ETHICAL HACKING

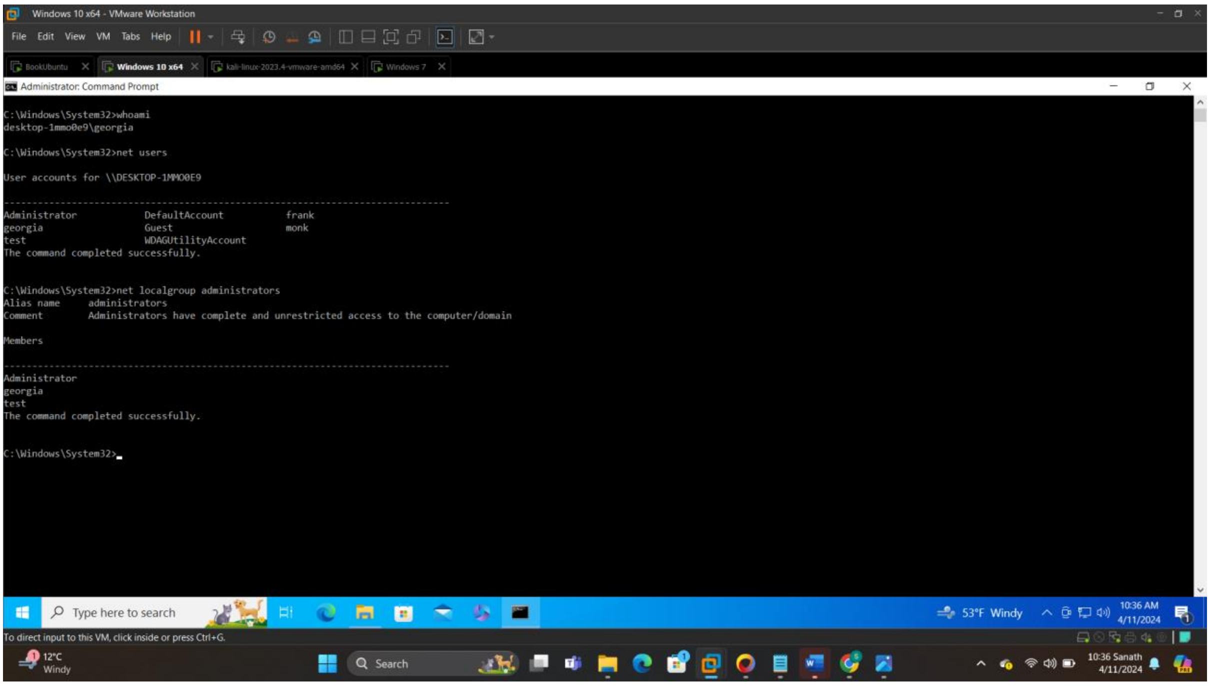
LAB ASSIGNMENT 12

Name: Dasari Sanath Kumar

ID: 700760349

Screenshot 1:

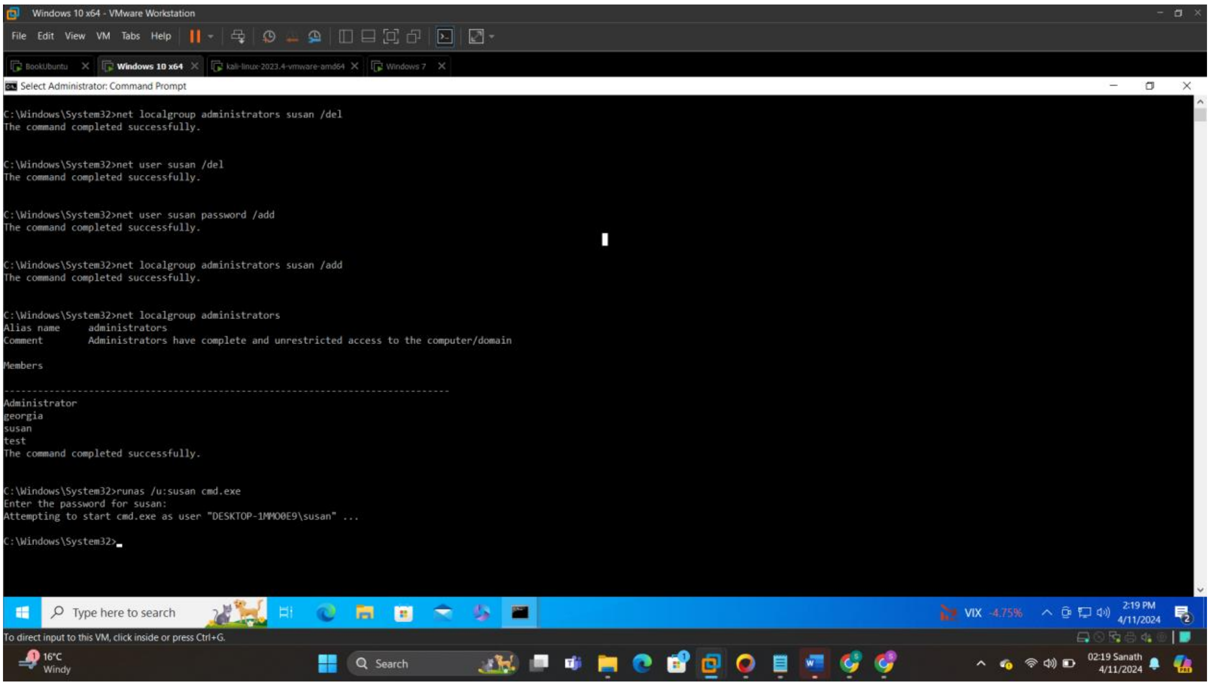
Here in this task we have listed all the local accounts on the machine. And got the list of users in the local administrators group. We have used the below mentioned commands in the screenshot.


Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
BookUbuntu
Windows 10 x64
kali-linux-2023.4-vmware-amd64
Windows 7
Administrator: Command Prompt
Type here to search
53°F Windy
10:36 AM
4/11/2024
To direct input to this VM, click inside or press Ctrl+G.
12°C
Windy
Search
10:36 Sanath
4/11/2024

