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.

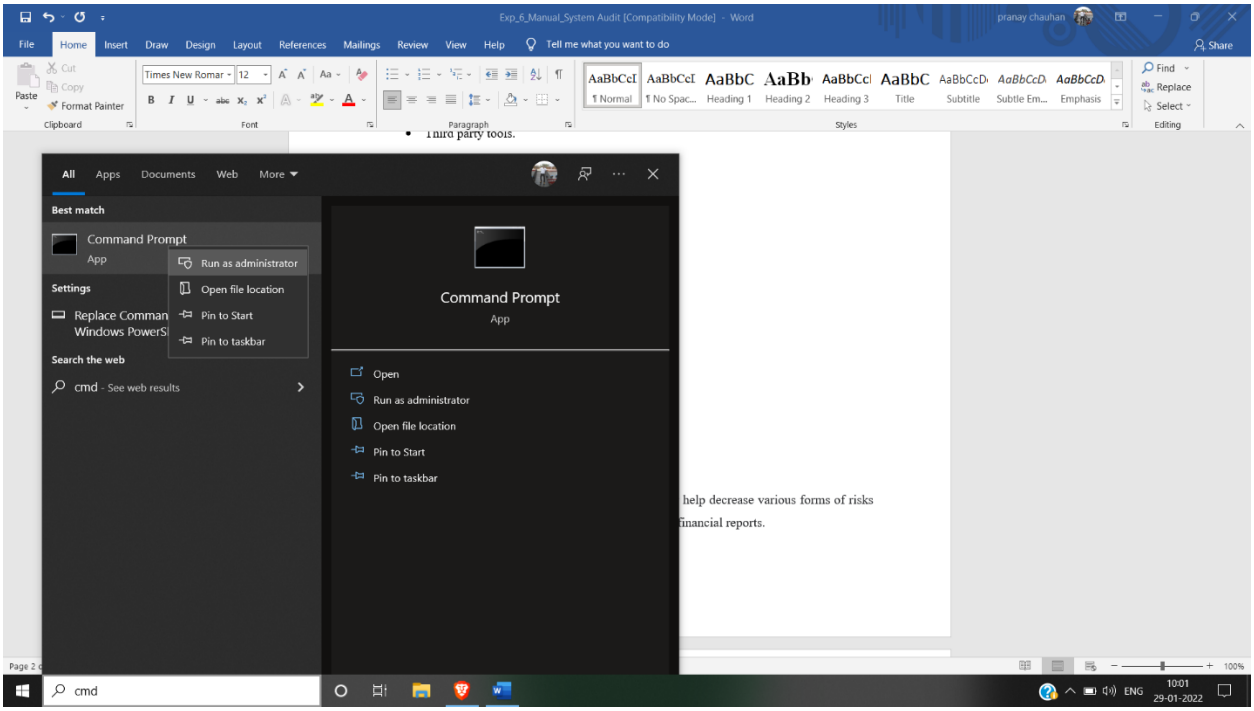
II. System Vulnerability is assessed.

