

Windows

Incident Response

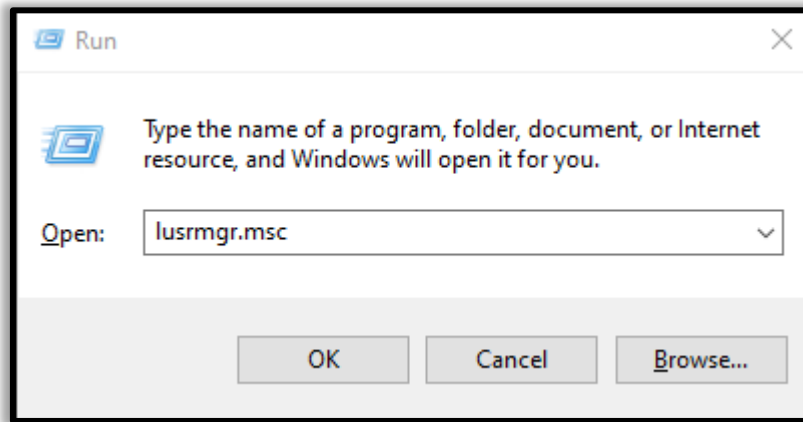
Users

In Incident response it is very necessary to investigate the user activity. It is used to find if there is any suspicious user account is present or any restricted permissions have been assigned to a user. By checking the user account one can be able to get answers to questions like which user is currently logged in and what kind of a user account one has.

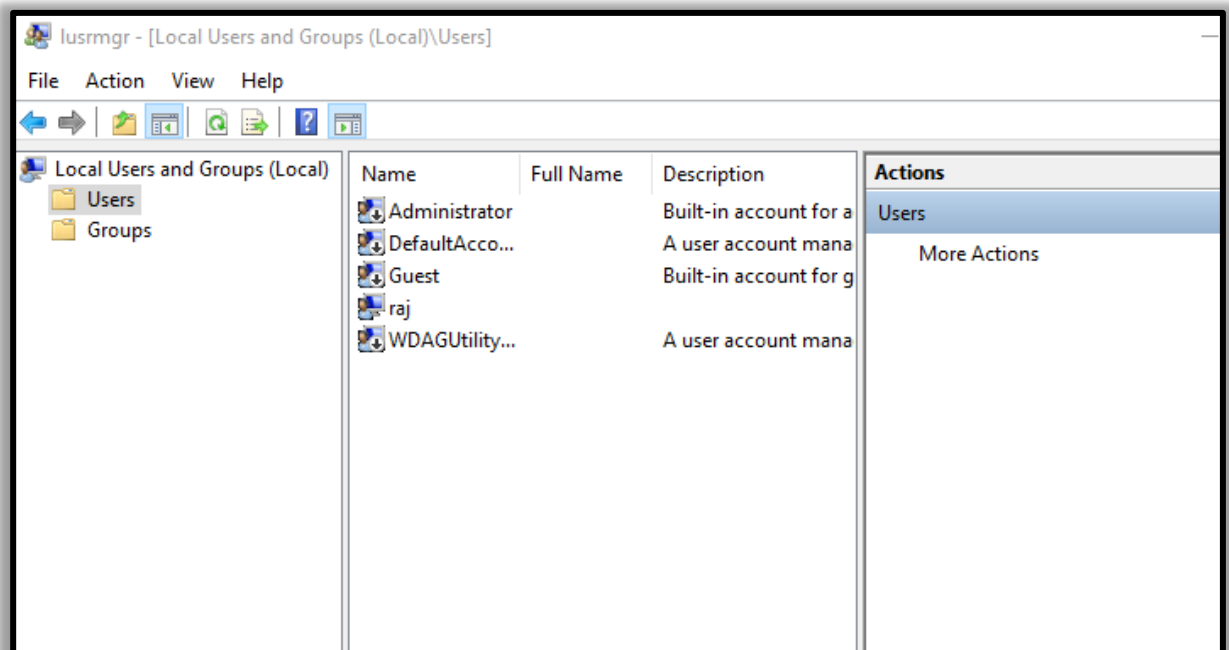
The ways one can view the user accounts are:

Local users

To view the local user accounts in GUI, press **'Windows+R'**, then type **'lusrmgr.msc'**.



Now click on **'okay'**, and here you will be able to see the user accounts and their descriptions.



net user

You can now open the command prompt and run it as an administrator. Then type the command '**net user**' and press enter. You can now see the user accounts for the system and the type of account it is.

net user

```
Microsoft Windows [Version 10.0.18362.1016]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\raj>net user

User accounts for \\DESKTOP-A0AP00M

-----
Administrator          DefaultAccount          Guest
raj                    WDAGUtilityAccount
The command completed successfully.

C:\Users\raj>
```

net localgroup

'**Net localgroup groupname**' command is used to manage local user groups on a system. By using this command, an administrator can add local or domain users to a group, delete users from a group, create new groups and delete existing groups.

Open Command prompt and run as an administrator then type '**net local group administrators**' and press enter.

net local group administrators

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

Members

-----
Administrator
raj
The command completed successfully.
```

Local user

To view the local user accounts in PowerShell, open PowerShell as an administrator, type '**Get-LocalUser**' and press enter. You will be able to see the local user accounts, with their names, if they are enabled and their description.

Get-LocalUser