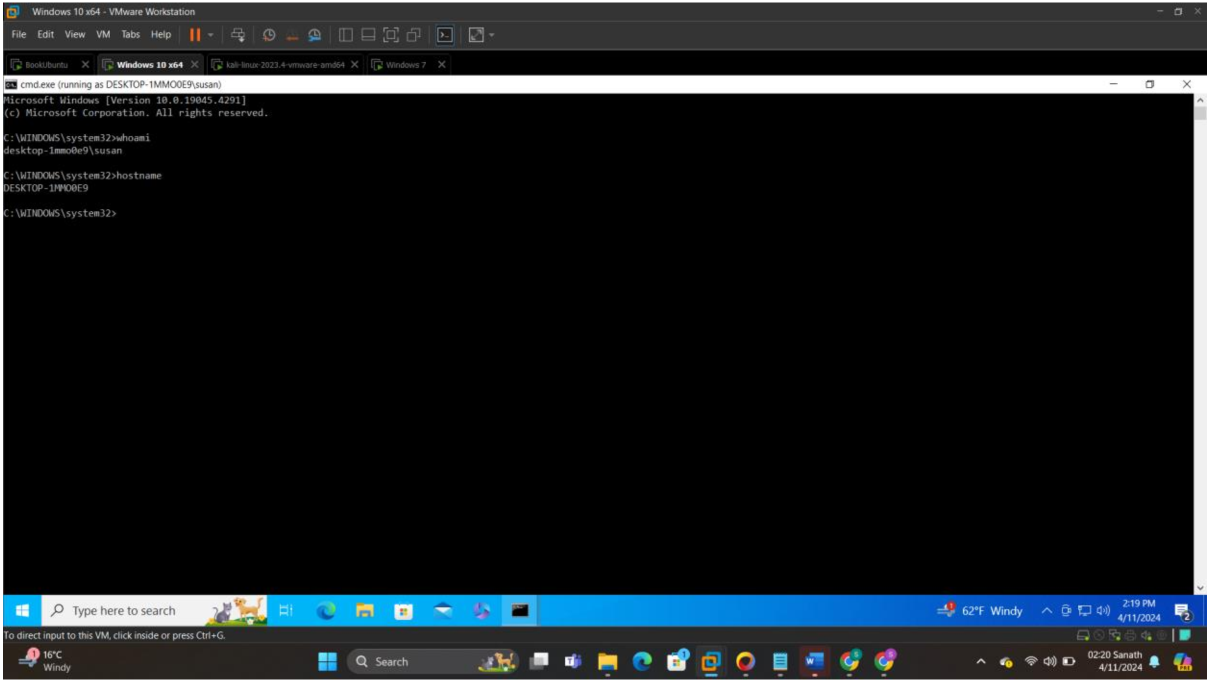
```
C:\Windows\System32>whoami
desktop-1mmo0e9\georgia

C:\Windows\System32>net users

User accounts for \\DESKTOP-1MMO0E9

-------------------------------------------------------------------------------
Administrator            DefaultAccount           frank
georgia                  Guest                    monk
test                     WDAGUtilityAccount
The command completed successfully.


C:\Windows\System32>net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
georgia
test
The command completed successfully.


C:\Windows\System32>_
```

Screenshot 2:

Here we have added a susan account


Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
BookUbuntu
Windows 10 x64
kali-linux-2023.4-vmware-amd64
Windows 7
Select Administrator: Command Prompt
Type here to search
VIX -4.75%
2:19 PM
4/11/2024
To direct input to this VM, click inside or press Ctrl+G.
16°C
Windy
Search
02:19 Sanath
4/11/2024

```
C:\Windows\System32>net localgroup administrators susan /del
The command completed successfully.


C:\Windows\System32>net user susan /del
The command completed successfully.


C:\Windows\System32>net user susan password /add
The command completed successfully.


C:\Windows\System32>net localgroup administrators susan /add
The command completed successfully.


C:\Windows\System32>net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
georgia
susan
test
The command completed successfully.


C:\Windows\System32>runas /u:susan cmd.exe
Enter the password for susan:
Attempting to start cmd.exe as user "DESKTOP-1MMO0E9\susan" ...

C:\Windows\System32>_
```


Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
BookUbuntu
Windows 10 x64
kali-linux-2023.4-vmware-amd64
Windows 7
cmd.exe (running as DESKTOP-1MMO0E9\susan)
Type here to search
62°F Windy
2:19 PM
4/11/2024
To direct input to this VM, click inside or press Ctrl+G.
16°C
Windy
Search
02:20 Sanath
4/11/2024

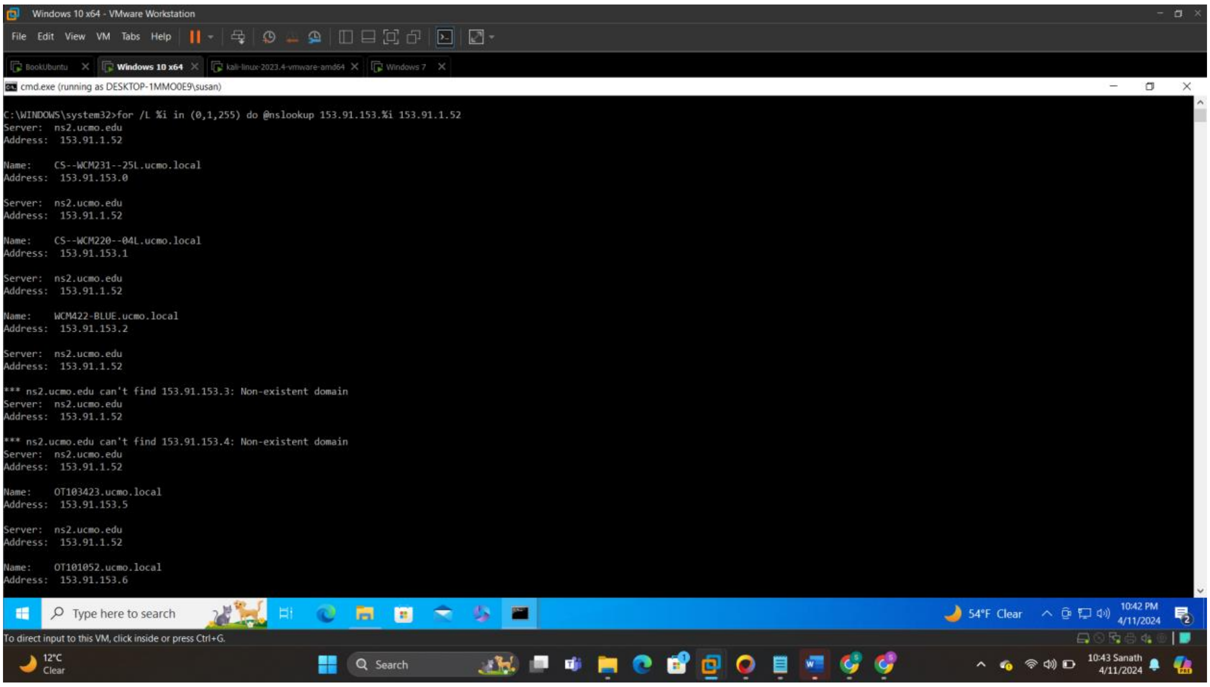
```
Microsoft Windows [Version 10.0.19045.4291]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
desktop-1mmo0e9\susan

C:\WINDOWS\system32>hostname
DESKTOP-1MMO0E9

C:\WINDOWS\system32>
```