III. Threats are identified.

IV. Internal Controls are analyzed.

V. Final Evaluation.

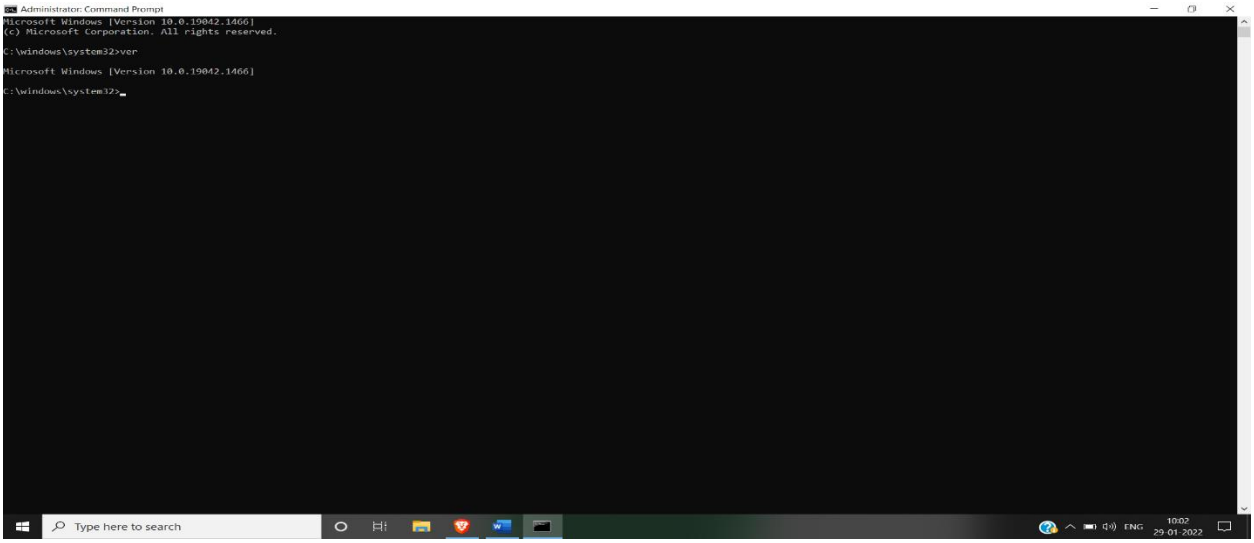
Step: 1 Run CMD as administrator



Step: 2