```
PS C:\Users\raj> Get-LocalUser

Name                Enabled Description
----                -
Administrator      False  Built-in account for administering the computer/domain
DefaultAccount      False  A user account managed by the system.
Guest               False  Built-in account for guest access to the computer/domain
raj                 True   A user account managed and used by the system for Windows
WDAGUtilityAccount False  A user account managed and used by the system for Windows
```

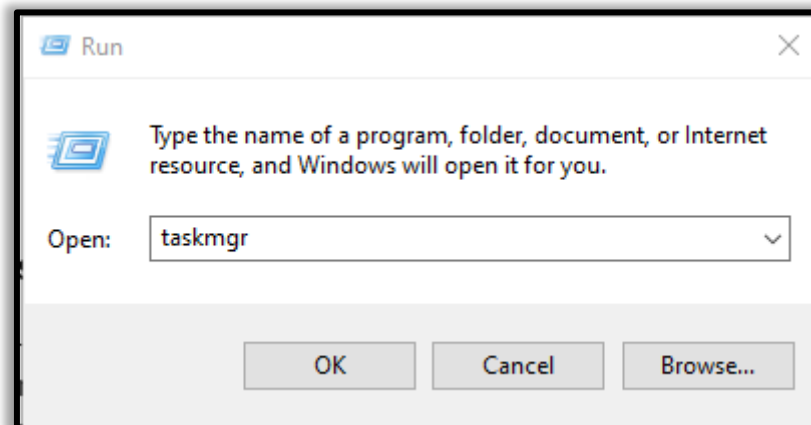
Processes

To get the list of all the processes running on the system, you can use '**tasklist**' command for this purpose. By making use of this command, you can get a list of the processes the memory space used, running time, image file name, services running in the process etc

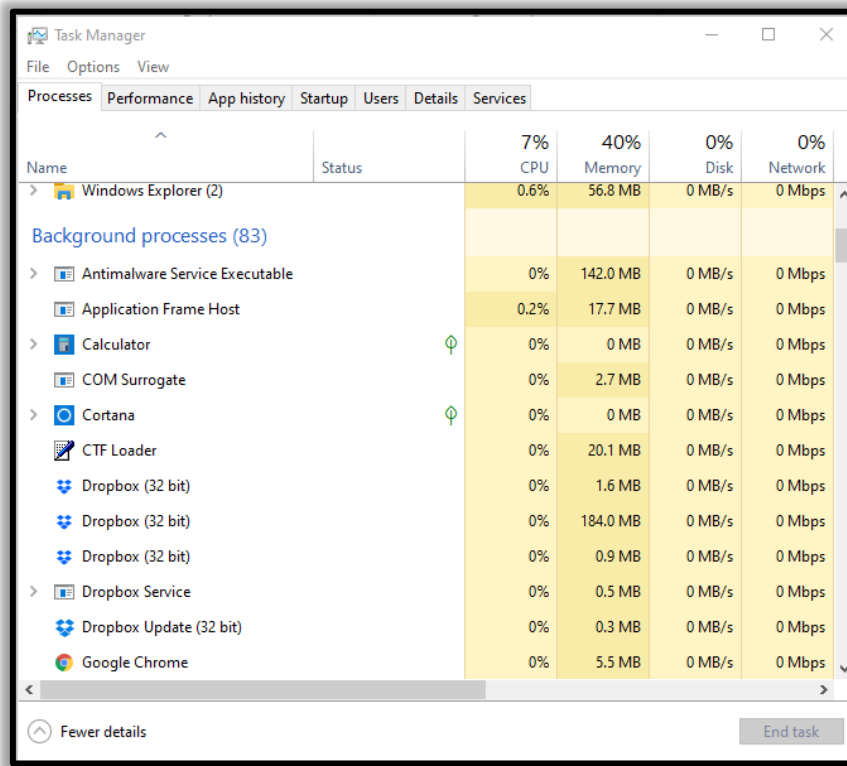
To view the processes, you can use the following methods;

Task Manager

To view the running processes in a GUI, press '**Windows+R**', then type '**taskmgr.exe**'.



Now click on '**OK**' and you will be able to see all the running processes in your system and will be able to check if there is any unnecessary process running.



tasklist

To view the processes in the command prompt, Open the command prompt as an administrator and type 'tasklist' and press enter. Here you will be able to see all the running processes with their Process ID (PID) and their session name and the amount of memory used.

tasklist

```
C:\Users\rnj>tasklist

Image Name                    PID Session Name        Session#    Mem Usage
=====
System Idle Process           0 Services             0             8 K
System                        4 Services             0          10,924 K
Registry                      120 Services             0          70,260 K
smss.exe                      476 Services             0           1,004 K
csrss.exe                     696 Services             0           5,092 K
wininit.exe                   784 Services             0           6,212 K
services.exe                  928 Services             0           9,424 K
lsass.exe                     936 Services             0          20,464 K
svchost.exe                   628 Services             0           3,268 K
svchost.exe                   632 Services             0          27,772 K
fontdrvhost.exe              776 Services             0           2,540 K
svchost.exe                   1072 Services            0          17,056 K
svchost.exe                   1124 Services             0           7,648 K
svchost.exe                   1340 Services             0           9,180 K
svchost.exe                   1380 Services             0           9,596 K
svchost.exe                   1388 Services             0           8,700 K
svchost.exe                   1400 Services             0           6,464 K
svchost.exe                   1396 Services             0           8,872 K
svchost.exe                   1548 Services             0           5,184 K
svchost.exe                   1556 Services             0           6,944 K
svchost.exe                   1724 Services             0          11,032 K
svchost.exe                   1772 Services             0          13,708 K
```

Powershell

To view the process list in PowerShell, run PowerShell as an administrator and type 'Get-Process' and press enter. It gets a list of all active processes running on the local computer.

```
get-process
```

```
PS C:\Users\raj> get-process
```

| Handles | NPM(K) | PM(K) | WS(K) | CPU(s) | Id | SI | ProcessName |
|---------|--------|--------|--------|--------|------|----|----------------------|
| 839 | 43 | 58120 | 53140 | 2.31 | 6932 | 3 | ApplicationFrameHost |
| 712 | 27 | 49920 | 41864 | 64.00 | 9812 | 0 | audiodg |
| 540 | 27 | 19396 | 9844 | 0.39 | 1472 | 3 | Calculator |
| 228 | 15 | 13956 | 25800 | 0.08 | 1968 | 3 | chrome |
| 897 | 77 | 831828 | 852736 | 633.58 | 2184 | 3 | chrome |
| 271 | 17 | 6752 | 16964 | 1.42 | 2992 | 3 | chrome |
| 532 | 36 | 31084 | 48220 | 41.77 | 4064 | 3 | chrome |
| 235 | 16 | 17460 | 37160 | 0.13 | 5720 | 3 | chrome |
| 322 | 21 | 70192 | 107132 | 8.31 | 5868 | 3 | chrome |
| 234 | 16 | 26116 | 38540 | 0.53 | 5968 | 3 | chrome |
| 321 | 10 | 2140 | 8896 | 0.09 | 6304 | 3 | chrome |

Windows system has an extremely powerful tool with the Windows Management Instrumentation Command (WMIC). Wmic is very useful when it comes to incident response. This tool is enough to notice some abnormal signs in the system. This command can be used in the Command-prompt as well as PowerShell when run as an administrator. The syntax is '**wmic process list full**'.