Screenshot 3:

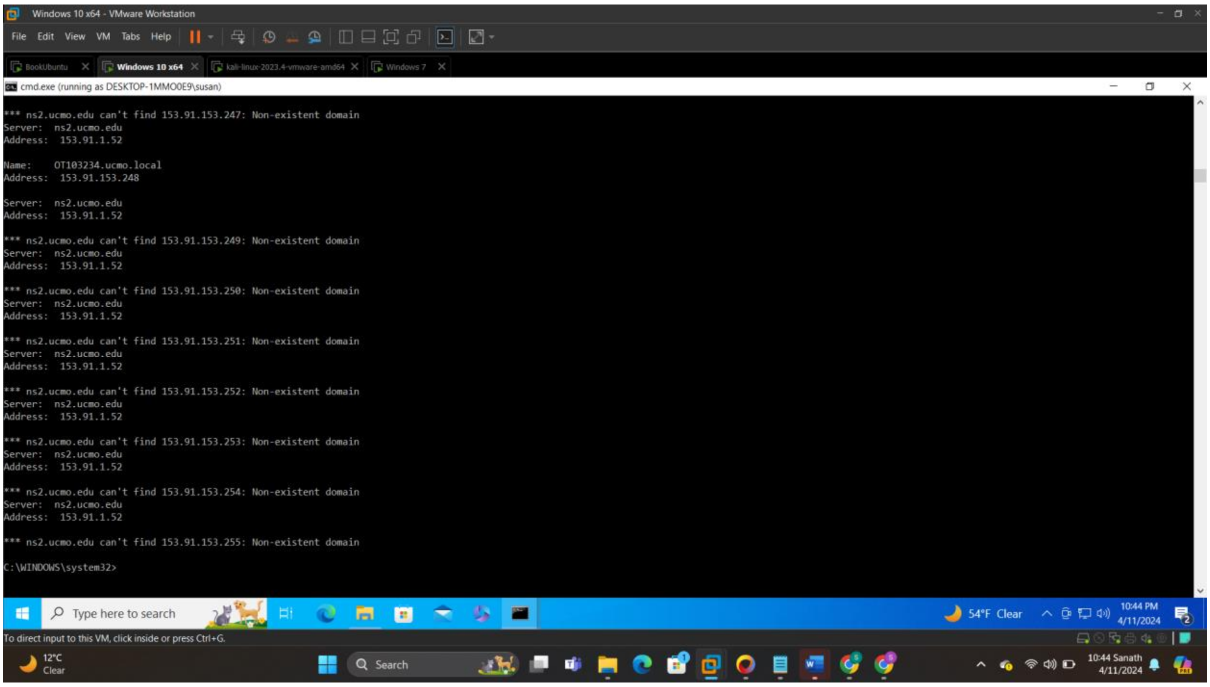
DNS Reverse lookup using /L loop for looping in the ip address range

Here we have done DNS reverse lookup for a netblock range of 192.91.153.0/24

Below are the screenshots for this particular task .


Windows 10 x64 - VMware Workstation
File
Edit
View
VM
Tabs
Help
BookUbuntu
Windows 10 x64
kali-linux-2023.4-vmware-amd64
Windows 7
cmd.exe (running as DESKTOP-1MMO0E9\susan)
Type here to search
54°F Clear
10:42 PM
4/11/2024
To direct input to this VM, click inside or press Ctrl+G.
12°C
Clear
Search
10:43 Sanath
4/11/2024

```
C:\WINDOWS\system32>for /L %i in (0,1,255) do @nslookup 153.91.153.%i 153.91.1.52
Server:  ns2.ucmo.edu
Address:  153.91.1.52

Name:    CS--WCM231--25L.ucmo.local
Address:  153.91.153.0

Server:  ns2.ucmo.edu
Address:  153.91.1.52

Name:    CS--WCM220--04L.ucmo.local
Address:  153.91.153.1

Server:  ns2.ucmo.edu
Address:  153.91.1.52

Name:    WCM422-BLUE.ucmo.local
Address:  153.91.153.2

Server:  ns2.ucmo.edu
Address:  153.91.1.52

*** ns2.ucmo.edu can't find 153.91.153.3: Non-existent domain
Server:  ns2.ucmo.edu
Address:  153.91.1.52

*** ns2.ucmo.edu can't find 153.91.153.4: Non-existent domain
Server:  ns2.ucmo.edu
Address:  153.91.1.52

Name:    OT103423.ucmo.local
Address:  153.91.153.5

Server:  ns2.ucmo.edu
Address:  153.91.1.52

Name:    OT101052.ucmo.local
Address:  153.91.153.6
```

