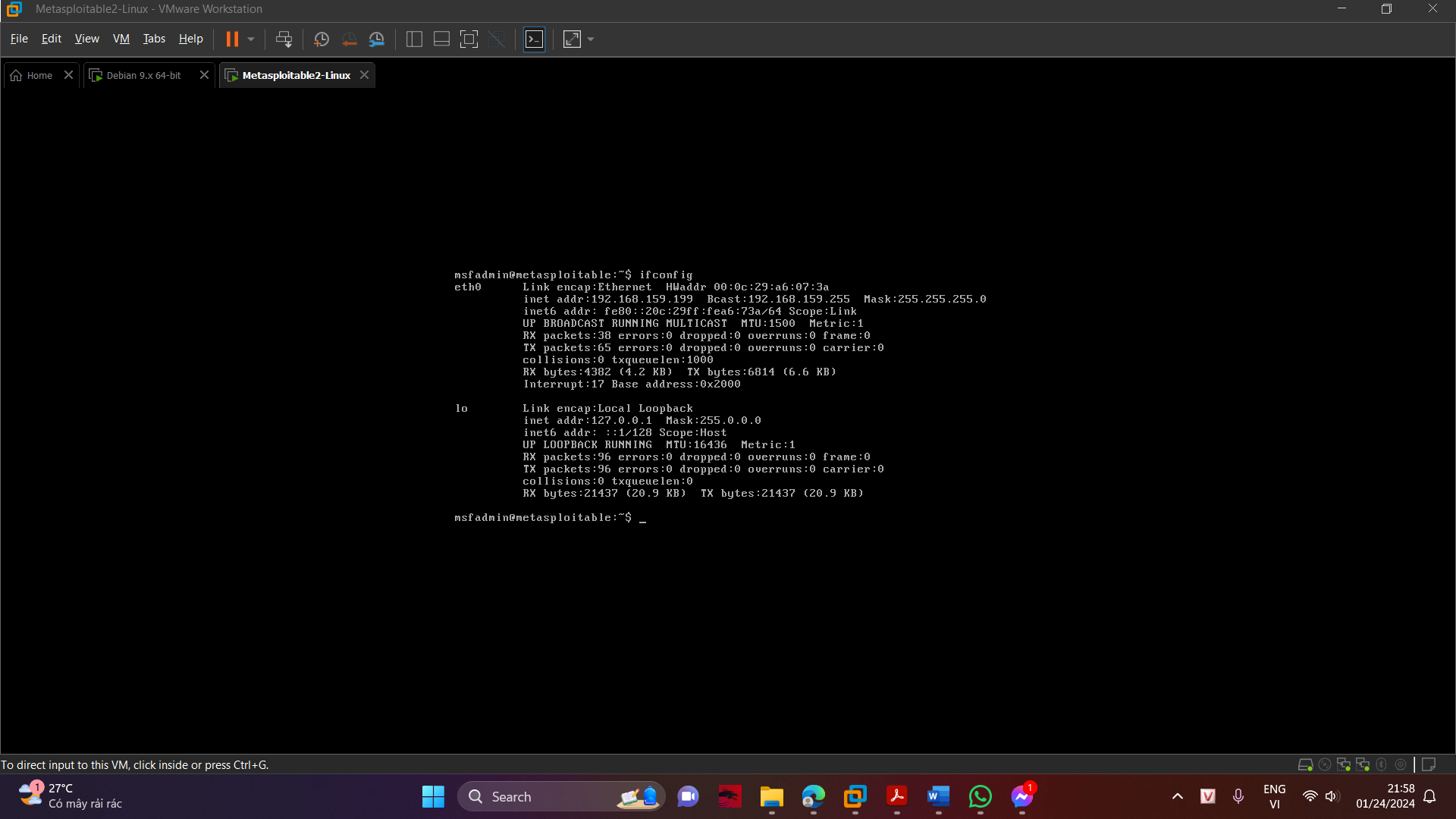