```
wmic process list full
```

```
PS C:\Windows\system32> wmic process list full
```

To get more details about the parent process IDs, Name of the process and the process ID, open PowerShell as an administrator and type '**wmic process get name,parentprocessid,processid**'. This would be the next step after you determine which process is performing a strange network activity. You will see the following details.

```
wmic process get name ,parentprocessid ,processid
```

```

PS C:\Windows\system32> wmic process get name,parentprocessid,processid
Name                                     ParentProcessId  ProcessId
-----
System Idle Process                     0                0
System                                   0                4
Registry                                 4                120
smss.exe                                 4                476
csrss.exe                                676              696
wininit.exe                              676              784
services.exe                             784              928
lsass.exe                                 784              936
svchost.exe                              928              628
svchost.exe                              928              632
fontdrvhost.exe                          784              776
svchost.exe                              928              1072
svchost.exe                              928              1124
svchost.exe                              928              1340
svchost.exe                              928              1380
svchost.exe                              928              1388
svchost.exe                              928              1400
svchost.exe                              928              1396
svchost.exe                              928              1548
svchost.exe                              928              1556
svchost.exe                              928              1724
svchost.exe                              928              1772
svchost.exe                              928              1780

```

To get the path of the Wmic process, open PowerShell and type **'wmic process where 'ProcessID=PID' get CommandLine'** and press enter.

```
wmic process where 'ProcessID=PID' get CommandLine
```

```

PS C:\Windows\system32> wmic process where "ProcessID=4420" get CommandLine
CommandLine
"C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe"

PS C:\Windows\system32>

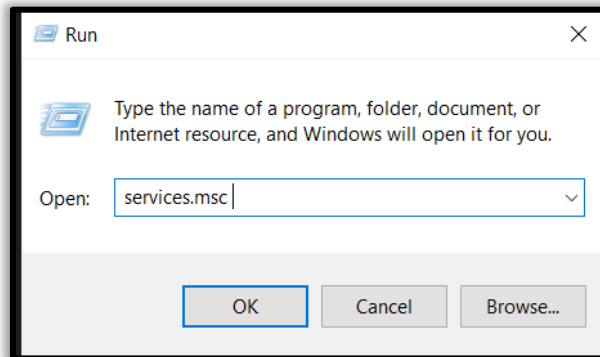
```

Services

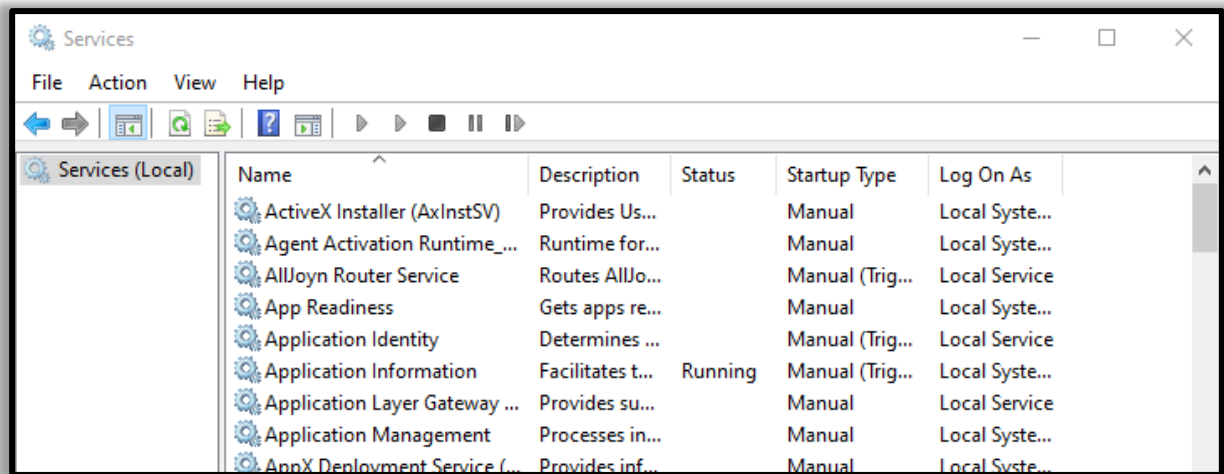
To identify if there is any abnormal service running in your system or some service is not functioning properly, you can view your services.

GUI

To view all the services in GUI, press '**Windows+R**' and type '**services.msc**'.



Now click on '**OK**' to see the list of processes.



net start

To start and view the list of services that are currently running in your system, open the command prompt as an administrator, type '**net start**' and press enter.

```
net start
```



```
C:\Users\raj>net start
These Windows services are started:
```

```
Application Information
AVCTP service
Background Tasks Infrastructure Service
Base Filtering Engine
Bluetooth Audio Gateway Service
Bluetooth Support Service
Capability Access Manager Service
Clipboard User Service_4f10ff4
```

sc query

To view whether a service is running and to get its more details like its service name, display name, etc.

[sc query | more](#)

```
C:\Users\raj>sc query | more

SERVICE_NAME: Appinfo
DISPLAY_NAME: Application Information
        TYPE               : 30  WIN32
        STATE                : 4  RUNNING
                        (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE      : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT          : 0x0
        WAIT_HINT           : 0x0

SERVICE_NAME: AudioEndpointBuilder
DISPLAY_NAME: Windows Audio Endpoint Builder
        TYPE               : 30  WIN32
        STATE                : 4  RUNNING
                        (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE      : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT          : 0x0
        WAIT_HINT           : 0x0

SERVICE_NAME: Audiosrv
DISPLAY_NAME: Windows Audio
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 4  RUNNING
                        (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE      : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT          : 0x0
        WAIT_HINT           : 0x0
```

Task Scheduler

tasklist

If you want a list of running processes with their associated services in the command prompt, run command prompt as an administrator, then type **'tasklist /svc'** and press enter.