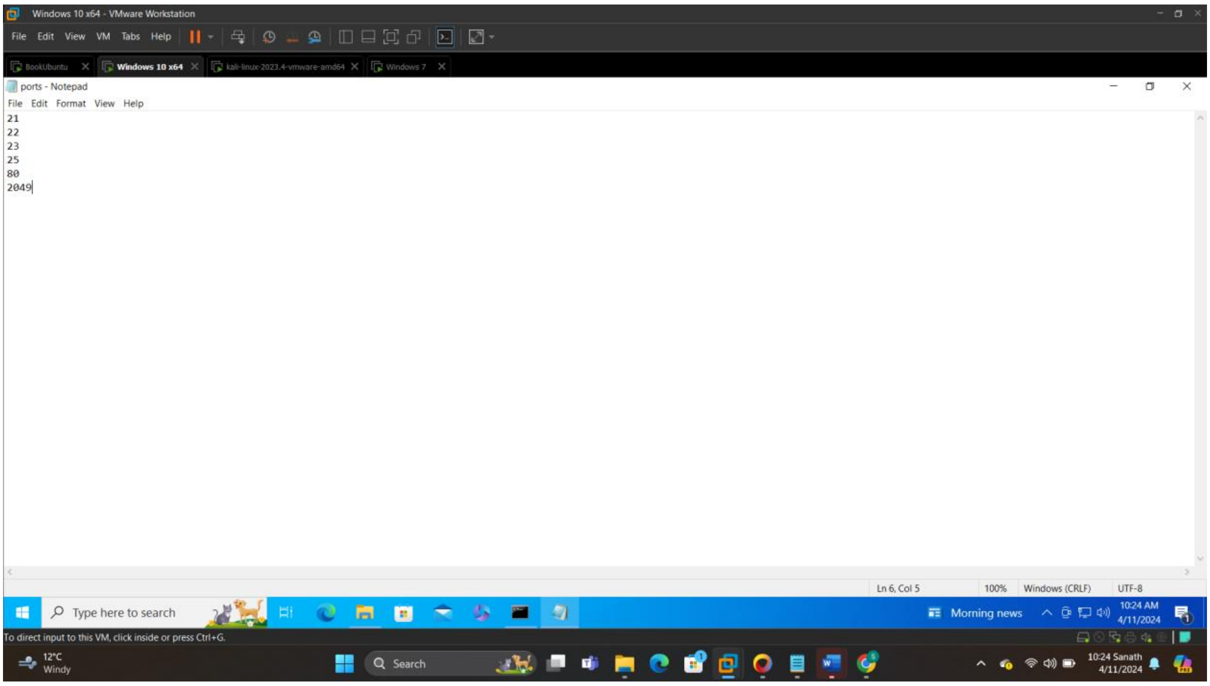

Windows 10 x64 - VMware Workstation
File
Edit
View
VM
Tabs
Help
BookUbuntu
Windows 10 x64
kali-linux-2023.4-vmware-amd64
Windows 7
cmd.exe (running as DESKTOP-1MMO0E9\susan)
Type here to search
54°F Clear
10:44 PM
4/11/2024
To direct input to this VM, click inside or press Ctrl+G.
12°C
Clear
Search
10:44 Sanath
4/11/2024

```
*** ns2.ucmo.edu can't find 153.91.153.247: Non-existent domain
Server:  ns2.ucmo.edu
Address:  153.91.1.52

Name:    OT103234.ucmo.local
Address:  153.91.153.248

Server:  ns2.ucmo.edu
Address:  153.91.1.52

*** ns2.ucmo.edu can't find 153.91.153.249: Non-existent domain
Server:  ns2.ucmo.edu
Address:  153.91.1.52

*** ns2.ucmo.edu can't find 153.91.153.250: Non-existent domain
Server:  ns2.ucmo.edu
Address:  153.91.1.52

*** ns2.ucmo.edu can't find 153.91.153.251: Non-existent domain
Server:  ns2.ucmo.edu
Address:  153.91.1.52

*** ns2.ucmo.edu can't find 153.91.153.252: Non-existent domain
Server:  ns2.ucmo.edu
Address:  153.91.1.52

*** ns2.ucmo.edu can't find 153.91.153.253: Non-existent domain
Server:  ns2.ucmo.edu
Address:  153.91.1.52

*** ns2.ucmo.edu can't find 153.91.153.254: Non-existent domain
Server:  ns2.ucmo.edu
Address:  153.91.1.52

*** ns2.ucmo.edu can't find 153.91.153.255: Non-existent domain

C:\WINDOWS\system32>
```

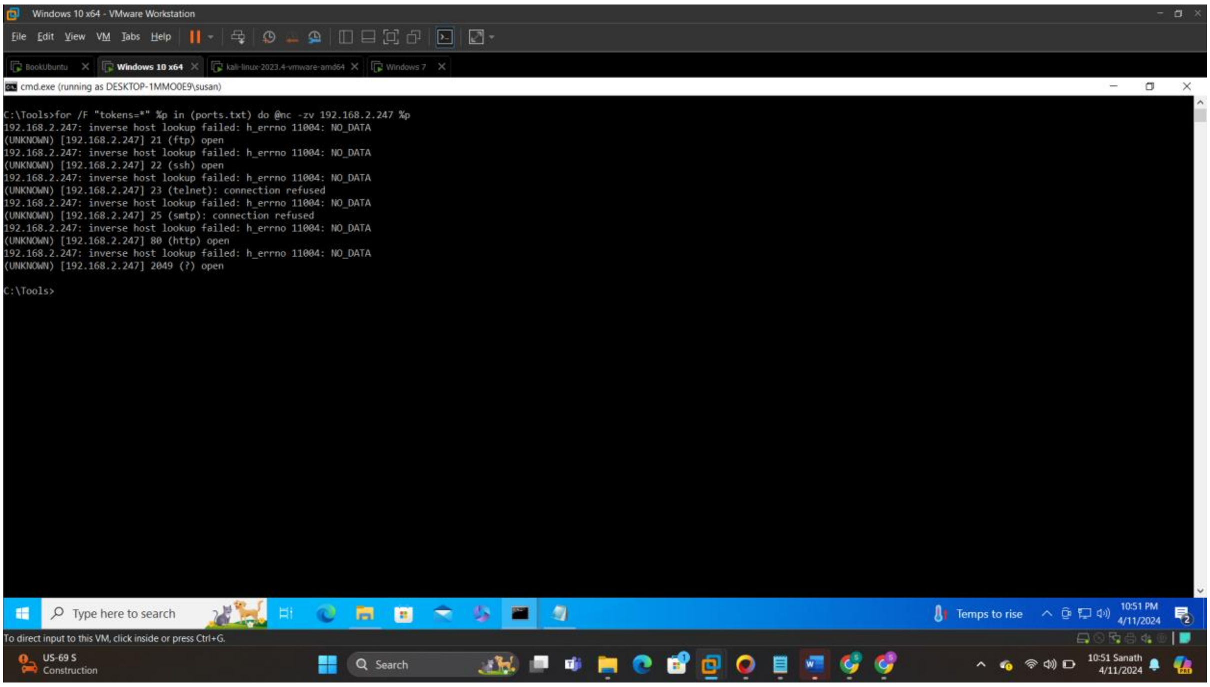
Screenshot 4:

Here I have used a text file named ports.txt and executed below command on my windows10.

This is task to ports scanning on my ubuntu machine.


Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
BookUbuntu
Windows 10 x64
kali-linux-2023.4-vmware-amd64
Windows 7
ports - Notepad
File Edit Format View Help
Ln 6, Col 5
100%
Windows (CRLF)
UTF-8
Type here to search
Morning news
10:24 AM
4/11/2024
To direct input to this VM, click inside or press Ctrl+G.
12°C
Windy
Search
10:24 Sanath
4/11/2024

```
21
22
23
25
80
2049
```


Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
BookUbuntu
Windows 10 x64
kali-linux-2023.4-vmware-amd64
Windows 7
cmd.exe (running as DESKTOP-1MMO0E9\susan)
Type here to search
Temps to rise
10:51 PM
4/11/2024
To direct input to this VM, click inside or press Ctrl+G.
US-69 S
Construction
Search
10:51 Sanath
4/11/2024