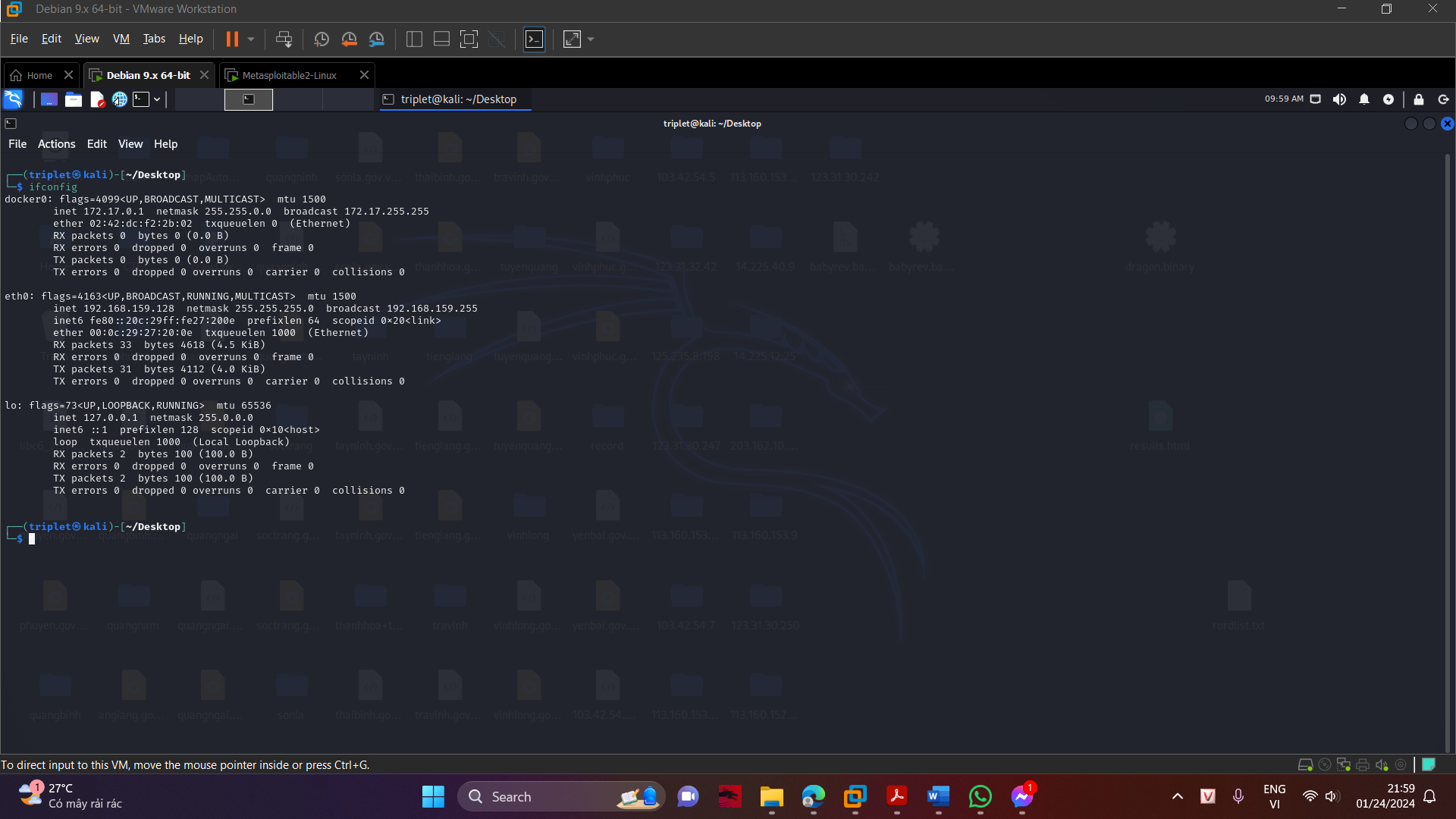
Họ và tên: Trần Minh Triết

