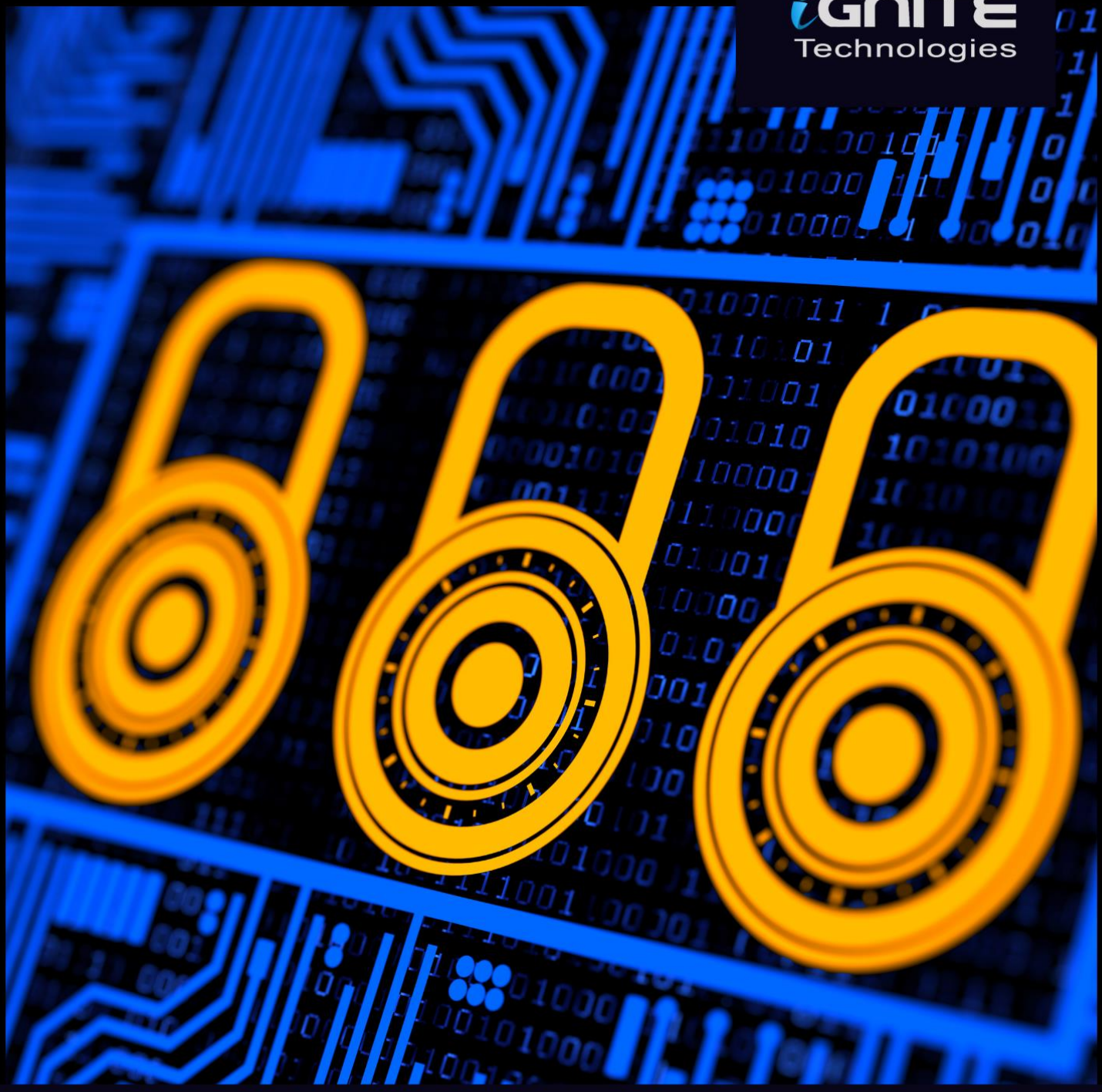
iGNITE Technologies



INCIDENT RESPONSE CHEATSHEET WINDOWS & LINUX

WWW.HACKINGARTICLES.IN

Table of Contents

Abstract

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 fishy 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.

Detecting any intrusion in your system is a very important step towards Incident response. Incident response is quite vast, but it is always better to start small. While performing incident response, you should always focus on suspected systems and the areas where it seems there could be a breach. Making use of Incident Response, you could detect a large number of attacks at the primary level.

The purpose of incident response is nothing but Live Forensics. The investigation can be carried out to obtain any digital evidence. This article mainly focuses on how incident response can be performed in a Linux system. So, to get you started with this cheat sheet, switch on your Linux machine and open the terminal to accomplish these commands.

Linux

Incident Response

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. As an Incident Responder, you should always be aware of what should be and should not be present in your systems.

The security incidents that could be overcome by:

- By examining the running processes
- By having insights into the contents of physical memory.
- By gathering details on the hostname, IP address, operating systems etc
- Gathering information on system services.
- By identifying all the known and unknown users logged onto the system.
- By inspecting network connections, open ports and any network activity.
- By determining the various files present

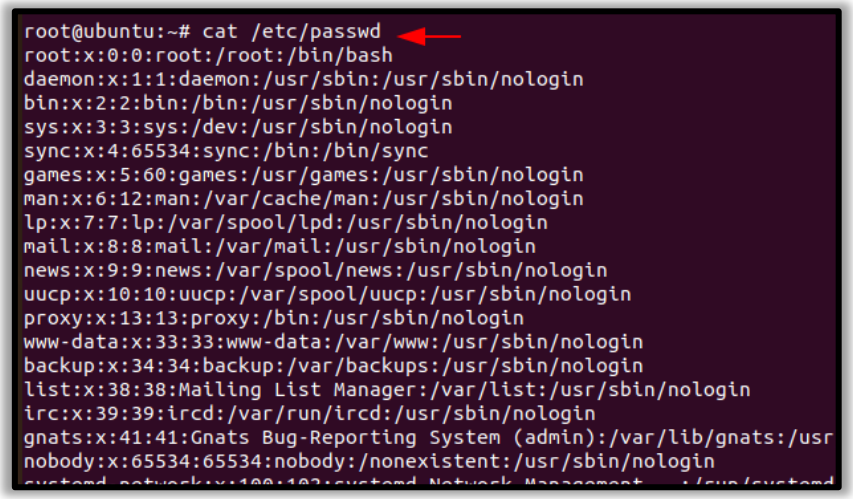
User Accounts

As an Incident Responder, it is very important to investigate the user account's activity. It helps you understand the logged-in users, the existing users, usual or unusual logins, failed login attempts, permissions, access by sudo etc.
The various commands to check the user account activity:

/etc/passwd

To identify whether there is an account entry in your system that may seem suspicious. This command usually fetches all the information about the user account. To do so, type

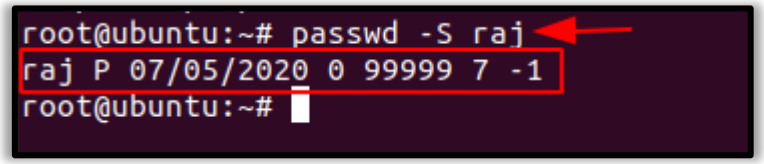
```
cat  /etc/passwd
```



passwd -S

The '**Setuid**' option in Linux is unique file permission. So, on a Linux system when a user wants to make the change of password, they can run the '**passwd**' command. As the root account is marked as setuid, you can get temporary permission.

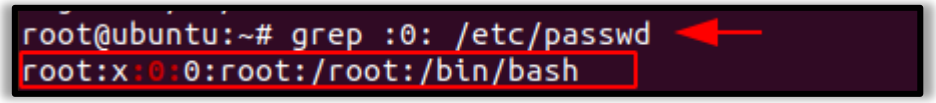
```
passwd -S raj
```



grep

Grep is used for searching plain- text for lines that match a regular expression. :0: is used to display '**UID 0**' files in /etc/passwd file.

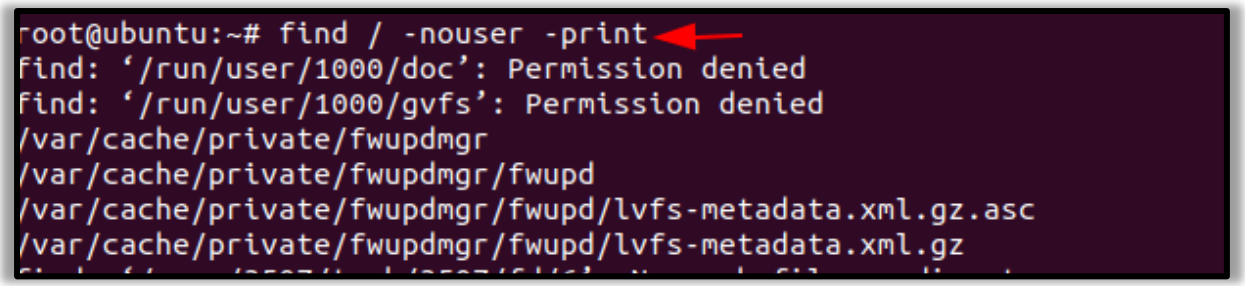
```
grep :0: /etc/passwd
```



find /-nouser

To Identify and display whether an attacker created any temporary user to perform an attack, type

```
find / -nouser -print
```



/etc/shadow

The /etc/shadow contains the encrypted password, details about the passwords and is only accessible by the root users.

