# LAB Manual
# PART A

(PART A : TO BE REFFERED BY STUDENTS)

## Experiment No. 6

## A.1 Aim:

To perform System Audit.

## A.2 Prerequisite:

Understanding on basics of audit system, use cases of audit system.

## A.3 Outcome:

**After successful completion of this experiment students will be able to** Know about the tactics and techniques of system audit, tools used for system audit.

## A.4 Theory:

**Audit:** An audit is the examination

**System Audit:** A system audit is an audit on a management system to validate whether or not the elements of the system are effective and properly implemented to meet the objectives or standards.

**Importance of system audit:** Strong audit systems can reduce or help decrease various forms of risks in businesses including the risk of material misstatement in financial reports. It also helps reduce the risk of misuse of assets, fraud and low quality management because of insufficient or lack of information on operations.

**Audit Benefits:**

a) Compliance.
b) Business Improvements / System Improvements.
c) Credibility.
d) Detect and Prevent Fraud.
e) Better Planning and Budgeting.

**Types of system audit:**

- Internal Audit.
- External Audit.
- Third Party Audit.
- Compliance Audit.

**Tools used for System Audit:**

- Compliance checklist.
- Inbuilt tools.
- Third party tools.

**Steps of performing a system audit:**

I. Review.

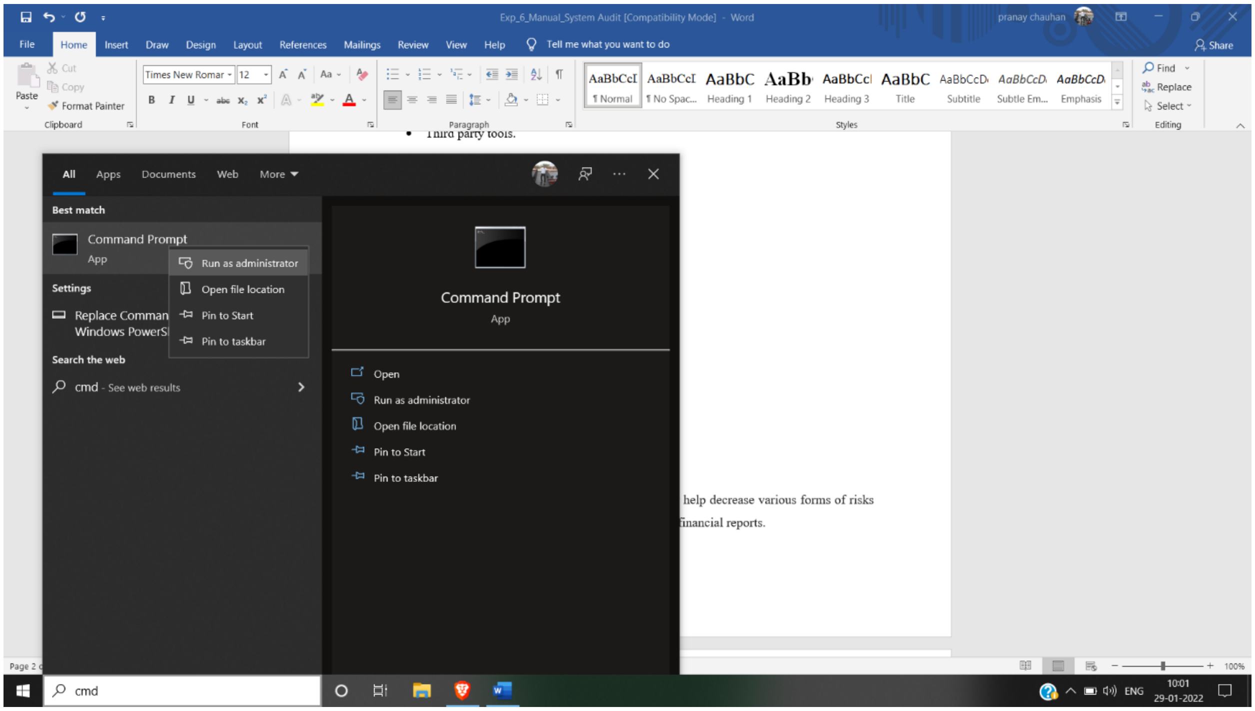
II. System Vulnerability is assessed.

III. Threats are identified.

IV. Internal Controls are analyzed.

V. Final Evaluation.

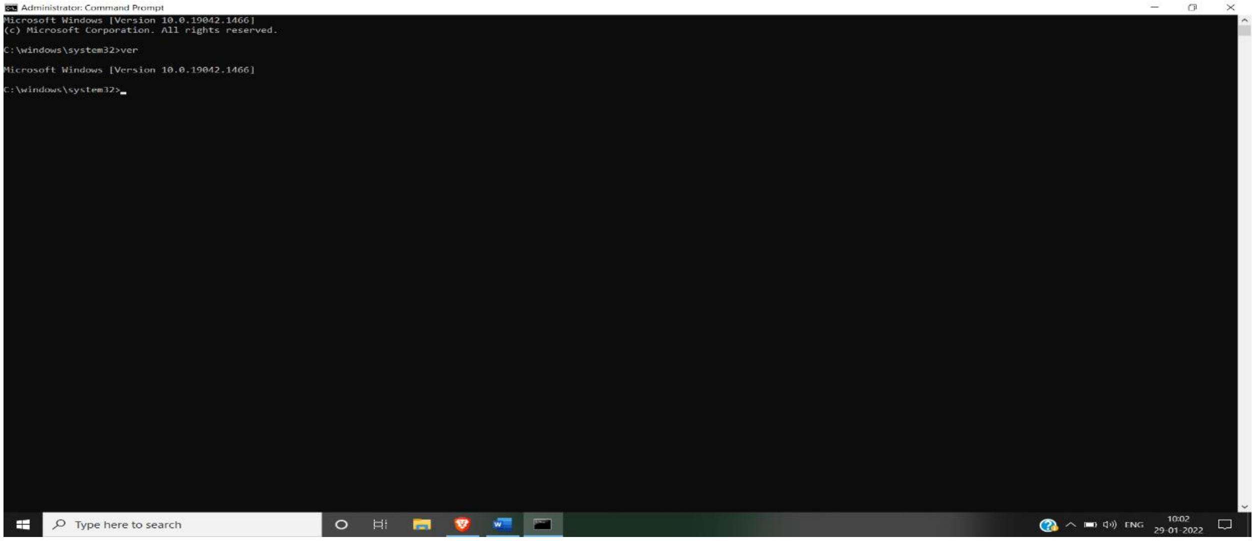
Step: 1 Run CMD as administrator



Step: 2

Check version of operating system to check updated version is used or not

Command : **ver**

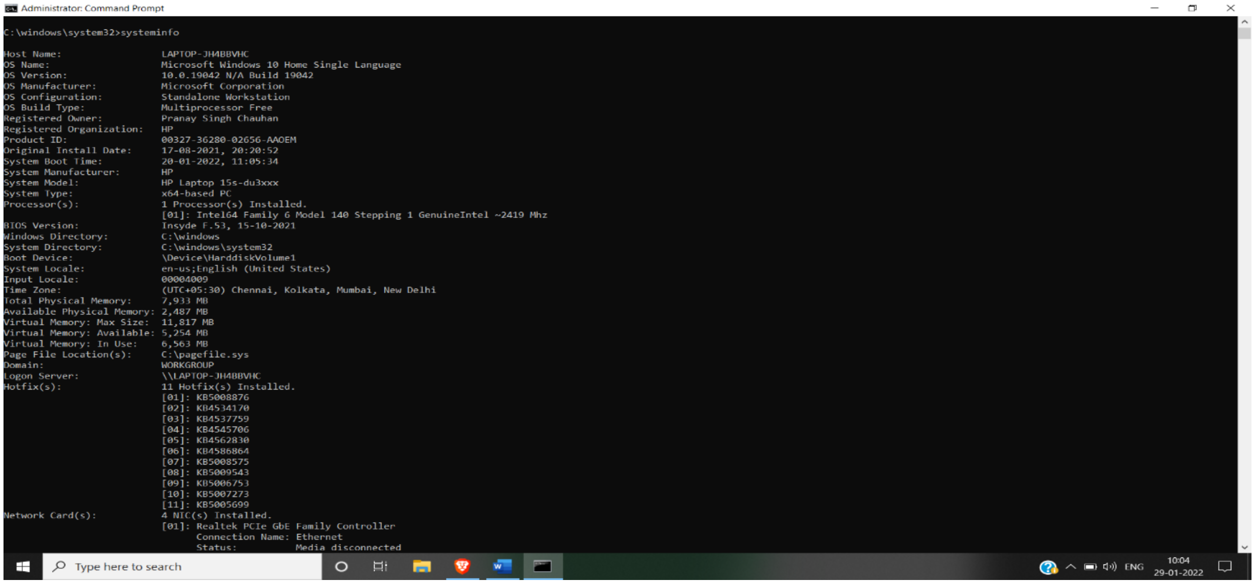


```
Microsoft Windows [Version 10.0.19042.1466]
(c) Microsoft Corporation. All rights reserved.

C:\windows\system32>ver

Microsoft Windows [Version 10.0.19042.1466]

C:\windows\system32>_
```