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

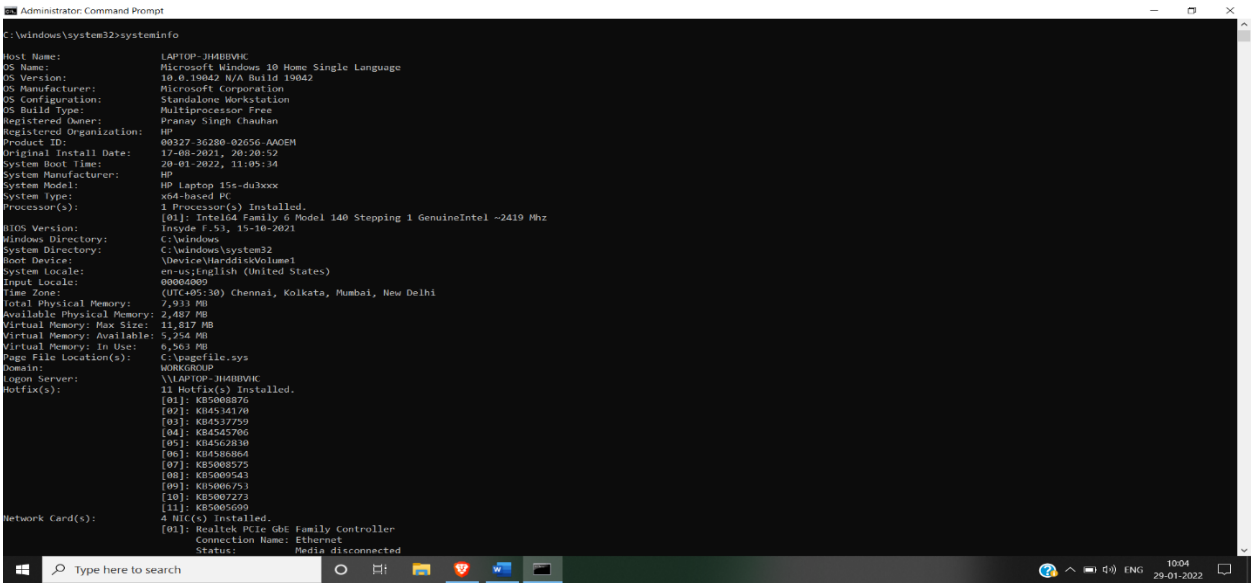
Command : **ver**



Step: 3: Check system information

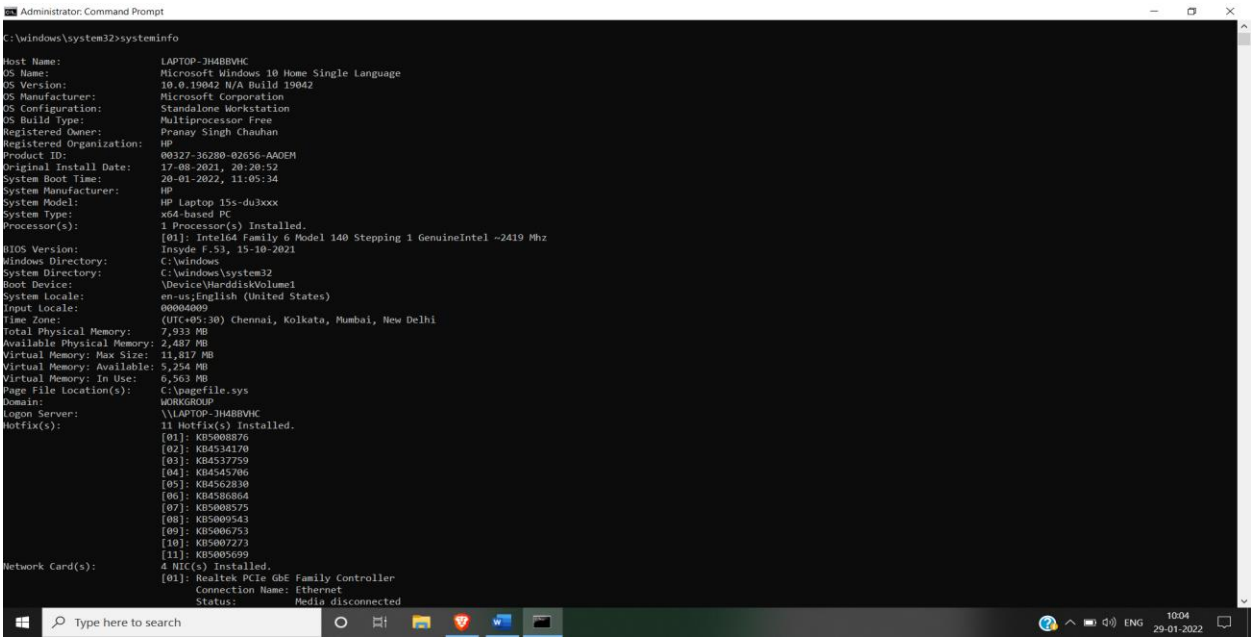
To check all the updates