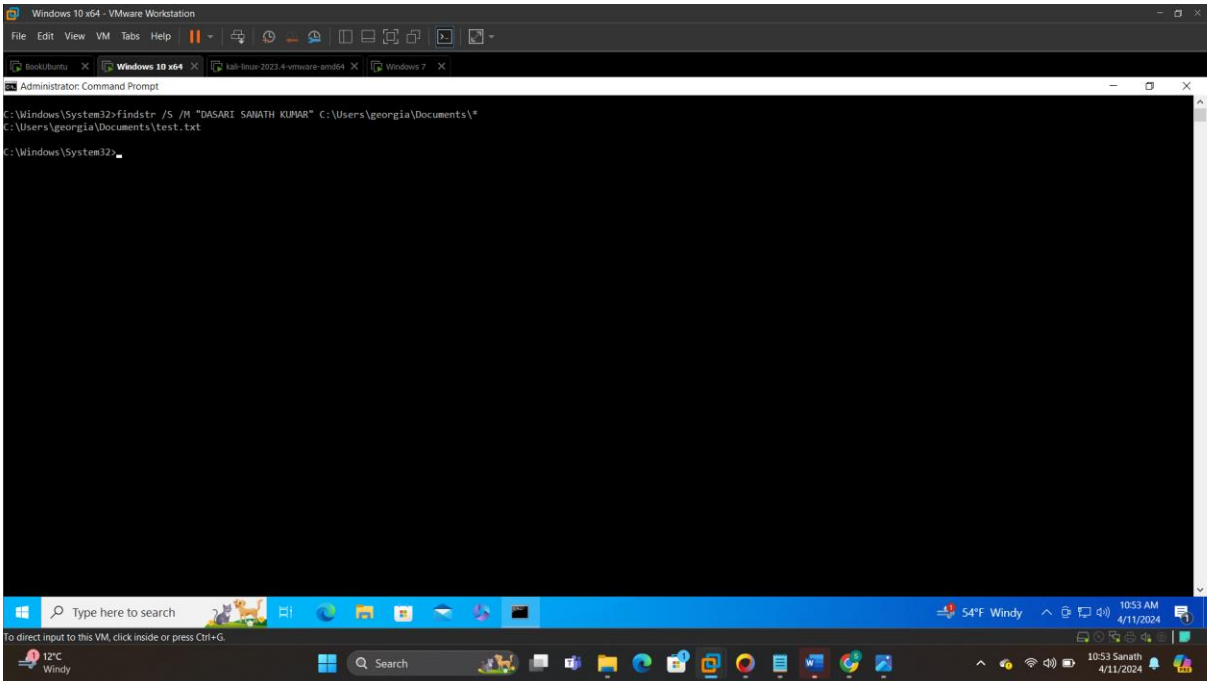
```
C:\Tools>for /F "tokens=*" %p in (ports.txt) do @nc -zv 192.168.2.247 %p
192.168.2.247: inverse host lookup failed: h_errno 11004: NO_DATA
(UNKNOWN) [192.168.2.247] 21 (ftp) open
192.168.2.247: inverse host lookup failed: h_errno 11004: NO_DATA
(UNKNOWN) [192.168.2.247] 22 (ssh) open
192.168.2.247: inverse host lookup failed: h_errno 11004: NO_DATA
(UNKNOWN) [192.168.2.247] 23 (telnet): connection refused
192.168.2.247: inverse host lookup failed: h_errno 11004: NO_DATA
(UNKNOWN) [192.168.2.247] 25 (smtp): connection refused
192.168.2.247: inverse host lookup failed: h_errno 11004: NO_DATA
(UNKNOWN) [192.168.2.247] 80 (http) open
192.168.2.247: inverse host lookup failed: h_errno 11004: NO_DATA
(UNKNOWN) [192.168.2.247] 2049 (?) open

C:\Tools>
```

Here we have done the port scanning on our ubuntu machine from windows10 and found ports 21,22,80,2049 ports are opened and 23,25 are refusing the connection

Screenshot 5:

In this task we have learnt about how to find a particular string in a files under some folder.

As a penetration tester it will be very helpful to search for sensitive files on a compromised machine. Below is the mentioned screenshot foe this task



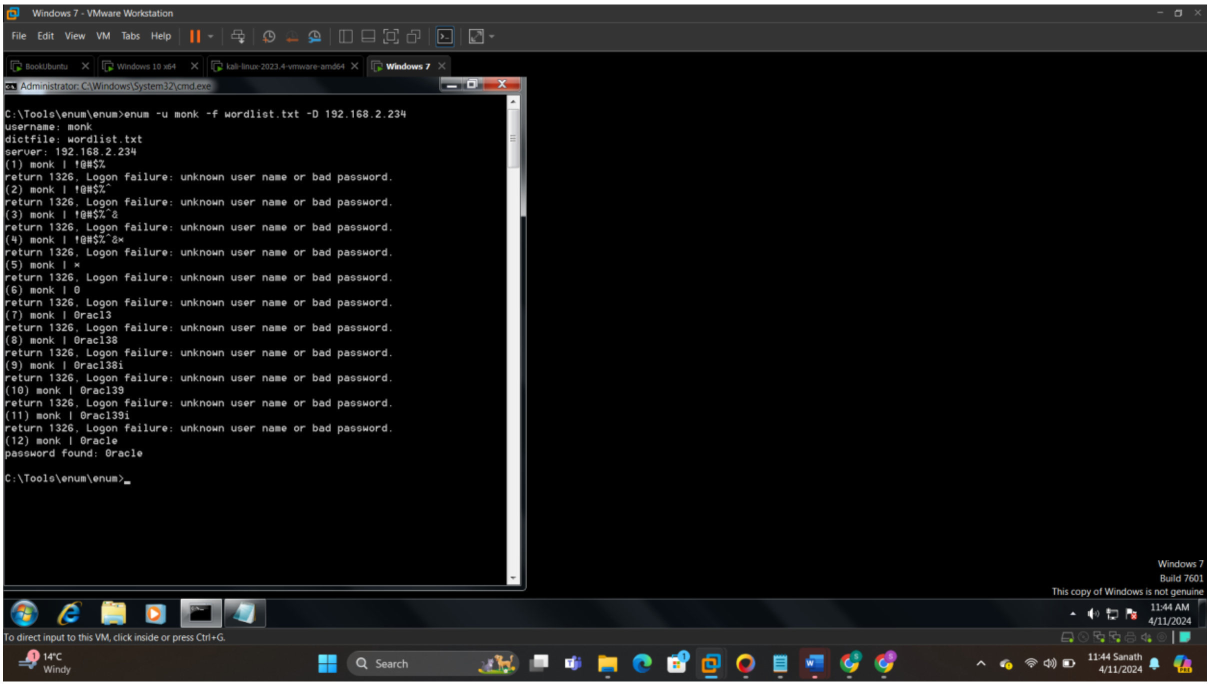
Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
BookUbuntu
Windows 10 x64
kali-linux-2023.4-vmware-amd64
Windows 7
Administrator: Command Prompt
Type here to search
54°F Windy
10:53 AM
4/11/2024
To direct input to this VM, click inside or press Ctrl+G.
12°C
Windy
Search
10:53 Sanath
4/11/2024

```
C:\Windows\System32>findstr /S /M "DASARI SANATH KUMAR" C:\Users\georgia\Documents\*
C:\Users\georgia\Documents\test.txt

C:\Windows\System32>_
```

➔ Which Nmap script can help identify the hostname too?

