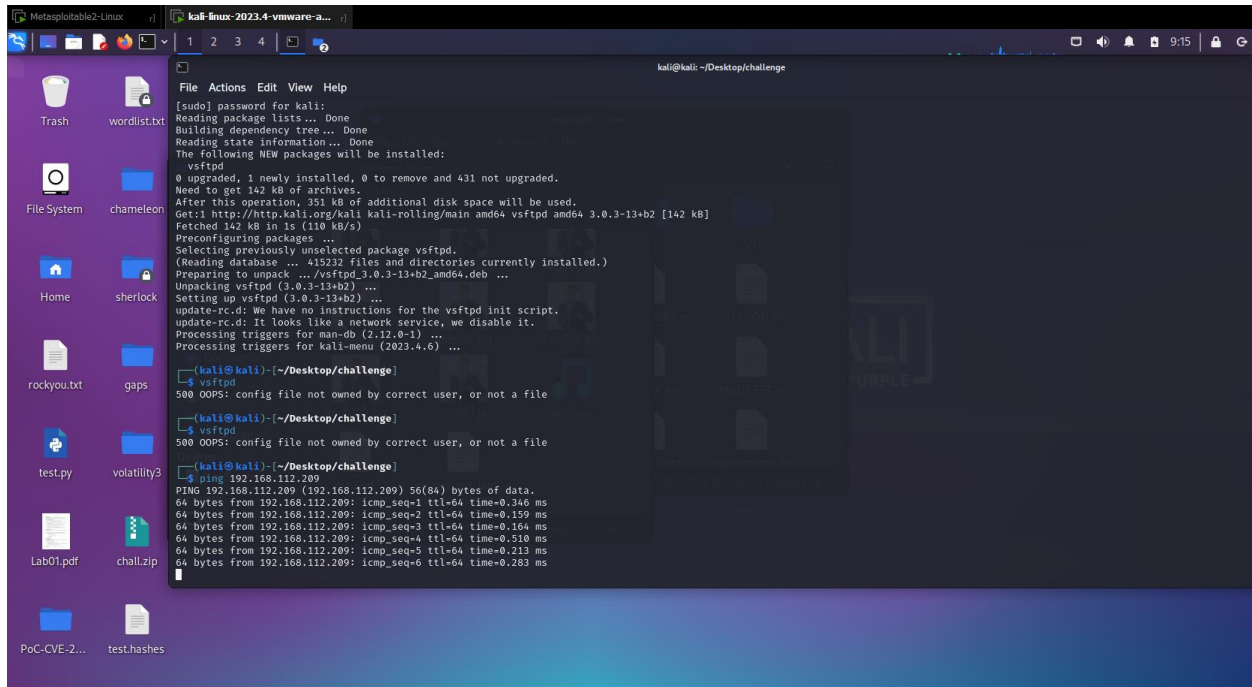


Start your Kali VM and log in as root with the password toor

Start your Metasploitable 2 VM and log in as msfadmin with the password msfadmin

Execute the ifconfig command on both machines and ping from one to the other. Make sure you get replies, as shown below.



## Task 1: Finding Hosts & Open Ports

In Kali, execute this command to locate all hosts on your network.

Replace the subnet address below with the correct subnet for your machine. Usually all you need is the first 3 bytes of

the IP address, as highlighted in the image above.

`netdiscover -r <subnet>`

As shown below, the scanner finds all the machines on your network. One of them should be your Metasploitable 2

machine.

