Windows

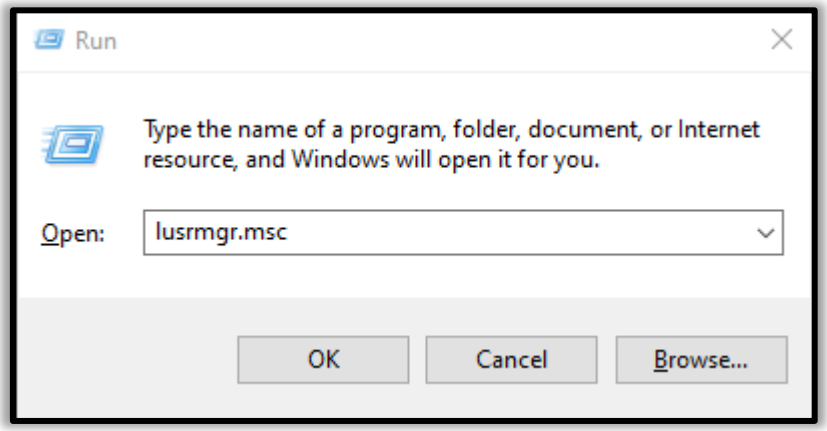
Incident Response

Users

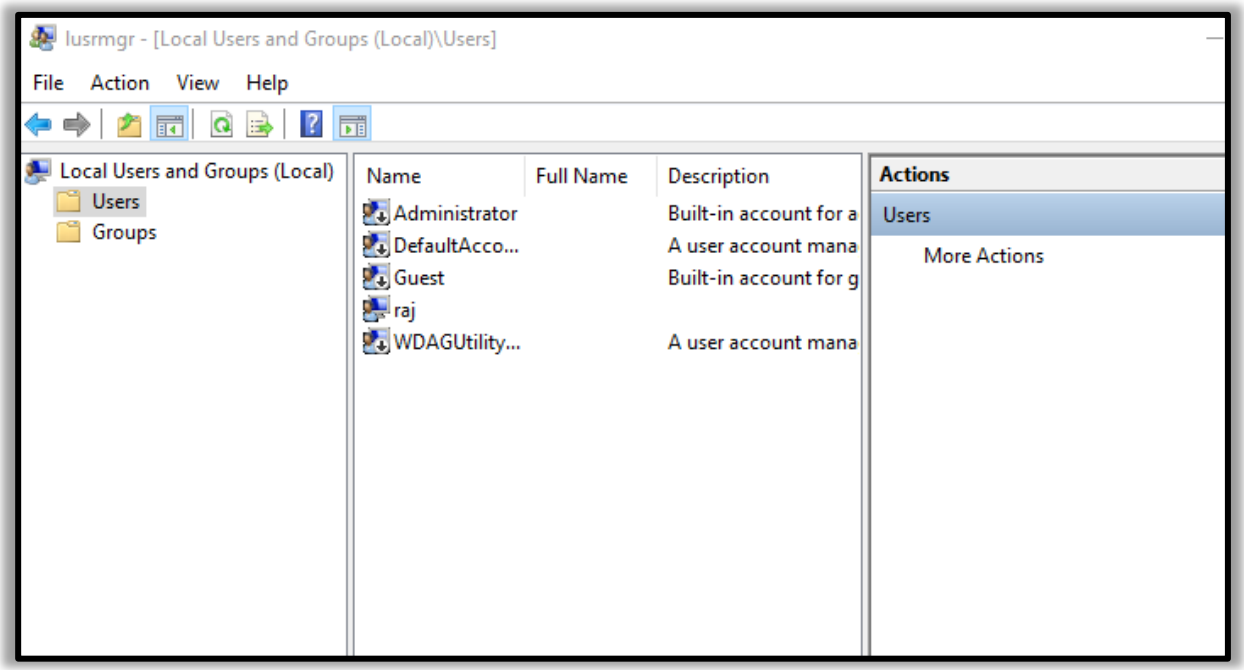
In Incident response it is very necessary to investigate the user activity. It is used to find if there is any suspicious user account is present or any restricted permissions have been assigned to a user. By checking the user account one can be able to get answers to questions like which user is currently 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-A0AP0OM

-------------------------------------------------------------------------------
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

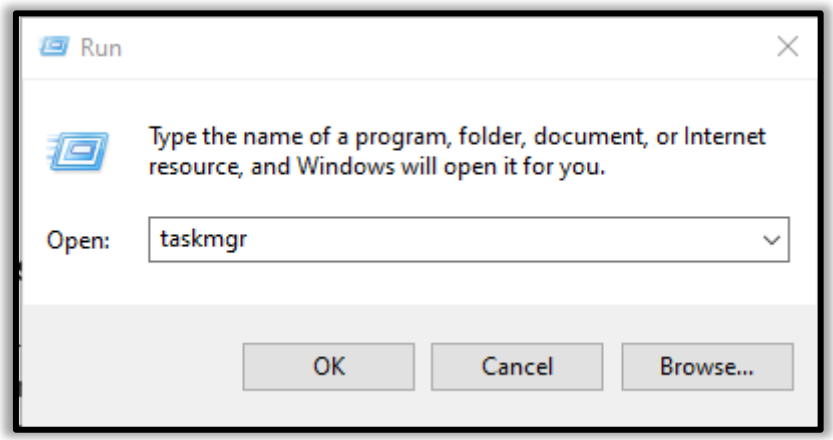
```
PS C:\Users\raj> Get-LocalUser

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
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.