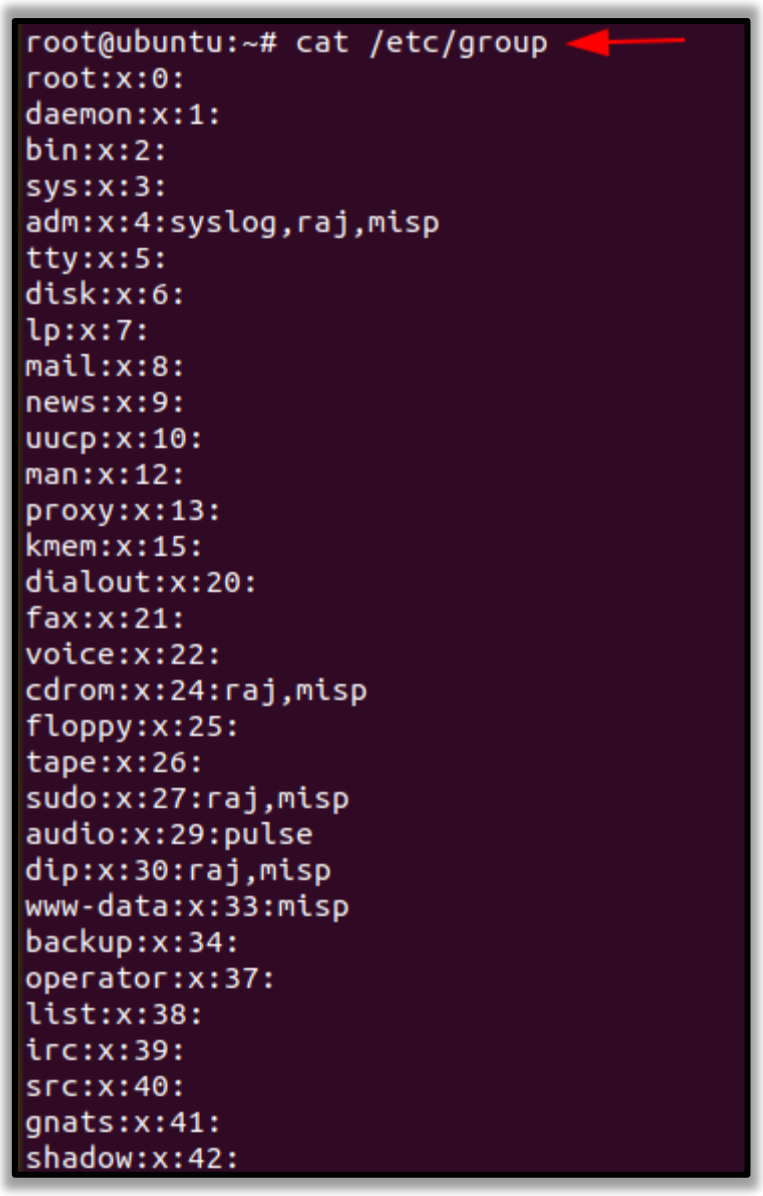
```
cat /etc/shadow
```

```
root@ubuntu:~# cat /etc/shadow
root:!:18448:0:99999:7:::
daemon:*:18375:0:99999:7:::
bin:*:18375:0:99999:7:::
sys:*:18375:0:99999:7:::
sync:*:18375:0:99999:7:::
games:*:18375:0:99999:7:::
man:*:18375:0:99999:7:::
lp:*:18375:0:99999:7:::
mail:*:18375:0:99999:7:::
news:*:18375:0:99999:7:::
uucp:*:18375:0:99999:7:::
proxy:*:18375:0:99999:7:::
www-data:*:18375:0:99999:7:::
backup:*:18375:0:99999:7:::
list:*:18375:0:99999:7:::
irc:*:18375:0:99999:7:::
gnats:*:18375:0:99999:7:::
nobody:*:18375:0:99999:7:::
systemd-network:*:18375:0:99999:7:::
systemd-resolve:*:18375:0:99999:7:::
systemd-timesync:*:18375:0:99999:7:::
messagebus:*:18375:0:99999:7:::
syslog:*:18375:0:99999:7:::
_apt:*:18375:0:99999:7:::
tss:*:18375:0:99999:7:::
uuidd:*:18375:0:99999:7:::
tcpdump:*:18375:0:99999:7:::
avahi-autoipd:*:18375:0:99999:7:::
usbmux:*:18375:0:99999:7:::
rtkit:*:18375:0:99999:7:::
dnsmasq:*:18375:0:99999:7:::
cups-pk-helper:*:18375:0:99999:7:::
speech-dispatcher:!:18375:0:99999:7:::
avahi:*:18375:0:99999:7:::
kernoops:*:18375:0:99999:7:::
saned:*:18375:0:99999:7:::
nm-openvpn:*:18375:0:99999:7:::
hplip:*:18375:0:99999:7:::
whoopsie:*:18375:0:99999:7:::
colord:*:18375:0:99999:7:::
geoclue:*:18375:0:99999:7:::
```

/etc/group

The group file displays the information of the groups used by the user. To view the details, type

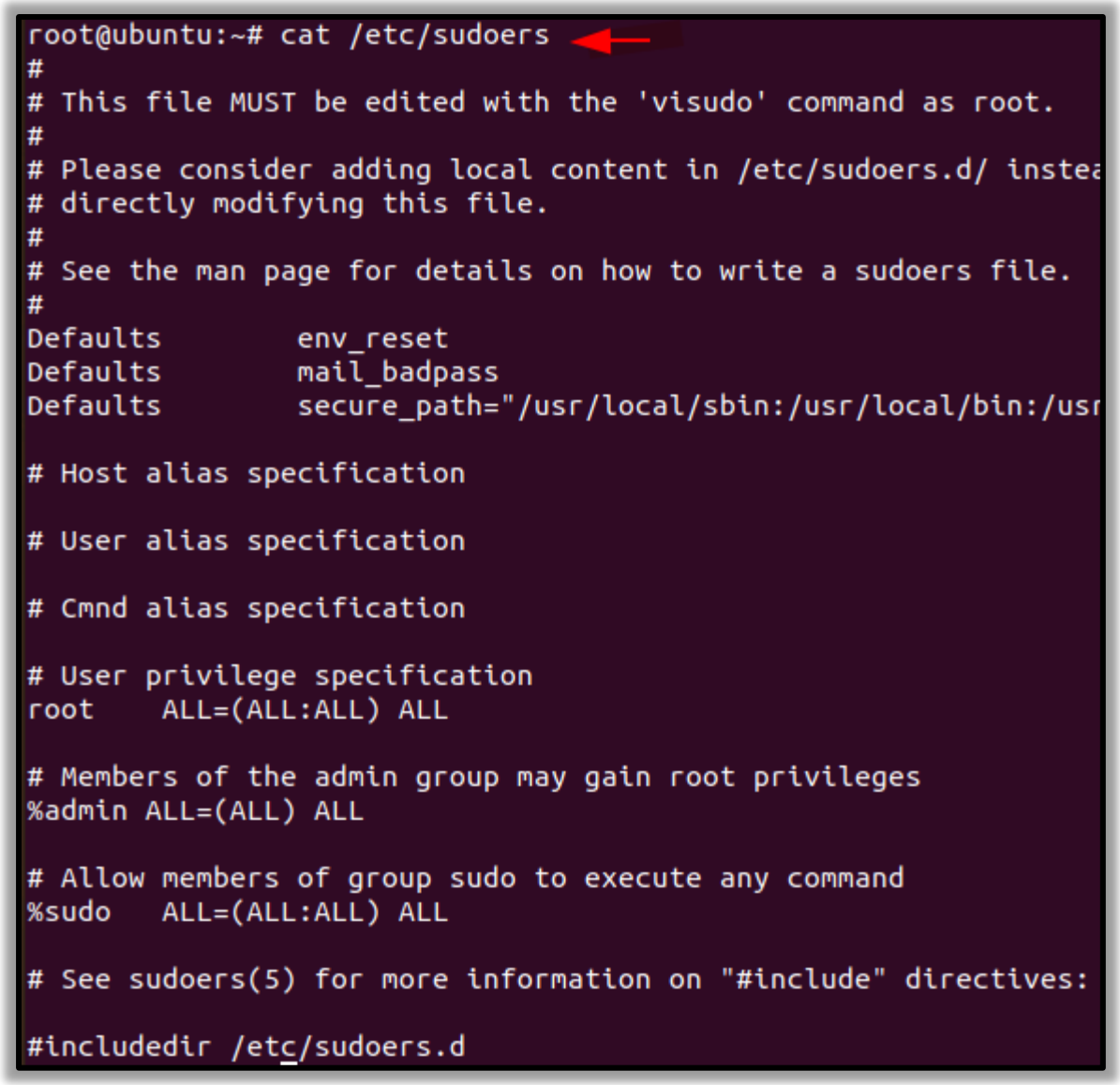
```
cat /etc/group
```



/etc/sudoers

If you want to view information about user and group privileges to be displayed, the/ etc/sudoers file can be viewed

```
cat /etc/sudoers
```