Command: systeminfo



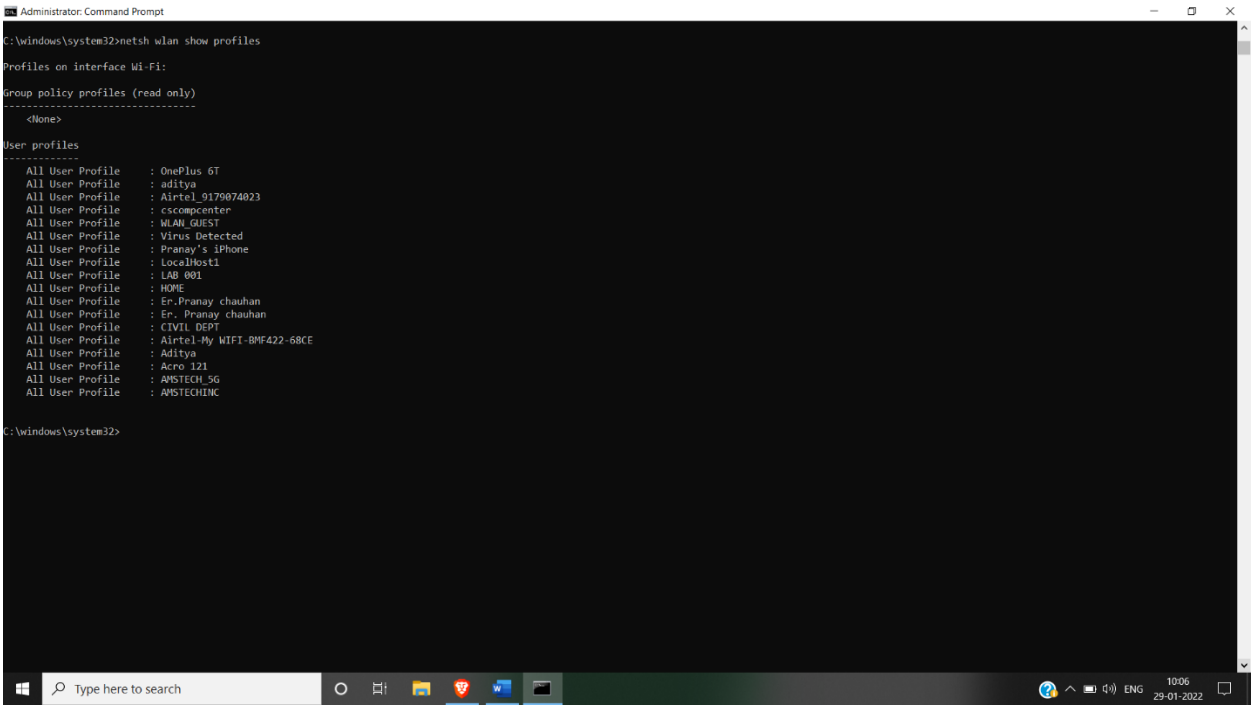
Step: 4: To check remotely open files

Command: openfiles



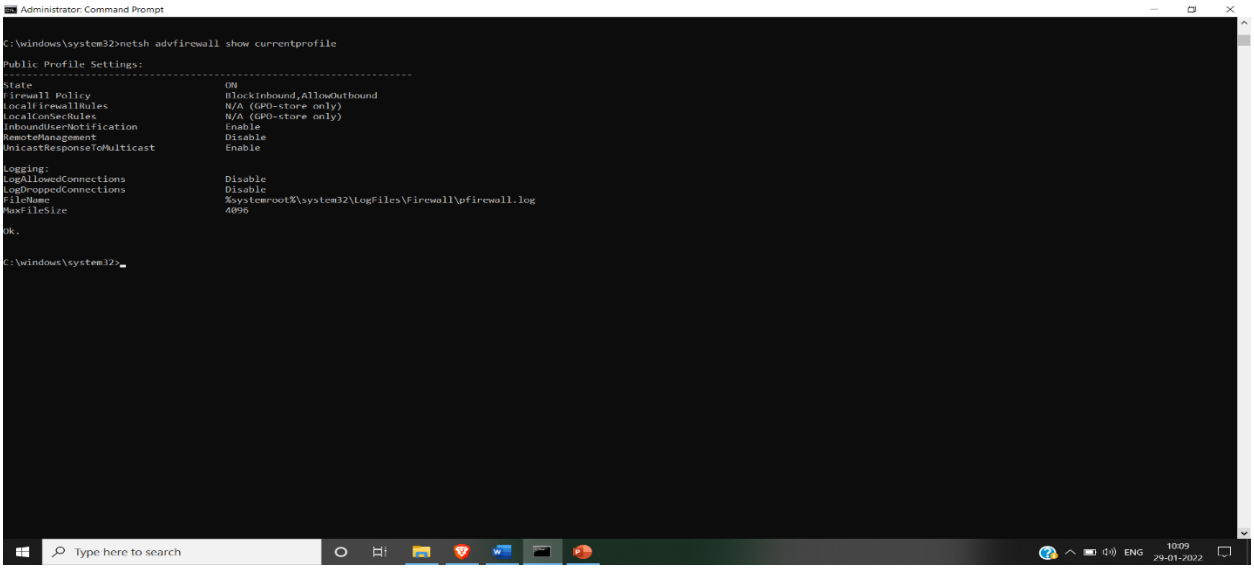
Step: 5: to Check all used wifi connections