Step: 3: Check system information

To check all the updates

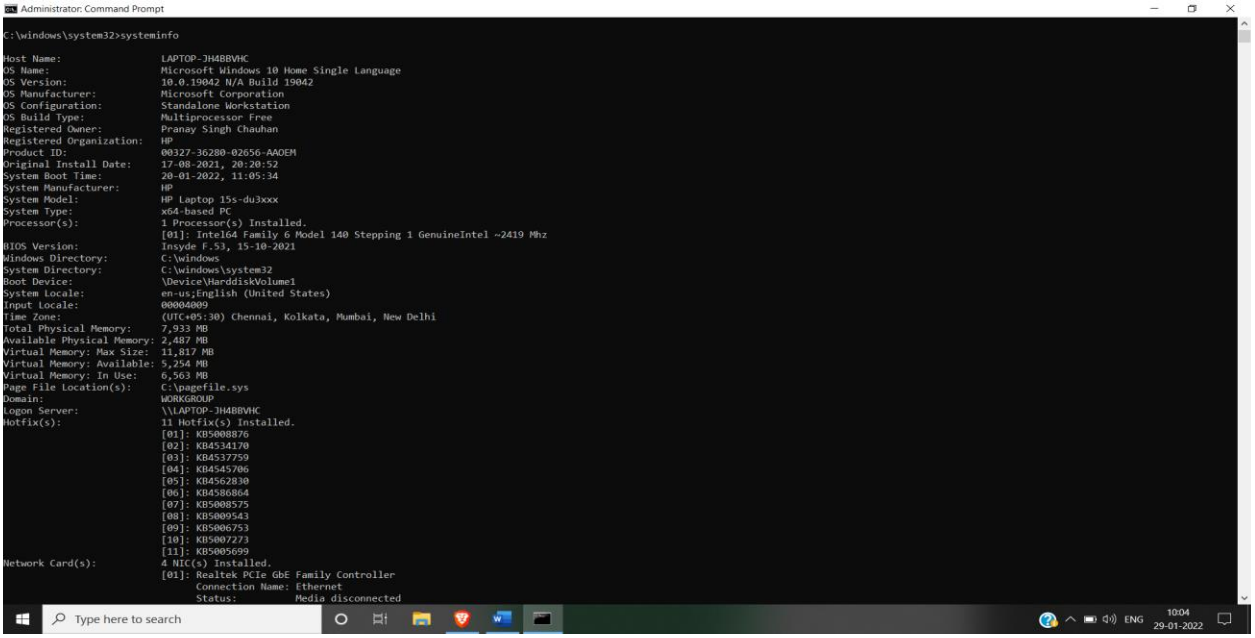
Command: systeminfo



```
C:\windows\system32>systeminfo

Host Name:                 LAPTOP-JH4BBVHC
OS Name:                   Microsoft Windows 10 Home Single Language
OS Version:                10.0.19042 N/A Build 19042
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Pranay Singh Chauhan
Registered Organization:   HP
Product ID:                00327-36280-02656-AAOEM
Original Install Date:     17-08-2021, 20:20:52
System Boot Time:          20-01-2022, 11:05:34
System Manufacturer:       HP
System Model:              HP Laptop 15s-du3xxx
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel ~2419 Mhz
BIOS Version:              Insyde F.53, 15-10-2021
Windows Directory:         C:\windows
System Directory:          C:\windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     7,933 MB
Available Physical Memory: 2,487 MB
Virtual Memory: Max Size:  11,817 MB
Virtual Memory: Available: 5,254 MB
Virtual Memory: In Use:    6,563 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\LAPTOP-JH4BBVHC
Hotfix(s):                 11 Hotfix(s) Installed.
                           [01]: KB5008876
                           [02]: KB4534170
                           [03]: KB4537759
                           [04]: KB4545706
                           [05]: KB4562830
                           [06]: KB4586864
                           [07]: KB5008575
                           [08]: KB5009543
                           [09]: KB5006753
                           [10]: KB5007273
                           [11]: KB5005699
Network Card(s):           4 NIC(s) Installed.
                           [01]: Realtek PCIe GbE Family Controller
                                 Connection Name: Ethernet
                                 Status:          Media disconnected
```

Step: 4: To check remotely open files

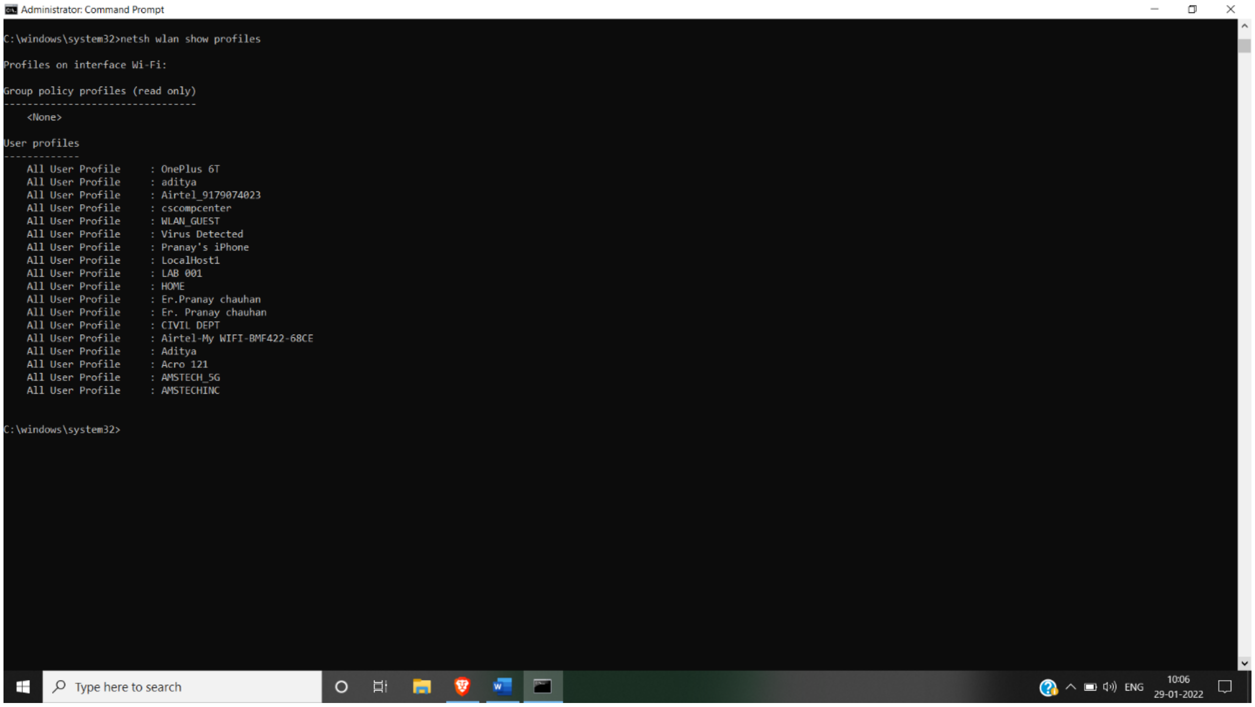
Command: openfiles



```
C:\windows\system32>systeminfo

Host Name:                 LAPTOP-JH4BBVHC
OS Name:                   Microsoft Windows 10 Home Single Language
OS Version:                10.0.19042 N/A Build 19042
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Pranay Singh Chauhan
Registered Organization:   HP
Product ID:                00327-36280-02656-AAOEM
Original Install Date:     17-08-2021, 20:20:52
System Boot Time:          20-01-2022, 11:05:34
System Manufacturer:       HP
System Model:              HP Laptop 15s-du3xxx
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel ~2419 Mhz
BIOS Version:              Insyde F.53, 15-10-2021
Windows Directory:         C:\windows
System Directory:          C:\windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     7,933 MB
Available Physical Memory: 2,487 MB
Virtual Memory: Max Size:  11,817 MB
Virtual Memory: Available: 5,254 MB
Virtual Memory: In Use:    6,563 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\LAPTOP-JH4BBVHC
Hotfix(s):                 11 Hotfix(s) Installed.
                           [01]: KB5008876
                           [02]: KB4534170
                           [03]: KB4537759
                           [04]: KB4545706
                           [05]: KB4562830
                           [06]: KB4586864
                           [07]: KB5008575
                           [08]: KB5009543
                           [09]: KB5006753
                           [10]: KB5007273
                           [11]: KB5005699
Network Card(s):           4 NIC(s) Installed.
                           [01]: Realtek PCIe GbE Family Controller
                                 Connection Name: Ethernet
                                 Status:          Media disconnected
```