Log Entries

Lastlog

To view the reports of the most recent login of a particular user or all the users in the Linux system, you can type,

```
lastlog
```

```
root@ubuntu:~# lastlog
Username         Port     From             Latest
root                                       **Never logged in**
daemon                                     **Never logged in**
bin                                        **Never logged in**
sys                                        **Never logged in**
sync                                       **Never logged in**
games                                      **Never logged in**
man                                        **Never logged in**
lp                                         **Never logged in**
mail                                       **Never logged in**
news                                       **Never logged in**
uucp                                       **Never logged in**
proxy                                      **Never logged in**
www-data                                   **Never logged in**
backup                                     **Never logged in**
list                                       **Never logged in**
```

Auth.log

To identify any curious SSH & telnet logins or authentication in the system, you can go to /var/log/ directory and then type

```
tail auth.log
```

```
root@ubuntu:/var/log# tail auth.log
Aug 19 08:12:32 ubuntu groupadd[4627]: new group: name=telnetd, GID=137
Aug 19 08:12:32 ubuntu useradd[4633]: new user: name=telnetd, UID=129, GID=137, home=/nonexistent,
Aug 19 08:12:32 ubuntu usermod[4641]: change user 'telnetd' password
Aug 19 08:12:32 ubuntu chage[4648]: changed password expiry for telnetd
Aug 19 08:12:32 ubuntu gpasswd[4653]: user telnetd added by root to group utmp
Aug 19 08:12:44 ubuntu pkexec: pam_unix(polkit-1:session): session opened for user root by (uid=100
Aug 19 08:12:44 ubuntu pkexec[5129]: raj: Executing command [USER=root] [TTY=unknown] [CWD=/home/ra
Aug 19 08:13:52 ubuntu sshd[5137]: Accepted password for raj from 192.168.0.110 port 54348 ssh2
Aug 19 08:13:52 ubuntu sshd[5137]: pam_unix(sshd:session): session opened for user raj by (uid=0)
```

```
root@ubuntu:/var/log# tail auth.log
Aug 19 08:13:52 ubuntu sshd[5137]: Accepted password for raj from 192.168.0.110 port 54348 s
Aug 19 08:13:52 ubuntu sshd[5137]: pam_unix(sshd:session): session opened for user raj by (u
Aug 19 08:13:52 ubuntu systemd-logind[790]: New session 5 of user raj.
Aug 19 08:16:35 ubuntu sshd[5137]: pam_unix(sshd:session): session closed for user raj
Aug 19 08:16:35 ubuntu systemd-logind[790]: Session 5 logged out. Waiting for processes to e
Aug 19 08:16:35 ubuntu systemd-logind[790]: Removed session 5.
Aug 19 08:16:46 ubuntu login[5343]: pam_unix(login:auth): Couldn't open /etc/securetty: No s
Aug 19 08:16:47 ubuntu login[5343]: pam_unix(login:auth): Couldn't open /etc/securetty: No s
Aug 19 08:16:47 ubuntu login[5343]: pam_unix(login:session): session opened for user raj by
Aug 19 08:16:47 ubuntu systemd-logind[790]: New session 6 of user raj.
```

History

To view the history of commands that the user has typed, you can type history with less or can even mention up to the number of commands you typed last. To view history, you can type

```
history| less
```

```
root@ubuntu:~# history | less
```

```
22  passwd -S raj
23  passwd -S misp
24  passwd -S raj
25  grep :0: /etc/passwd
26  grep :1: /etc/passwd
27  grep :2: /etc/passwd
28  grep :15: /etc/passwd
29  grep :12: /etc/passwd
30  find / -nouser -print
31  ifconfig
32  apt install net-tools
33  ifconfig
34  apt install openssh-server telnetd
35  clear
```

System Resources

System resources can tell you a lot about system logging information, uptime of the system, the memory space and utilisation of the system etc.

Uptime

To know whether your Linux system has been running overtime or to see how long the server has been running for, the current time in the system, how many users have currently logged on, and the load averages of the system, then you can type:

```
uptime
```

```
root@ubuntu:~# uptime
 08:26:34 up 21 min,  1 user,  load average: 0.14, 0.13, 0.09
root@ubuntu:~#
```

Free

To view the memory utilisation by the system in Linux, the used physical and swap memory in the system, as well as the buffers used by the kernel, you can type,

```
free
```

```
root@ubuntu:~# free
               total        used        free      shared  buff/cache   available
Mem:         4002256     1369744      726588        5480     1905924     2339648
Swap:         945416           0      945416
```

/proc/memory

As an incident responder to check the detail information of the ram, memory space available, buffers and swap on the system, you can type

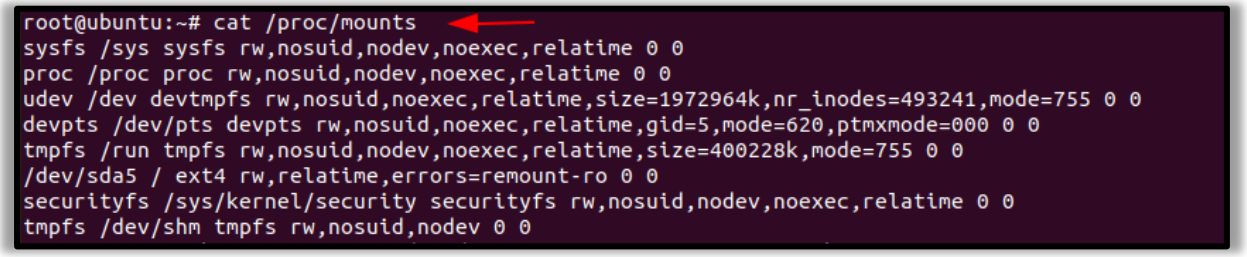
```
cat /proc/meminfo
```

```
root@ubuntu:~# cat /proc/meminfo
MemTotal:        4002256 kB
MemFree:          309152 kB
MemAvailable:    1280208 kB
Buffers:          220452 kB
Cached:           937176 kB
SwapCached:          440 kB
```

/proc/mounts

As an incident responder, it's your responsibility to check if there is an unknown mount on your system, to check the mount present on your system, you can type

```
cat /proc/mounts
```



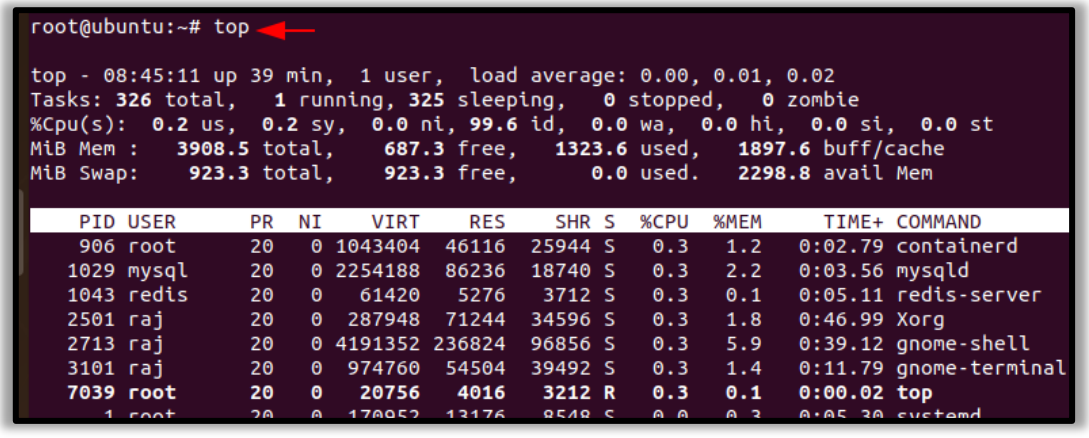
Processes

As an incident responder, you should be always curious when you are looking through the output generated by your system. Your curiosity should compel you to view the programs that are currently running in the system, if they necessary to run and if they should be running, and usage of the CPU usage by these processes etc.

top

To get a dynamic and a real-time visual of all the processes running in the Linux system, a summary of the information of the system and the list of processes and their ID numbers or threads managed by Linux Kernel, you can make use of

```
top
```



ps aux

To see the process status of your Linux and the currently running processes system and the PID. To identify abnormal processes that could indicate any malicious activity in the Linux system, you can use

```
ps aux
```

```
root@ubuntu:~# ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.2  0.3 168904 13140 ?        Ss   08:05   0:04 /sbin/init auto noprompt
root           2  0.0  0.0      0     0 ?        S    08:05   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   08:05   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   08:05   0:00 [rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   08:05   0:00 [kworker/0:0H-kblockd]
root           9  0.0  0.0      0     0 ?        I<   08:05   0:00 [mm_percpu_wq]
root          10  0.0  0.0      0     0 ?        S    08:05   0:00 [ksoftirqd/0]
root          11  0.1  0.0      0     0 ?        I    08:05   0:02 [rcu_sched]
root          12  0.0  0.0      0     0 ?        S    08:05   0:00 [migration/0]
root          13  0.0  0.0      0     0 ?        S    08:05   0:00 [idle_inject/0]
root          14  0.0  0.0      0     0 ?        S    08:05   0:00 [cpuhp/0]
root          15  0.0  0.0      0     0 ?        S    08:05   0:00 [cpuhp/1]
root          16  0.0  0.0      0     0 ?        S    08:05   0:00 [idle_inject/1]
```

