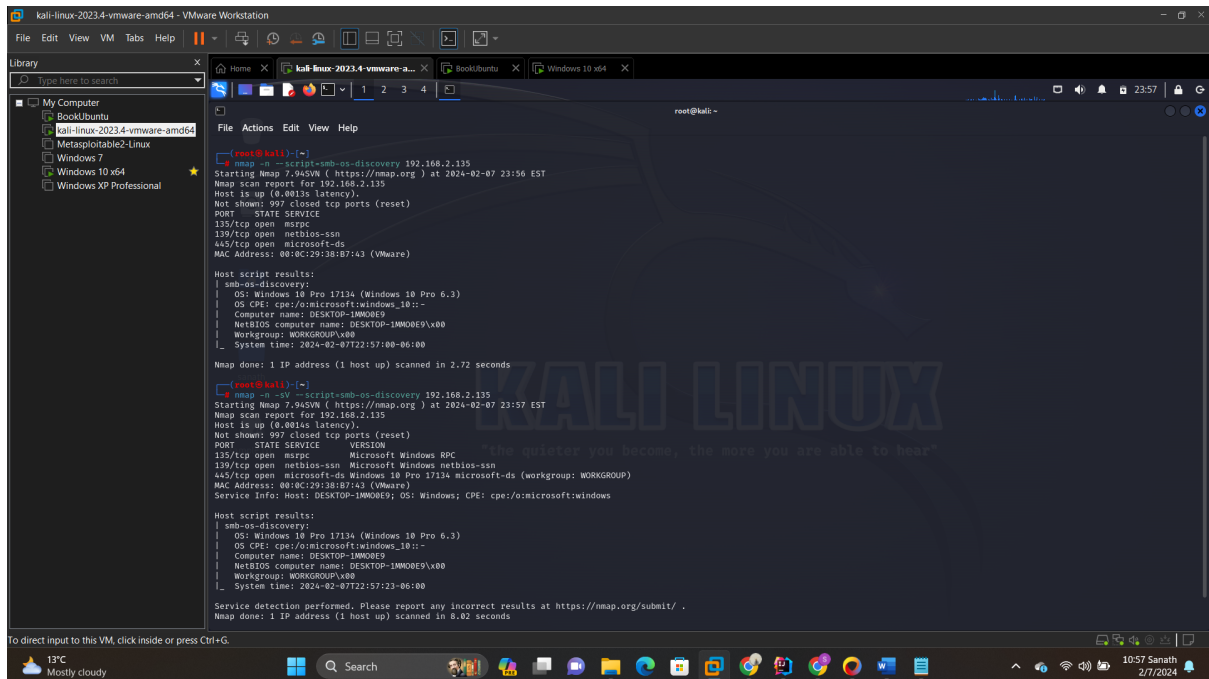
The command **nmap -n -sV 192.168.1.38** is used to perform a version scan (-sV) on the specified IP address while skipping DNS resolution (-n).

After Task has completed now changing the port to 22 as show in Screenshot below.



Now TCP is listening to port 22.

Task 2:



```
(root@kali) ~# nmap -n --script=smb-os-discovery 192.168.2.135
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-07 23:56 EST
Nmap scan report for 192.168.2.135
Host is up (0.0013s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 08:0C:29:38:B7:43 (VMware)

Host script results:
| smb-os-discovery:
|   OS: Windows 10 Pro 17134 (Windows 10 Pro 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10:-
|   Computer name: DESKTOP-IMMOE9VX00
|   NetBIOS computer name: DESKTOP-IMMOE9VX00
|   Workgroup: WORKGROUP\X00
|   System time: 2024-02-07T22:57:00-06:00
Nmap done: 1 IP address (1 host up) scanned in 2.72 seconds

(root@kali) ~# nmap -n --script=smb-os-discovery 192.168.2.135
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-07 23:57 EST
Nmap scan report for 192.168.2.135
Host is up (0.0013s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds  Windows 10 Pro 17134 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 08:0C:29:38:B7:43 (VMware)
Service Info: Host: DESKTOP-IMMOE9V; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows 10 Pro 17134 (Windows 10 Pro 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10:-
|   Computer name: DESKTOP-IMMOE9V
|   NetBIOS computer name: DESKTOP-IMMOE9VX00
|   Workgroup: WORKGROUP\X00
|   System time: 2024-02-07T22:57:23-06:00
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.02 seconds
```

