

# Incident Response: Windows Cheatsheet

August 18, 2020 By Raj Chandel

For some people who use their computer systems, their systems might seem normal to them, but they might never realise that there could be something really phishy or even that fact that their systems could have been compromised. Making use of Incident Response a large number of attacks at the primary level could be detected. The investigation can be carried out to obtain any digital evidence.

This article mainly focuses on Incident response for Windows systems. So, let's begin with this cheat sheet to get you going.

## Table of Contents

- **What is Incident Response**
- **User Accounts**
- **Processes**
- **Services**
- **Task Scheduler**
- **Startup**
- **Registry Entries**
- **Active TCP & UDP ports**
- **File Shares**
- **Files**
- **Firewall Settings**
- **Sessions with other Systems**
- **Open Sessions**
- **Log Entries**

## What is Incident Response?

Incident response can be defined as a course of action that is taken whenever a computer or network security incident occurs.

The security events that could have occurred:

- Unauthorized use of system privileges and sensitive data
- Any cause of System crashes or flooding of packets
- Presence of malware or any malicious program

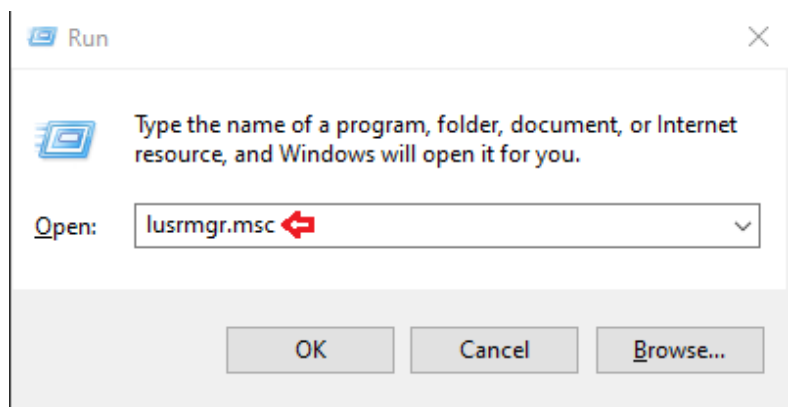
## User Accounts

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 the questions like which user is currently logged in and what kind of a user account one has.

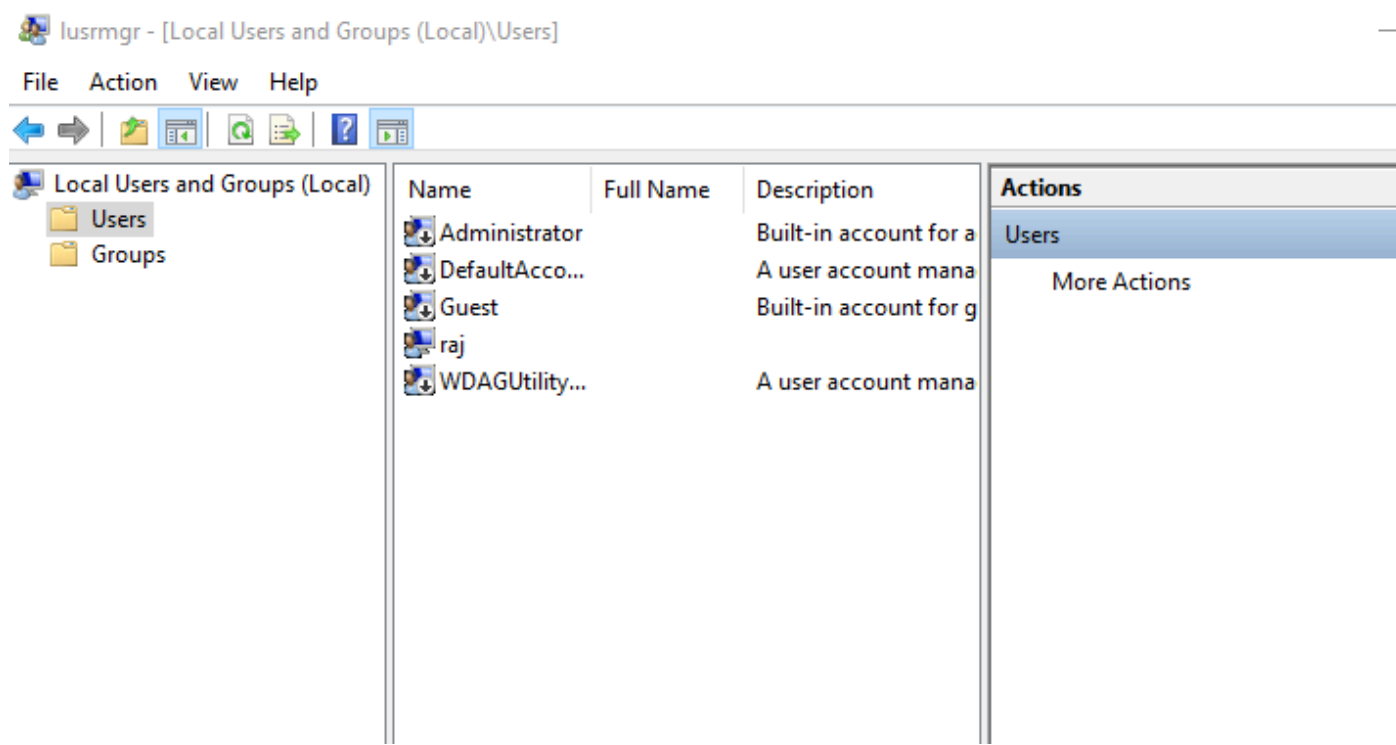
The ways one can view the user accounts are:

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.