```
tasklist /svc
```

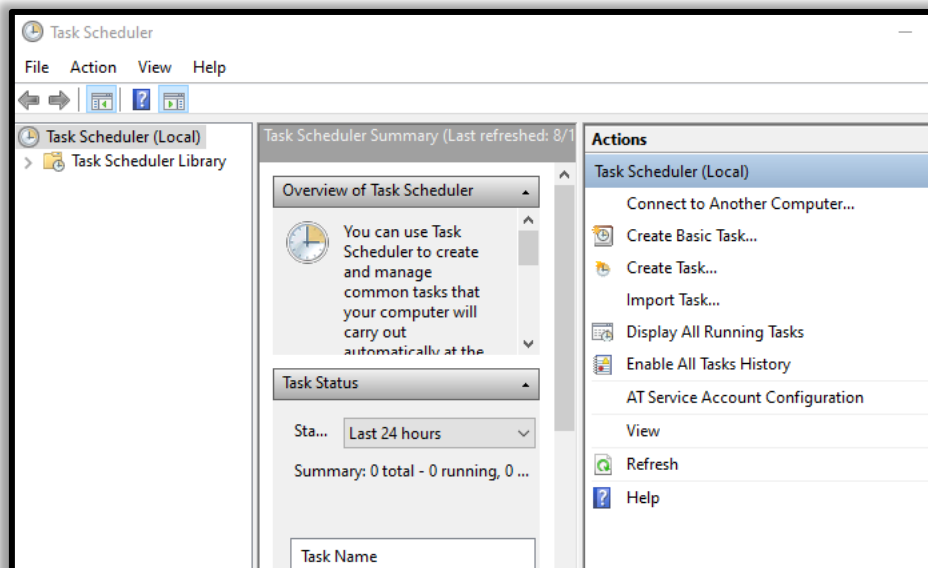
```
C:\Users\raj>tasklist /svc

Image Name                PID Services
-----
System Idle Process       0 N/A
System                    4 N/A
Registry                  120 N/A
smss.exe                  476 N/A
csrss.exe                 696 N/A
wininit.exe              784 N/A
services.exe             928 N/A
lsass.exe                 936 EFS, KeyIso, SamSs, VaultSvc
svchost.exe               628 PlugPlay
svchost.exe               632 BrokerInfrastructure, DcomLaunch, Power,
                        CustomEventBroker
```

GUI

Task Scheduler is a component in the Windows which provides the ability to schedule the launch of programs or any scripts at a pre-defined time or after specified time intervals. You can view these scheduled tasks which are of high privileges and look suspicious. To view the task scheduler in GUI, then go the path and press enter.

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools



Schtasks

To view the schedule tasks in the command prompt, run command prompt as an administrator, type 'schtasks' and press enter.

schtasks

```
C:\Users\raj>schtasks

Folder: \
TaskName                               Next Run Time           Status
-----
JavaUpdateSched                        N/A                     Running
update-S-1-5-21-1097824736-1555393654-24 8/17/2020 8:25:00 PM    Ready
User_Feed_Synchronization-{CE537D28-0D95 8/17/2020 8:50:34 PM    Ready

Folder: \Microsoft
TaskName                               Next Run Time           Status
-----
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Office
TaskName                               Next Run Time           Status
-----
Office 15 Subscription Heartbeat        8/18/2020 2:26:03 AM    Ready
OfficeTelemetryAgentFallBack           N/A                     Ready
OfficeTelemetryAgentLogOn              N/A                     Ready

Folder: \Microsoft\OneCore
TaskName                               Next Run Time           Status
-----
INFO: There are no scheduled tasks presently available at your access level.
```

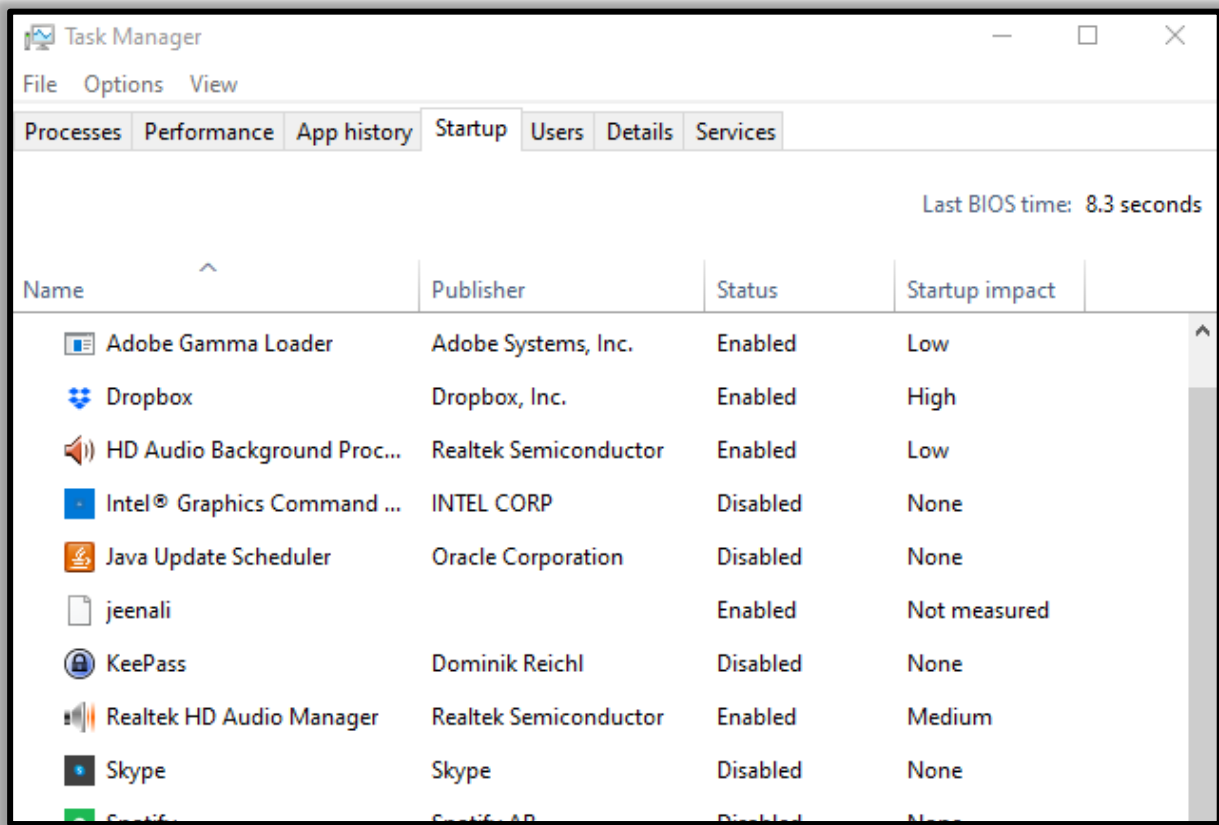
Startup

The startup folder in Windows, automatically runs applications when you log on. So, an incident handler, you should observe the applications that auto start.

GUI

To view the applications in Startup menu in GUI, open the task manager and click on the 'Startup' menu. By doing this, you can see which applications are enabled and disabled on startup. On opening the following path, it will give you the same option