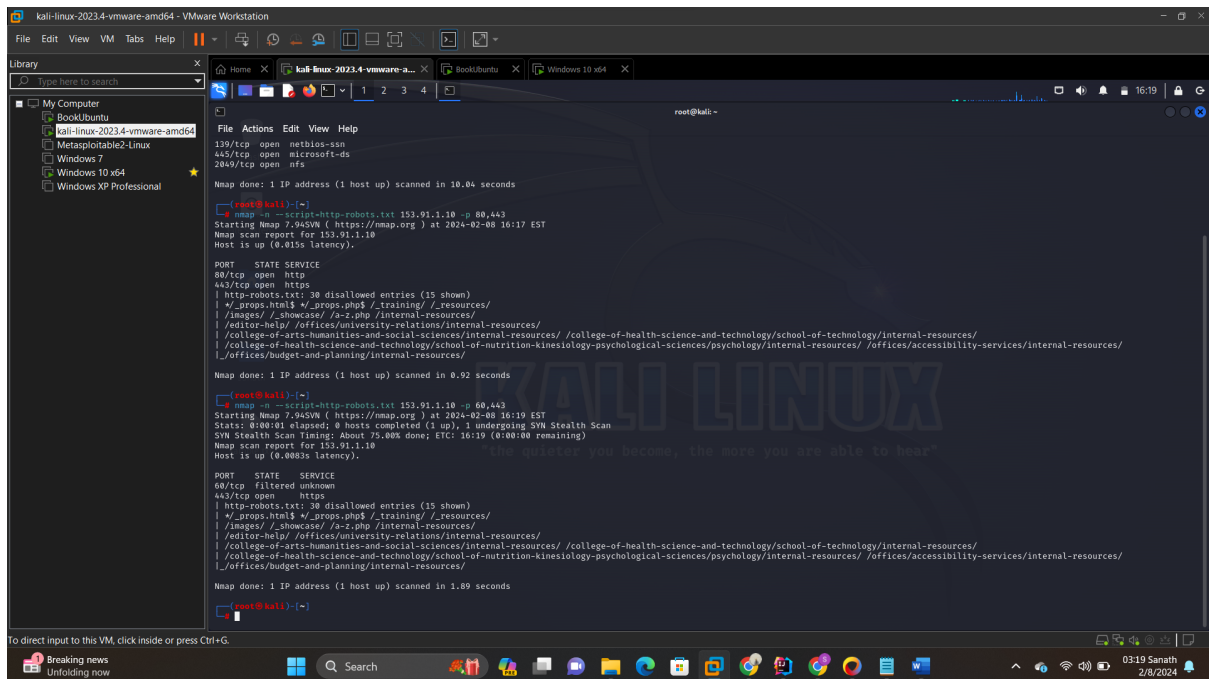
`nmap -n --script=smb-os-discovery [192.168.2.135]`

Attempts to determine the operating system, computer name, domain, workgroup, and current time over the SMB protocol (ports 445 or 139). This is done by starting a session with the anonymous account (or with a proper user account, if one is given; it likely doesn't make a difference); in response to a session starting, the server will send back all this information.

The following fields may be included in the output, depending on the circumstances (e.g. the workgroup name is mutually exclusive with domain and forest names) and the information available:

OS, Computer name, Domain name, Forest name, FQDN, NetBIOS computer name, NetBIOS domain name, Workgroup, System time.