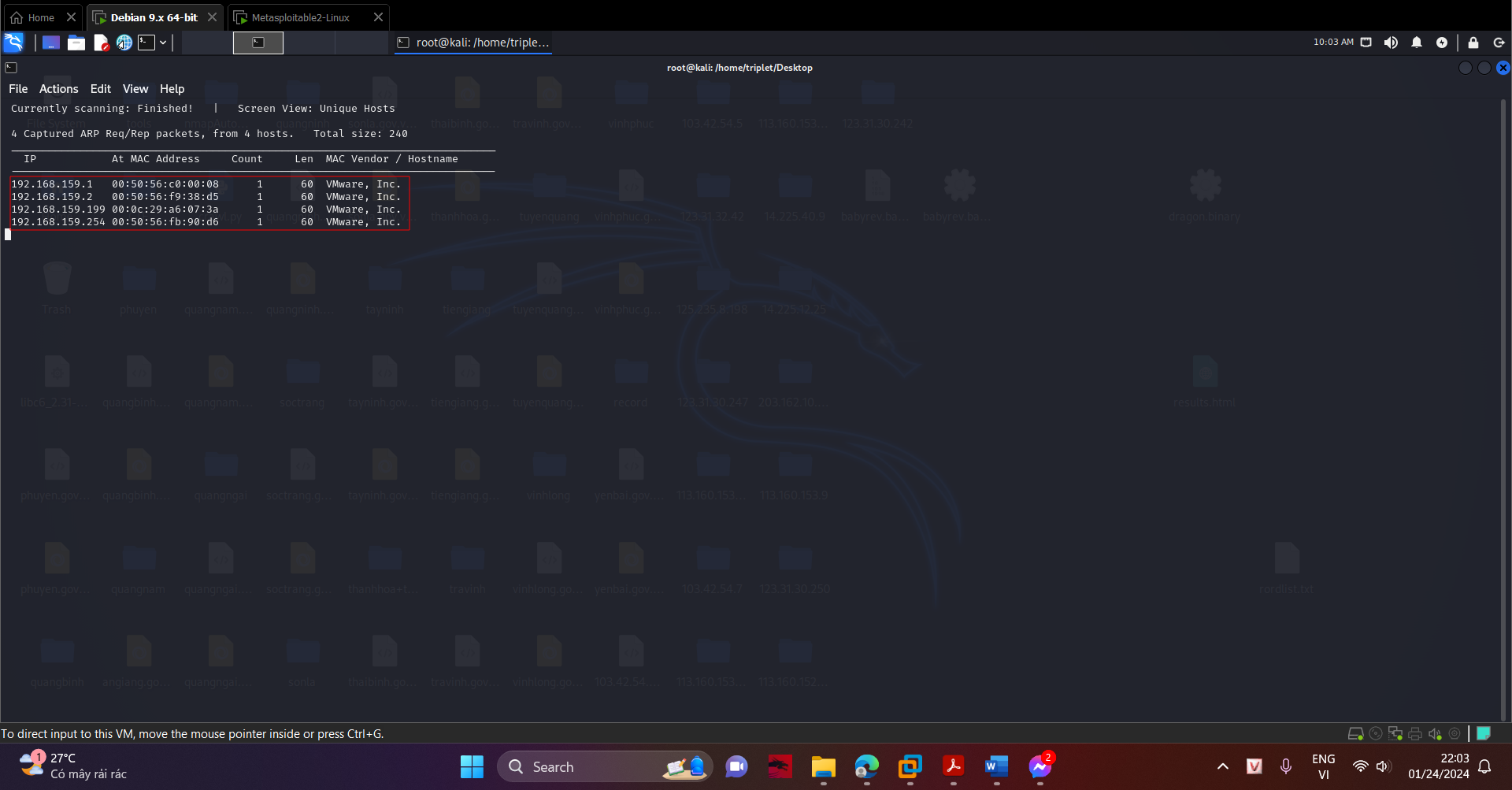
MSSV: SE172241

Class: IA1703

**Lab 3: Enumerating Metasploitable 2**



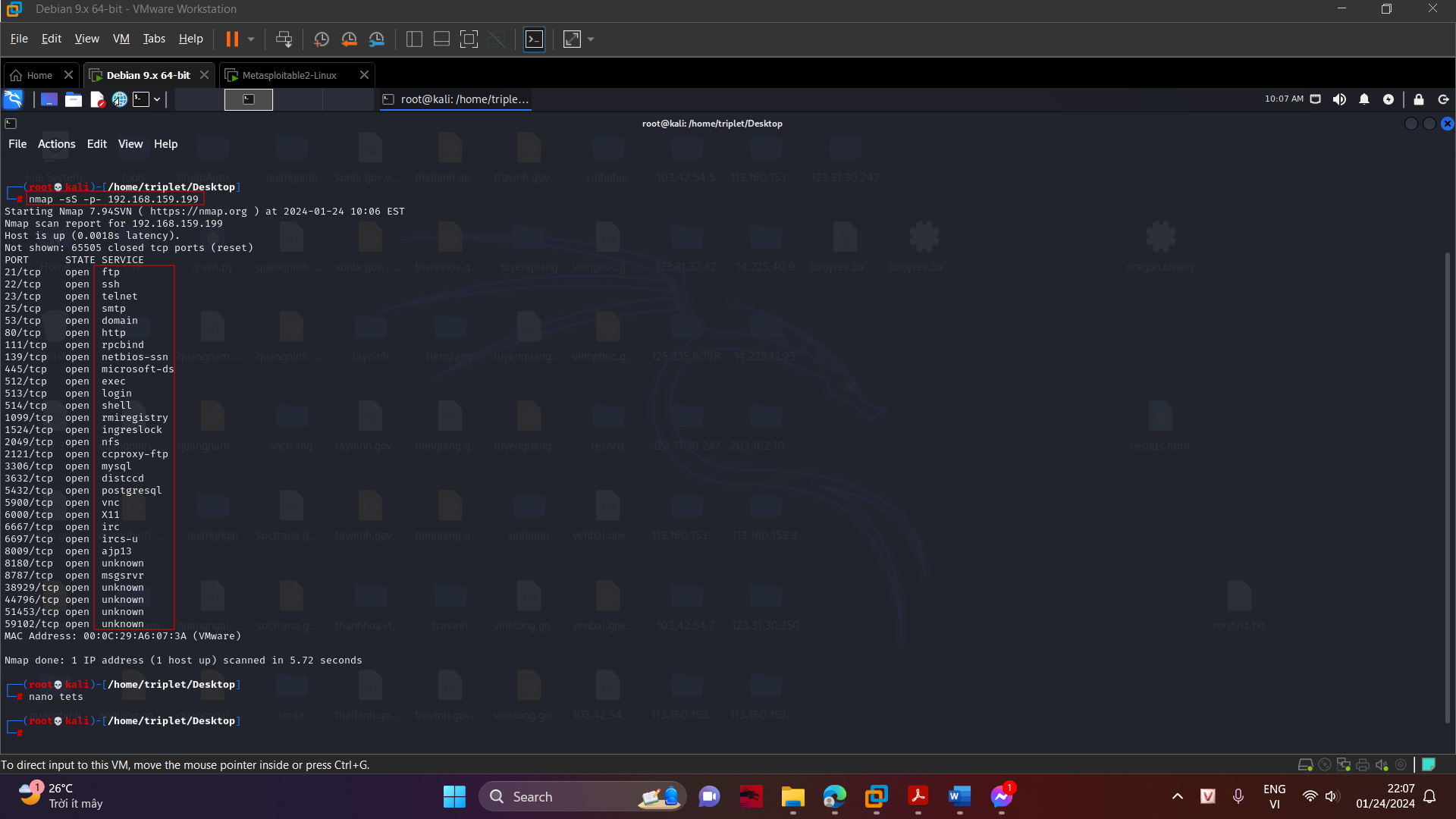