```
dir /s /b "C:\Users\raj\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup"
```



Powershell

To view, the startup applications in the PowerShell run the PowerShell as an administrator, type 'wmic startup get caption,command' and press enter.

```
wmic startup get caption,command
```

```
PS C:\Windows\system32> wmic startup get caption,command
Caption          Command
OneDriveSetup   C:\Windows\SysWOW64\OneDriveSetup.exe /thfirstsetup
OneDriveSetup   C:\Windows\SysWOW64\OneDriveSetup.exe /thfirstsetup
jeenali          jeenali.txt
uTorrent         "C:\Users\raj\AppData\Roaming\uTorrent\uTorrent.exe" /MINIMIZED
Adobe Gamma Loader C:\PROGRA~2\COMMON~1\Adobe\CALIBR~1\ADOBEG~1.EXE
SecurityHealth  %windir%\system32\SecurityHealthSystray.exe
RtHdVcpl        "C:\Program Files\Realtek\Audio\HDA\RtkNGUI64.exe" /s
RtHdVbg_PushButton "C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe" /IM
WavesSvc        "C:\Windows\System32\DriverStore\FileRepository\oem49.inf_amd64_5ff3

PS C:\Windows\system32>
```

To get a detailed list of the AutoStart applications in **PowerShell**, you can run it as an administrator and type 'Get-CimInstance Win32_StartupCommand | Select-Object Name, command, Location, User | Format-List' and press enter.

Get-CimInstance Win32_StartupCommand | Select-Object Name, command, Location, User | Format-List'

```
PS C:\Windows\system32> Get-CimInstance Win32_StartupCommand | Select-Object Name, command, Location, User | Format-List

Name       : OneDriveSetup
command    : C:\Windows\SysWOW64\OneDriveSetup.exe /thfirstsetup
Location   : HKU\S-1-5-19\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
User       : NT AUTHORITY\LOCAL SERVICE

Name       : OneDriveSetup
command    : C:\Windows\SysWOW64\OneDriveSetup.exe /thfirstsetup
Location   : HKU\S-1-5-20\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
User       : NT AUTHORITY\NETWORK SERVICE

Name       : jeenali
command    : jeenali.txt
Location   : Startup
User       : DESKTOP-A0AP00M\raj

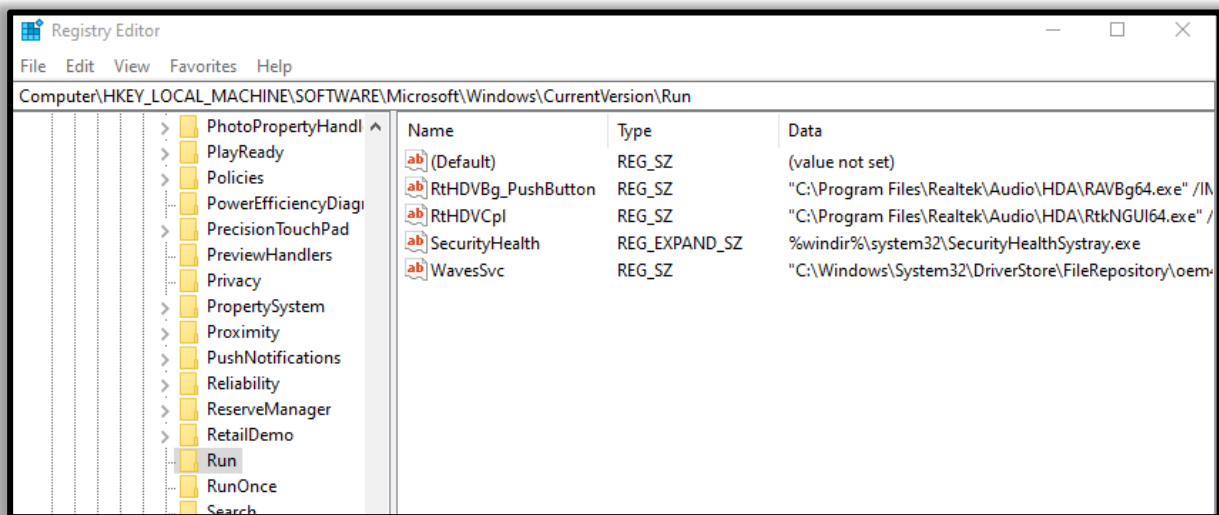
Name       : uTorrent
command    : "C:\Users\raj\AppData\Roaming\uTorrent\uTorrent.exe" /MINIMIZED
Location   : HKU\S-1-5-21-1097824736-1555393654-2427635684-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
User       : DESKTOP-A0AP00M\raj
```

Registry

Sometimes if there is a presence of unsophisticated malware it can be found by taking a look at the Windows Registry's run key.

GUI

To view the GUI of the registry key, you can open REGEDIT reach the run key manually.



PowerShell

You can also view the registry of the Local Machine of the Run key in the PowerShell, by running it as an administrator and then type

'reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' and press enter.