Command: netsh wlan show profiles



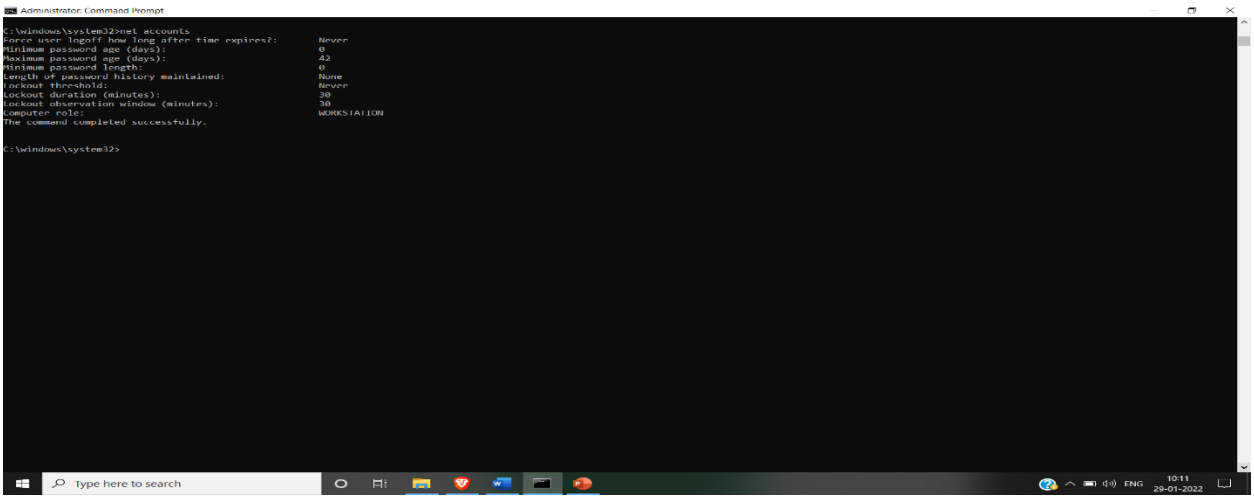
Step: 6 : To check firewall enabled services in desktop