To now see the **user accounts** for the system and the type of account it is. Run command prompt as administrator and type command

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 group name** is used in order 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 localgroup 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.
```

To see the local user accounts, with their names, if they are enabled and their description. Run PowerShell as an administrator, type

Get-LocalUser

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

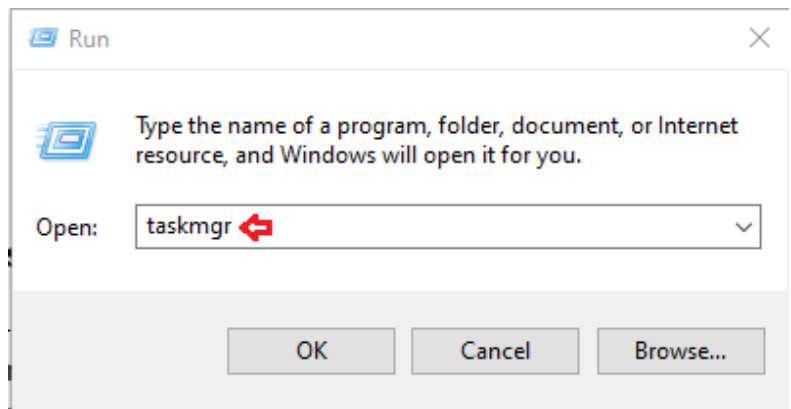
Name	Enabled	Description
Administrator	False	Built-in account for administering the computer/domain
DefaultAccount	False	A user account managed by the system.
Guest	False	Built-in account for guest access to the computer/domain
raj	True	
WDAGUtilityAccount	False	A user account managed and used by the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

## Processes

In order 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 +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; 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.

Task Manager					
File Options View					
Processes Performance App history Startup Users Details Services					
Name	Status	7% CPU	40% Memory	0% Disk	0% Network
> Windows Explorer (2)		0.6%	56.8 MB	0 MB/s	0 Mbps
Background processes (83)					
> Antimalware Service Executable		0%	142.0 MB	0 MB/s	0 Mbps
Application Frame Host		0.2%	17.7 MB	0 MB/s	0 Mbps
> Calculator	🔒	0%	0 MB	0 MB/s	0 Mbps
COM Surrogate		0%	2.7 MB	0 MB/s	0 Mbps
> Cortana	🔒	0%	0 MB	0 MB/s	0 Mbps
CTF Loader		0%	20.1 MB	0 MB/s	0 Mbps
Dropbox (32 bit)		0%	1.6 MB	0 MB/s	0 Mbps
Dropbox (32 bit)		0%	184.0 MB	0 MB/s	0 Mbps
Dropbox (32 bit)		0%	0.9 MB	0 MB/s	0 Mbps
> Dropbox Service		0%	0.5 MB	0 MB/s	0 Mbps
Dropbox Update (32 bit)		0%	0.3 MB	0 MB/s	0 Mbps
Google Chrome		0%	5.5 MB	0 MB/s	0 Mbps

To see all the running processes with their Process ID (PID) and their session name and the amount of memory used. Run command prompt as an administrator and type

```
tasklist
```

```
C:\Users\raj>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
svchost.exe	1780	Services	0	7,504 K
svchost.exe	1820	Services	0	9,284 K
igfxCUIService.exe	1880	Services	0	7,460 K

To gets a list of all active processes running on the local computer run PowerShell as an administrator and type

```
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
246	19	104956	131400	12.03	6728	3	chrome
248	18	40428	65888	10.44	7104	3	chrome
298	20	50384	92968	8.30	7644	3	chrome
246	16	20460	45244	0.56	7828	3	chrome
242	16	17628	39252	0.50	8180	3	chrome
279	19	48420	81316	4.91	10296	3	chrome
237	16	22572	46940	0.56	10372	3	chrome
1621	40	399856	402324	230.92	11328	3	chrome
282	20	58704	103372	7.98	11768	3	chrome
426	27	72380	113796	16.20	13212	3	chrome
220	14	11648	21232	0.05	13328	3	chrome
280	18	52356	90120	1.30	13792	3	chrome
321	20	56616	92840	1.78	14028	3	chrome
2040	338	130924	221032	187.95	14232	3	chrome
289	20	71872	111492	5.30	14252	3	chrome
75	5	3364	4012	0.00	14332	3	cmd
217	12	13244	21124	1.39	9996	3	conhost
276	14	4360	15800	0.06	11460	3	conhost
676	23	1972	5080		696	0	csrss
707	35	2600	6100		6704	3	csrss
554	19	22776	39832	6.14	10780	3	ctfmon
149	10	2552	4824		3688	0	DbxSvc
245	23	5900	14188	0.22	11424	3	dllhost
5745	154	213700	264232	49.70	5580	3	Dropbox
316	15	2928	11336	0.03	10416	3	Dropbox
197	13	2064	8860	0.05	13244	3	Dropbox
221	14	2164	1072		6100	0	DropboxUpdate
1542	60	139684	168640		13664	3	dwm

Windows system have 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 running as an administrator. The syntax is **wmic process list full**

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

[www.hackingarticles.in](http://www.hackingarticles.in)

After you determine which process is performing a strange network activity. 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
```

```
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
```