PID

To display more details on a particular process, you can use,

```
lsof -p [pid]
```

```
root@ubuntu:~# lsof -p 6047
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
lsof: WARNING: can't stat() fuse file system /run/user/1000/doc
      Output information may be incomplete.
COMMAND  PID     USER   FD      TYPE DEVICE SIZE/OFF   NODE NAME
apache2 6047 www-data  cwd       DIR    8,5     4096      2 /
apache2 6047 www-data  rtd       DIR    8,5     4096      2 /
apache2 6047 www-data  txt       REG    8,5   704520 397677 /usr/sbin/apache2
apache2 6047 www-data  DEL       REG    0,1          210006 /dev/zero
apache2 6047 www-data  DEL       REG    0,1          210005 /dev/zero
apache2 6047 www-data  mem       REG    8,5  1168056 401435 /usr/lib/x86_64-linux-gnu/libg
apache2 6047 www-data  mem       REG    8,5 28046896 401665 /usr/lib/x86_64-linux-gnu/libi
apache2 6047 www-data  mem       REG    8,5    51832 401899 /usr/lib/x86_64-linux-gnu/libn
apache2 6047 www-data  mem       REG    8,5   231544 393313 /usr/lib/x86_64-linux-gnu/libn
apache2 6047 www-data  mem       REG    8,5   104984 401422 /usr/lib/x86_64-linux-gnu/libg
apache2 6047 www-data  mem       REG    8,5  1952928 402203 /usr/lib/x86_64-linux-gnu/libs
apache2 6047 www-data  mem       REG    8,5    92320 401357 /usr/lib/x86_64-linux-gnu/libe
apache2 6047 www-data  mem       REG    8,5   264632 402455 /usr/lib/x86_64-linux-gnu/libx
apache2 6047 www-data  mem       REG    8,5    35080 415279 /usr/lib/php/20190902/xsl.so
apache2 6047 www-data  DEL       REG    0,1          210007 /dev/zero
```

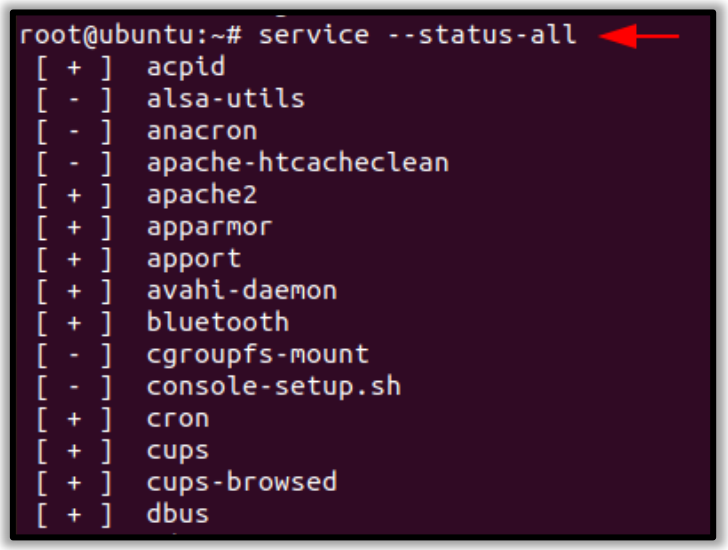
Services

The services in the Linux system can be classified into system and network services. System services include the status of services, cron, etc and network services include file transfer, domain name resolution, firewalls, etc. As an incident responder, you identify if there is an anomaly in the services.

Service

To find any abnormally running services, you can use

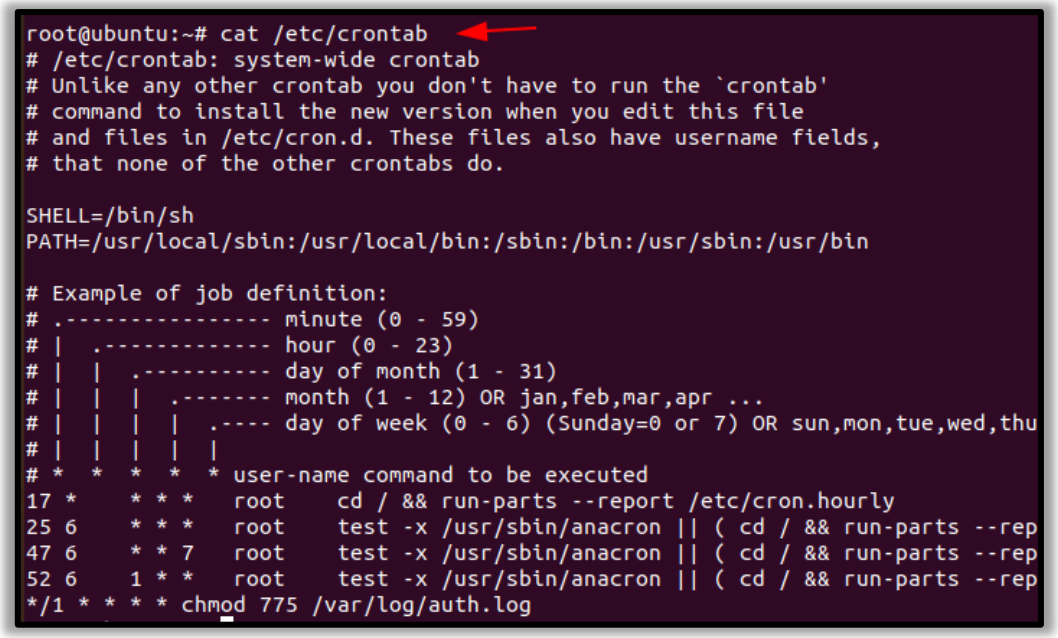
```
service --status-all
```



/etc/cronjob

The incident responder should look for any suspicious scheduled tasks and jobs. To find the scheduled tasks, you can use,

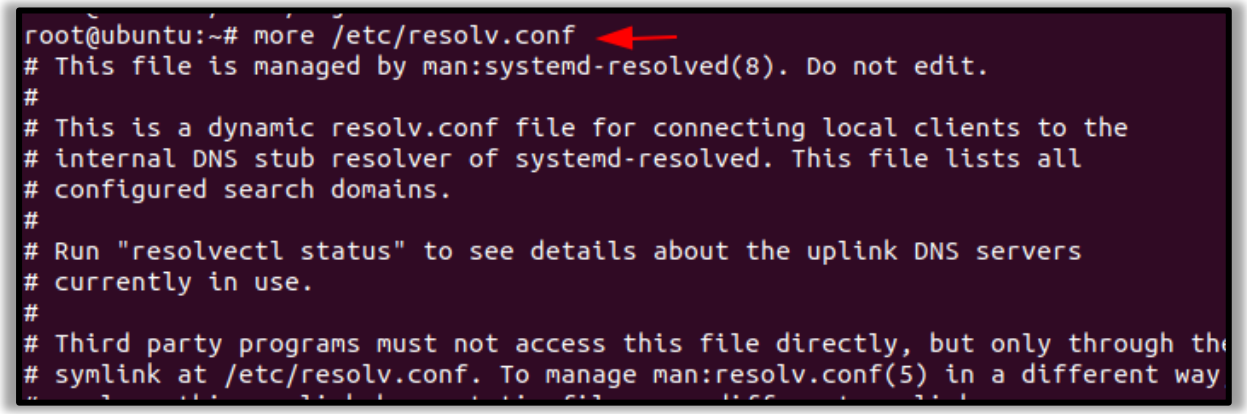
```
cat /etc/crontab
```



/etc/resolv.conf

To resolve DNS configuration issues and to avail a list of keywords with values that provide the various types of resolver information, you can use

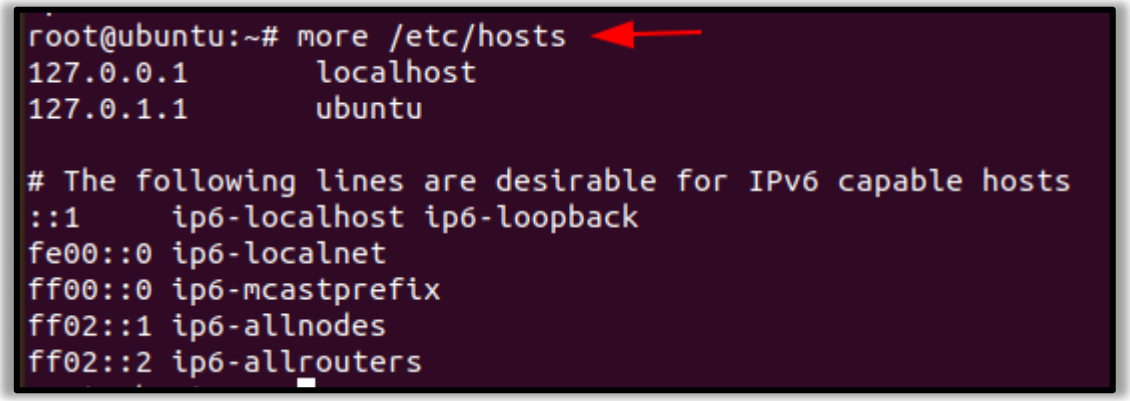
```
more /etc/resolv.conf
```



/etc/hosts

To check file that translates hostnames or domain names to IP addresses, which is useful for testing changes to the website or the SSL setup, you can use