Press Ctrl+C to exit netdiscover.

```
kali@kali: ~/Desktop/challenge

File Actions Edit View Help
Currently scanning: 192.168.175.0/16 | Screen View: Unique Hosts

20 Captured ARP Req/Rep packets, from 4 hosts. Total size: 1200

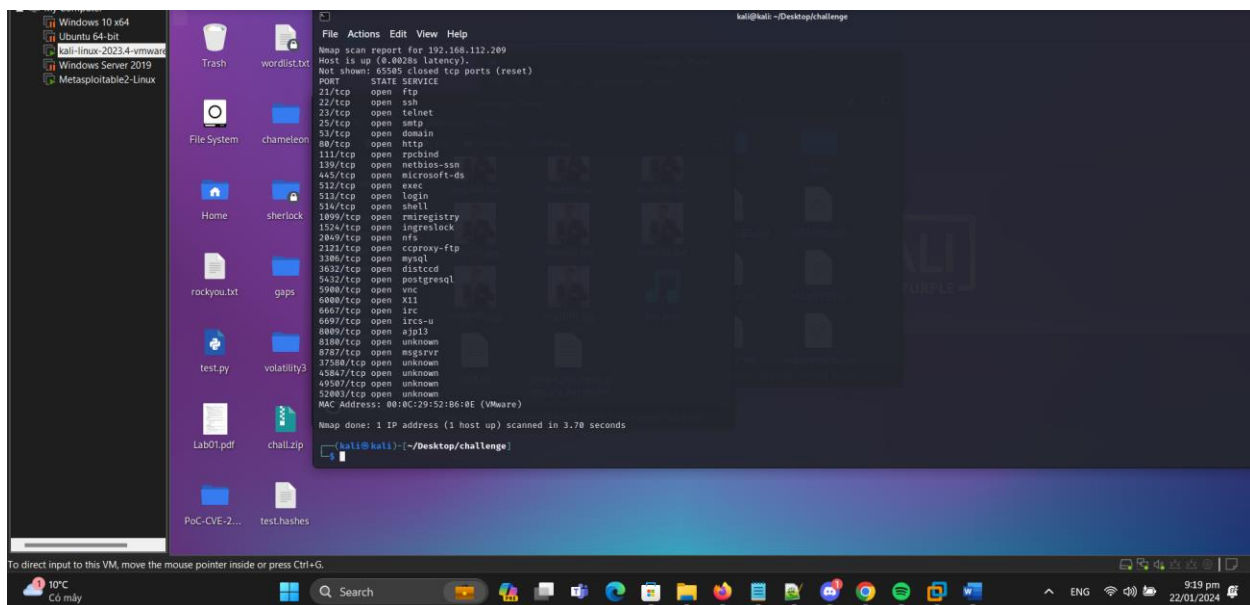
+-----+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+-----+
| 192.168.112.1 | 00:50:56:c0:00:08 | 17    | 1020 | VMware, Inc.          |
| 192.168.112.2 | 00:50:56:fe:ed:47 | 1     | 60   | VMware, Inc.          |
| 192.168.112.209 | 00:0c:29:52:b6:0e | 1     | 60   | VMware, Inc.          |
| 192.168.112.254 | 00:50:56:ea:13:52 | 1     | 60   | VMware, Inc.          |
+-----+-----+-----+-----+-----+-----+

(kali@kali)-[~/Desktop/challenge]
$
```

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- 192.168.112.209
```

This scan quickly finds all open ports, as shown below, but it doesn't find versions of the services



```
kali@kali: ~/Desktop/challenge

File Actions Edit View Help
Nmap scan report for 192.168.112.209
Host is up (0.0028s latency).
Not shown: 65509 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2869/tcp  open  nfs
2322/tcp  open  ccoraxy-ftp
3386/tcp  open  mysql
3632/tcp  open  distccd
5632/tcp  open  postgresql
5900/tcp  open  vnc
6080/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8080/tcp  open  ajp13
8388/tcp  open  unknown
8787/tcp  open  msgsrvr
37588/tcp open  unknown
45887/tcp open  unknown
49587/tcp open  unknown
52083/tcp open  unknown
MAC address: 00:0C:29:52:B6:0E (VMware)