Step: 5: to Check all used wifi connections

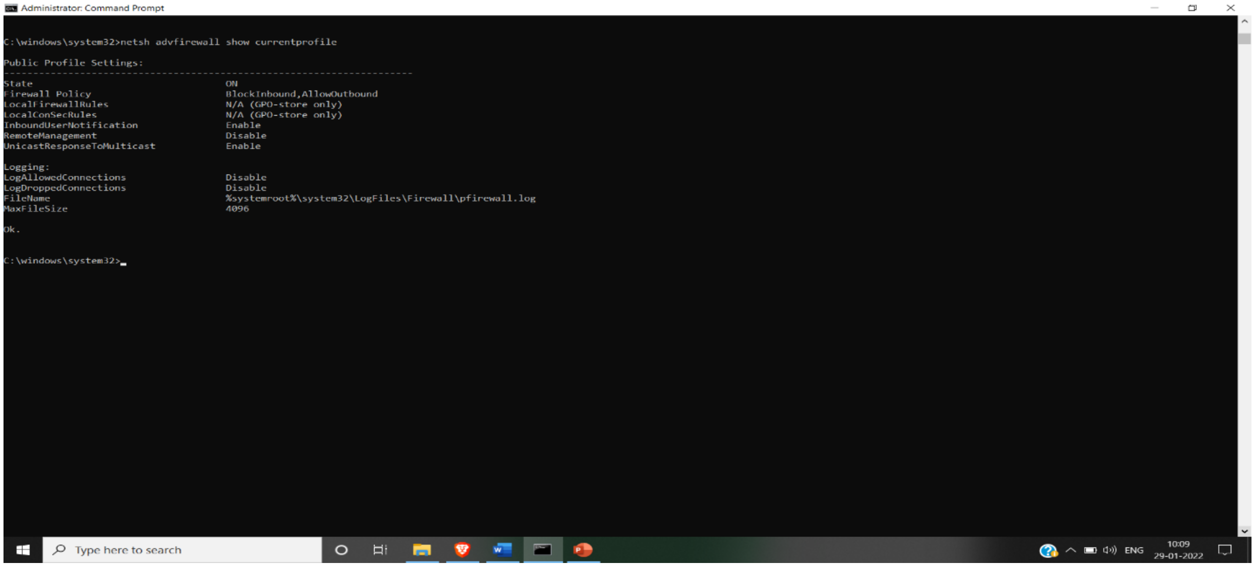
Command: netsh wlan show profiles



```
C:\windows\system32>netsh wlan show profiles

Profiles on interface Wi-Fi:

Group policy profiles (read only)
---------------------------------
    <None>

User profiles
-------------
    All User Profile     : OnePlus 6T
    All User Profile     : aditya
    All User Profile     : Airtel_9179074023
    All User Profile     : cscompcenter
    All User Profile     : WLAN_GUEST
    All User Profile     : Virus Detected
    All User Profile     : Pranay's iPhone
    All User Profile     : LocalHost1
    All User Profile     : LAB 001
    All User Profile     : HOME
    All User Profile     : Er.Pranay chauhan
    All User Profile     : Er. Pranay chauhan
    All User Profile     : CIVIL DEPT
    All User Profile     : Airtel-My WIFI-BMF422-68CE
    All User Profile     : Aditya
    All User Profile     : Acro 121
    All User Profile     : AMSTECH_5G
    All User Profile     : AMSTECHINC


C:\windows\system32>
```

Step: 6 : To check firewall enabled services in desktop

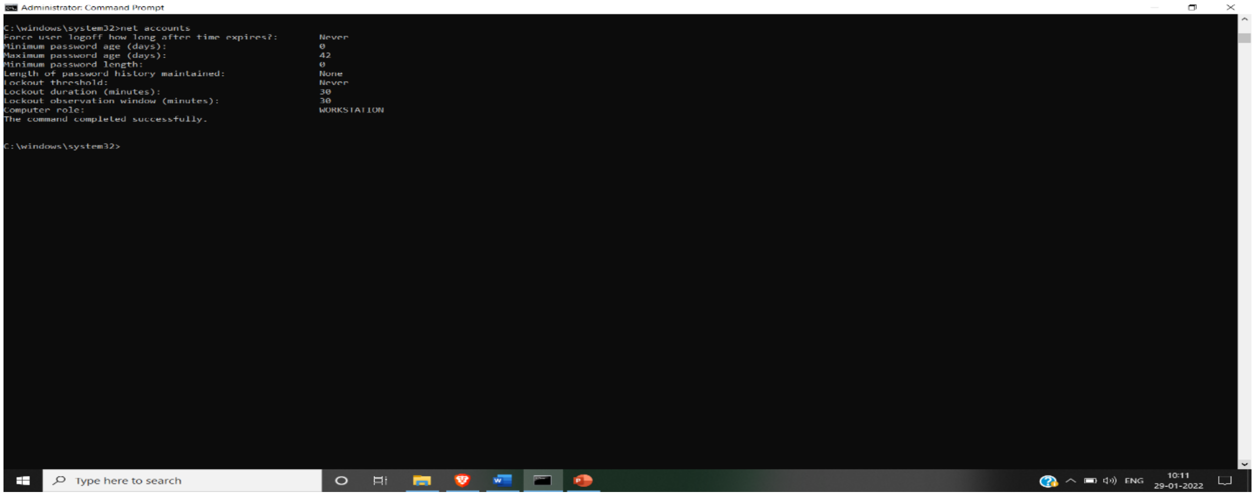
Command : netsh advfirewall show currentprofile



```
C:\windows\system32>netsh advfirewall show currentprofile

Public Profile Settings:
----------------------------------------------------------------------
State                                 ON
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096

Ok.


C:\windows\system32>
```

Step: 7: To check network account state

Command: net account



```
C:\windows\system32>net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          42
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    Never
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        WORKSTATION
The command completed successfully.


C:\windows\system32>
```

Step: 8: To check, scan and repair corrupted system file

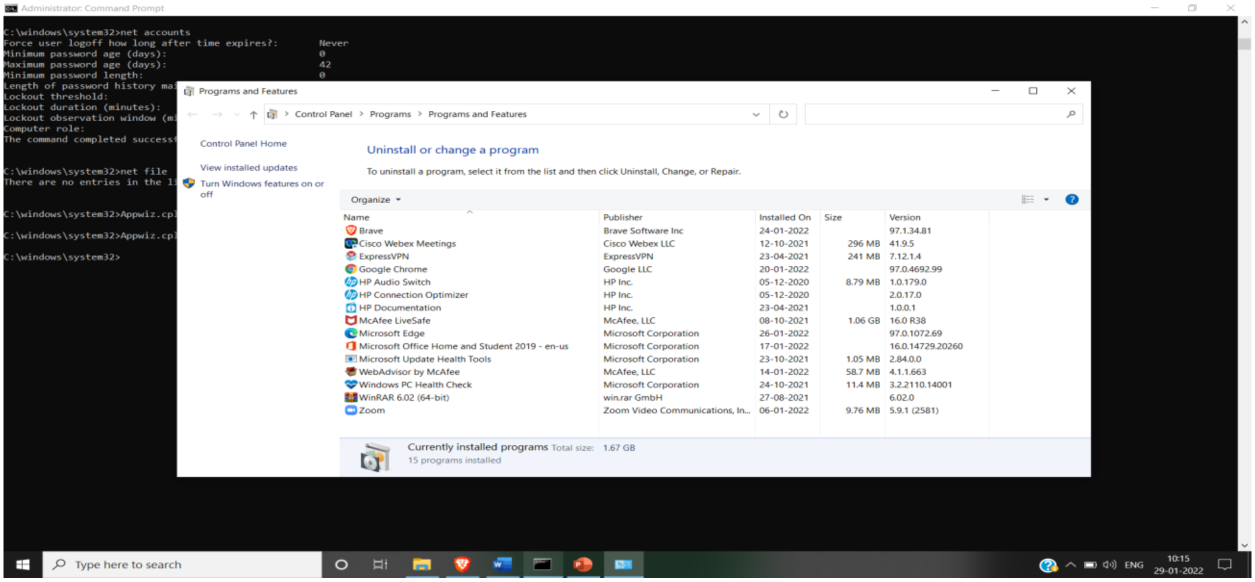
Command: sfc/scannow

Step: 9: To check network files

Command: net file

Step: 10: To check all installed softwares

Command: Appwiz.cpl



Administrator: Command Prompt
Programs and Features
Control Panel > Programs > Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Organize
Type here to search
ENG
10:15
29-01-2022

```
C:\windows\system32>net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          42
Minimum password length:                              0
Length of password history mai
Lockout threshold:
Lockout duration (minutes):
Lockout observation window (mi
Computer role:
The command completed successf

C:\windows\system32>net file
There are no entries in the li

C:\windows\system32>Appwiz.cpl

C:\windows\system32>Appwiz.cpl

C:\windows\system32>
```