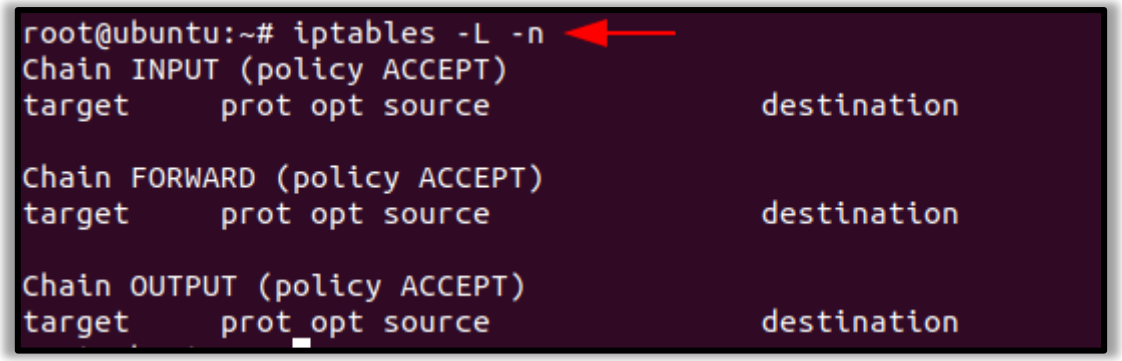
```
more /etc/hosts
```



iptables

To check and manage the IPv4 packet filtering and NAT in Linux systems, you can use iptables and can make use of a variety of commands like:

```
iptables -L -n
```



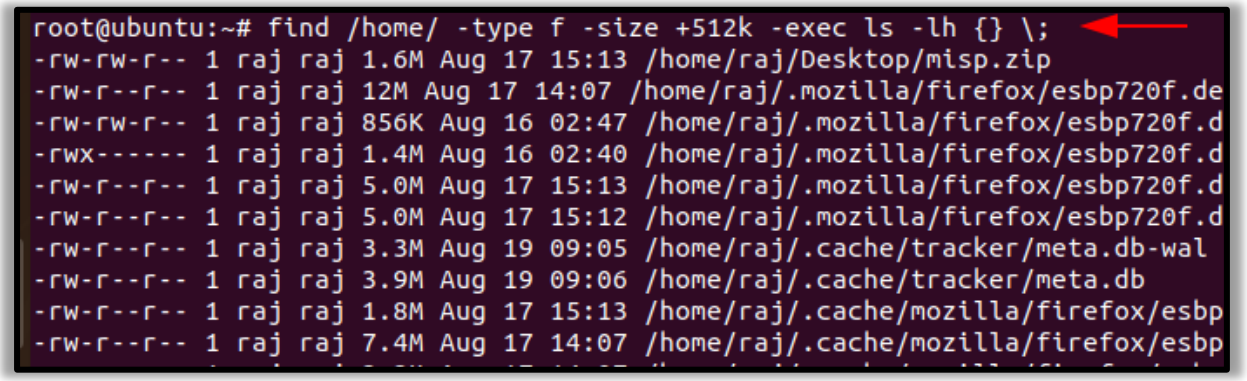
Files

As an incident responder, you should be aware of any abnormal-looking files in your system.

Large Files

To identify any overly large files in your system and their permissions with their destination, you can use

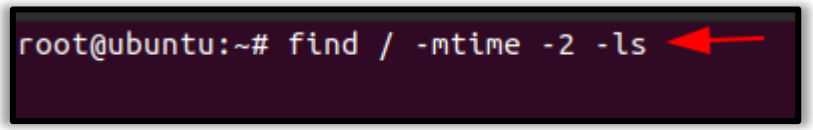
```
find /home/ -type f -size +512k -exec ls -lh {} \;
```



mtime

As an incident responder, if you want to see an anomalous file that has been present in the system for 2 days, you can use the command,

```
find / -mtime -2 -ls
```



Network Settings

As an incident responder, you should have a keen eye on the Network activity and setting. It is extremely vital to identify the overall picture of a system network and its health.

ifconfig

To obtain the network activity information, you can use various commands.

```
ifconfig
```

To see all the network interfaces, you can use

```
ifconfig -a
```

```
root@ubuntu:~# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.196  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::c418:3516:30f3:cf62  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:c8:9c:50  txqueuelen 1000  (Ethernet)
        RX packets 67369  bytes 84475766 (84.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 38278  bytes 4161560 (4.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 17330  bytes 1228801 (1.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17330  bytes 1228801 (1.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Open files

To list all the processes that are listening to ports with their PID, you can use

```
lsof -i
```

```
root@ubuntu:~# lsof -i
COMMAND     PID            USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd-r   744 systemd-resolve   12u  IPv4  30603      0t0  UDP localhost:domain
systemd-r   744 systemd-resolve   13u  IPv4  30604      0t0  TCP localhost:domain (LISTEN)
avahi-dae   761           avahi   12u  IPv4  34902      0t0  UDP *:mdns
avahi-dae   761           avahi   13u  IPv6  34903      0t0  UDP *:mdns
avahi-dae   761           avahi   14u  IPv4  34904      0t0  UDP *:54114
```

netstat

To display all the listening ports in the network use

```
netstat -nap
```

```
root@ubuntu:~# netstat -nap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      744/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      925/sshd: /usr/sbin
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      4619/inetd
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      982/cupsd
tcp        0      0 127.0.0.1:39711         0.0.0.0:*               LISTEN      906/containerd
tcp        0      0 127.0.0.1:6666          0.0.0.0:*               LISTEN      887/python
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      1029/mysqld
tcp        0      0 127.0.0.1:6379          0.0.0.0:*               LISTEN      1043/redis-server 1
tcp        0      0 127.0.0.1:33498         127.0.0.1:6379          ESTABLISHED 1396/bash
tcp        0      0 127.0.0.1:6379          127.0.0.1:33504         ESTABLISHED 1043/redis-server 1
tcp        0      0 127.0.0.1:33508         127.0.0.1:6379          ESTABLISHED 1608/bash
```

arp

To display the system ARP cache, you can type

```
arp -a
```

```
root@ubuntu:~# arp -a
? (192.168.0.110) at 8c:ec:4b:71:c5:de [ether] on ens33
_gateway (192.168.0.1) at d8:47:32:e9:3f:34 [ether] on ens33
```

path

The $PATH displays a list of directories that tells the shell which directories to search for executable files, to check for directories that are in your path you can use.