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

PS C:\Windows\system32>
```

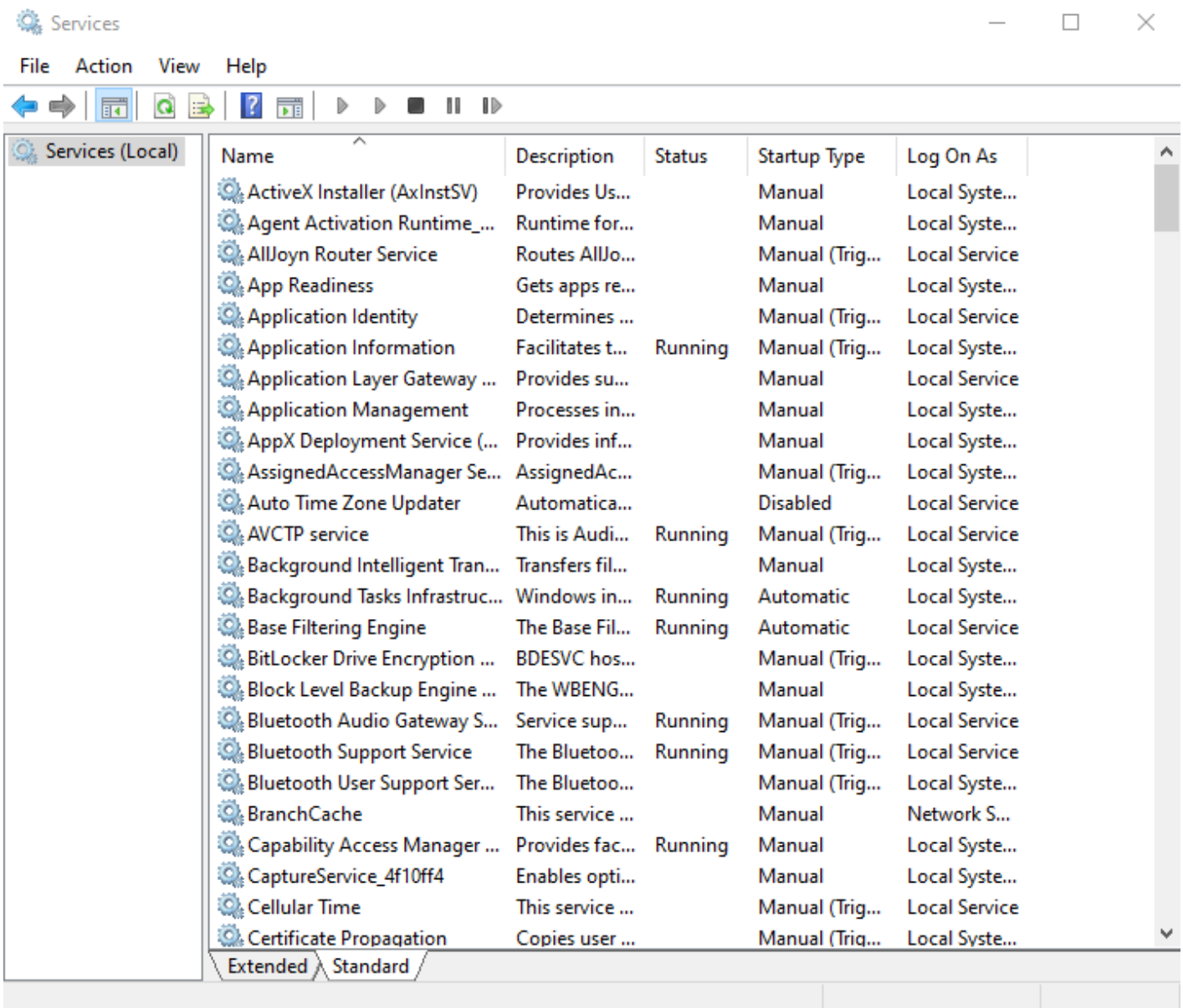
## Services

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

To view all the services in GUI, press ‘**Windows+R**’ and type

```
services.msc
```

Now click on ‘**Ok**’ to see the list of processes.



To start and view the list of services that are currently running in your system, open command prompt as an administrator, type

```
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
CNG Key Isolation
COM+ Event System
Connected Devices Platform Service
Connected Devices Platform User Service_4f10ff4
Connected User Experiences and Telemetry
CoreMessaging
Credential Manager
Cryptographic Services
Data Sharing Service
Data Usage
DbxSvc
DCOM Server Process Launcher
Delivery Optimization
Device Association Service
DHCP Client
Diagnostic Policy Service
Diagnostic Service Host
Diagnostic System Host
Display Enhancement Service
Display Policy Service
Distributed Link Tracking Client
```

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

SERVICE_NAME: BFE
DISPLAY_NAME: Base Filtering Engine
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE                : 4  RUNNING
                           (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0  (0x0)
        SERVICE_EXIT_CODE    : 0  (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0