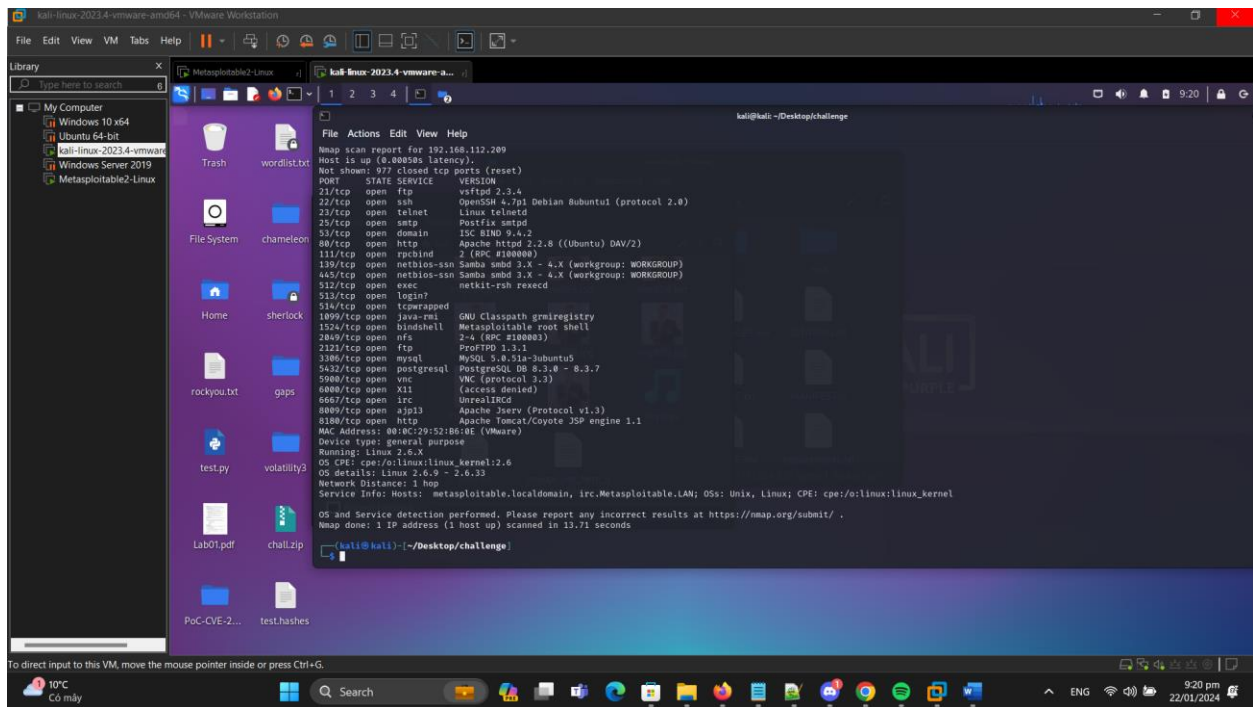
Nmap done: 1 IP address (1 host up) scanned in 3.78 seconds

(kali@kali)-[~/Desktop/challenge]
$
```

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 192.168.112.209
```