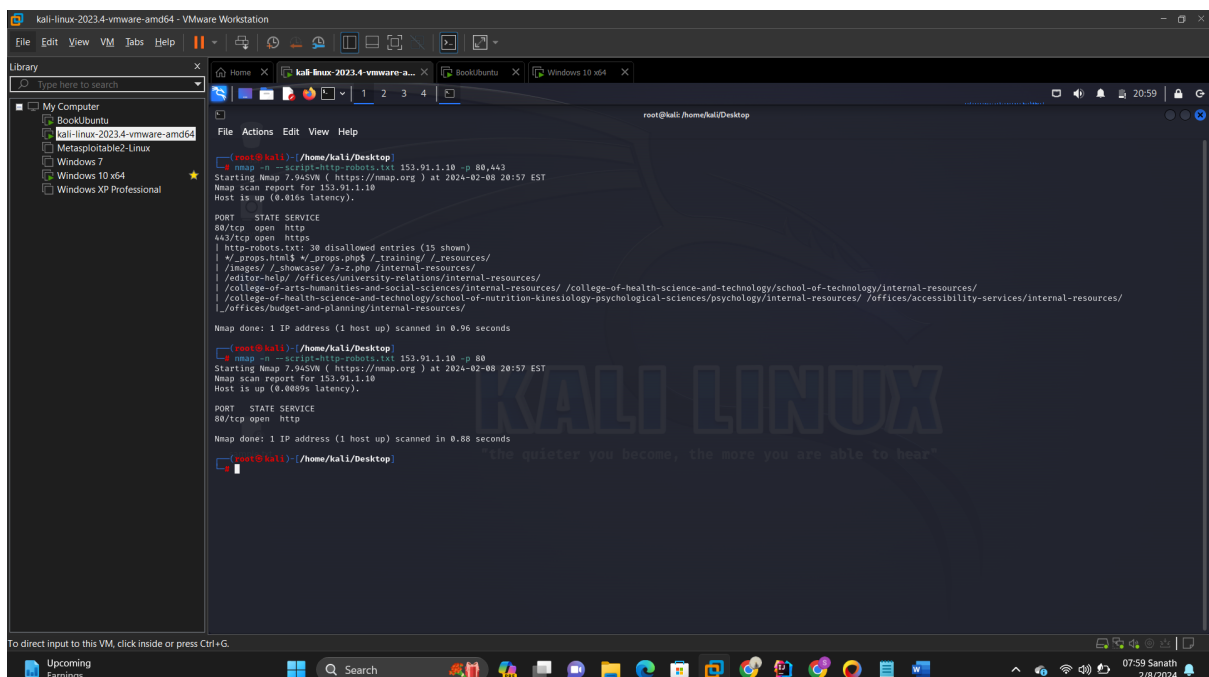
Task 3:



```
kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
BookUbuntu
kali-linux-2023.4-vmware-amd64
Metasploitable2-Linux
Windows 7
Windows 10 x64
Windows XP Professional

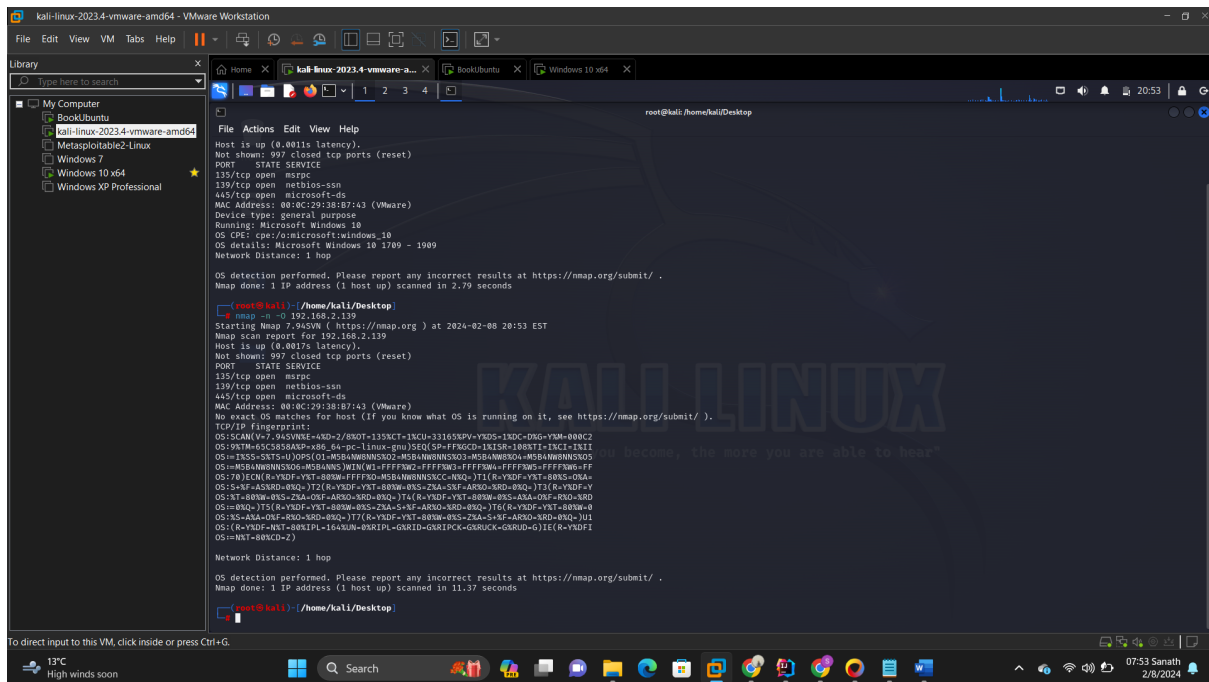
root@kali: ~
File Actions Edit View Help
139/tcp open netbios-ssn
445/tcp open microsoft-ds
2049/tcp open nfs
Nmap done: 1 IP address (1 host up) scanned in 10.84 seconds
root@kali: ~# nmap -n --script=http-robots.txt 153.91.1.10 -p 80,443
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08 16:17 EST
Nmap scan report for 153.91.1.10
Host is up (0.015s latency).
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
|_ http-robots.txt: 30 disallowed entries (15 shown)
|_ /_props.html$ /_props.php$ /_training/ /_resources/
|_ /images/ /_showcase/ /_a-2.php /internal-resources/
|_ /editor-help/ /offices/university-relations/internal-resources/
|_ /college-of-arts-humanities-and-social-sciences/internal-resources/ /college-of-health-science-and-technology/school-of-technology/internal-resources/
|_ /college-of-health-science-and-technology/school-of-nutrition-kinesiology-psychological-sciences/psychology/internal-resources/ /offices/accessibility-services/internal-resources/
|_ /offices/budget-and-planning/internal-resources/
Nmap done: 1 IP address (1 host up) scanned in 0.92 seconds
root@kali: ~# nmap -n --script=http-robots.txt 153.91.1.10 -p 60,443
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08 16:19 EST
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 75.00% done; ETC: 16:19 (0:00:00 remaining)
Nmap scan report for 153.91.1.10
Host is up (0.0083s latency).
PORT      STATE SERVICE
60/tcp    filtered unknown
443/tcp    open  https
|_ http-robots.txt: 30 disallowed entries (15 shown)
|_ /_props.html$ /_props.php$ /_training/ /_resources/
|_ /images/ /_showcase/ /_a-2.php /internal-resources/
|_ /editor-help/ /offices/university-relations/internal-resources/
|_ /college-of-arts-humanities-and-social-sciences/internal-resources/ /college-of-health-science-and-technology/school-of-technology/internal-resources/
|_ /college-of-health-science-and-technology/school-of-nutrition-kinesiology-psychological-sciences/psychology/internal-resources/ /offices/accessibility-services/internal-resources/
|_ /offices/budget-and-planning/internal-resources/
Nmap done: 1 IP address (1 host up) scanned in 1.89 seconds
root@kali: ~#
```