```
echo $PATH
```

```
raj@ubuntu:~$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
```

Windows

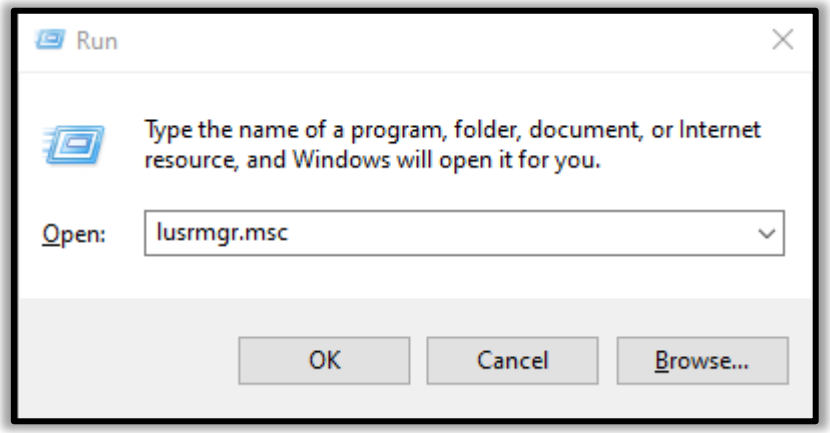
Incident Response

Users

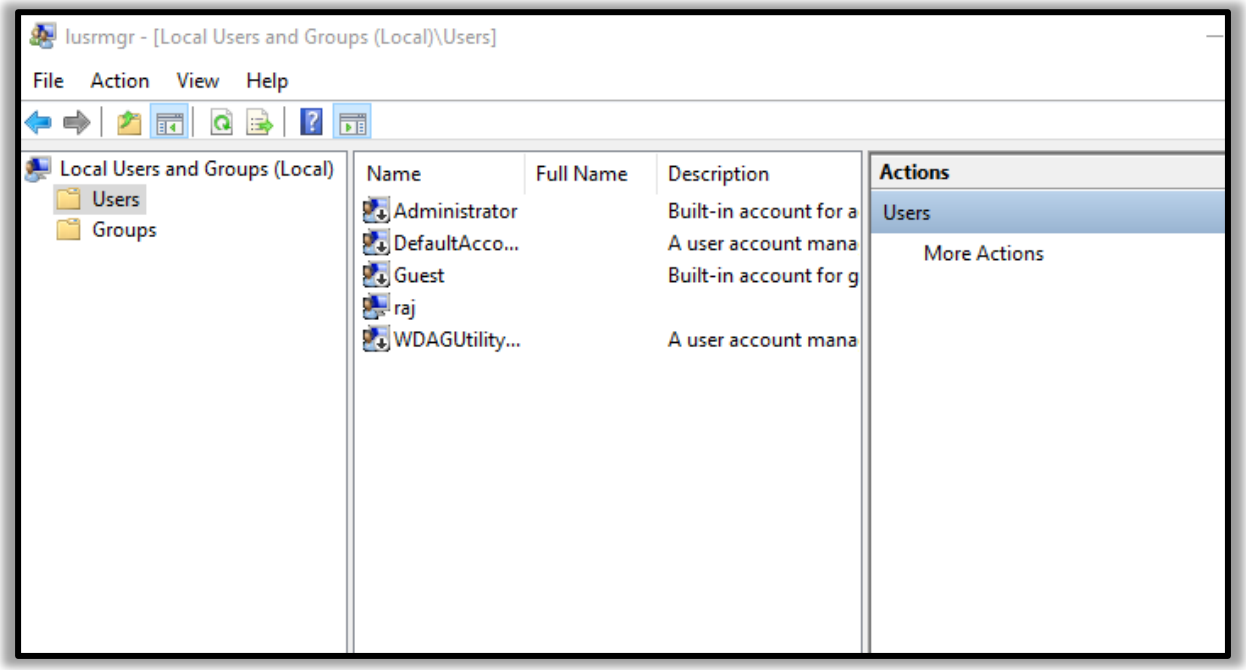
In Incident response it is very necessary to investigate the user activity. It is used to find if there is any suspicious user account is present or any restricted permissions have been assigned to a user. By checking the user account one can be able to get answers to questions like which user is currently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

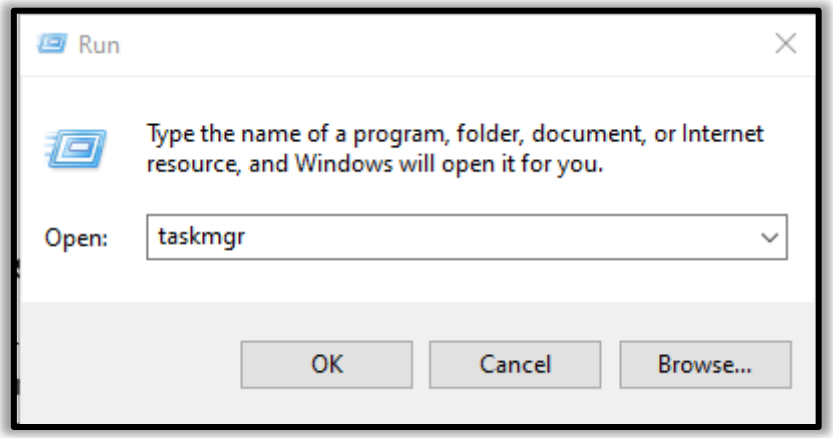
```
PS C:\Users\raj> Get-LocalUser

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

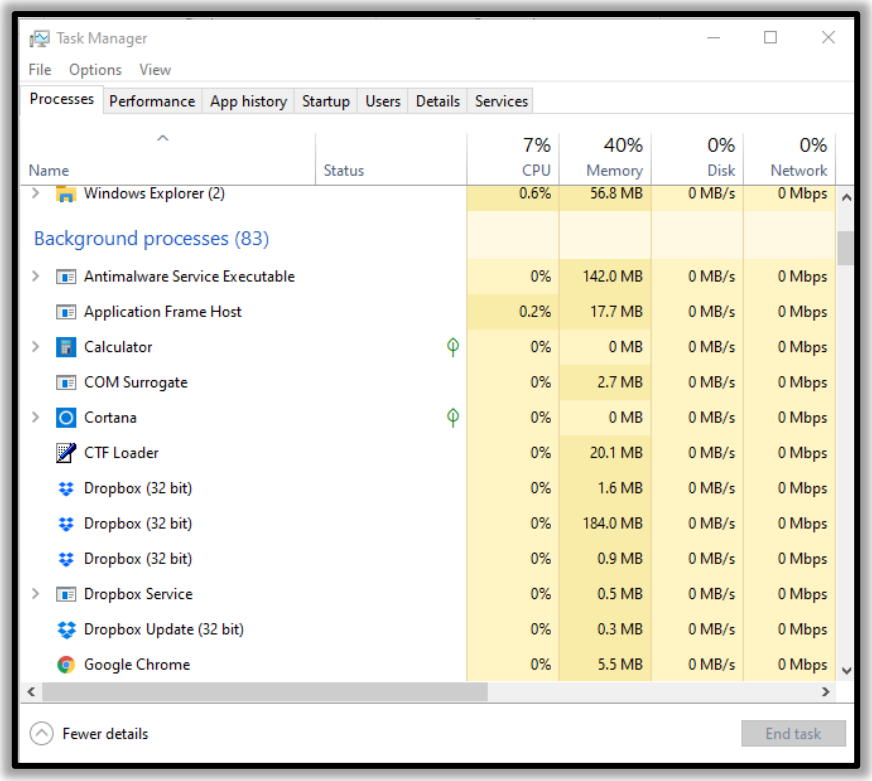
To get the list of all the processes running on the system, you can use '***tasklist***' command for this purpose. By making use of this command, you can get a list of the processes the memory space used, running time, image file name, services running in the process etc
To view the processes, you can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



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\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
```

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
```

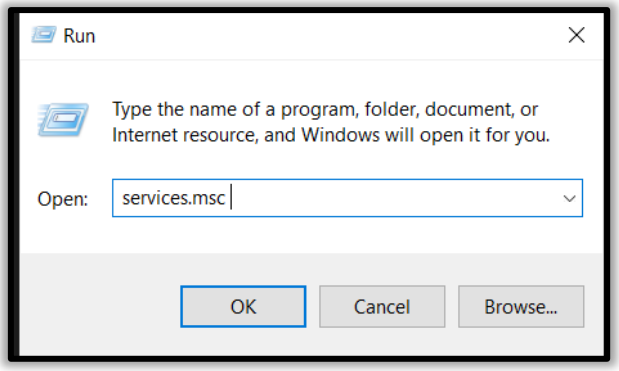
```
PS C:\Windows\system32> wmic process where "ProcessID=4420" get CommandLine
CommandLine
"C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe"

PS C:\Windows\system32>
```

Services

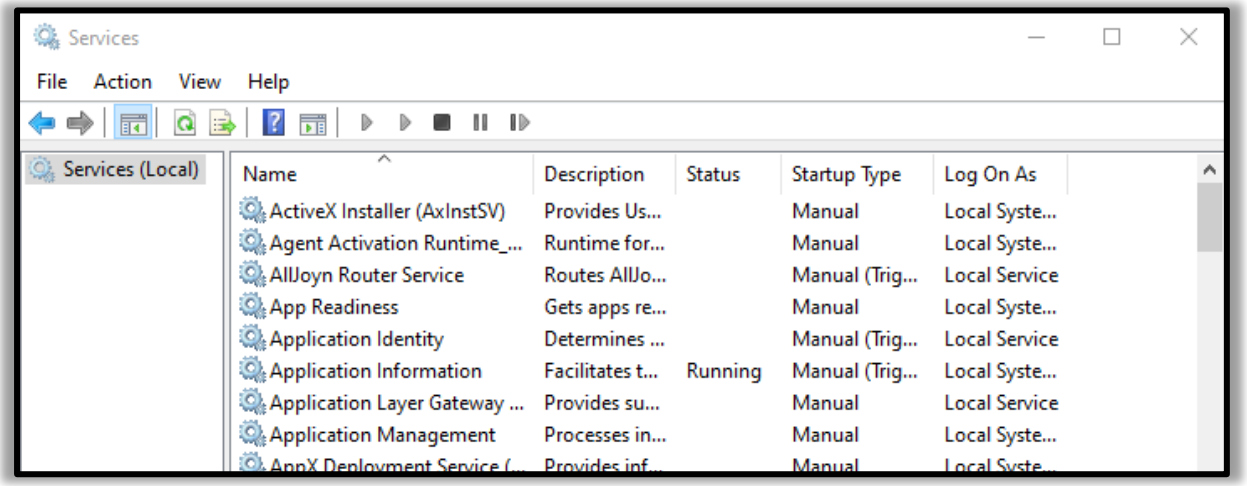
To identify if there is any abnormal service running in your system or some service is not functioning properly, you can view your services.

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.