```
reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

```
PS C:\Windows\system32> reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
SecurityHealth    REG_EXPAND_SZ    %windir%\system32\SecurityHealthSystray.exe
RtHDVCp1         REG_SZ           "C:\Program Files\Realtek\Audio\HDA\RtkNGUI64.exe" /s
RtHDVBg_PushButton REG_SZ           "C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe" /IM
WavesSvc         REG_SZ           "C:\Windows\System32\DriverStore\FileRepository\oem49.inf_amd64_5ff30...
```

You can also view the registry of the Current User of the Run key in the PowerShell, by running it as an administrator and then type

'reg query HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' and press enter.

```
reg query HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

```
PS C:\Windows\system32> reg query HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
uTorrent         REG_SZ           "C:\Users\raj\AppData\Roaming\uTorrent\uTorrent.exe" /MINIMIZED

PS C:\Windows\system32>
```

Active TCP and UDP Port

As an Incident Responder you should carefully pay attention to the active TCP and UDP ports of your system.

netstat

The network statistics of a system can be using a tool. The criteria tested are incoming and outgoing connections, routing tables, port listening, and usage statistics. Open the command prompt, type 'netstat -ano' and press enter.

netstat -ano

```
C:\Users\raj>netstat -ano

Active Connections

Proto Local Address          Foreign Address        State                   PID
TCP   0.0.0.0:135             0.0.0.0:0              LISTENING               1072
TCP   0.0.0.0:443            0.0.0.0:0              LISTENING               5700
TCP   0.0.0.0:445            0.0.0.0:0              LISTENING                4
TCP   0.0.0.0:808            0.0.0.0:0              LISTENING               3836
TCP   0.0.0.0:903            0.0.0.0:0              LISTENING               3828
TCP   0.0.0.0:913            0.0.0.0:0              LISTENING               3828
TCP   0.0.0.0:1688           0.0.0.0:0              LISTENING               3820
TCP   0.0.0.0:5040           0.0.0.0:0              LISTENING               6216
TCP   0.0.0.0:7680           0.0.0.0:0              LISTENING               2792
TCP   0.0.0.0:9001           0.0.0.0:0              LISTENING                4
TCP   0.0.0.0:17500          0.0.0.0:0              LISTENING               5580
TCP   0.0.0.0:49664          0.0.0.0:0              LISTENING               936
TCP   0.0.0.0:49665          0.0.0.0:0              LISTENING               784
TCP   0.0.0.0:49666          0.0.0.0:0              LISTENING               1892
```

Powershell

Well, this can also be checked in the PowerShell with a different command. Run PowerShell and type 'Get-NetTCPConnection -LocalAddress 192.168.0.110 | Sort-Object LocalPort' and press enter. You will get detailed information about the IP and the local ports.

```
Get-NetTCPConnection -LocalAddress 192.168.0.110 | Sort-Object LocalPort
```

```
PS C:\Windows\system32> Get-NetTCPConnection -LocalAddress 192.168.0.110 | Sort-Object LocalPort

LocalAddress          LocalPort RemoteAddress          RemotePort State
-----
192.168.0.110         139       0.0.0.0                 0          Listen
192.168.0.110         57631     23.54.90.8              443        CloseWait
192.168.0.110         57632     23.54.90.8              443        CloseWait
192.168.0.110         57633     23.54.90.8              443        CloseWait
192.168.0.110         57634     23.54.90.8              443        CloseWait
192.168.0.110         57635     23.54.90.8              443        CloseWait
192.168.0.110         57636     23.215.197.169          80         CloseWait
192.168.0.110         57637     23.215.197.169          80         CloseWait
192.168.0.110         57638     23.215.197.169          80         CloseWait
192.168.0.110         57639     23.215.197.169          80         CloseWait
192.168.0.110         57640     23.215.197.169          80         CloseWait
192.168.0.110         57641     23.215.197.169          80         CloseWait
192.168.0.110         57642     23.60.172.136           443        CloseWait
192.168.0.110         57643     23.60.172.136           443        CloseWait
192.168.0.110         57646     23.54.90.8              443        CloseWait
192.168.0.110         57917     104.244.42.134          443        CloseWait
```

File Sharing

As an incident responder you should make sure that every file share is accountable and reasonable and there is no unnecessary file sharing.

net view

In order to check up on the file sharing options in command prompt, type 'net view \\<localhost>' and press enter.

```
net view \\127.0.0.1
```

```
C:\Users\raj>net view \\127.0.0.1
Shared resources at \\127.0.0.1

Share name  Type  Used as  Comment
-----
jeenali     Disk
Users       Disk
The command completed successfully.
```

SMBShare

To see the file sharing in PowerShell, you can type 'Get-SMBShare' and press enter.

```
Get-SMBShare
```

```
PS C:\Windows\system32> Get-SMBShare

Name      ScopeName Path      Description
-----
ADMIN$    *         C:\Win$   Remote Admin
C$        *         C:\       Default share
D$        *         D:\       Default share
IPC$      *         Remote IPC
jeenali   *         D:\jeenali
Users     *         C:\Users
```


Files

To view the files which could be malicious or end with a particular extension, you can use 'forfiles' command. Forfiles is a command line utility software. It was shipped with Microsoft Windows Vista. During that time, management of multiples files through the command line was difficult as most of the commands at that time we made to work on single files

Forfiles

To view the .exe files with their path to locate them in the command prompt, type 'forfiles /D -10 /S /M *.exe /C "cmd /c echo @path"' and press enter.