Ans:- nmap –script dns-nsid <TargetIp Addr>

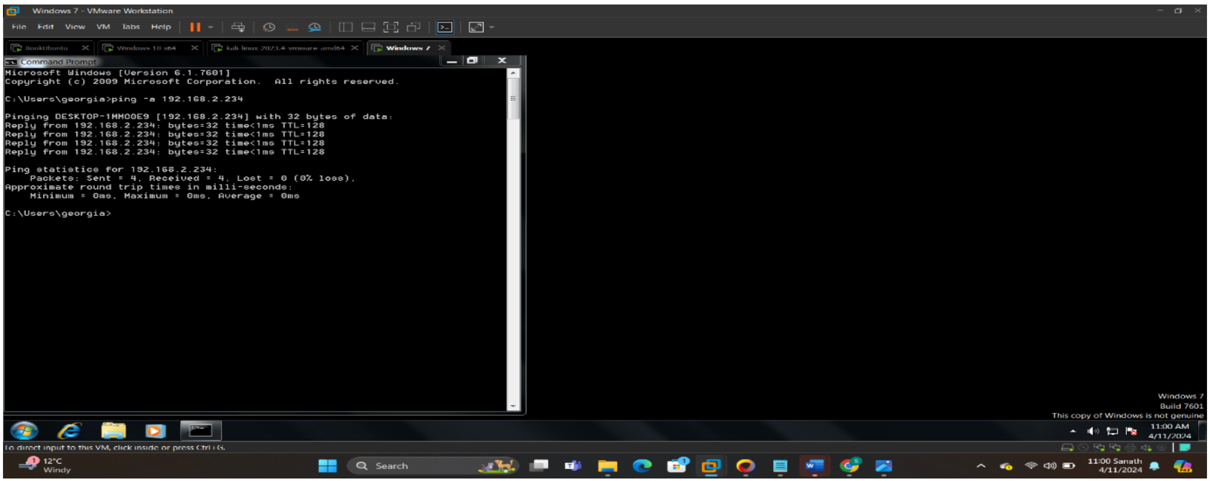
screenshot 6:



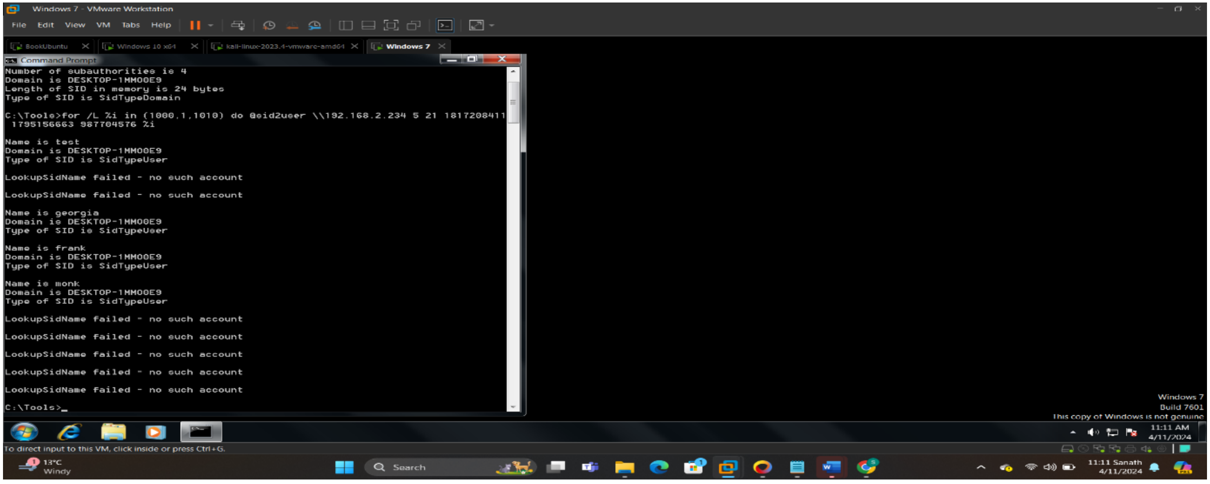
Windows 7 - VMware Workstation
File Edit View VM Tabs Help
BookUbuntu
Windows 10 x64
kali-linux-2023.4-vmware-amd64
Windows 7
Administrator: C:\Windows\System32\cmd.exe
Windows 7
Build 7601
This copy of Windows is not genuine
11:44 AM
4/11/2024
To direct input to this VM, click inside or press Ctrl+G.
14°C
Windy
Search
11:44 Sanath
4/11/2024

```
C:\Tools\enum\enum>enum -u monk -f wordlist.txt -D 192.168.2.234
username: monk
dictfile: wordlist.txt
server: 192.168.2.234
(1) monk | !@#$%
return 1326, Logon failure: unknown user name or bad password.
(2) monk | !@#$%^
return 1326, Logon failure: unknown user name or bad password.
(3) monk | !@#$%^&
return 1326, Logon failure: unknown user name or bad password.
(4) monk | !@#$%^&*
return 1326, Logon failure: unknown user name or bad password.
(5) monk | *
return 1326, Logon failure: unknown user name or bad password.
(6) monk | 0
return 1326, Logon failure: unknown user name or bad password.
(7) monk | 0racl3
return 1326, Logon failure: unknown user name or bad password.
(8) monk | 0racl38
return 1326, Logon failure: unknown user name or bad password.
(9) monk | 0racl38i
return 1326, Logon failure: unknown user name or bad password.
(10) monk | 0racl39
return 1326, Logon failure: unknown user name or bad password.
(11) monk | 0racl39i
return 1326, Logon failure: unknown user name or bad password.
(12) monk | 0racle
password found: 0racle

C:\Tools\enum\enum>_
```