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

| Name | Publisher | Installed On | Size | Version |
|---|---|---|---|---|
| Brave | Brave Software Inc | 24-01-2022 | | 97.1.34.81 |
| Cisco Webex Meetings | Cisco Webex LLC | 12-10-2021 | 296 MB | 41.9.5 |
| ExpressVPN | ExpressVPN | 23-04-2021 | 241 MB | 7.12.1.4 |
| Google Chrome | Google LLC | 20-01-2022 | | 97.0.4692.99 |
| HP Audio Switch | HP Inc. | 05-12-2020 | 8.79 MB | 1.0.179.0 |
| HP Connection Optimizer | HP Inc. | 05-12-2020 | | 2.0.17.0 |
| HP Documentation | HP Inc. | 23-04-2021 | | 1.0.0.1 |
| McAfee LiveSafe | McAfee, LLC | 08-10-2021 | 1.06 GB | 16.0 R38 |
| Microsoft Edge | Microsoft Corporation | 26-01-2022 | | 97.0.1072.69 |
| Microsoft Office Home and Student 2019 - en-us | Microsoft Corporation | 17-01-2022 | | 16.0.14729.20260 |
| Microsoft Update Health Tools | Microsoft Corporation | 23-10-2021 | 1.05 MB | 2.84.0.0 |
| WebAdvisor by McAfee | McAfee, LLC | 14-01-2022 | 58.7 MB | 4.1.1.663 |
| Windows PC Health Check | Microsoft Corporation | 24-10-2021 | 11.4 MB | 3.2.2110.14001 |
| WinRAR 6.02 (64-bit) | win.rar GmbH | 27-08-2021 | | 6.02.0 |
| Zoom | Zoom Video Communications, In... | 06-01-2022 | 9.76 MB | 5.9.1 (2581) |

Currently installed programs Total size: 1.67 GB
15 programs installed

Other utilities can be used:

- query
- query termserver
- route table\
- route print
- arp –a
- services.msc (It will show all the services)

**Note: Students can prepare audit checklist/ questionnaire based on above utilities.**

**Sample: Checklist for password policy**

**Password Policy**

- Is there any policy for minimum password characters?
- Did any mechanism for minimum password verification.
- Is there any two-step verification process for accessing passwords?
- Did Periodic password changes are mandatory
- Are there any options for least login attempts for user-entered passwords before blocking the account?
- Are there any options for password hints?
- Are there any options for multi-factor authentication (MFA)?

**Need of system Audit:** Strong audit systems can reduce or help decrease various forms of risks in businesses including the risk of material misstatement in financial reports.

It also helps reduce the risk of misuse of assets, fraud and low-quality management because of insufficient or lack of information on operations.

# PART B

(PART B: TO BE COMPLETED BY STUDENTS)

***(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no Black board access available)***

| | |
|---|---|
| Roll. No. A016 | Name: Varun Khadayate |
| Class B.Tech CsBs | Batch: 1 |
| Date of Experiment: 11-02-2022 | Date of Submission: 11-02-2022 |
| Grade: | |

## B.1 Software Code written by student:

***(Paste your Java code completed during the 2 hours of practical in the lab here)***

Command Prompt is being used here.

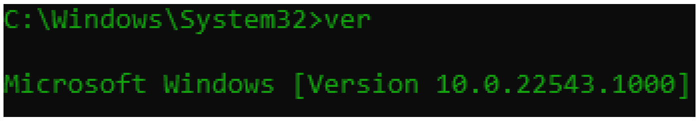
## B.2 Input and Output:

***(Paste your program input and output in following format, If there is error then paste the specific error in the output part. In case of error with due permission of the faculty extension can be given to submit the error free code with output in due course of time. Students will be graded accordingly.)***

# Input:

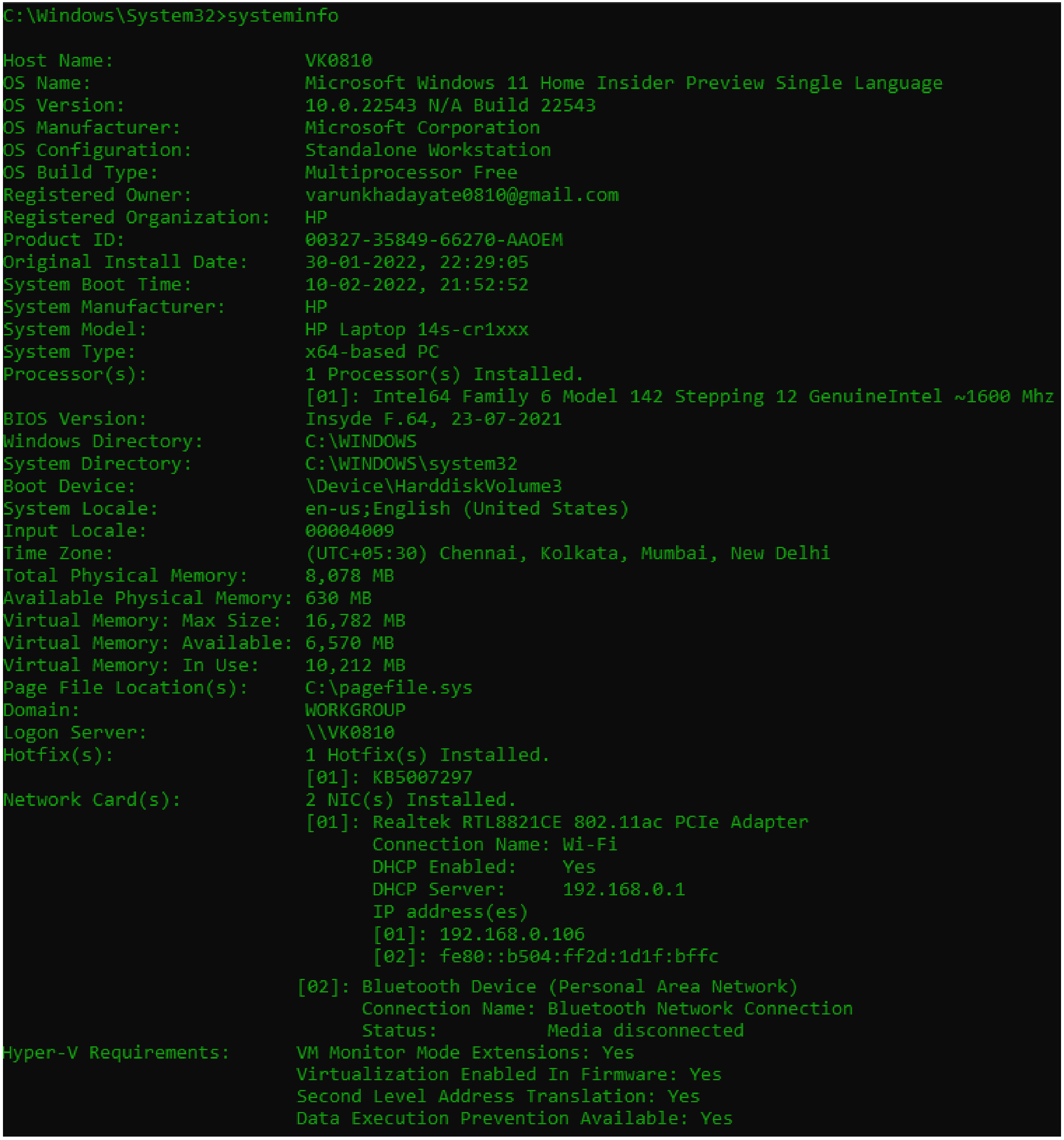
*Perform the system audit commands*

ver



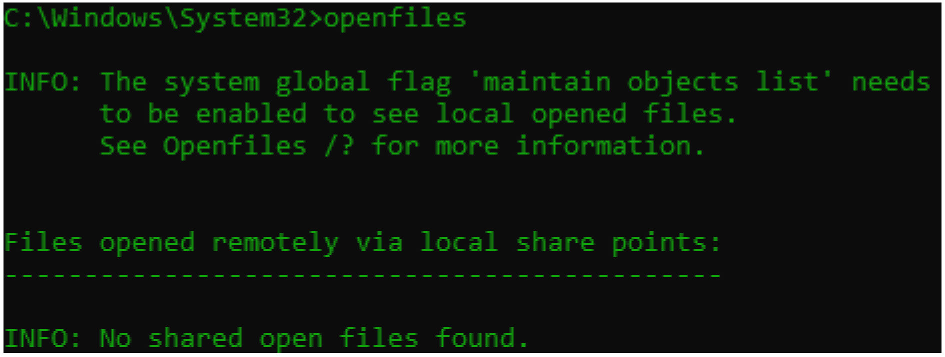
```
C:\Windows\System32>ver

Microsoft Windows [Version 10.0.22543.1000]
```