Execute this command to scan all 65,536 TCP ports on the target, replacing the IP address with the IP address of your

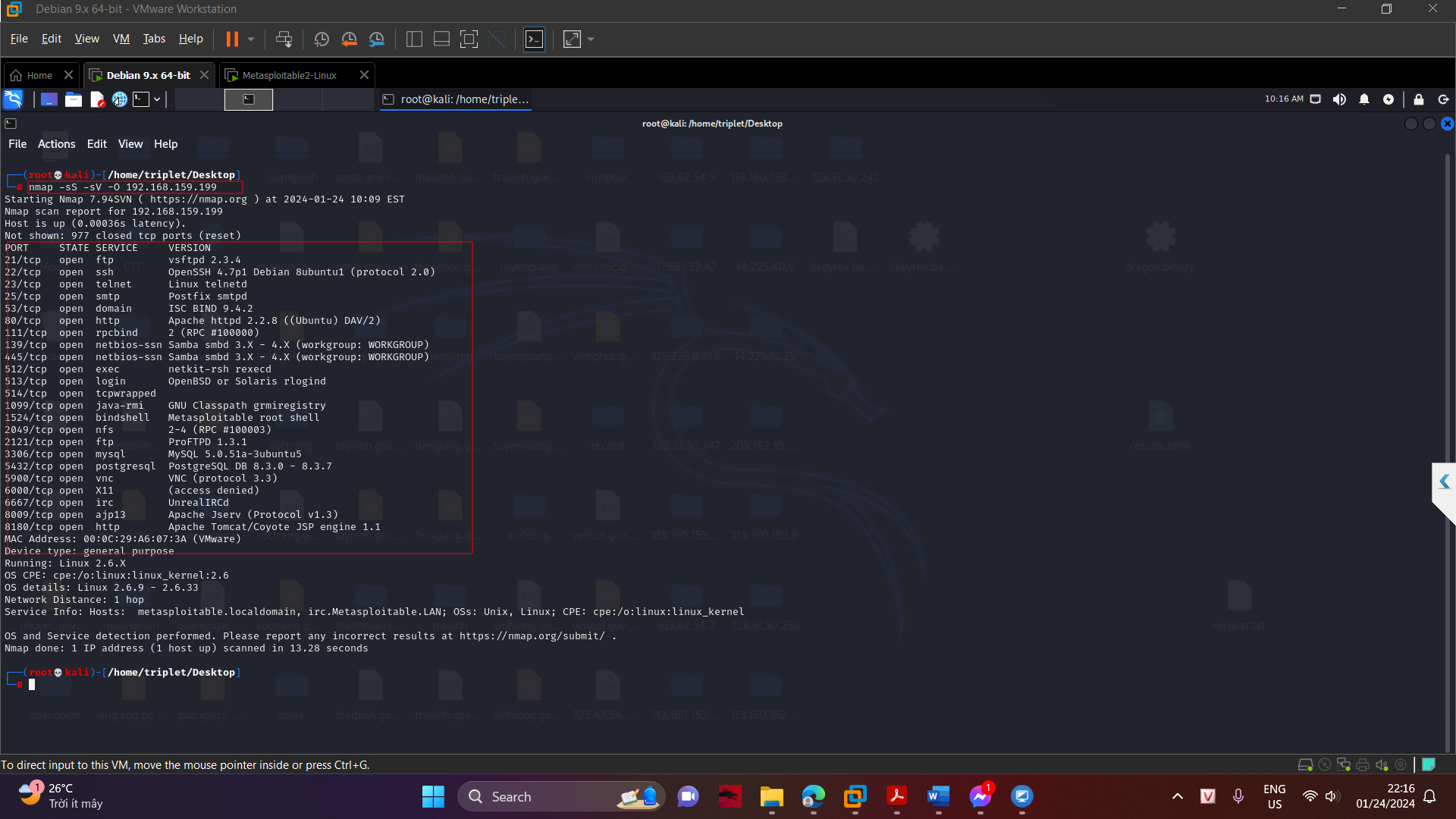
Metasploitable 2 VM.