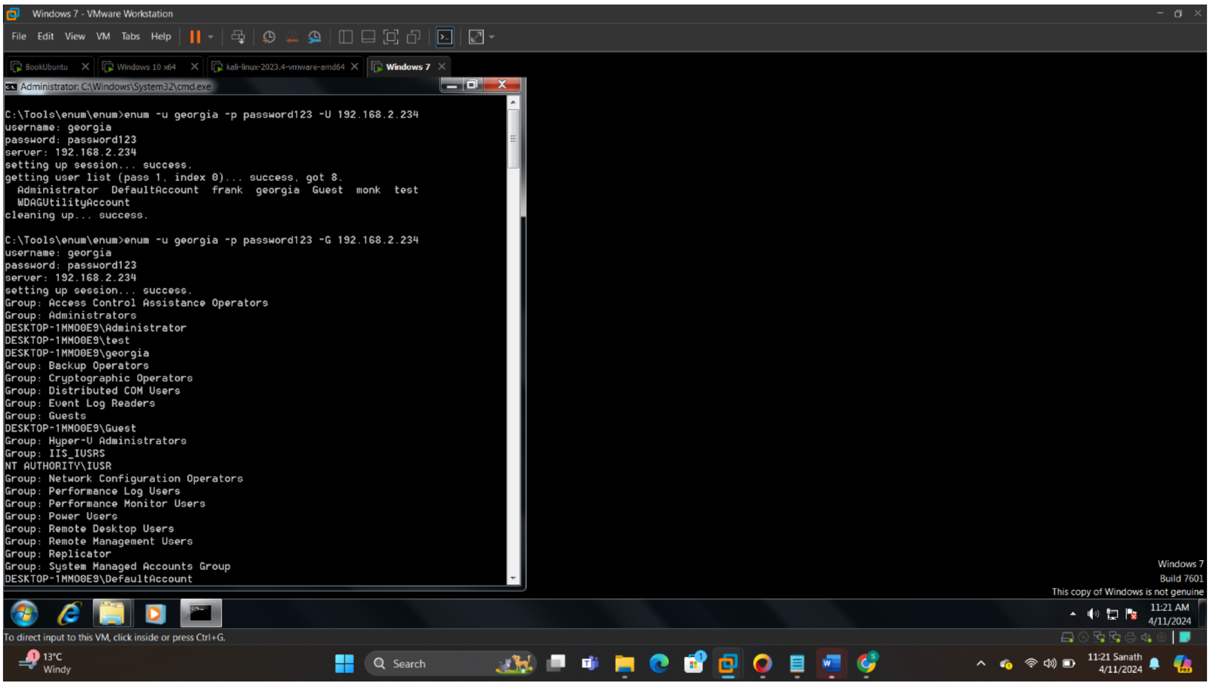
Additional Lab Report screenshots:


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
BookUbuntu
Windows 10 x64
kali-linux-2023.4-vmware-amd64
Windows 7
Command Prompt
Windows 7
Build 7601
This copy of Windows is not genuine
11:00 AM
4/11/2024
To direct input to this VM, click inside or press Ctrl+G.
12°C
Windy
Search
11:00 Sanath
4/11/2024

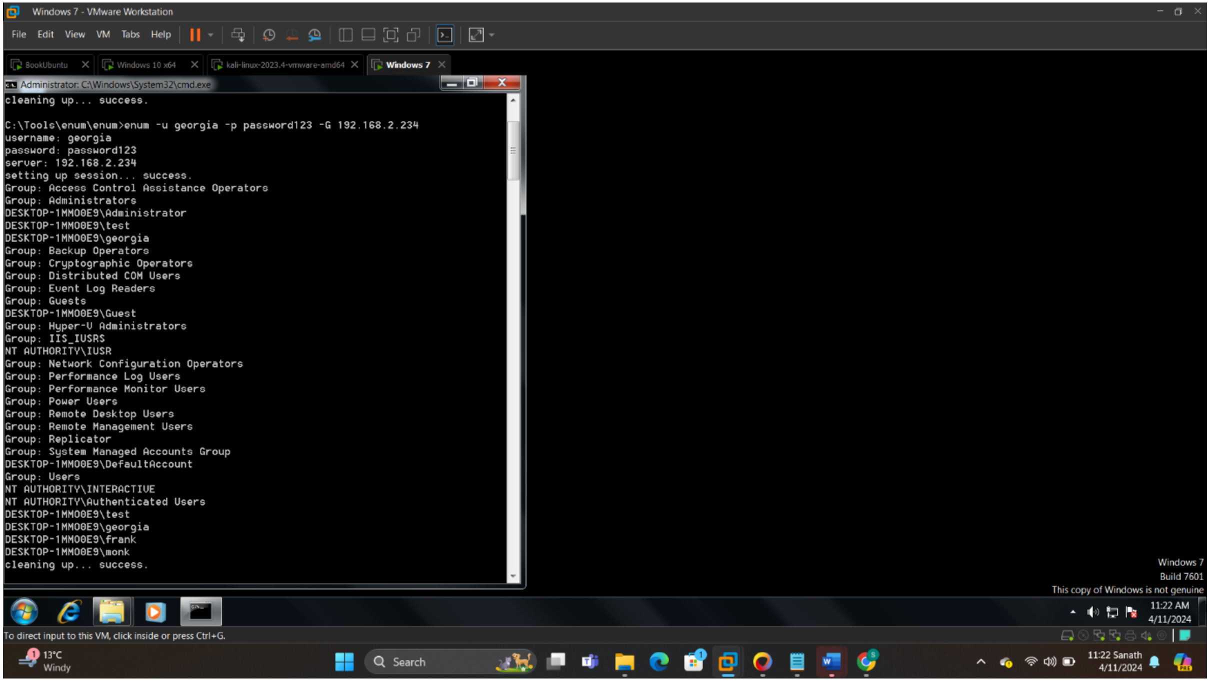
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\georgia>ping -a 192.168.2.234

Pinging DESKTOP-1MMO0E9 [192.168.2.234] with 32 bytes of data:
Reply from 192.168.2.234: bytes=32 time<1ms TTL=128
Reply from 192.168.2.234: bytes=32 time<1ms TTL=128
Reply from 192.168.2.234: bytes=32 time<1ms TTL=128
Reply from 192.168.2.234: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.234:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\georgia>
```


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
BookUbuntu
Windows 10 x64
kali-linux-2023.4-vmware-amd64
Windows 7
Command Prompt
Windows 7
Build 7601
This copy of Windows is not genuine
11:11 AM
4/11/2024
To direct input to this VM, click inside or press Ctrl+G.
13°C
Windy
Search
11:11 Sanath
4/11/2024

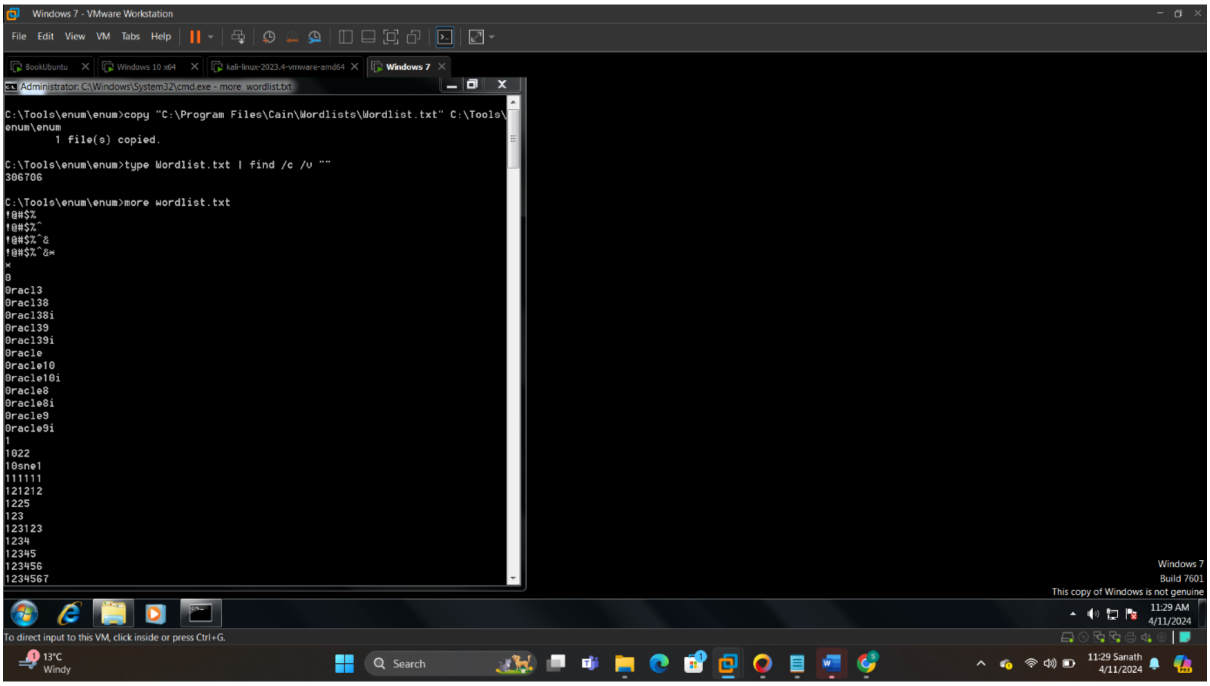
```
Number of subauthorities is 4
Domain is DESKTOP-1MMO0E9
Length of SID in memory is 24 bytes
Type of SID is SidTypeDomain