systeminfo



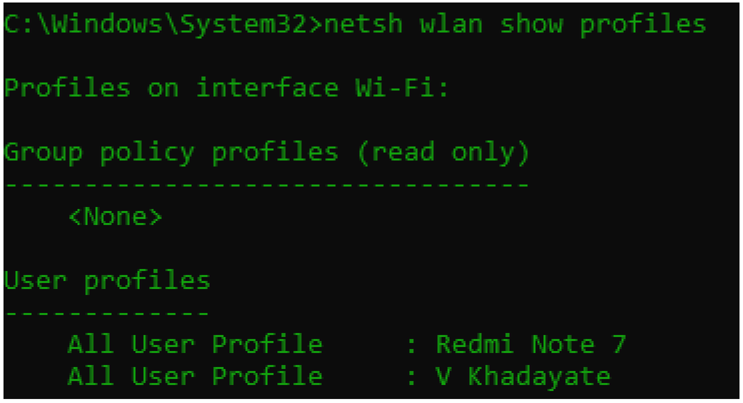
```
C:\Windows\System32>systeminfo

Host Name:                 VK0810
OS Name:                   Microsoft Windows 11 Home Insider Preview Single Language
OS Version:                10.0.22543 N/A Build 22543
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          varunkhadayate0810@gmail.com
Registered Organization:   HP
Product ID:                00327-35849-66270-AAOEM
Original Install Date:     30-01-2022, 22:29:05
System Boot Time:          10-02-2022, 21:52:52
System Manufacturer:       HP
System Model:              HP Laptop 14s-cr1xxx
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 142 Stepping 12 GenuineIntel ~1600 Mhz
BIOS Version:              Insyde F.64, 23-07-2021
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume3
System Locale:             en-us;English (United States)
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     8,078 MB
Available Physical Memory: 630 MB
Virtual Memory: Max Size:  16,782 MB
Virtual Memory: Available: 6,570 MB
Virtual Memory: In Use:    10,212 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\VK0810
Hotfix(s):                 1 Hotfix(s) Installed.
                           [01]: KB5007297
Network Card(s):           2 NIC(s) Installed.
                           [01]: Realtek RTL8821CE 802.11ac PCIe Adapter
                                 Connection Name: Wi-Fi
                                 DHCP Enabled:    Yes
                                 DHCP Server:     192.168.0.1
                                 IP address(es)
                                 [01]: 192.168.0.106
                                 [02]: fe80::b504:ff2d:1d1f:bffc

                          [02]: Bluetooth Device (Personal Area Network)
                                Connection Name: Bluetooth Network Connection
                                Status:          Media disconnected
Hyper-V Requirements:     VM Monitor Mode Extensions: Yes
                          Virtualization Enabled In Firmware: Yes
                          Second Level Address Translation: Yes
                          Data Execution Prevention Available: Yes
```

## openfiles



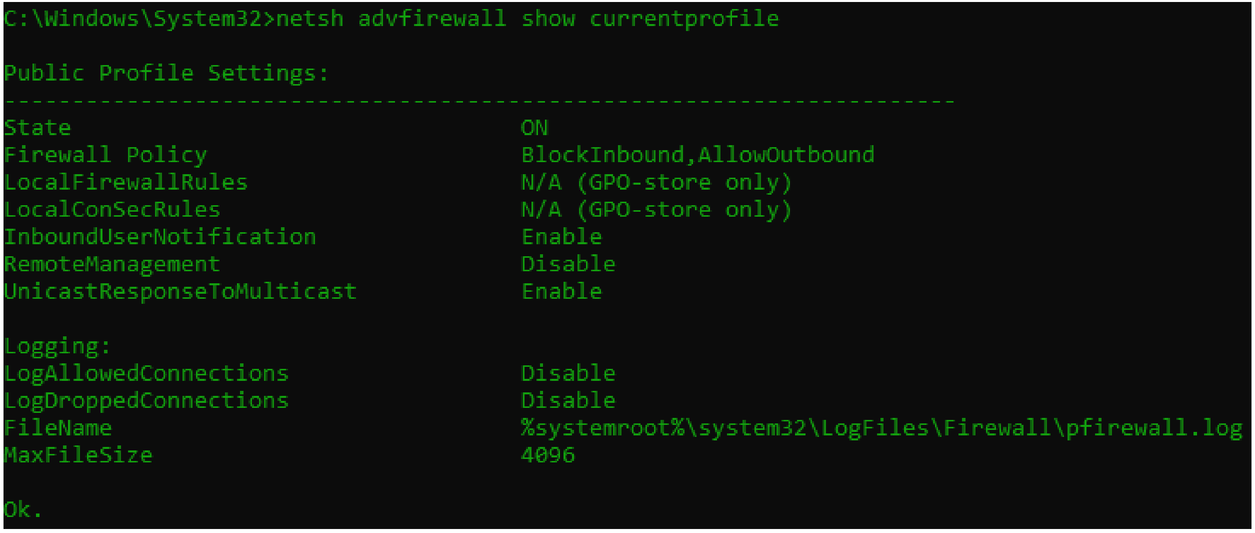
```
C:\Windows\System32>openfiles

INFO: The system global flag 'maintain objects list' needs
      to be enabled to see local opened files.
      See Openfiles /? for more information.


Files opened remotely via local share points:
---------------------------------------------

INFO: No shared open files found.
```

## netsh wlan show profiles



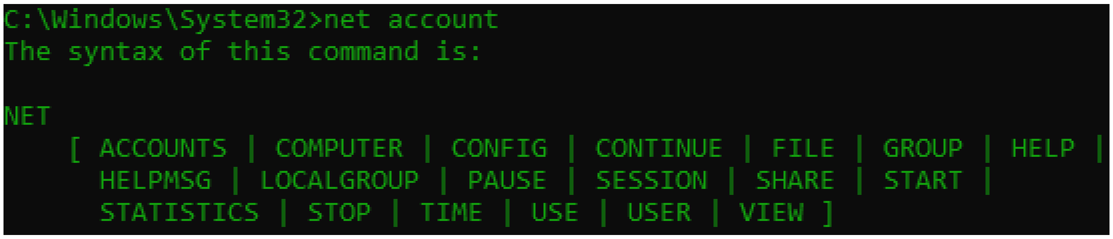
```
C:\Windows\System32>netsh wlan show profiles

Profiles on interface Wi-Fi:

Group policy profiles (read only)
---------------------------------
    <None>

User profiles
-------------
    All User Profile     : Redmi Note 7
    All User Profile     : V Khadayate
```

## netsh advfirewall show currentprofile



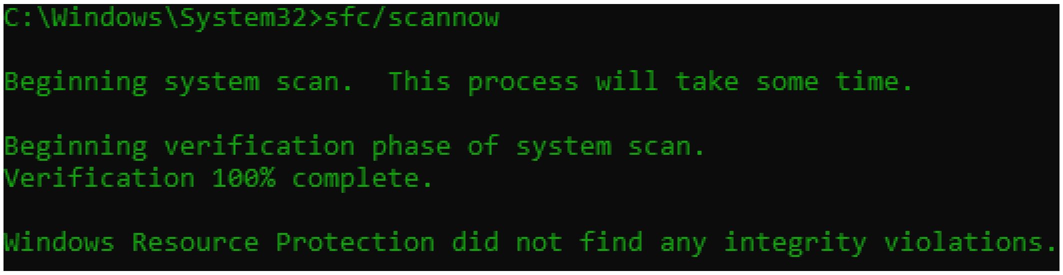
```
C:\Windows\System32>netsh advfirewall show currentprofile

Public Profile Settings:
----------------------------------------------------------------------
State                                 ON
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096

Ok.
```

net account



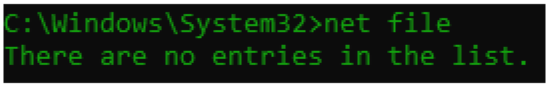
```
C:\Windows\System32>net account
The syntax of this command is:

NET
    [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
      STATISTICS | STOP | TIME | USE | USER | VIEW ]
```