This scan finds many version numbers, as shown below

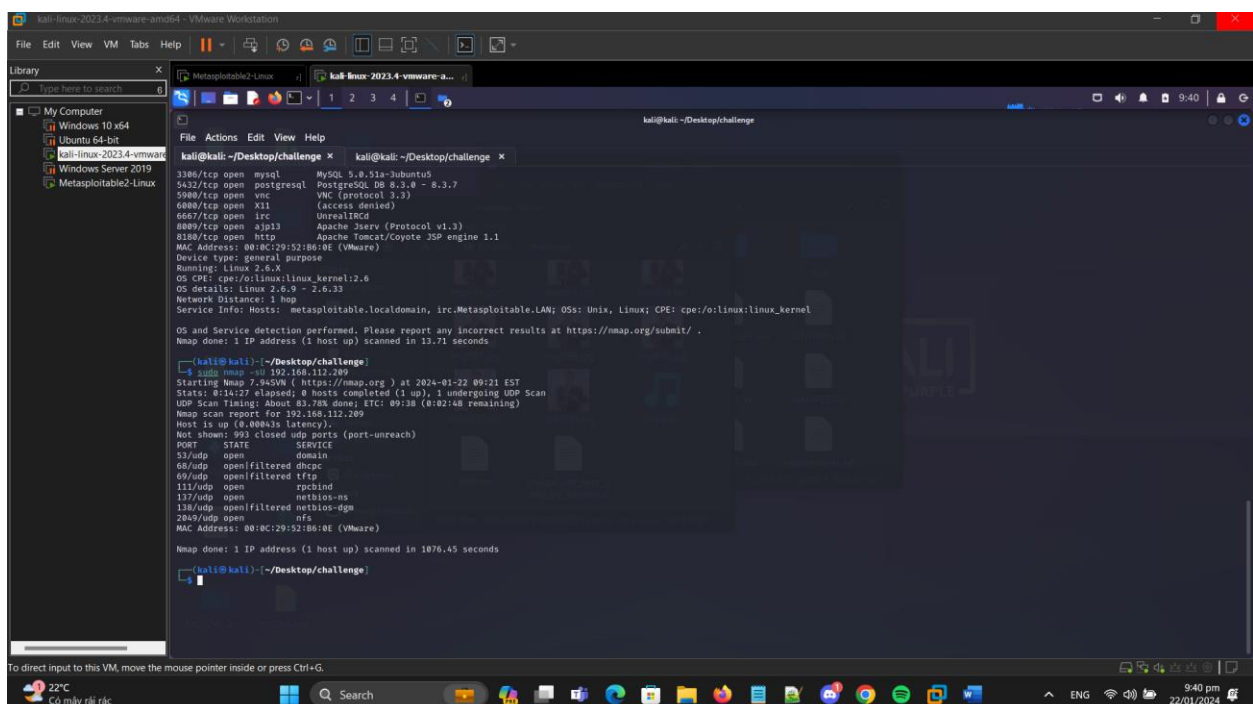


Execute this command to scan UDP ports on the target.

`nmap -sU 192.168.112.209`

This scan will take about 15 minutes to run, so leave it going and open a new Terminal window to continue with the rest of the project while it runs.

When it finishes, it finds several UDP-based services, as shown below.