```

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
```

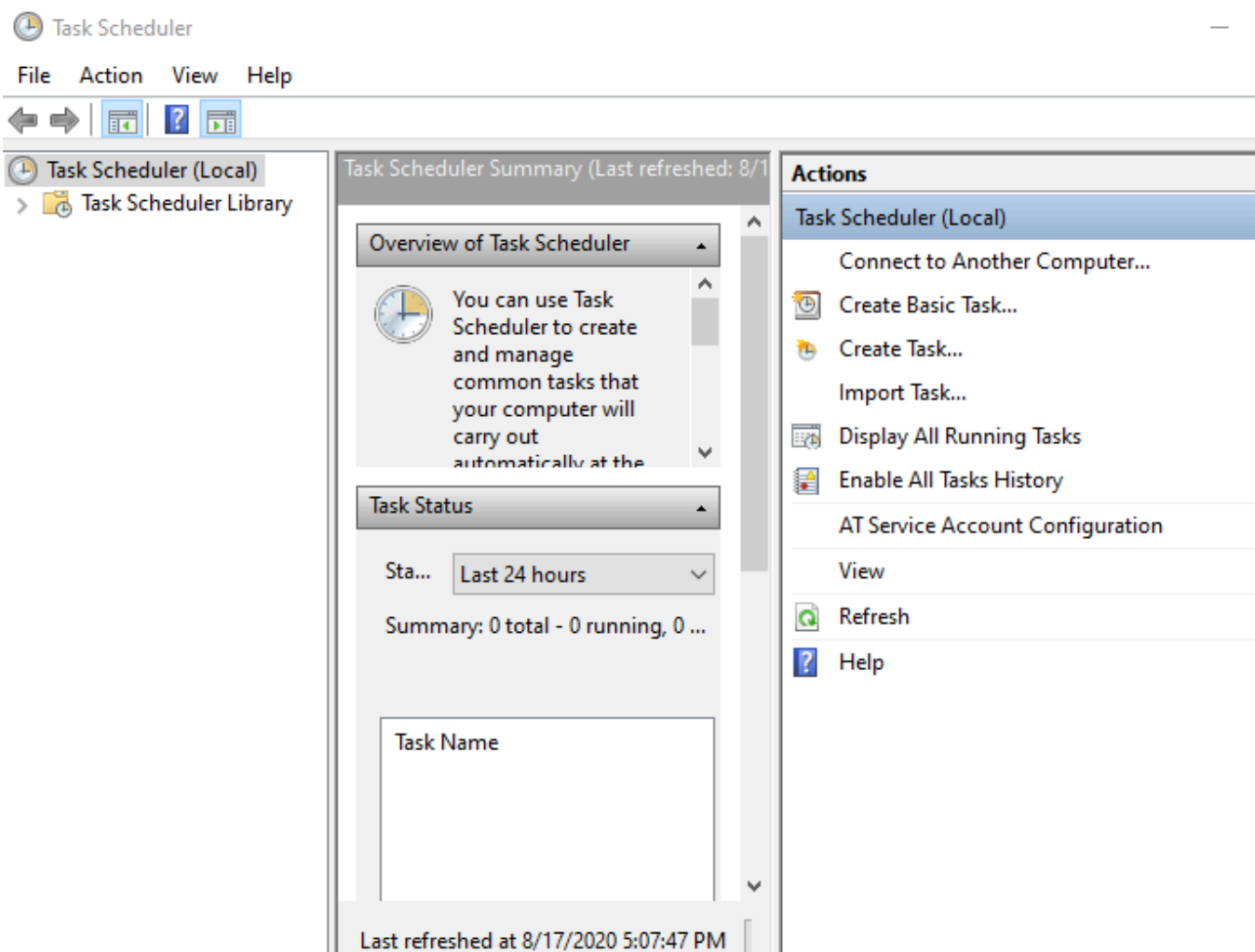
```
C:\Users\raj>tasklist /svc ↵
```

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, SystemEventsBroker
fontdrvhost.exe	776	N/A
svchost.exe	1072	RpcEptMapper, RpcSs
svchost.exe	1124	LSM
svchost.exe	1340	NcbService
svchost.exe	1380	TimeBrokerSvc
svchost.exe	1388	bthserv
svchost.exe	1400	BTAGService
svchost.exe	1396	BthAvctpSvc
svchost.exe	1548	hidserv
svchost.exe	1556	EventSystem
svchost.exe	1724	ProfSvc
svchost.exe	1772	Schedule
svchost.exe	1780	SENS
svchost.exe	1820	SEMgrSvc
igfxCUIService.exe	1880	igfxCUIService2.0.0.0
svchost.exe	1892	EventLog
svchost.exe	1952	CoreMessagingRegistrar
svchost.exe	1996	UserManager
svchost.exe	1536	Themes
svchost.exe	1692	SysMain
svchost.exe	2056	nsi
svchost.exe	2104	AudioEndpointBuilder
svchost.exe	2116	FontCache