sfc/scannow



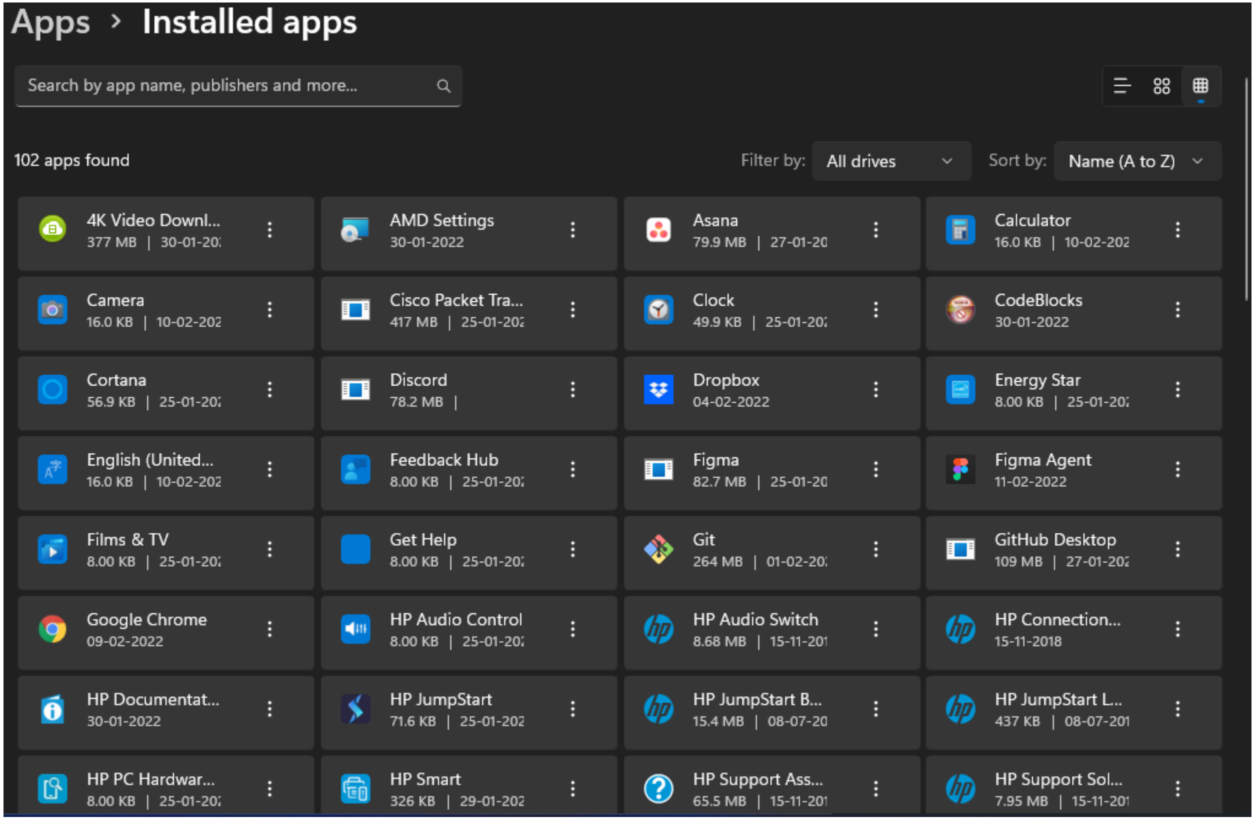
```
C:\Windows\System32>sfc/scannow

Beginning system scan.  This process will take some time.

Beginning verification phase of system scan.
Verification 100% complete.

Windows Resource Protection did not find any integrity violations.
```

net file



```
C:\Windows\System32>net file
There are no entries in the list.
```

Appwiz.cpl



Apps › Installed apps

102 apps found

Filter by: All drives

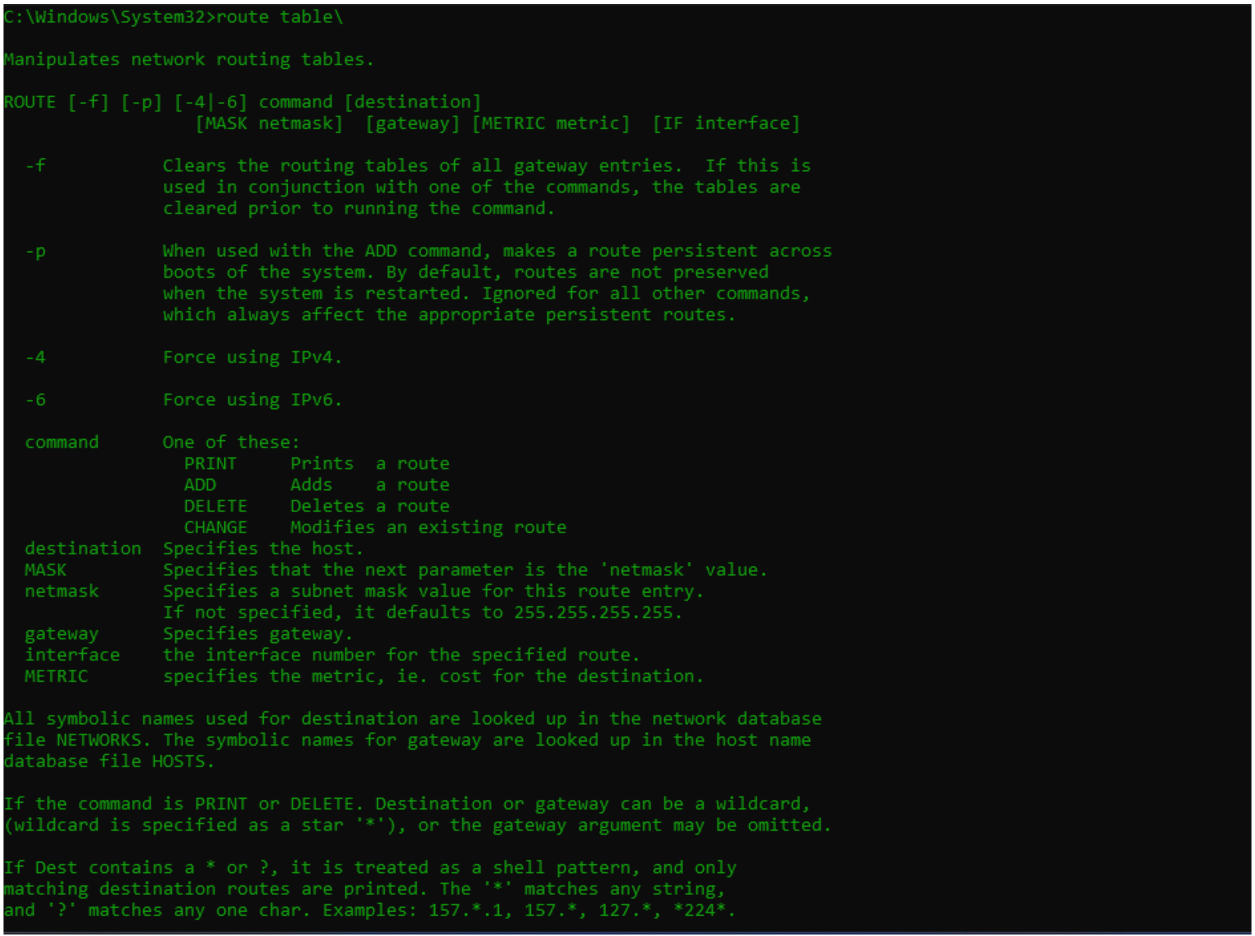
Sort by: Name (A to Z)

| | | | |
|---|---|---|---|
| 4K Video Downl...<br>377 MB \| 30-01-20 | AMD Settings<br>30-01-2022 | Asana<br>79.9 MB \| 27-01-20 | Calculator<br>16.0 KB \| 10-02-202 |
| Camera<br>16.0 KB \| 10-02-202 | Cisco Packet Tra...<br>417 MB \| 25-01-20 | Clock<br>49.9 KB \| 25-01-20 | CodeBlocks<br>30-01-2022 |
| Cortana<br>56.9 KB \| 25-01-20 | Discord<br>78.2 MB \| | Dropbox<br>04-02-2022 | Energy Star<br>8.00 KB \| 25-01-20 |
| English (United...<br>16.0 KB \| 10-02-202 | Feedback Hub<br>8.00 KB \| 25-01-20 | Figma<br>82.7 MB \| 25-01-20 | Figma Agent<br>11-02-2022 |
| Films & TV<br>8.00 KB \| 25-01-20 | Get Help<br>8.00 KB \| 25-01-20 | Git<br>264 MB \| 01-02-20 | GitHub Desktop<br>109 MB \| 27-01-20 |
| Google Chrome<br>09-02-2022 | HP Audio Control<br>8.00 KB \| 25-01-20 | HP Audio Switch<br>8.68 MB \| 15-11-201 | HP Connection...<br>15-11-2018 |
| HP Documentat...<br>30-01-2022 | HP JumpStart<br>71.6 KB \| 25-01-202 | HP JumpStart B...<br>15.4 MB \| 08-07-20 | HP JumpStart L...<br>437 KB \| 08-07-201 |
| HP PC Hardwar...<br>8.00 KB \| 25-01-20 | HP Smart<br>326 KB \| 29-01-202 | HP Support Ass...<br>65.5 MB \| 15-11-201 | HP Support Sol...<br>7.95 MB \| 15-11-201 |