Command : netsh advfirewall show currentprofile



Step: 7: To check network account state

Command: net account



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

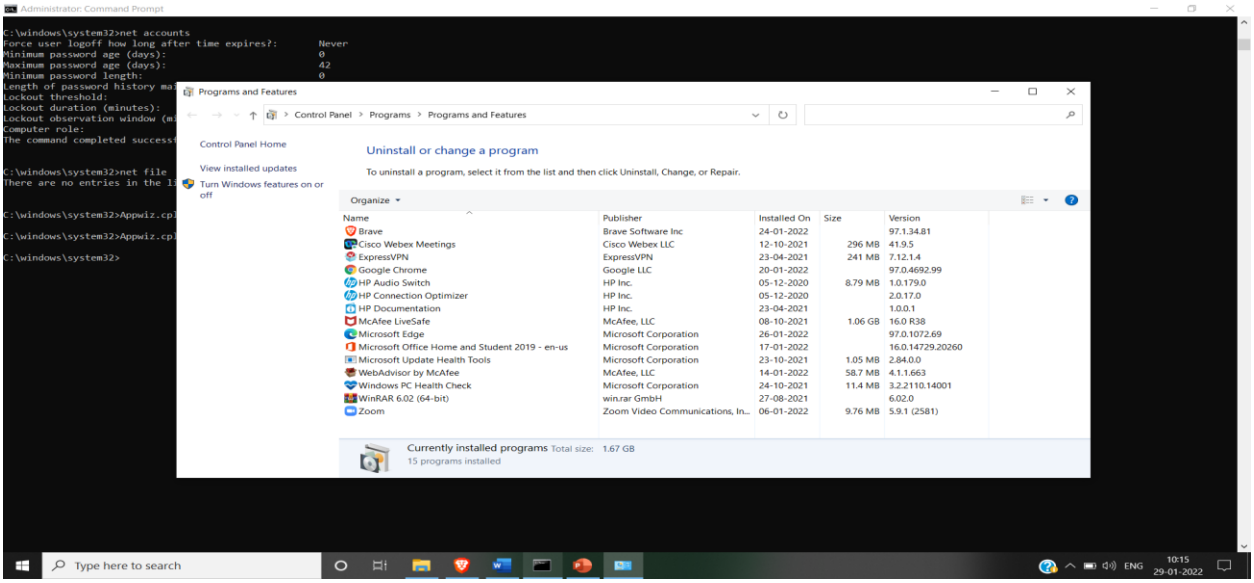
Command: sfc/scannow

Step: 9: To check network files

Command: net file

Step: 10: To check all installed softwares

Command: Appwiz.cpl



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. A022	Name: Kartik Padave
Class: B.Tech	Batch: 1
Date of Experiment:	Date of Submission:
Grade:	

B.1 Software Code written by student:

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

Instead of Java 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:

1. Perform the system audit commands

1. **Ver**

```
C:\WINDOWS\system32>ver

Microsoft Windows [Version 10.0.19044.1526]
```

2. **Systeminfo**

```
C:\WINDOWS\system32>systeminfo

Host Name:                 CRYPTOLEO
OS Name:                   Microsoft Windows 10 Home Single Language
OS Version:                10.0.19044 N/A Build 19044
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Leo
Registered Organization:   HP
Product ID:                00327-35846-39277-AAOEM
Original Install Date:     25-07-2020, 16:35:46
System Boot Time:          15-02-2022, 21:57:17
System Manufacturer:       HP
System Model:              HP Laptop 15-da1xxx
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.18, 15-03-2019
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:     8,078 MB
Available Physical Memory: 1,796 MB
Virtual Memory: Max Size:  13,198 MB
Virtual Memory: Available: 5,305 MB
Virtual Memory: In Use:    7,893 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\CRYPTOLEO
Hotfix(s):                 20 Hotfix(s) Installed.
                           [01]: KB5009467
                           [02]: KB4561600
                           [03]: KB4562830
                           [04]: KB4566785
                           [05]: KB4570334
                           [06]: KB4577266
                           [07]: KB4577586
                           [08]: KB4580325
                           [09]: KB4586864
                           [10]: KB4589212
                           [11]: KB4593175
                           [12]: KB4598481
                           [13]: KB5000736
                           [14]: KB5003791
                           [15]: KB5008575
                           [16]: KB5010342
                           [17]: KB5006753
                           [18]: KB5007273
```

```
                            [19]: KB5011352
                            [20]: KB5005699
Network Card(s):            3 NIC(s) Installed.
                            [01]: Realtek PCIe GbE Family Controller
                                  Connection Name: Ethernet
                                  Status:          Media disconnected
                            [02]: Realtek RTL8723DE 802.11b/g/n PCIe Adapter
                                  Connection Name: Wi-Fi
                                  DHCP Enabled:    Yes
                                  DHCP Server:     10.130.64.1
                                  IP address(es)
                                  [01]: 10.130.64.80
                            [03]: VirtualBox Host-Only Ethernet Adapter
                                  Connection Name: VirtualBox Host-Only Network
                                  DHCP Enabled:    No
                                  IP address(es)
                                  [01]: 192.168.56.1
                                  [02]: fe80::8048:6214:2b80:8155
Hyper-V Requirements:       VM Monitor Mode Extensions: Yes
                            Virtualization Enabled In Firmware: Yes
                            Second Level Address Translation: Yes
                            Data Execution Prevention Available: Yes
```