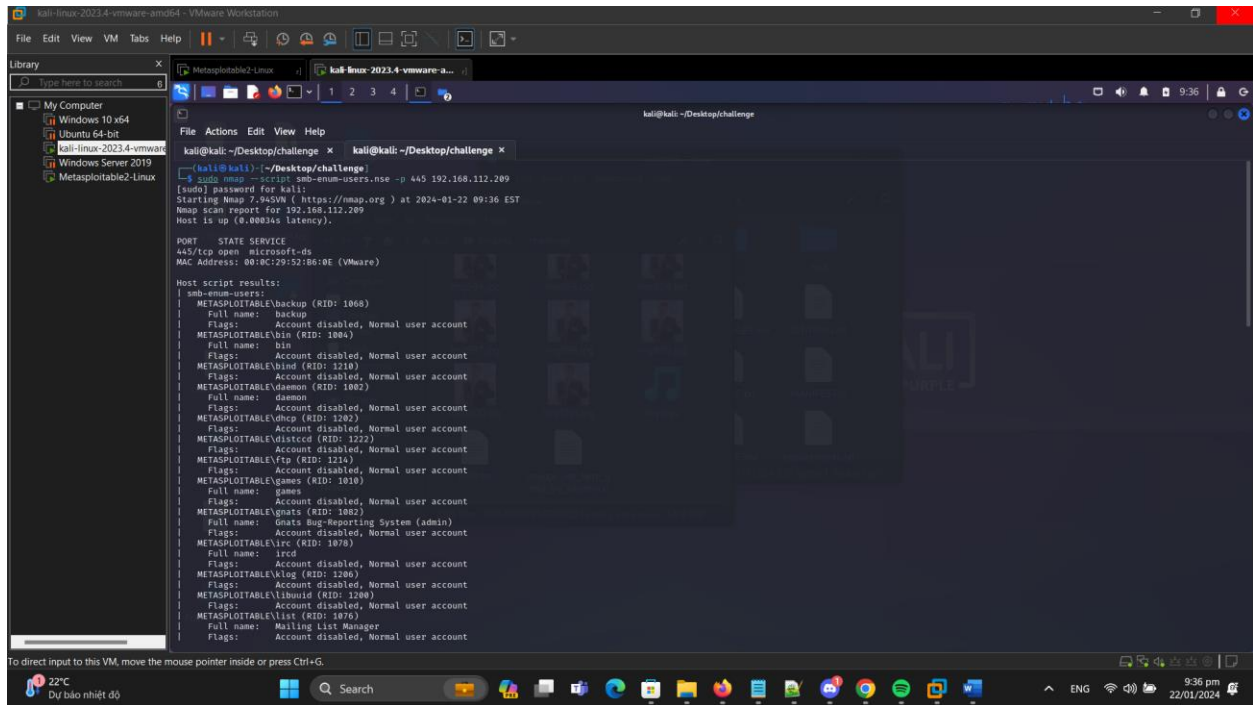
## Task 2: Enumerating Users

### Enumerating with Nmap

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 445 192.168.112.209
```

This produces a long list of user accounts, as shown below



```
kali@kali: ~/Desktop/challenge
$ sudo nmap --script smb-enum-users.nse -p 445 192.168.112.209
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-22 09:36 EST
Nmap scan report for 192.168.112.209
Host is up (0.0003s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 08:0C:129:52:B6:BE (VMware)

Host script results:
| smb-enum-users:
| METASPLOITABLE\backup (RID: 1060)
|   Full name: backup
|   Flags: Account disabled, Normal user account
| METASPLOITABLE\bin (RID: 1084)
|   Full name: bin
|   Flags: Account disabled, Normal user account
| METASPLOITABLE\wind (RID: 1218)
|   Full name: wind
|   Flags: Account disabled, Normal user account
| METASPLOITABLE\daemon (RID: 1082)
|   Full name: daemon
|   Flags: Account disabled, Normal user account
| METASPLOITABLE\dhcp (RID: 1202)
|   Full name: dhcp
|   Flags: Account disabled, Normal user account
| METASPLOITABLE\distcc (RID: 1222)