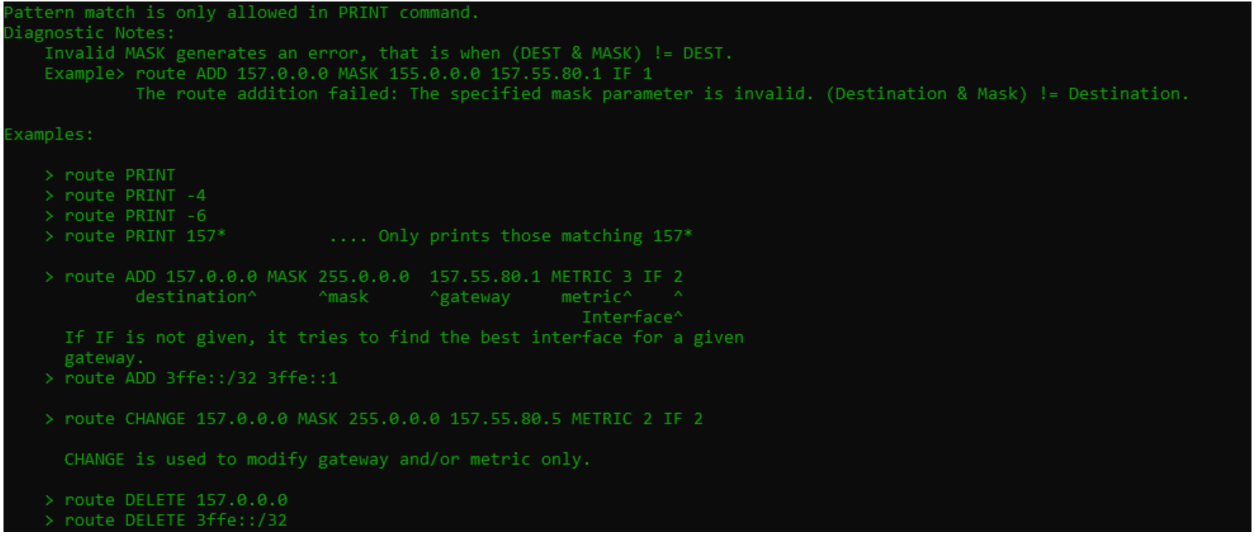
query

query termserver

## route table\

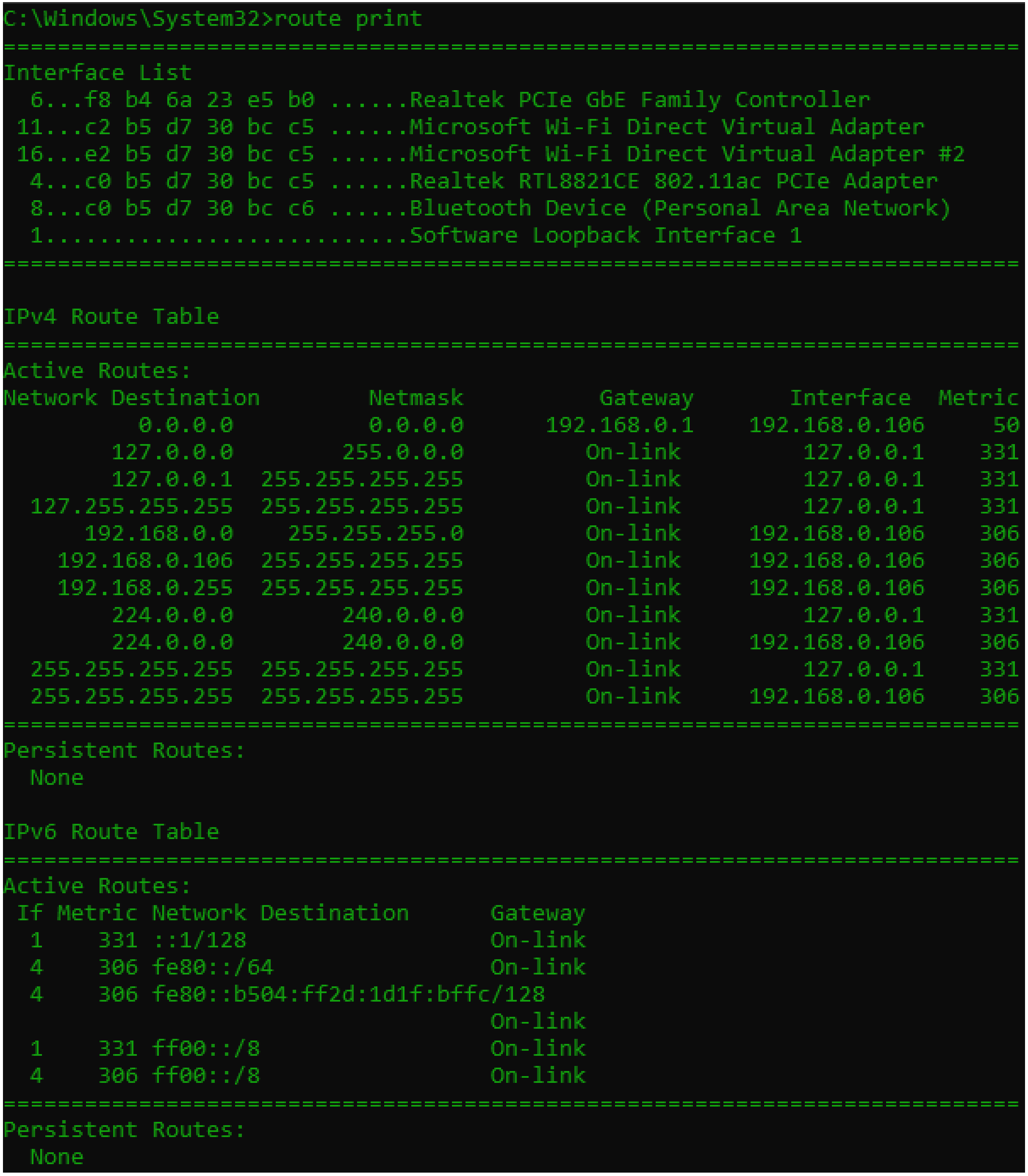


```
C:\Windows\System32>route table\

Manipulates network routing tables.

ROUTE [-f] [-p] [-4|-6] command [destination]
                  [MASK netmask]  [gateway] [METRIC metric]  [IF interface]

  -f           Clears the routing tables of all gateway entries.  If this is
               used in conjunction with one of the commands, the tables are
               cleared prior to running the command.

  -p           When used with the ADD command, makes a route persistent across
               boots of the system. By default, routes are not preserved
               when the system is restarted. Ignored for all other commands,
               which always affect the appropriate persistent routes.

  -4           Force using IPv4.

  -6           Force using IPv6.

  command      One of these:
                 PRINT     Prints  a route
                 ADD       Adds    a route
                 DELETE    Deletes a route
                 CHANGE    Modifies an existing route
  destination  Specifies the host.
  MASK         Specifies that the next parameter is the 'netmask' value.
  netmask      Specifies a subnet mask value for this route entry.
               If not specified, it defaults to 255.255.255.255.
  gateway      Specifies gateway.
  interface    the interface number for the specified route.
  METRIC       specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database
file NETWORKS. The symbolic names for gateway are looked up in the host name
database file HOSTS.

If the command is PRINT or DELETE. Destination or gateway can be a wildcard,
(wildcard is specified as a star '*'), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed. The '*' matches any string,
and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.
```



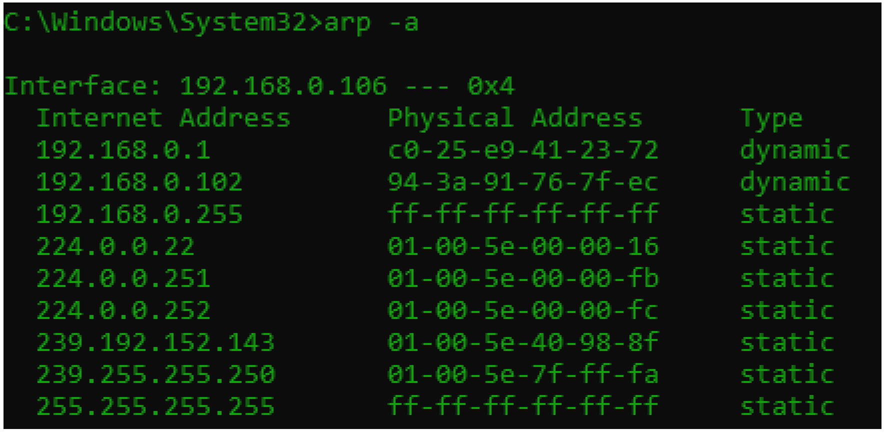
```
Pattern match is only allowed in PRINT command.
Diagnostic Notes:
    Invalid MASK generates an error, that is when (DEST & MASK) != DEST.
    Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
             The route addition failed: The specified mask parameter is invalid. (Destination & Mask) != Destination.

Examples:

    > route PRINT
    > route PRINT -4
    > route PRINT -6
    > route PRINT 157*          .... Only prints those matching 157*

    > route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
             destination^      ^mask      ^gateway     metric^    ^
                                                         Interface^
      If IF is not given, it tries to find the best interface for a given
      gateway.
    > route ADD 3ffe::/32 3ffe::1

    > route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2

      CHANGE is used to modify gateway and/or metric only.

    > route DELETE 157.0.0.0
    > route DELETE 3ffe::/32
```