3. **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.
```

4. **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     : SVKM NMIMS
    All User Profile     : LeoStark
    All User Profile     : PRIYA
    All User Profile     : JioFi2_10CA1B
    All User Profile     : Redmi
    All User Profile     : UniversalFreight
    All User Profile     : Chetan @ Oppo
    All User Profile     : Varun-2.4ghz
    All User Profile     : Priya
    All User Profile     : Aqua Craze
    All User Profile     : AndroidAP
    All User Profile     : I am Batman
    All User Profile     : Simran's iPhone
    All User Profile     : NMIMS-WIFI
    All User Profile     : Interstellar
```

5. 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.
```

6. **net account**

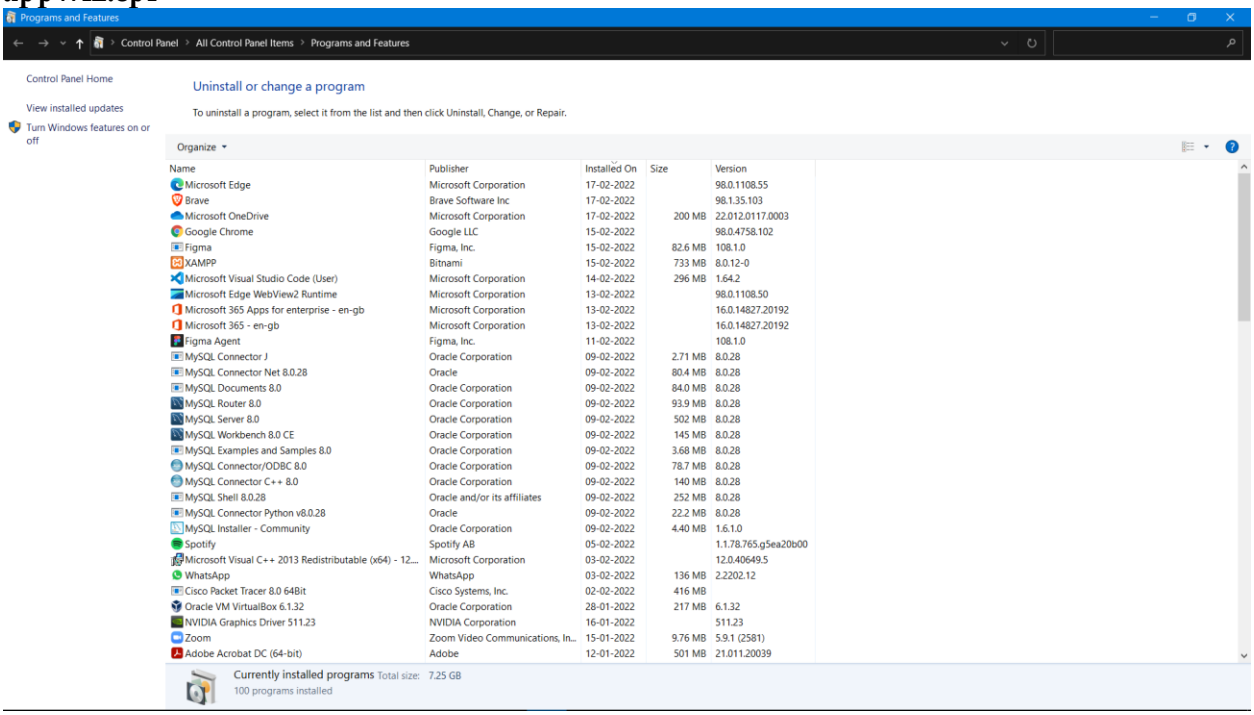
```
C:\WINDOWS\system32>net account
The syntax of this command is:

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

7. **net file**

```
C:\WINDOWS\system32>net file
There are no entries in the list.
```