## Task Scheduler

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**



To view the schedule tasks in the command prompt, run command prompt as an administrator, type

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.

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

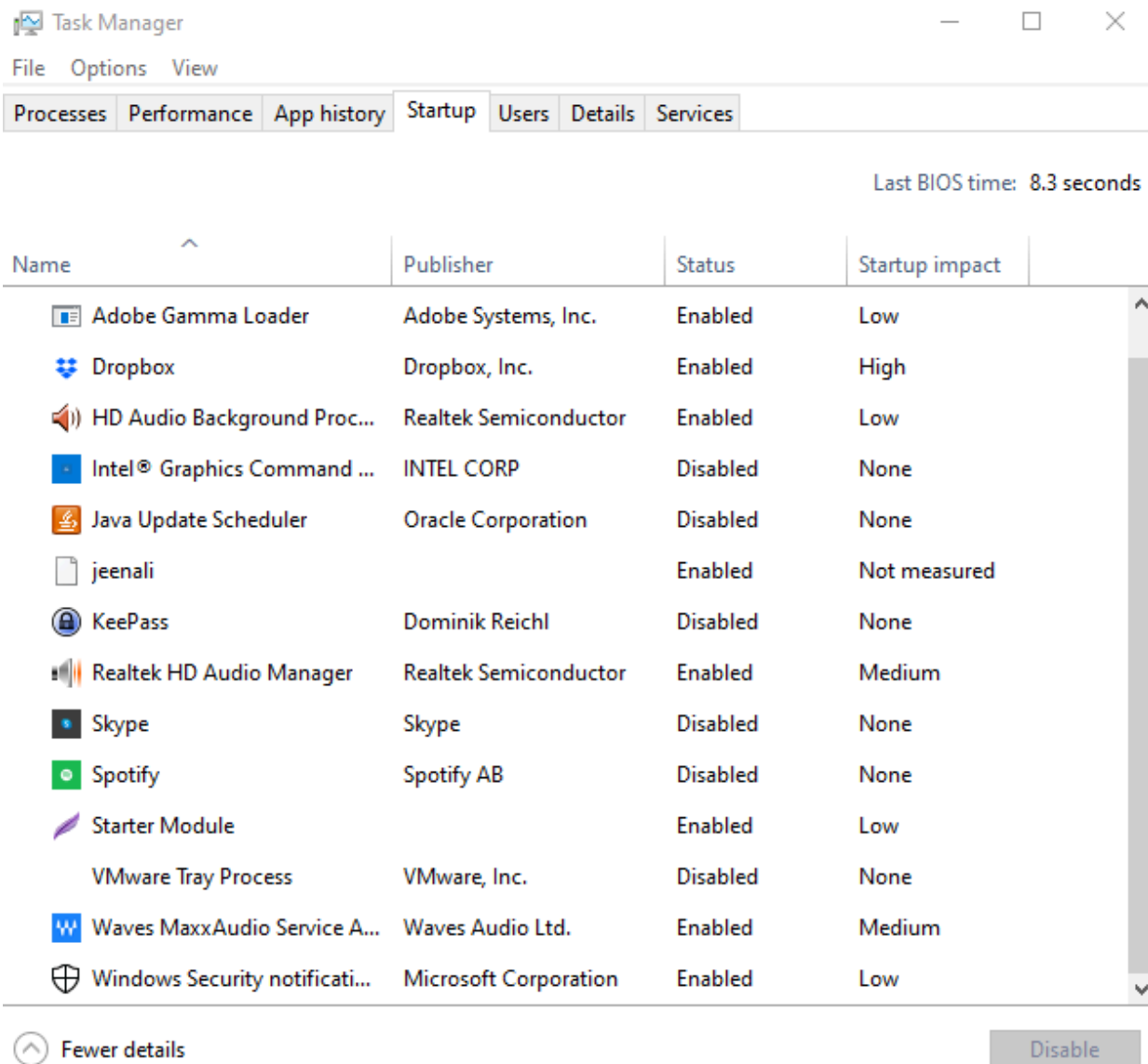
Folder: \Microsoft\Windows\.NET Framework
TaskName                                     Next Run Time                               Status
=====
.NET Framework NGEN v4.0.30319               N/A                                          Ready
.NET Framework NGEN v4.0.30319 64             N/A                                          Ready
.NET Framework NGEN v4.0.30319 64 Critic     N/A                                          Disabled
.NET Framework NGEN v4.0.30319 Critical       N/A                                          Disabled
```