nmap -sS -p- 192.168.159.199

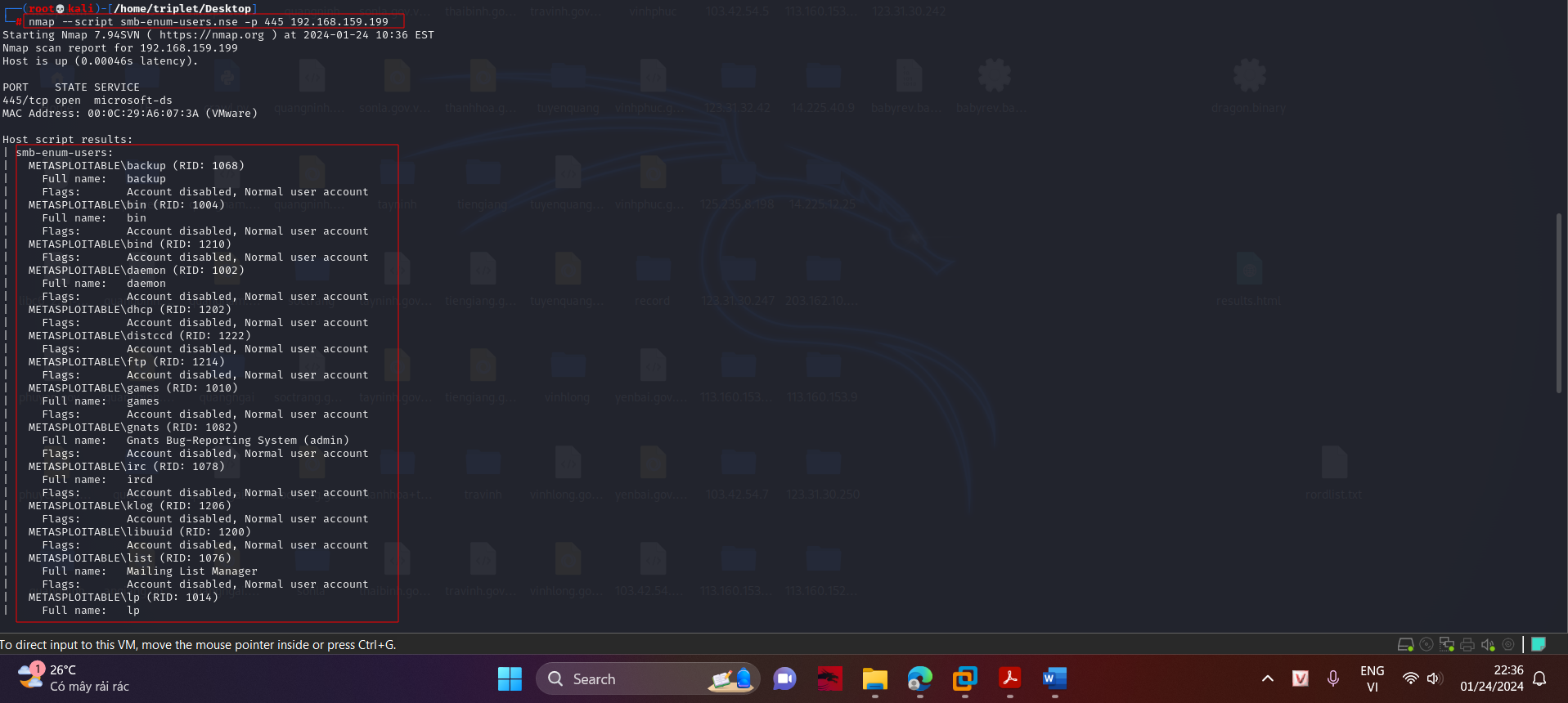


Execute this command to scan 1000 common ports on the target, with version detection and OS detection. Replace the IP address with the IP address of your Metasploitable 2 VM.