In the above screenshot we can see both ports 80,443 and 60,443 are open. Using the 'http-robots.txt' script, the command 'nmap -n --script=http-robots.txt 153.91.1.10 -p 80,443' initiates a Nmap scan on port 80 and '443' of the IP address 153.91.1.10, retrieving the contents of the robots.txt file from web servers utilizing both ports. The purpose of this script is to find out if the web server has a robots.txt file and, if so, to retrieve its contents. This file is commonly used to limit access to particular sections of a website for search engine visitors.



```
kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
BookUbuntu
kali-linux-2023.4-vmware-amd64
Metasploitable2-Linux
Windows 7
Windows 10 x64
Windows XP Professional

root@kali: /home/kali/Desktop
File Actions Edit View Help
nmap -n --script=http-robots.txt 153.91.1.10 -p 80,443
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08 20:57 EST
Nmap scan report for 153.91.1.10
Host is up (0.016s latency).
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
|_ http-robots.txt: 30 disallowed entries (15 shown)
|_ /_props.html$ /_props.php$ /_training/ /_resources/
|_ /images/ /_showcase/ /_a-2.php /internal-resources/
|_ /editor-help/ /offices/university-relations/internal-resources/
|_ /college-of-arts-humanities-and-social-sciences/internal-resources/ /college-of-health-science-and-technology/school-of-technology/internal-resources/
|_ /college-of-health-science-and-technology/school-of-nutrition-kinesiology-psychological-sciences/psychology/internal-resources/ /offices/accessibility-services/internal-resources/
|_ /offices/budget-and-planning/internal-resources/
Nmap done: 1 IP address (1 host up) scanned in 0.96 seconds
root@kali: /home/kali/Desktop# nmap -n --script=http-robots.txt 153.91.1.10 -p 80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08 20:57 EST
Nmap scan report for 153.91.1.10
Host is up (0.0089s latency).
PORT      STATE SERVICE
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 0.88 seconds
root@kali: /home/kali/Desktop#
```