8. **appwiz.cpl**



Name	Publisher	Installed On	Size	Version
Microsoft Edge	Microsoft Corporation	17-02-2022		98.0.1108.55
Brave	Brave Software Inc	17-02-2022		98.1.35.103
Microsoft OneDrive	Microsoft Corporation	17-02-2022	200 MB	22.012.0117.0003
Google Chrome	Google LLC	15-02-2022		98.0.4758.102
Figma	Figma, Inc.	15-02-2022	82.6 MB	108.1.0
XAMPP	Bitnami	15-02-2022	733 MB	8.0.12-0
Microsoft Visual Studio Code (User)	Microsoft Corporation	14-02-2022	296 MB	1.64.2
Microsoft Edge WebView2 Runtime	Microsoft Corporation	13-02-2022		98.0.1108.50
Microsoft 365 Apps for enterprise - en-gb	Microsoft Corporation	13-02-2022		16.0.14827.20192
Microsoft 365 - en-gb	Microsoft Corporation	13-02-2022		16.0.14827.20192
Figma Agent	Figma, Inc.	11-02-2022		108.1.0
MySQL Connector J	Oracle Corporation	09-02-2022	2.71 MB	8.0.28
MySQL Connector Net 8.0.28	Oracle	09-02-2022	80.4 MB	8.0.28
MySQL Documents 8.0	Oracle Corporation	09-02-2022	84.0 MB	8.0.28
MySQL Router 8.0	Oracle Corporation	09-02-2022	93.9 MB	8.0.28
MySQL Server 8.0	Oracle Corporation	09-02-2022	502 MB	8.0.28
MySQL Workbench 8.0 CE	Oracle Corporation	09-02-2022	145 MB	8.0.28
MySQL Examples and Samples 8.0	Oracle Corporation	09-02-2022	3.68 MB	8.0.28
MySQL Connector/ODBC 8.0	Oracle Corporation	09-02-2022	78.7 MB	8.0.28
MySQL Connector C++ 8.0	Oracle Corporation	09-02-2022	140 MB	8.0.28
MySQL Shell 8.0.28	Oracle and/or its affiliates	09-02-2022	252 MB	8.0.28
MySQL Connector Python v8.0.28	Oracle	09-02-2022	22.2 MB	8.0.28
MySQL Installer - Community	Oracle Corporation	09-02-2022	4.40 MB	1.6.1.0
Spotify	Spotify AB	05-02-2022		1.1.78.765.g5ea20b00
Microsoft Visual C++ 2013 Redistributable (x64) - 12...	Microsoft Corporation	03-02-2022		12.0.40649.5
WhatsApp	WhatsApp	03-02-2022	136 MB	2.2202.12
Cisco Packet Tracer 8.0 64Bit	Cisco Systems, Inc.	02-02-2022	416 MB	
Oracle VM VirtualBox 6.1.32	Oracle Corporation	28-01-2022	217 MB	6.1.32
NVIDIA Graphics Driver 511.23	NVIDIA Corporation	16-01-2022		511.23
Zoom	Zoom Video Communications, In...	15-01-2022	9.76 MB	5.9.1 (2581)
Adobe Acrobat DC (64-bit)	Adobe	12-01-2022	501 MB	21.011.20039

9. **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.
```

10. **route print/**

```
C:\WINDOWS\system32>route print/

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.
```

11. **arp -a**

```
C:\WINDOWS\system32>arp -a

Interface: 192.168.56.1 --- 0x2
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.9             01-00-5e-00-00-09     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
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 10.130.64.80 --- 0xa
  Internet Address      Physical Address      Type
  10.130.64.1           70-f3-5a-d8-b9-4c     dynamic
  10.130.95.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.9             01-00-5e-00-00-09     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
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

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)

After successful completion of this experiment, we know about the tactics and techniques of system audit, tools used for system audit.

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)

After successful completion of this experiment, we know about the tactics and techniques of system audit, tools used for 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

1. **SolarWinds Network Configuration**
   Top pick for network security auditing. Configuration management tool with vulnerability scanning, reporting, and alerts.
2. **Intruder**
   A cloud-based vulnerability scanner with the monthly scans, on-demand scanning, and the services of a pen-testing team.
3. **ManageEngine Vulnerability Manager Plus**
   This package of system security checks sweeps your network and checks for security weaknesses. Runs on Windows and Windows Server.
4. **N-able RMM**
   Remote monitoring and management software that includes a risk intelligence module to protect and report on PII.