```
forfiles /D -10 /S /M *.exe /C "cmd /c echo @path"
```

```
C:\Users\raj>forfiles /D -10 /S /M *.exe /C "cmd /c echo @path"
"C:\Users\raj\AppData\Local\JxBrowser\browsercore-64.0.3282.24.unknown\browsercore32.exe"
"C:\Users\raj\AppData\Local\Microsoft\WindowsApps\GameBarElevatedFT_Alias.exe"
"C:\Users\raj\AppData\Local\Microsoft\WindowsApps\MicrosoftEdge.exe"
"C:\Users\raj\AppData\Local\Microsoft\WindowsApps\python.exe"
"C:\Users\raj\AppData\Local\Microsoft\WindowsApps\python3.exe"
"C:\Users\raj\AppData\Local\Microsoft\WindowsApps\Microsoft.DesktopAppInstaller_8wekyb3d8bbwe\python.exe"
"C:\Users\raj\AppData\Local\Microsoft\WindowsApps\Microsoft.DesktopAppInstaller_8wekyb3d8bbwe\python3.exe"
"C:\Users\raj\AppData\Local\Microsoft\WindowsApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\MicrosoftEdge.exe"
"C:\Users\raj\AppData\Local\Microsoft\WindowsApps\Microsoft.XboxGamingOverlay_8wekyb3d8bbwe\GameBarElevated
"C:\Users\raj\AppData\Local\VMware\vmware-download-2B3C\cdstmp_ws-windows_15.5.6_16341506\VMware-workstatio
"C:\Users\raj\AppData\Roaming\utorrent\helper\helper.exe"
"C:\Users\raj\AppData\Roaming\utorrent\updates\3.5.5_45724.exe"
"C:\Users\raj\AppData\Roaming\utorrent\updates\3.5.5_45724\utorrentie.exe"
"C:\Users\raj\Downloads\AnyDesk.exe"
"C:\Users\raj\Downloads\ARM_Setup_2020.2.1.exe"
```

To View files without its path and more details of the particular file extension and its modification date, type 'forfiles /D -10 /S /M *.exe /C "cmd /c echo @ext @fname @fdate"' and press enter.

```
forfiles /D -10 /S /M *.exe /C "cmd /c echo @ext @fname @fdate"
```

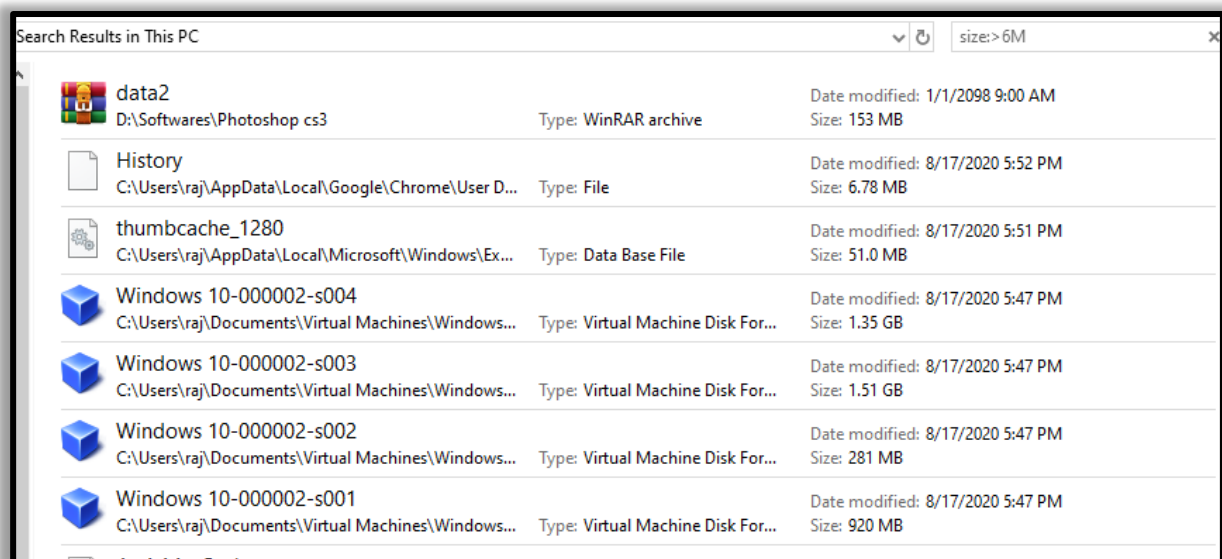
```
C:\Users\raj>forfiles /D -10 /S /M *.exe /C "cmd /c echo @ext @fname @fdate"
"exe" "browsercore32" 8/6/2018
"exe" "GameBarElevatedFT_Alias" 6/30/2020
"exe" "MicrosoftEdge" 7/2/2020
"exe" "python" 6/29/2020
"exe" "python3" 6/29/2020
"exe" "python" 6/29/2020
"exe" "python3" 6/29/2020
"exe" "MicrosoftEdge" 7/2/2020
"exe" "GameBarElevatedFT_Alias" 6/30/2020
"exe" "VMware-workstation-15.5.6-16341506" 6/29/2020
"exe" "helper" 8/7/2020
"exe" "3.5.5_45724" 7/27/2020
```

To check for files modified in the last 10 days type 'forfiles /p c: /S /D -10'.

```
forfiles /p c: /S /D -10
```

```
C:\>forfiles /p c: /S /D -10
"$Recycle.Bin"
"Android"
"Documents and Settings"
"MSOCache"
"PerfLogs"
"Project.log"
"Recovery"
"Users"
"S-1-5-18"
"S-1-5-21-1097824736-1555393654-2427635684-1000"
ERROR: Access is denied for "C:\$Recycle.Bin\S-1-5-18\".
ERROR: Access is denied for "C:\$Recycle.Bin\S-1-5-21-1097824736-1
"$I2IEYQS"
"desktop.ini"
".android"
"adb.exe"
"AdbWinApi.dll"
"AdbWinUsbApi.dll"
"fastboot.exe"
"adb_usb.ini"
ERROR: Access is denied for "C:\MSOCache\".
ERROR: Access is denied for "C:\PerfLogs\".
"Common Files"
"desktop.ini"
```

To check for file size below 6MB, you can use the file explorer's search box and enter "size:>6M"



Firewall Settings

The incident responder should pay attention to the firewall configurations and settings and should maintain it regularly.

To view the firewall configurations in the command prompt, type 'netsh firewall show config' and press enter to view the inbound and outbound traffic.