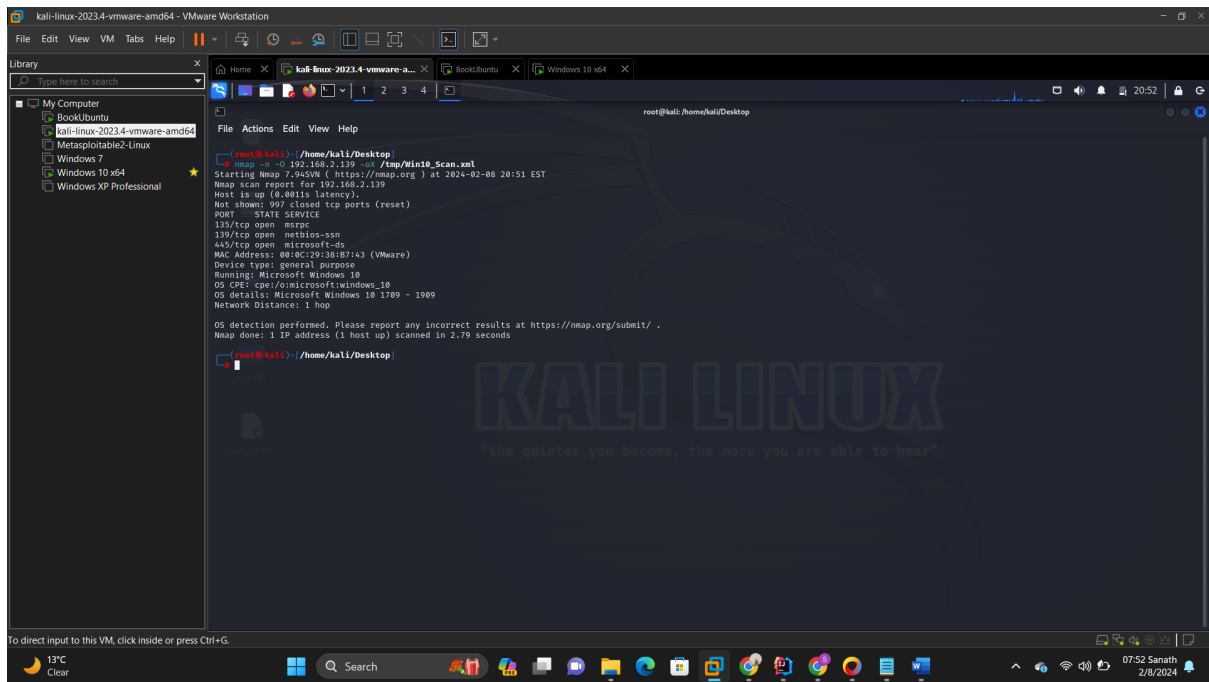


The command "nmap -n -O" is used with the Nmap network scanning tool. Here's what each option means:

-n: This option tells Nmap not to do DNS resolution. By default, Nmap will attempt to resolve hostnames to IP addresses, but using -n skips this step, which can speed up the scanning process.

-O: This option enables operating system detection. Nmap will attempt to determine the operating system running on the target hosts based on various characteristics observed during the scan, such as the responses to network probes.