|   Full name: distcc
|   Flags: Account disabled, Normal user account
| METASPLOITABLE\ftp (RID: 1214)
|   Full name: ftp
|   Flags: Account disabled, Normal user account
| METASPLOITABLE\games (RID: 1010)
|   Full name: games
|   Flags: Account disabled, Normal user account
| METASPLOITABLE\gnats (RID: 1062)
|   Full name: gnats Bug-Reporting System (admin)
|   Flags: Account disabled, Normal user account
| METASPLOITABLE\irc (RID: 1070)
|   Full name: irc
|   Flags: Account disabled, Normal user account
| METASPLOITABLE\ircd (RID: 1206)
|   Full name: ircd
|   Flags: Account disabled, Normal user account
| METASPLOITABLE\libuid (RID: 1200)
|   Full name: libuid
|   Flags: Account disabled, Normal user account
| METASPLOITABLE\list (RID: 1076)
|   Full name: Mailing list manager
|   Flags: Account disabled, Normal user account
```

### Enumerating with rpcclient

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

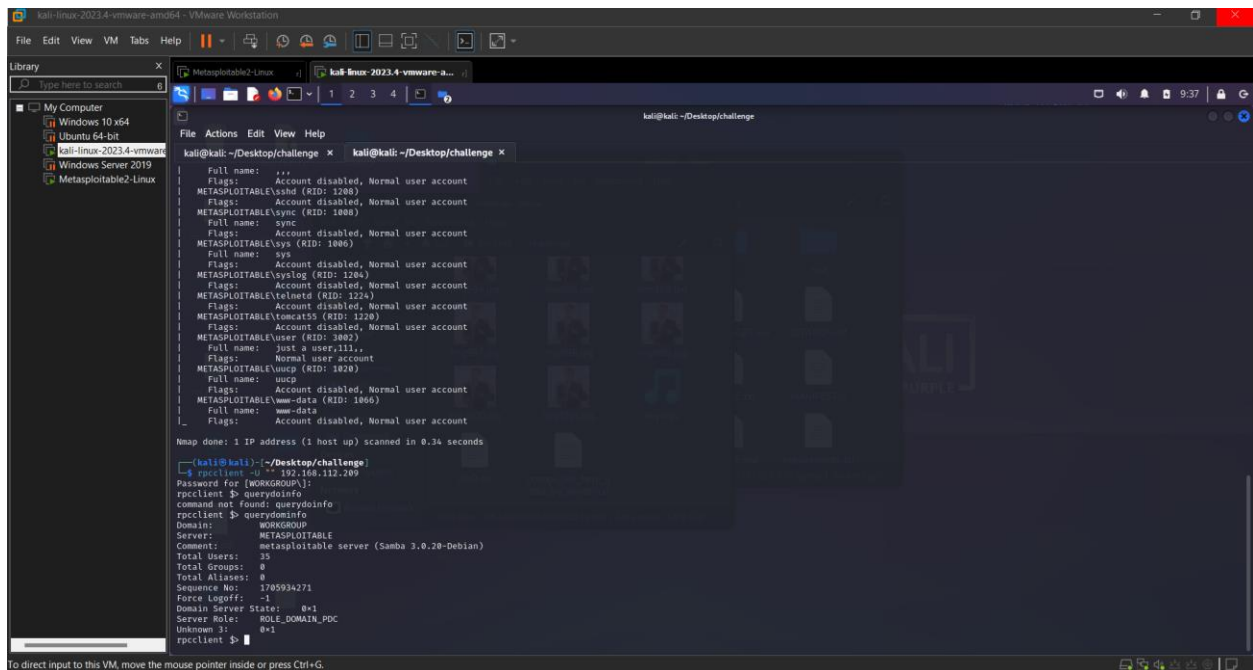
```
rpcclient -U "" 192.168.112.209
```

When it asks for a password, press Enter.

This displays an "rpcclient \$>" prompt. Execute this command:

```
querydominfo
```

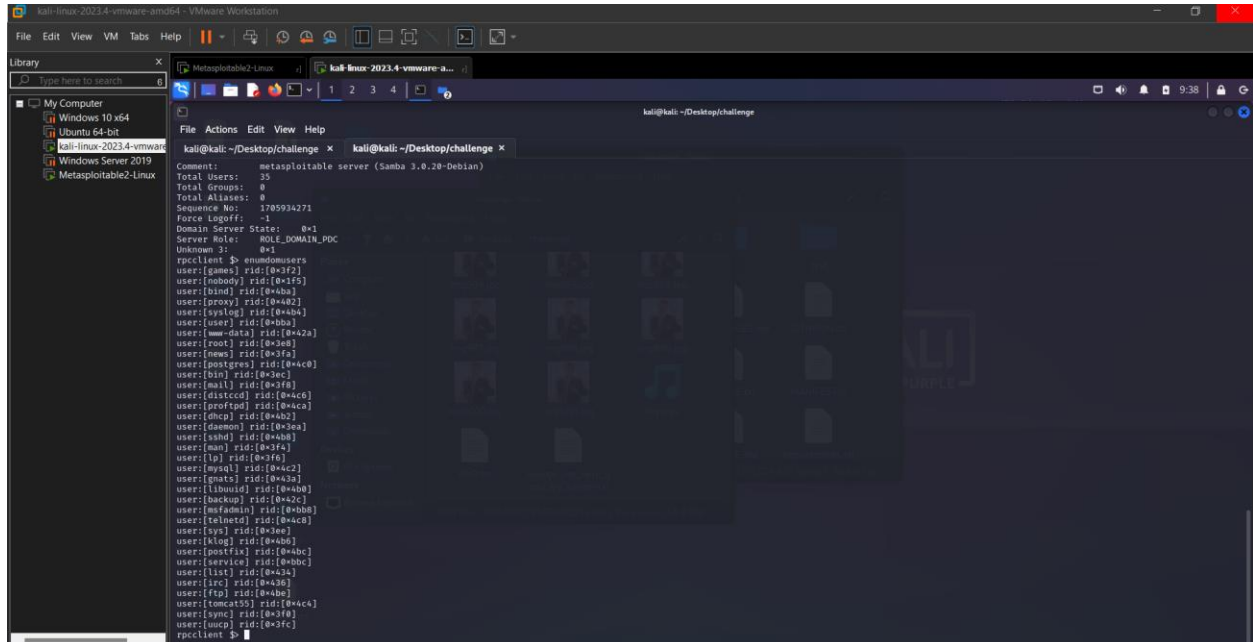
This shows that there are 35 users on the system, as shown below



Execute this command to list all 35 user accounts.

enumdomusers

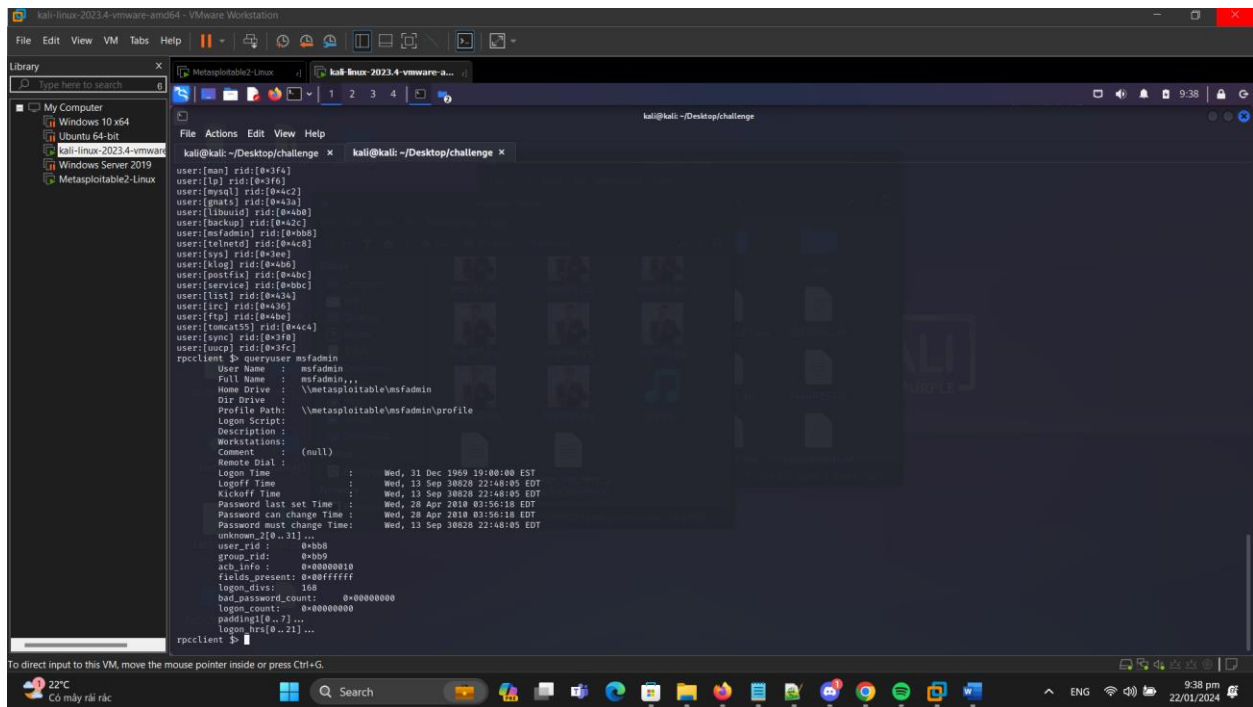
This lists all the user accounts, with their "Relative ID" numbers (rid), as shown below.



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.



Execute the exit command to leave "rpcclient".

## Enumerating with enum4linux

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.

```
enum4linux --help
```

Not specifying any options runs them all. Execute this command to enumerate the target:

```
enum4linux 192.168.112.209
```

A lot of output scrolls by. First there are a couple lists of all the usernames, as we found previously with other tools.

Then a "Share Enumeration" appears, showing that the /tmp folder is shared, as shown below. This has a note of "oh

noes!" because /tmp is world-writeable. This means we can probably upload scripts into that folder and execute them