route print



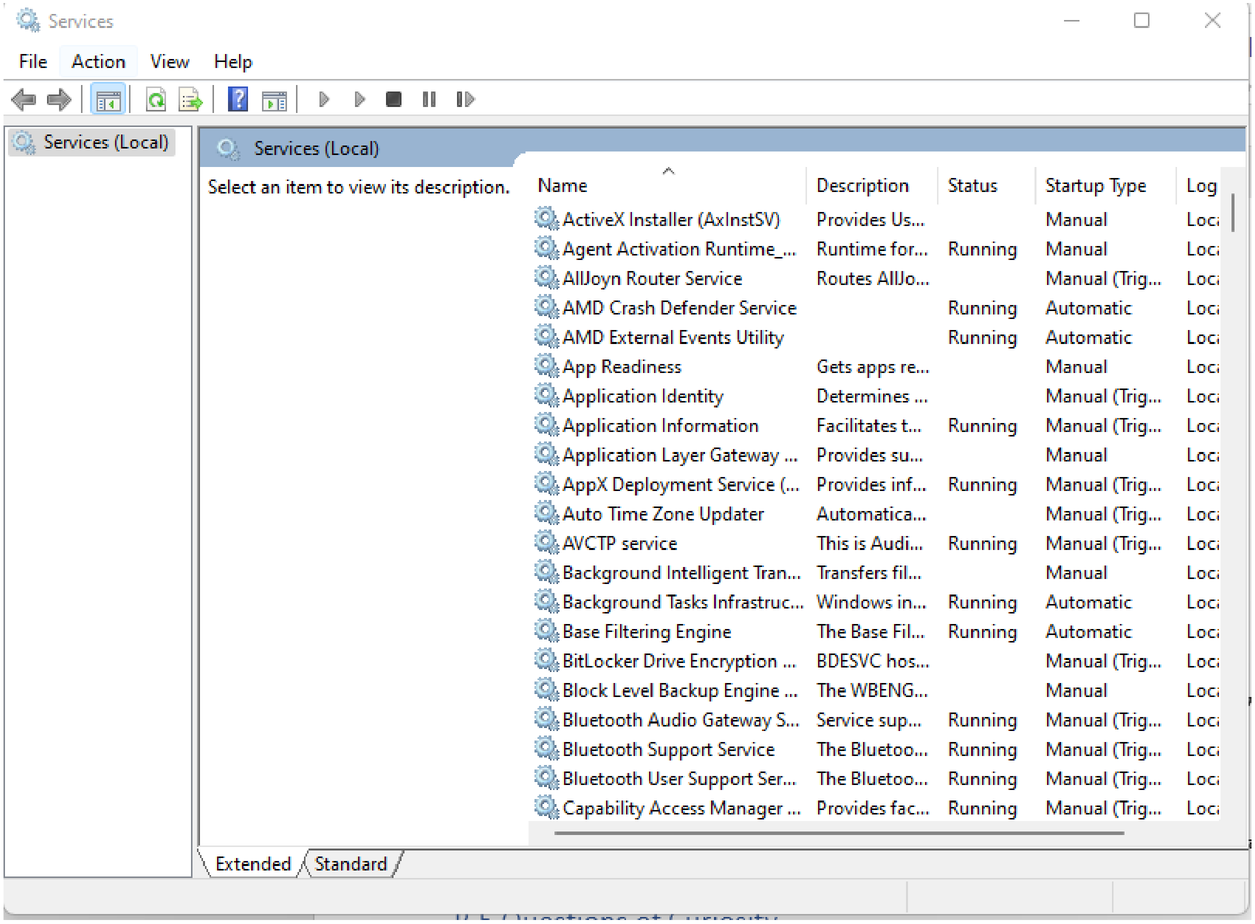
```
C:\Windows\System32>route print
===========================================================================
Interface List
  6...f8 b4 6a 23 e5 b0 ......Realtek PCIe GbE Family Controller
 11...c2 b5 d7 30 bc c5 ......Microsoft Wi-Fi Direct Virtual Adapter
 16...e2 b5 d7 30 bc c5 ......Microsoft Wi-Fi Direct Virtual Adapter #2
  4...c0 b5 d7 30 bc c5 ......Realtek RTL8821CE 802.11ac PCIe Adapter
  8...c0 b5 d7 30 bc c6 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.0.1    192.168.0.106     50
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.0.0    255.255.255.0         On-link     192.168.0.106    306
    192.168.0.106  255.255.255.255         On-link     192.168.0.106    306
    192.168.0.255  255.255.255.255         On-link     192.168.0.106    306
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link     192.168.0.106    306
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link     192.168.0.106    306
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
  4    306 fe80::/64                On-link
  4    306 fe80::b504:ff2d:1d1f:bffc/128
                                    On-link
  1    331 ff00::/8                 On-link
  4    306 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

arp –a



```
C:\Windows\System32>arp -a

Interface: 192.168.0.106 --- 0x4
  Internet Address      Physical Address      Type
  192.168.0.1           c0-25-e9-41-23-72     dynamic
  192.168.0.102         94-3a-91-76-7f-ec     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.192.152.143       01-00-5e-40-98-8f     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

services.msc (It will show all the services)



Select an item to view its description.

| Name | Description | Status | Startup Type | Log |
|---|---|---|---|---|
| ActiveX Installer (AxInstSV) | Provides Us... | | Manual | Loc |
| Agent Activation Runtime_... | Runtime for... | Running | Manual | Loc |
| AllJoyn Router Service | Routes AllJo... | | Manual (Trig... | Loc |
| AMD Crash Defender Service | | Running | Automatic | Loc |
| AMD External Events Utility | | Running | Automatic | Loc |
| App Readiness | Gets apps re... | | Manual | Loc |
| Application Identity | Determines ... | | Manual (Trig... | Loc |
| Application Information | Facilitates t... | Running | Manual (Trig... | Loc |
| Application Layer Gateway ... | Provides su... | | Manual | Loc |
| AppX Deployment Service (... | Provides inf... | Running | Manual (Trig... | Loc |
| Auto Time Zone Updater | Automatica... | | Manual (Trig... | Loc |
| AVCTP service | This is Audi... | Running | Manual (Trig... | Loc |
| Background Intelligent Tran... | Transfers fil... | | Manual | Loc |
| Background Tasks Infrastruc... | Windows in... | Running | Automatic | Loc |
| Base Filtering Engine | The Base Fil... | Running | Automatic | Loc |
| BitLocker Drive Encryption ... | BDESVC hos... | | Manual (Trig... | Loc |
| Block Level Backup Engine ... | The WBENG... | | Manual | Loc |
| Bluetooth Audio Gateway S... | Service sup... | Running | Manual (Trig... | Loc |
| Bluetooth Support Service | The Bluetoo... | Running | Manual (Trig... | Loc |
| Bluetooth User Support Ser... | The Bluetoo... | Running | Manual (Trig... | Loc |
| Capability Access Manager ... | Provides fac... | Running | Manual (Trig... | Loc |

# Output:

Checklist for Internal System Audit

*Is there any policy for minimum password characters?*

No

*Did any mechanism for minimum password verification.*

No

*Is there any two-step verification process for accessing passwords?*

Yes

*Did Periodic password changes are mandatory*

Yes

*Are there any options for least login attempts for user-entered passwords before blocking the account?*

Yes

*Are there any options for password hints?*

No

*Are there any options for multi-factor authentication (MFA)?*

Yes

*Is the Windows Software Updated?*

Yes

*Is there any integrity violation?*

No

*Are the active routes same as available routes?*

Yes

*Are there any open shared files on the network?*

No

*Are there any persistent routes on your server?*

Yes

*Did your system have disabled remote management in firewall?*

No

*Does your firewall have blocked inbound?*

Yes

*Has your system connected to any malicious WiFi that you don't know about?*

No

*Does your system show any malicious software in sfc/scannow?*

No

## B.3 Observations and learning:

***(Students are expected to comment on the output obtained with clear observations and learning for each task/ sub part assigned)***

**Hence, we were able to make the system audit internally**

## B.4 Conclusion:

***(Students must write the conclusion as per the attainment of individual outcome listed above and learning/observation noted in section B.3)***

Hence, were able to perform an Internal System Audit.

## B.5 Questions of Curiosity

***(To be answered by student based on the practical performed and learning/observations)***

# Q1: Tools used for system audits

### *SolarWinds Network Configuration*

Top pick for network security auditing. Configuration management tool with vulnerability scanning, reporting, and alerts.

### *Intruder*

A cloud-based vulnerability scanner with the monthly scans, on-demand scanning, and the services of a pen-testing team.

### *ManageEngine Vulnerability Manager Plus*

This package of system security checks sweeps your network and checks for security weaknesses. Runs on Windows and Windows Server.

### *N-able RMM*

Remote monitoring and management software that includes a risk intelligence module to protect and report on PII.

### *Atera*

A SaaS platform for managed service providers that includes remote monitoring and management systems, such as its auditor report generator.

### *Netwrix Auditor*

Network security auditing software with configuration monitoring, automated alerts, and a Rest API.

### *Nessus*

Free vulnerability assessment tool with over 450 configuration templates and customizable reports.

### *Nmap*

Open-source port scanner and network mapper available as a command-line interface or as a GUI (Zenmap).

### *OpenVAS*

Vulnerability assessment tool for Linux users with regular updates.

### *Acunetix*

A Web application security scanner that can detect over 50,000 network vulnerabilities when integrated with OpenVAS.

### *Kaseya VSA*

RMM software with IT asset discovery, custom dashboards, reports, and automation.

### *Spiceworks Inventory*

Network inventory tool that automatically discovers network devices.

### *Network Inventory Advisor*

Inventory scanning tool compatible with Windows, Mac OS, and Linux devices.

### *Metasploit*

Penetration testing tool that allows you to hack into exploits in your network.