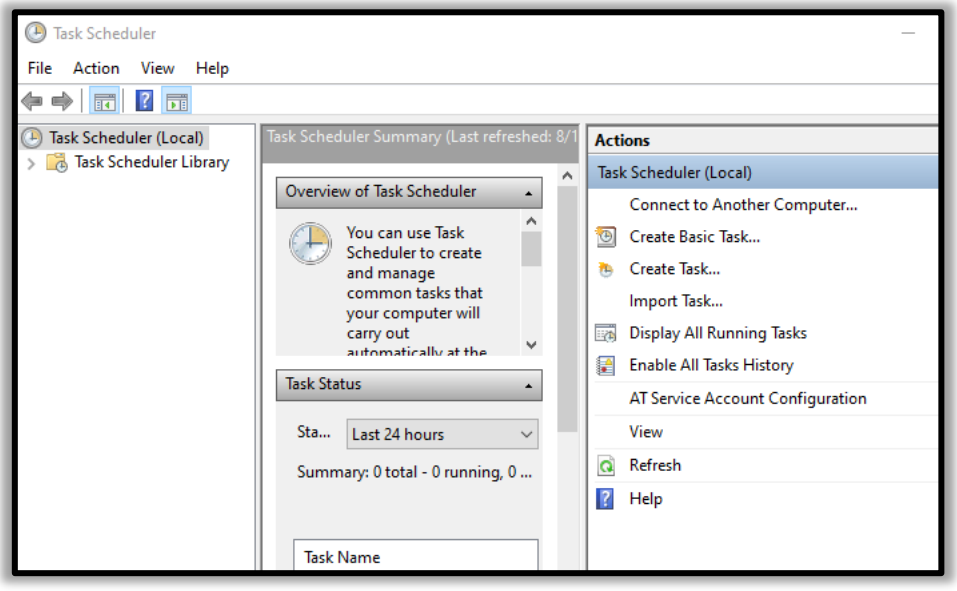
```
tasklist /svc
```

```
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,
```

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.
```

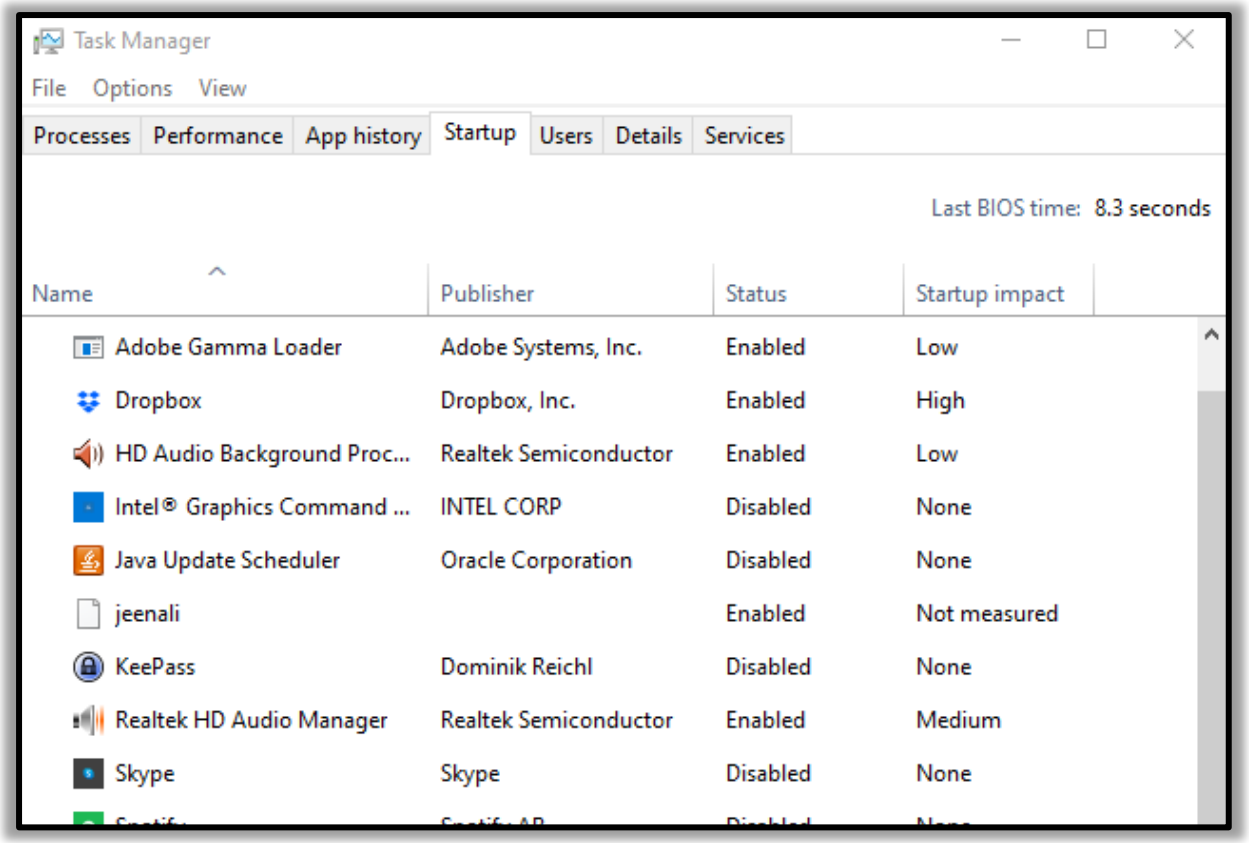
Startup

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'
```

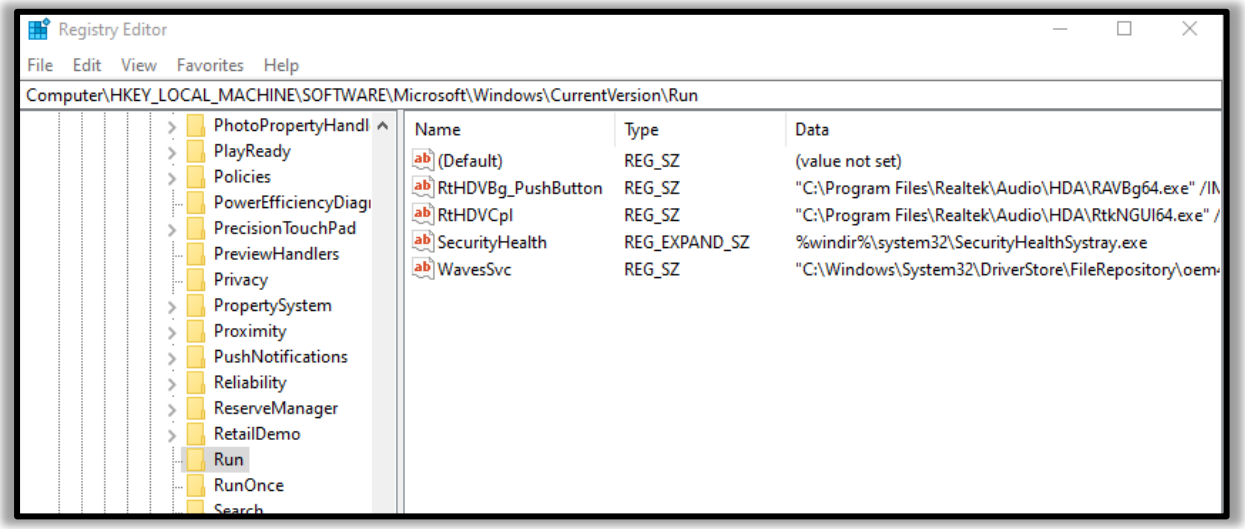
```
PS C:\Windows\system32> Get-CimInstance Win32_StartupCommand | Select-Object Name, command, Location, User | Format-List


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-A0AP0OM\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-A0AP0OM\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

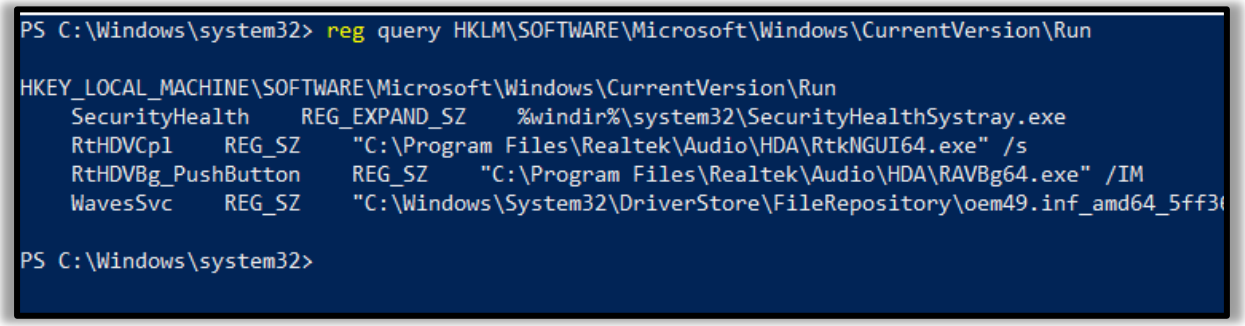
To view the GUI of the registry key, you can open REGEDIT reach the run key manually.



PowerShell

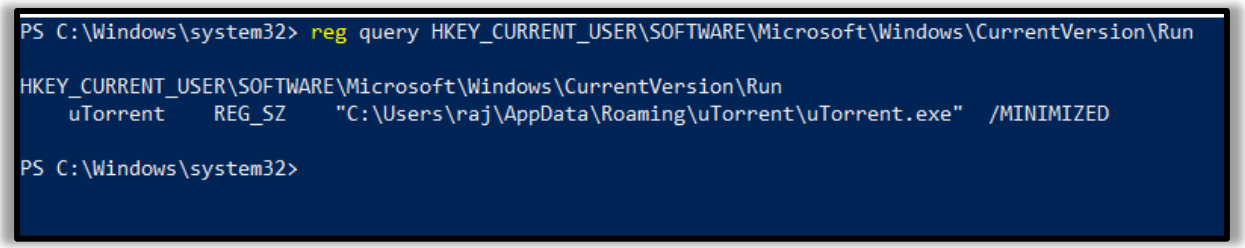
You can also view the registry of the Local Machine of the Run key in the PowerShell, by running it as an administrator and then type
'reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' and press enter.

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



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
```