**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.

To view the applications in the Startup menu in the 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

```
taskmgr
```



To view, the startup applications in the PowerShell run the PowerShell as an administrator, type

```
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

```
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

Name      : Adobe Gamma Loader
command   : C:\PROGRA~2\COMMON~1\Adobe\CALIBR~1\ADOBEG~1.EXE
Location  : Common Startup
User      : Public

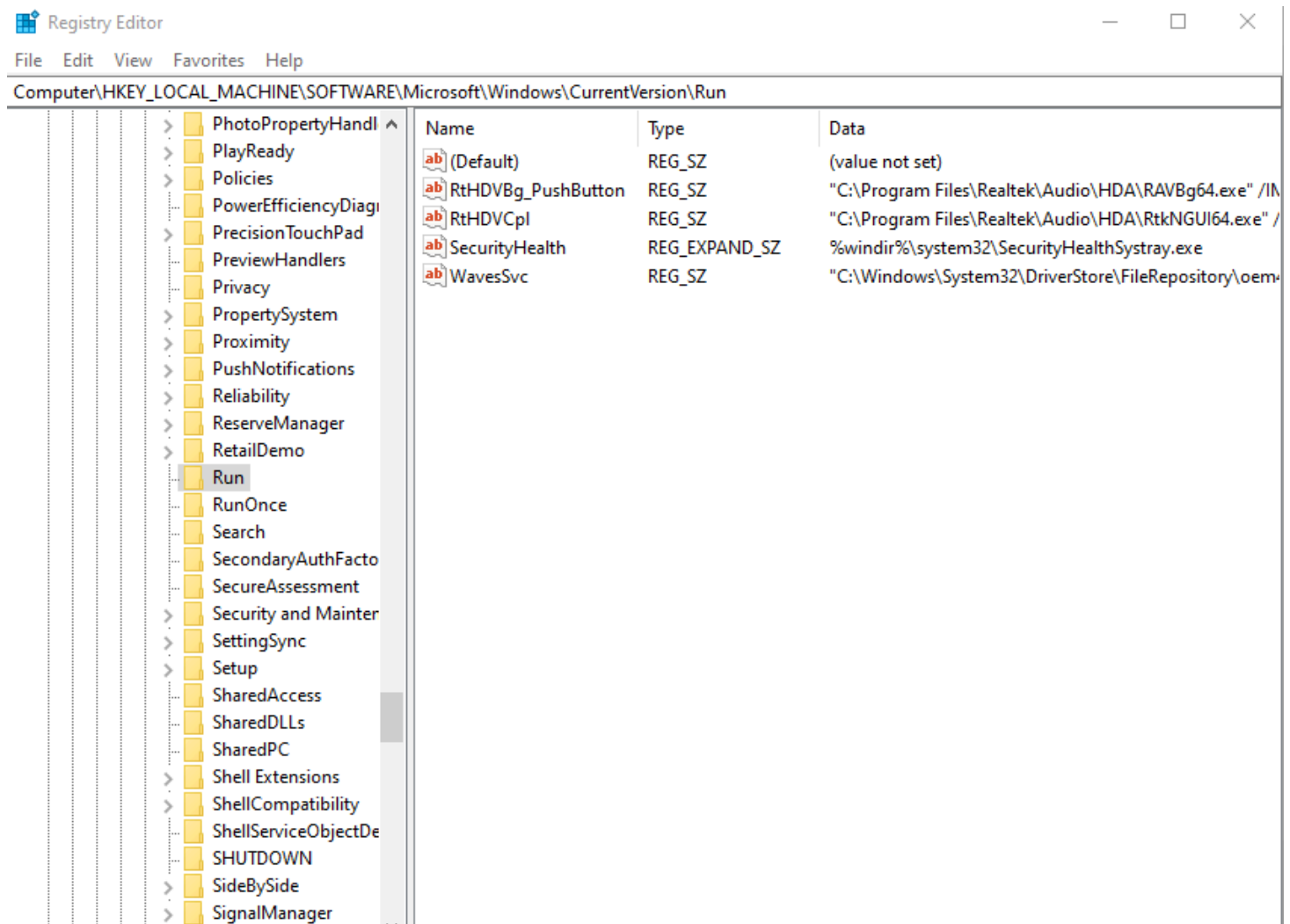
Name      : SecurityHealth
command   : %windir%\system32\SecurityHealthSystray.exe
Location  : HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
User      : Public

Name      : RtHdVCpl
command   : "C:\Program Files\Realtek\Audio\HDA\RtkNGUI64.exe" /s
Location  : HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
User      : Public

Name      : RtHdVBg_PushButton
command   : "C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe" /IM
Location  : HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
User      : Public
```

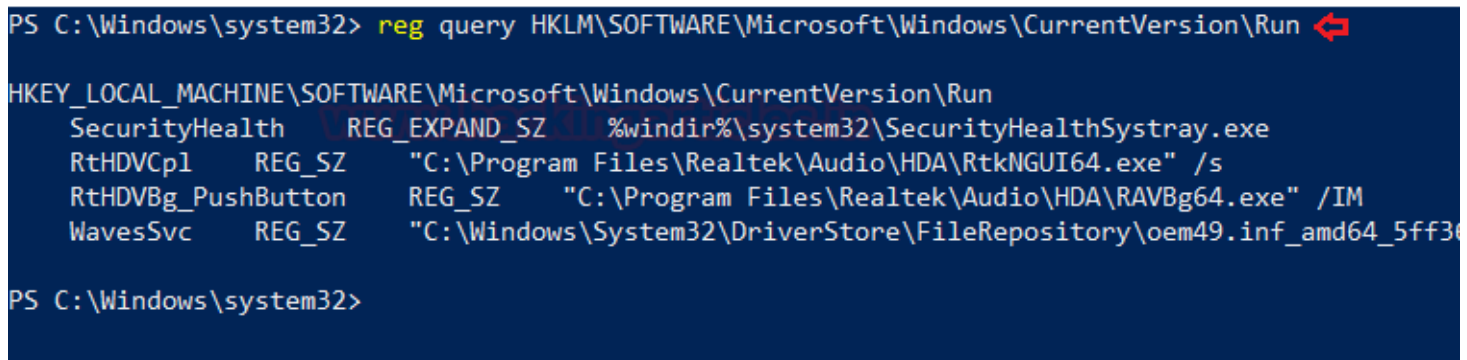
# Registry Entries

Sometimes if there is a presence of unsophisticated malware it can be found by taking a look at the Windows Registry's run key. To view the GUI of the registry key, you can open **REGEDIT** reach the run key manually.



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
```



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
```

```
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 & UDP ports

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

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
```

```
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
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	1772
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	3228
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING	928
TCP	127.0.0.1:443	127.0.0.1:58656	ESTABLISHED	5700
TCP	127.0.0.1:843	0.0.0.0:0	LISTENING	5580
TCP	127.0.0.1:5939	0.0.0.0:0	LISTENING	4420
TCP	127.0.0.1:5939	127.0.0.1:58534	ESTABLISHED	4420
TCP	127.0.0.1:5939	127.0.0.1:58543	ESTABLISHED	4420
TCP	127.0.0.1:8307	0.0.0.0:0	LISTENING	5700