nmap -sS -sV -O 192.168.159.199

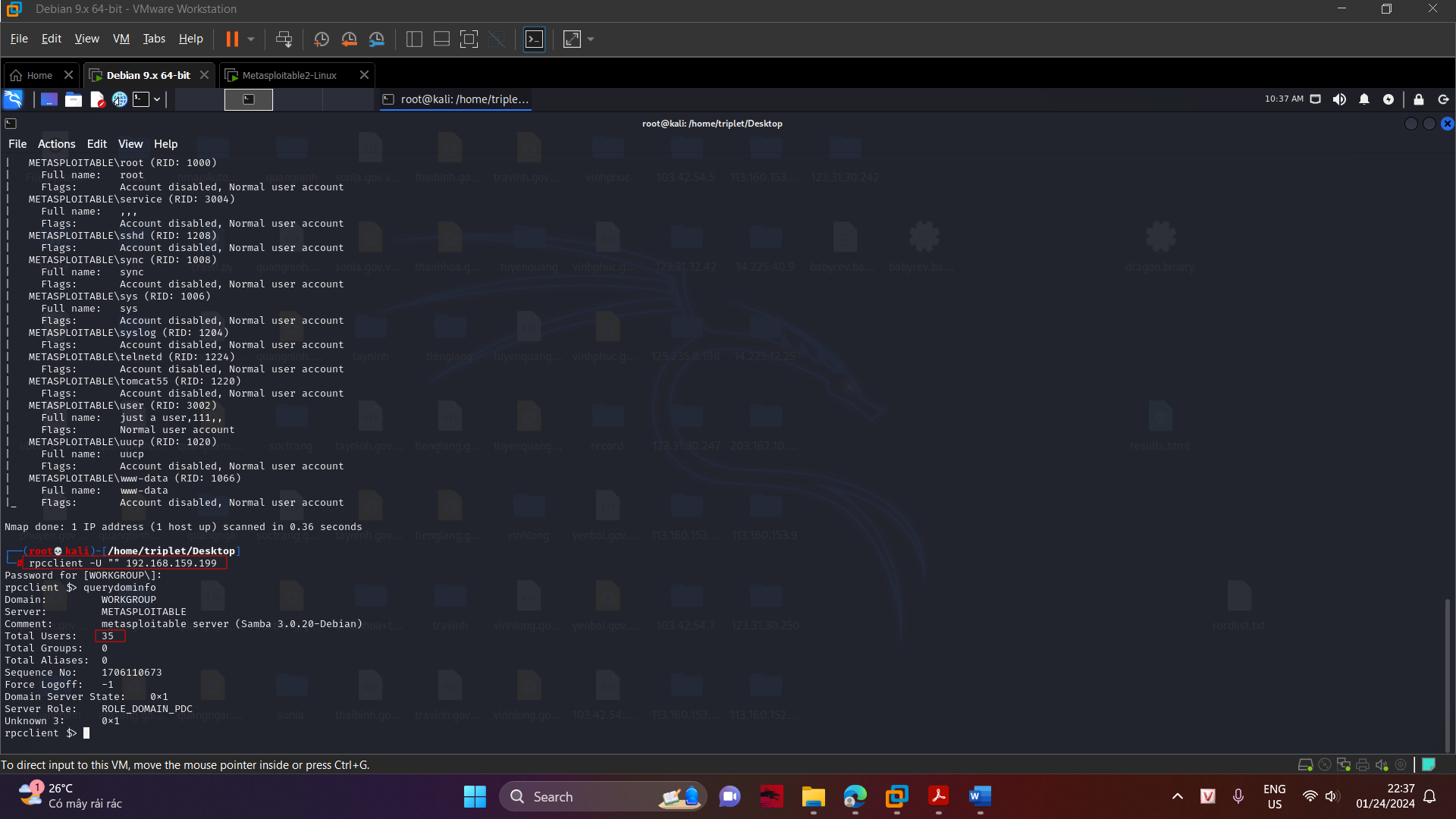


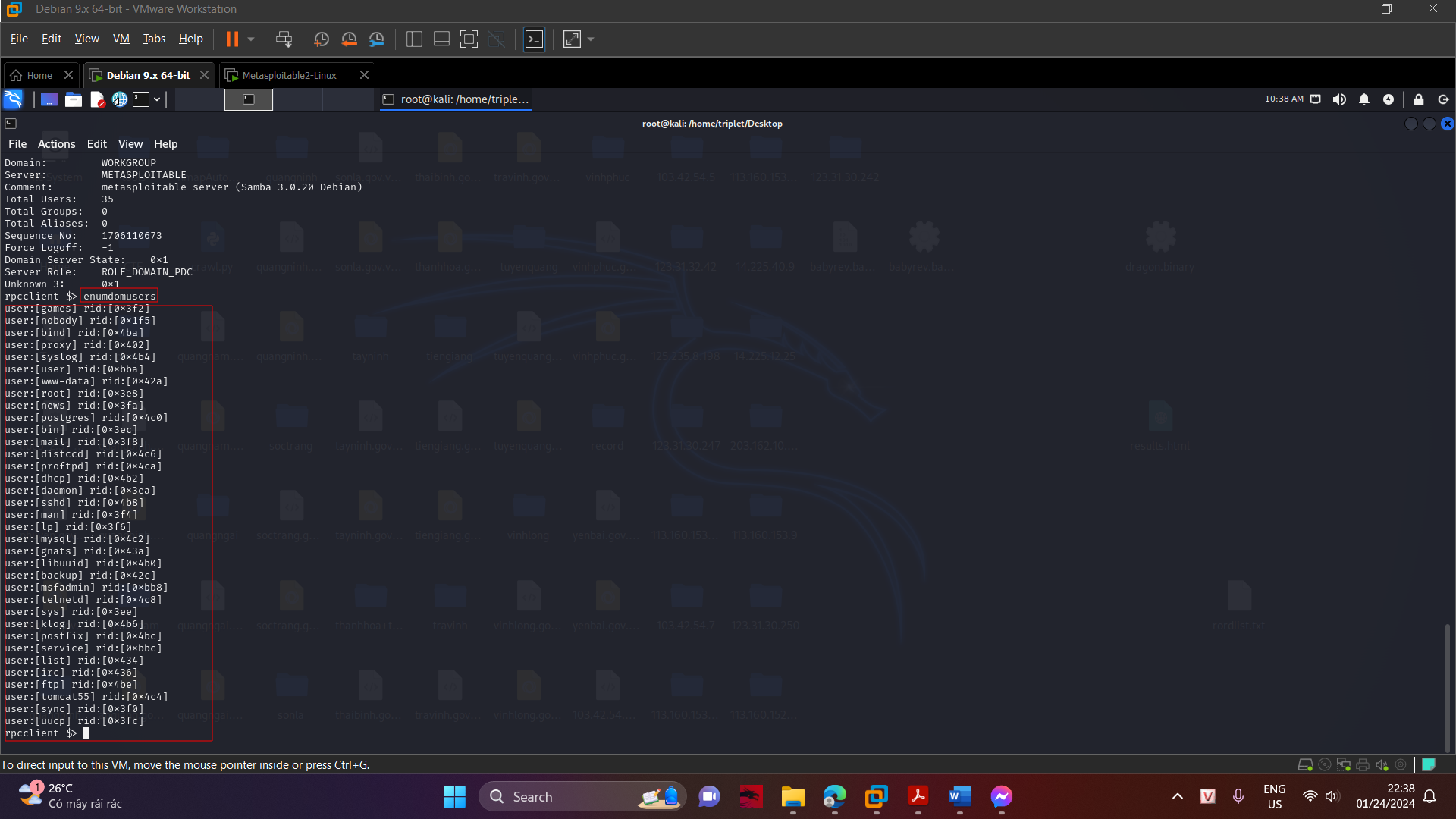
Execute this command to run the Nmap script "smb-enum-users" on the target. This will find a list of user accounts from the SMB service, which is available if a host is sharing files with Windows systems.