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 differentcommand. 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
```

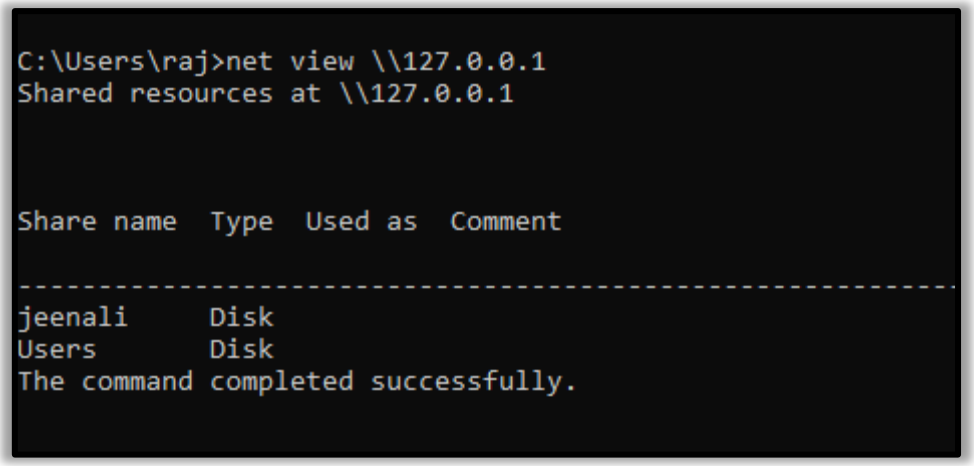
File Sharing

As an incident responder you should make sure that every file share is accountable and reasonable and there in 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.

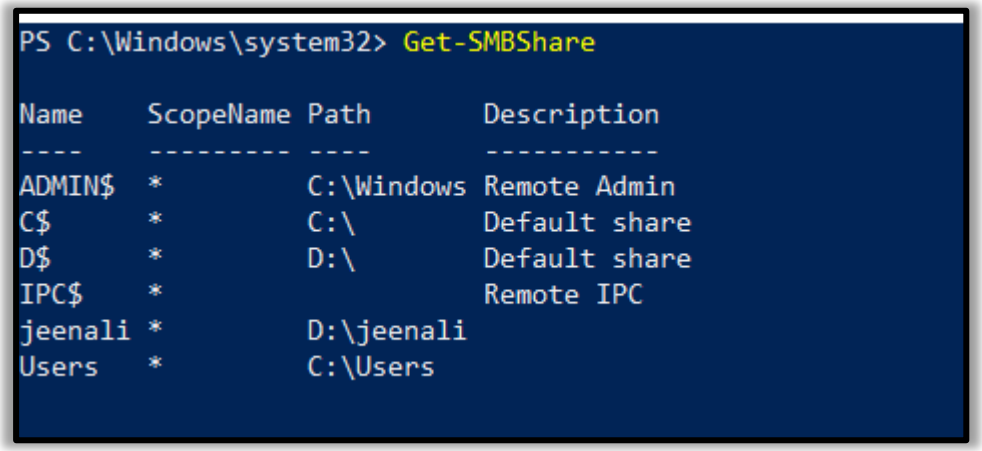
```
net view \\127.0.0.1
```



SMBShare

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

```
Get-SMBShare
```



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"
```

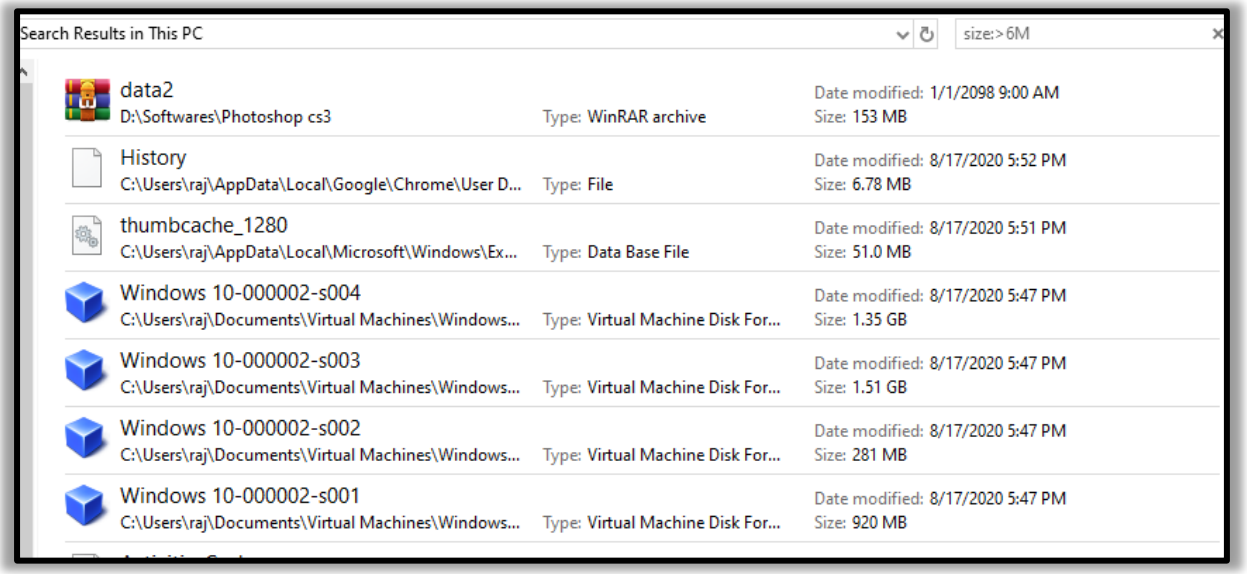
```
C:\Users\raj>forfiles /D -10 /S /M *.exe /C "cmd /c echo @ext @fname @fdate"

"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\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' 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.

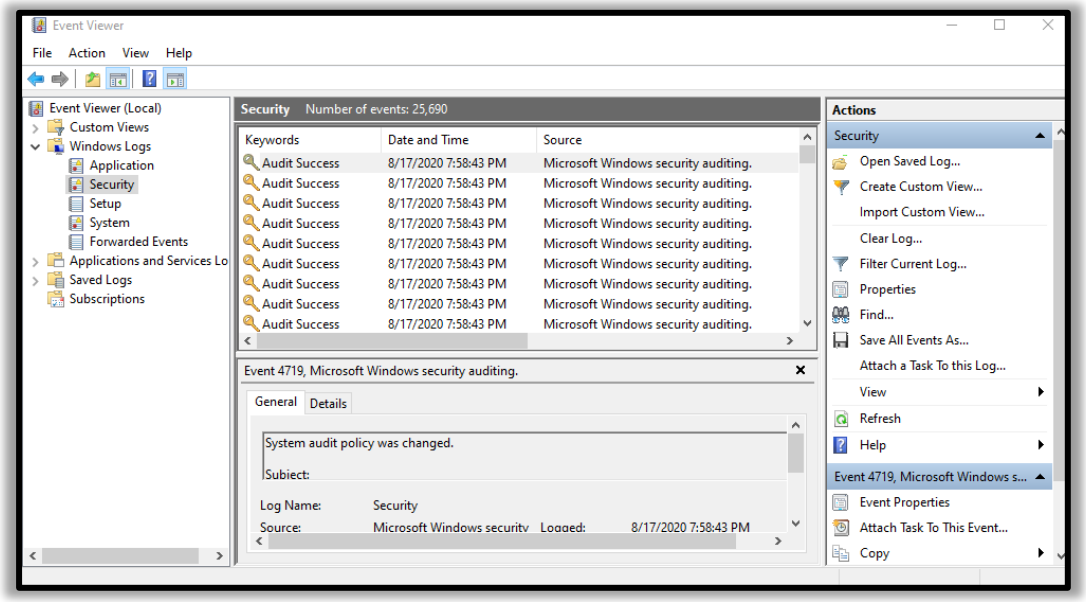
```
net session
```

```
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                             0 00:02:31
The command completed successfully.


C:\Users\Administrator>
```

Log Enteries

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 OAlerts
     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: OAlerts

   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...
```