So, when you run "nmap -n -O", you're instructing Nmap to perform a scan without DNS resolution and to attempt to identify the operating systems of the target hosts.



The command you provided, `nmap -n -O 192.168.152.131 -oX /tmp/Win10_Scan.xml`, is an Nmap command used to perform an operating system detection scan on a target host with the IP address **192.168.152.131**, assuming it's running Windows 10. Let's break down the components of the command:

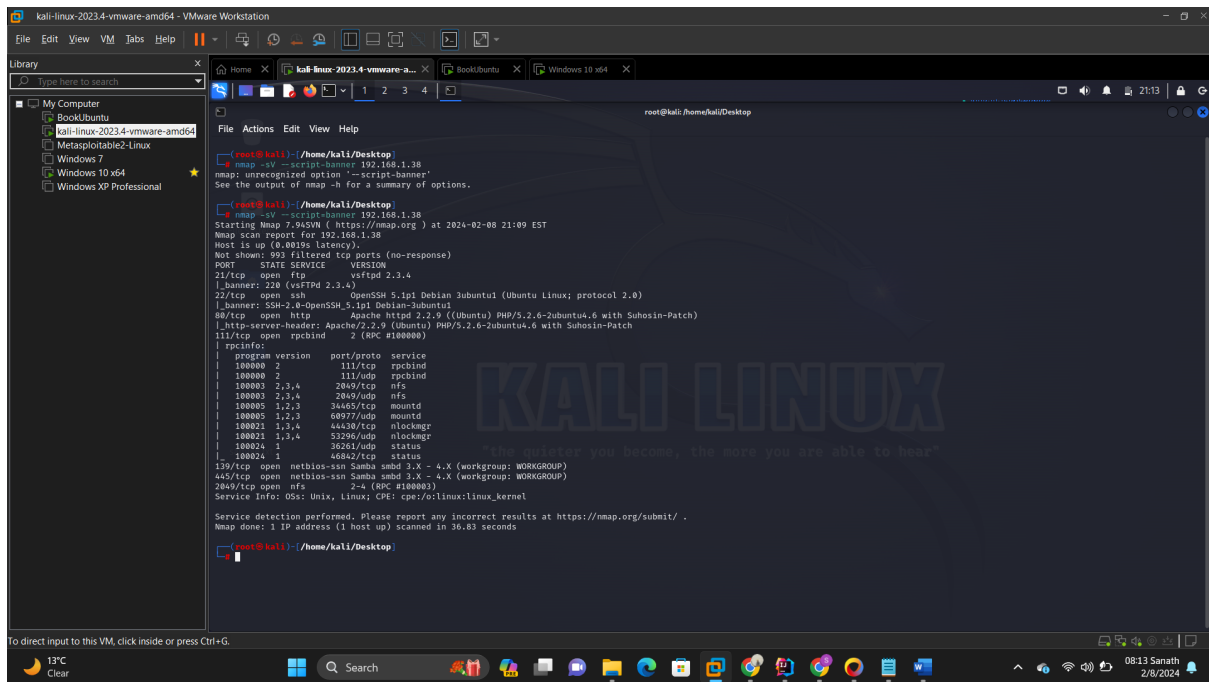
So, when we run this command, Nmap will scan the specified target host for operating system detection, which is Windows 10. It will then save the scan results to the XML file `"/tmp/Win10_Scan.xml"`.

2. Review the information about the whois-ip script at <https://nmap.org/nsedoc/scripts/whoisip.html>. Run the script against an UCM IP address. Provide a screenshot showing the output of the script.

The **'whois'** command is a powerful utility in the Linux toolkit, capable of providing detailed information about a domain or IP address.

Queries the WHOIS services of Regional Internet Registries (RIR) and attempts to retrieve information about the IP Address Assignment which contains the Target IP Address.

In using this script your IP address will be sent to iana.org. moreover, your address and the address of the target of the scan will be sent to one of the RIRs. Please check SS below:



--script=banner: This option tells Nmap to run the script named "banner" against the target. The "banner" script is used to retrieve the banners sent by network services when a connection is established. These banners often contain information about the software and version running on the target service.