nmap --script smb-enum-users.nse -p 445 172.16.1.190 

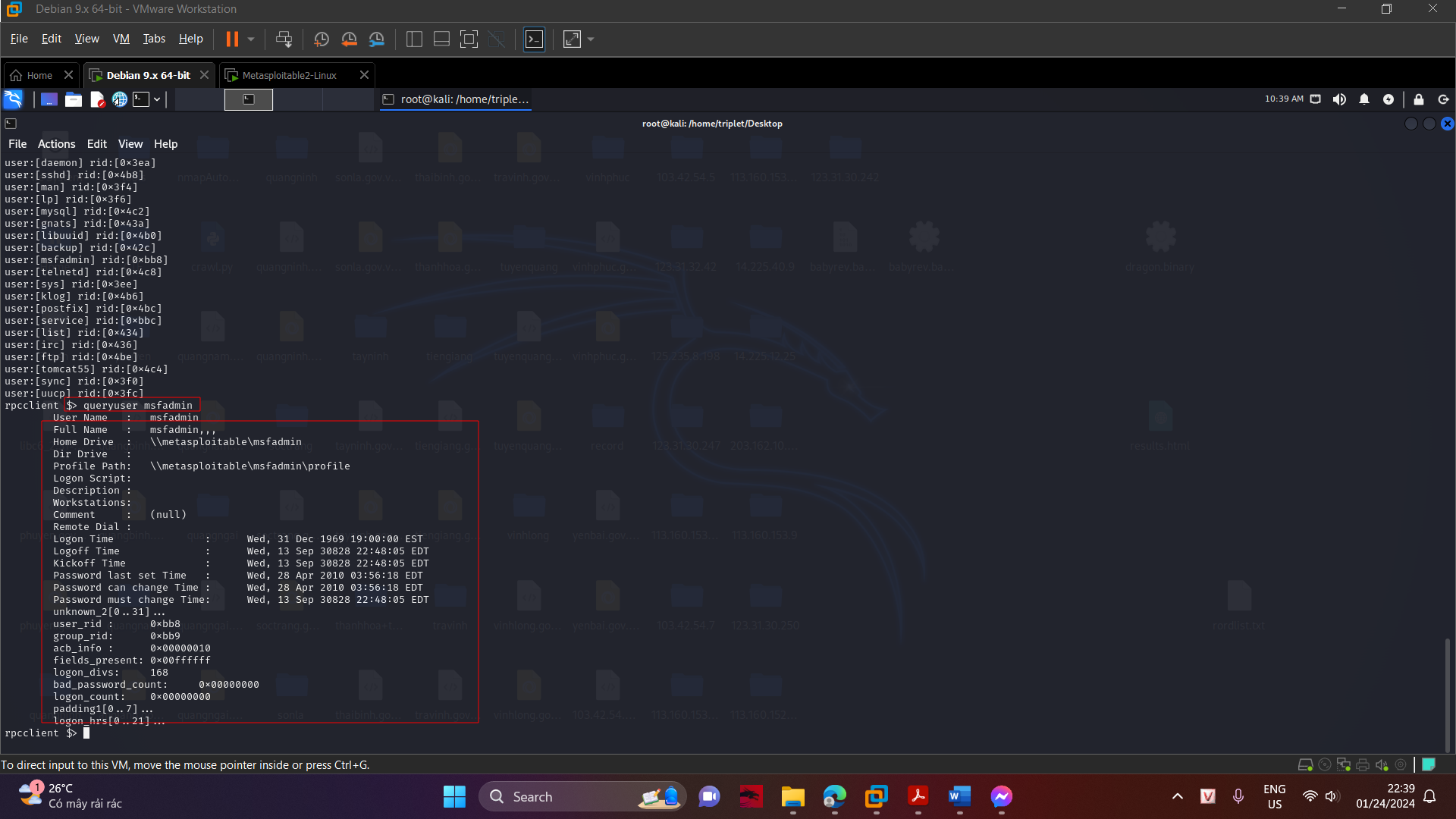
You can also enumerate users via Null sessions with the "rpcclient" command. Execute this command:

rpcclient -U "" 192.168.159.199





Execute this command to get more information about the "msfadmin" account. queryuser msfadmin. This shows that user's profile path, and other information, as shown below.



enum4linux is a Perl script that uses smbclient, rpcclient, net, and nmblookup to automatically enumerate a target. Execute this command to see the options for the enum4linux command.