Well, this can also be checked in the PowerShell with a different command to see the IP and the local ports. Run PowerShell and type

```
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
192.168.0.110	57921	104.244.42.66	443	CloseWait
192.168.0.110	57923	192.229.237.101	443	CloseWait
192.168.0.110	57934	104.244.43.131	443	CloseWait
192.168.0.110	57939	117.18.232.102	443	CloseWait
192.168.0.110	57940	152.199.43.83	443	CloseWait
192.168.0.110	57945	151.101.18.164	443	CloseWait
192.168.0.110	58489	104.18.26.211	443	Established
192.168.0.110	58491	52.139.250.253	443	Established
192.168.0.110	58495	74.125.68.188	5228	Established
192.168.0.110	58496	192.0.78.23	443	Established
192.168.0.110	58504	172.67.133.142	443	Established
192.168.0.110	58527	23.211.192.142	443	CloseWait
192.168.0.110	58535	37.252.229.173	443	Established
192.168.0.110	58542	213.227.184.134	443	Established
192.168.0.110	58632	185.199.111.153	443	Established
192.168.0.110	58658	13.227.178.85	443	Established
192.168.0.110	58662	172.217.167.131	443	Established

## 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.

In order to check up on the file-sharing options in the command prompt, type

```
net view \\<localhost>'
```

```
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.
```

To see the file-sharing in PowerShell, you can type

```
Get-SMBShare
```

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

Name      ScopeName Path      Description
-----
ADMIN$    *        C:\Windows 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

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"
```

```
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"
```

```
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
"exe" "utorrentie" 7/27/2020
"exe" "AnyDesk" 7/6/2020
"exe" "ARM Setup 2020.2.1" 6/15/2020
```

To check for files modified in the last 10 days type








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



```
C:\>forfiles /p c: /S /D -10 ↵  
"$Recycle.Bin"  
"Android"  
"Documents and Settings"  
"MSOCache"  
"PerfLogs"  
"Project.log"  
"Recovery"  
"Users"  
"S-1-5-18"  
"S-1-5-21-1097824736-1555393654-2427635684-1000"  
ERROR: Access is denied for "C:\$Recycle.Bin\S-1-5-18\".  
ERROR: Access is denied for "C:\$Recycle.Bin\S-1-5-21-1097824736-1555393654-2427635684-1000\".  
"$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"  
"HeidiSQL"  
"Internet Explorer"  
"JAM Software"  
"KMSpico"  
"Microsoft Analysis Services"  
"Microsoft Office"  
"Microsoft SQL Server"  
"Microsoft.NET"  
"ModifiableWindowsApps"  
"Mozilla Firefox"  
"MSBuild"  
"Notepad++"  
"Npcap"  
"PuTTY"  
"Realtek"  
"Reference Assemblies"  
"SumatraPDF"  
"Uninstall Information"  
"UNP"  
"waves"
```

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

```
size:>6M
```

Search Results in This PC				size:>6M	✕
	<b>data2</b> D:\Softwares\Photoshop cs3	Type: WinRAR archive	Date modified: 1/1/2098 9:00 AM Size: 153 MB		
	<b>History</b> C:\Users\raj\AppData\Local\Google\Chrome\User D...	Type: File	Date modified: 8/17/2020 5:52 PM Size: 6.78 MB		
	<b>thumbcache_1280</b> C:\Users\raj\AppData\Local\Microsoft\Windows\Ex...	Type: Data Base File	Date modified: 8/17/2020 5:51 PM Size: 51.0 MB		
	<b>Windows 10-000002-s004</b> C:\Users\raj\Documents\Virtual Machines\Windows...	Type: Virtual Machine Disk For...	Date modified: 8/17/2020 5:47 PM Size: 1.35 GB		
	<b>Windows 10-000002-s003</b> C:\Users\raj\Documents\Virtual Machines\Windows...	Type: Virtual Machine Disk For...	Date modified: 8/17/2020 5:47 PM Size: 1.51 GB		
	<b>Windows 10-000002-s002</b> C:\Users\raj\Documents\Virtual Machines\Windows...	Type: Virtual Machine Disk For...	Date modified: 8/17/2020 5:47 PM Size: 281 MB		
	<b>Windows 10-000002-s001</b> C:\Users\raj\Documents\Virtual Machines\Windows...	Type: Virtual Machine Disk For...	Date modified: 8/17/2020 5:47 PM Size: 920 MB		

## Firewall Settings

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

To view the firewall configurations and the inbound and outbound traffic in the command prompt, type

```
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\uTo

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\uTo
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
```

```

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 Systems

To check the session details that are created with other systems, you can run command prompt and type

```
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

To see any open sessions of your system, you can get the details about the duration of the session run the command prompt and type

```
net session
```