```
netsh firewall show config
```

```
C:\>netsh firewall show config

Domain profile configuration:
-----
Operational mode           = Enable
Exception mode             = Enable
Multicast/broadcast response mode = Enable
Notification mode         = Enable

Allowed programs configuration for Domain profile:
Mode   Traffic direction   Name / Program
-----
Enable Inbound          µTorrent (TCP-In) / C:\Users\raj\AppData\Roaming\µTo

Port configuration for Domain profile:
Port   Protocol  Mode   Traffic direction   Name
-----

Standard profile configuration (current):
-----
Operational mode           = Enable
Exception mode             = Enable
Multicast/broadcast response mode = Enable
Notification mode         = Enable

Service configuration for Standard profile:
Mode   Customized  Name
-----
Enable No         Network Discovery

Allowed programs configuration for Standard profile:
Mode   Traffic direction   Name / Program
-----
Enable Inbound          µTorrent (TCP-In) / C:\Users\raj\AppData\Roaming\µTo
Enable Inbound          Firefox (C:\Program Files\Mozilla Firefox) / C:\Prog

Port configuration for Standard profile:
Port   Protocol  Mode   Traffic direction   Name
-----

Log configuration:
-----
File location   = C:\Windows\system32\LogFiles\Firewall\pfirewall.log
Max file size   = 4096 KB
Dropped packets = Disable
Connections    = Disable
```

To view the firewall settings of the current profile in the command prompt, type 'netsh advfirewall show currentprofile' and press enter.

```
netsh advfirewall show currentprofile
```

```
C:\>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.
```

Sessions with other system

To check the session details that are created with other systems, you can type 'net use' in command prompt and press enter.

```
net use
```

```
Microsoft Windows [Version 10.0.18362.1016]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\raj>net use
New connections will be remembered.

Status          Local          Remote          Network
-----
OK              \\192.168.0.106\IPC$  Microsoft Windows Network
The command completed successfully.

C:\Users\raj>
```

Open Sessions

You can type 'net session' in the command prompt and press enter to see any open sessions of your system. It gives you the details about the duration of the session.

`net session`

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>net session

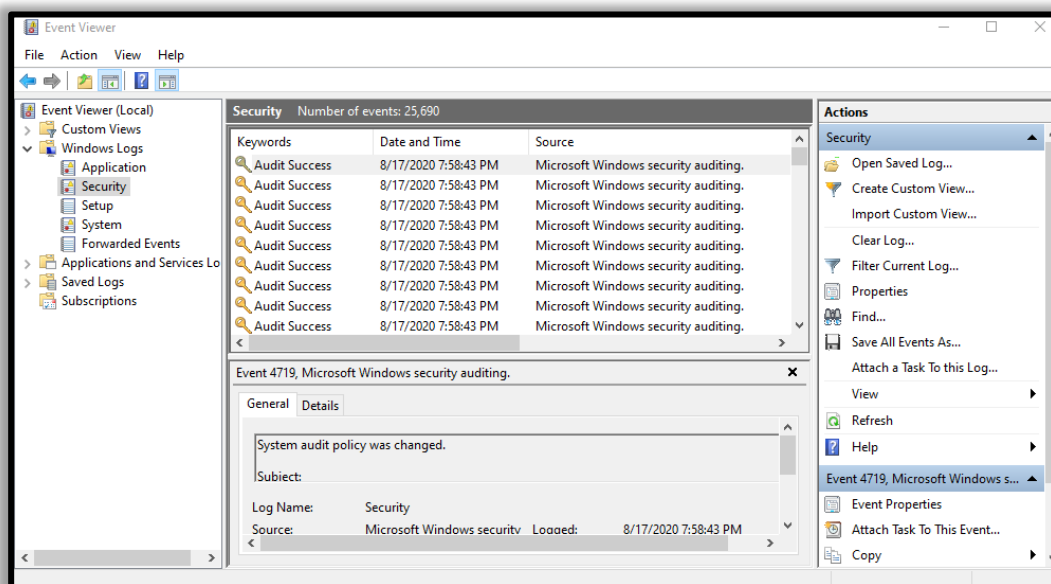
Computer                User name                Client Type              Opens Idle time
-----
\\192.168.0.110         administrator            Microsoft Windows        0 00:02:31
The command completed successfully.

C:\Users\Administrator>
```

Log Entries

To view the log entries in GUI you can open the event viewer and see the logs. Press 'Windows+R' and type 'eventvwr.msc' and press 'OK'.

Event Viewer



Cmd

To export certain logs of a particular event in command prompt type 'wevtutil qe security' and press enter.

```
wevtutil qe security
```

```
C:\Windows\system32>wevtutil qe security
```

PowerShell

To get the event log list in the PowerShell, type 'Get-EventLog -list' and type the particular event in the supply value and you will get event details of that particular event.

```
Get-Eventlog -List
```

```
PS C:\Users\raj> Get-EventLog -List
```

| Max(K) | Retain | OverflowAction | Entries | Log |
|--------|--------|-------------------|---------|------------------------|
| 20,480 | 0 | OverwriteAsNeeded | 12,676 | Application |
| 20,480 | 0 | OverwriteAsNeeded | 0 | HardwareEvents |
| 512 | 7 | OverwriteOlder | 0 | Internet Explorer |
| 20,480 | 0 | OverwriteAsNeeded | 0 | Key Management Service |
| 128 | 0 | OverwriteAsNeeded | 128 | 0Alerts |
| 512 | 7 | OverwriteOlder | 2 | OneApp_IGCC |
| | | | | Security |
| 20,480 | 0 | OverwriteAsNeeded | 7,887 | System |
| 15,360 | 0 | OverwriteAsNeeded | 422 | Windows PowerShell |

```
PS C:\Users\raj> Get-EventLog
```

```
cmdlet Get-EventLog at command pipeline position 1  
Supply values for the following parameters:  
LogName: 0Alerts
```

| Index | Time | EntryType | Source | InstanceID | Message |
|-------|--------------|-------------|----------------------|------------|-------------------|
| 128 | Aug 16 12:55 | Information | Microsoft Office ... | 300 | Microsoft Word... |
| 127 | Aug 16 02:22 | Information | Microsoft Office ... | 300 | Microsoft Word... |

Conclusion

Hence, one can make use of these commands as an incident responder and keep their systems away from threat.

References

- <https://www.hackingarticles.in/incident-response-linux-cheatsheet/>
- <https://www.hackingarticles.in/incident-response-windows-cheatsheet/>