C:\Tools>for /L %i in (1000,1,1010) do @sid2user \\192.168.2.234 5 21 1817208411
 1795156663 987704576 %i

Name is test
Domain is DESKTOP-1MMO0E9
Type of SID is SidTypeUser

LookupSidName failed - no such account

LookupSidName failed - no such account

Name is georgia
Domain is DESKTOP-1MMO0E9
Type of SID is SidTypeUser

Name is frank
Domain is DESKTOP-1MMO0E9
Type of SID is SidTypeUser

Name is monk
Domain is DESKTOP-1MMO0E9
Type of SID is SidTypeUser

LookupSidName failed - no such account

LookupSidName failed - no such account

LookupSidName failed - no such account

LookupSidName failed - no such account

LookupSidName failed - no such account

C:\Tools>_
```


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
BookUbuntu
Windows 10 x64
kali-linux-2023.4-vmware-amd64
Windows 7
Administrator: C:\Windows\System32\cmd.exe
Windows 7
Build 7601
This copy of Windows is not genuine
11:21 AM
4/11/2024
To direct input to this VM, click inside or press Ctrl+G.
13°C
Windy
Search
11:21 Sanath
4/11/2024

```
C:\Tools\enum\enum>enum -u georgia -p password123 -U 192.168.2.234
username: georgia
password: password123
server: 192.168.2.234
setting up session... success.
getting user list (pass 1, index 0)... success, got 8.
  Administrator  DefaultAccount  frank  georgia  Guest  monk  test
  WDAGUtilityAccount
cleaning up... success.

C:\Tools\enum\enum>enum -u georgia -p password123 -G 192.168.2.234
username: georgia
password: password123
server: 192.168.2.234
setting up session... success.
Group: Access Control Assistance Operators
Group: Administrators
DESKTOP-1MMO0E9\Administrator
DESKTOP-1MMO0E9\test
DESKTOP-1MMO0E9\georgia
Group: Backup Operators
Group: Cryptographic Operators
Group: Distributed COM Users
Group: Event Log Readers
Group: Guests
DESKTOP-1MMO0E9\Guest
Group: Hyper-V Administrators
Group: IIS_IUSRS
NT AUTHORITY\IUSR
Group: Network Configuration Operators
Group: Performance Log Users
Group: Performance Monitor Users
Group: Power Users
Group: Remote Desktop Users
Group: Remote Management Users
Group: Replicator
Group: System Managed Accounts Group
DESKTOP-1MMO0E9\DefaultAccount
```


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
BookUbuntu
Windows 10 x64
kali-linux-2023.4-vmware-amd64
Windows 7
Administrator: C:\Windows\System32\cmd.exe
Windows 7
Build 7601
This copy of Windows is not genuine
11:22 AM
4/11/2024
To direct input to this VM, click inside or press Ctrl+G.
13°C
Windy
Search
11:22 Sanath
4/11/2024

```
cleaning up... success.

C:\Tools\enum\enum>enum -u georgia -p password123 -G 192.168.2.234
username: georgia
password: password123
server: 192.168.2.234
setting up session... success.
Group: Access Control Assistance Operators
Group: Administrators
DESKTOP-1MMO0E9\Administrator
DESKTOP-1MMO0E9\test
DESKTOP-1MMO0E9\georgia
Group: Backup Operators
Group: Cryptographic Operators
Group: Distributed COM Users
Group: Event Log Readers
Group: Guests
DESKTOP-1MMO0E9\Guest
Group: Hyper-V Administrators
Group: IIS_IUSRS
NT AUTHORITY\IUSR
Group: Network Configuration Operators
Group: Performance Log Users
Group: Performance Monitor Users
Group: Power Users
Group: Remote Desktop Users
Group: Remote Management Users
Group: Replicator
Group: System Managed Accounts Group
DESKTOP-1MMO0E9\DefaultAccount
Group: Users
NT AUTHORITY\INTERACTIVE
NT AUTHORITY\Authenticated Users
DESKTOP-1MMO0E9\test
DESKTOP-1MMO0E9\georgia
DESKTOP-1MMO0E9\frank
DESKTOP-1MMO0E9\monk
cleaning up... success.
```



Windows 7 - VMware Workstation
File
Edit
View
VM
Tabs
Help
BookUbuntu
Windows 10 x64
kali-linux-2023.4-vmware-amd64
Windows 7
Administrator: C:\Windows\System32\cmd.exe - more wordlist.txt
Windows 7
Build 7601
This copy of Windows is not genuine
11:29 AM
4/11/2024
To direct input to this VM, click inside or press Ctrl+G.
13°C
Windy
Search
11:29 Sanath
4/11/2024

```
C:\Tools\enum\enum>copy "C:\Program Files\Cain\Wordlists\Wordlist.txt" C:\Tools\
enum\enum
        1 file(s) copied.

C:\Tools\enum\enum>type Wordlist.txt | find /c /v ""
306706

C:\Tools\enum\enum>more wordlist.txt
!@#$%
!@#$%^
!@#$%^&
!@#$%^&*
*
0
0racl3
0racl38
0racl38i
0racl39
0racl39i
0racle
0racle10
0racle10i
0racle8
0racle8i
0racle9
0racle9i
1
1022
10sne1
111111
121212
1225
123
123123
1234
12345
123456
1234567
```