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

C:\Users\Administrator>net session ↵

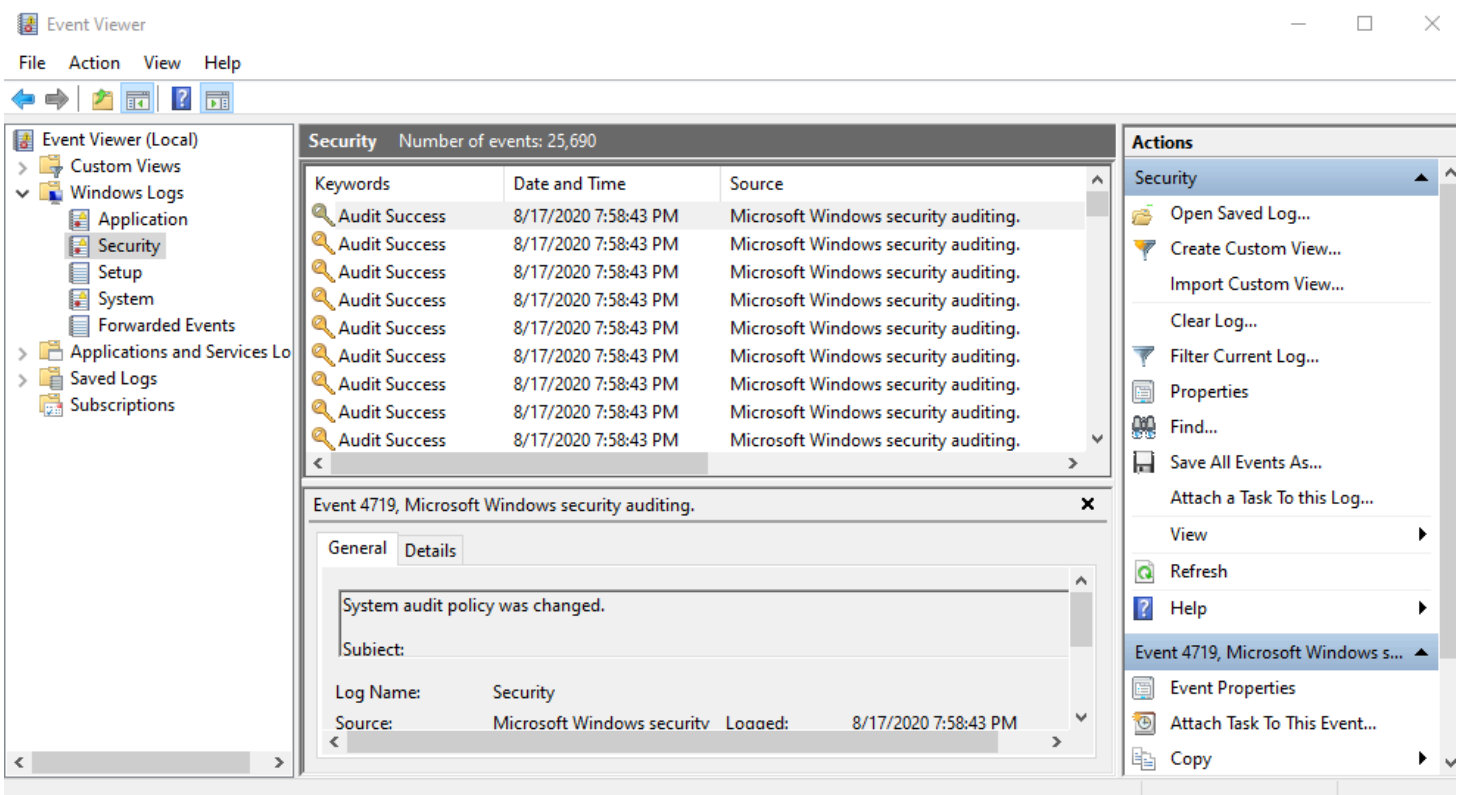
Computer                User name                Client Type              Opens Idle time
-----
\\192.168.0.110         administrator            Microsoft Windows security auditing. 0 00:02:31
The command completed successfully.

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



To export certain logs of a particular event in command prompt type

wevtutil qe security

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

To get the event log list in the PowerShell, type

```
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	OAler
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: OAler
```

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...
126	Aug 16 01:59	Information	Microsoft Office ...	300	Microsoft Word...
125	Aug 15 04:11	Information	Microsoft Office ...	300	Microsoft Word...
124	Aug 14 19:33	Information	Microsoft Office ...	300	Microsoft Word...
123	Aug 14 18:13	Information	Microsoft Office ...	300	Microsoft Word...
122	Aug 14 16:25	Information	Microsoft Office ...	300	Microsoft Word...
121	Aug 14 04:33	Information	Microsoft Office ...	300	Microsoft Word...
120	Aug 14 00:07	Information	Microsoft Office ...	300	Microsoft Word...
119	Aug 13 21:33	Information	Microsoft Office ...	300	Microsoft Word...
118	Aug 12 21:13	Information	Microsoft Office ...	300	Microsoft Word...
117	Aug 12 16:52	Information	Microsoft Office ...	300	Microsoft Word...
116	Aug 12 12:30	Information	Microsoft Office ...	300	Microsoft Word...
115	Aug 12 12:30	Information	Microsoft Office ...	300	Microsoft Word...
114	Aug 12 12:06	Information	Microsoft Office ...	300	Microsoft Word...
113	Aug 12 11:29	Information	Microsoft Office ...	300	Microsoft Word...
112	Aug 11 22:58	Information	Microsoft Office ...	300	Microsoft Word...
111	Aug 11 22:02	Information	Microsoft Office ...	300	Microsoft Word...

And type the particular event in the supply value and you will get event details of that particular event.

## Conclusion

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