VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

School of Information Technology & Engineering

WINTER 2022 - 23

Programme : B.Tech **Due Date : 11-03-2022**
Course Title : Information Security Management **Course Code : CSE3502**

Name: SHUBHAM AGARWAL
RegNo: 19BIT0010

Q1) Information Security Incident Management (use the NIST checklist and DOS, Powershell commands)

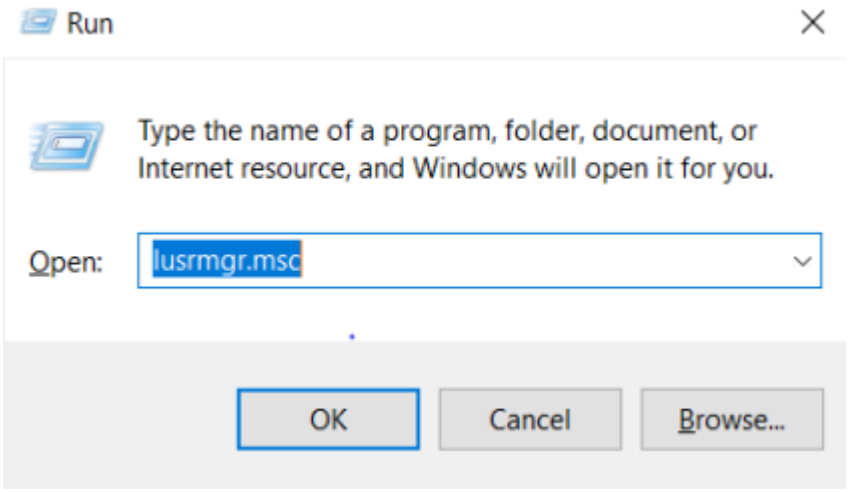
ANS:

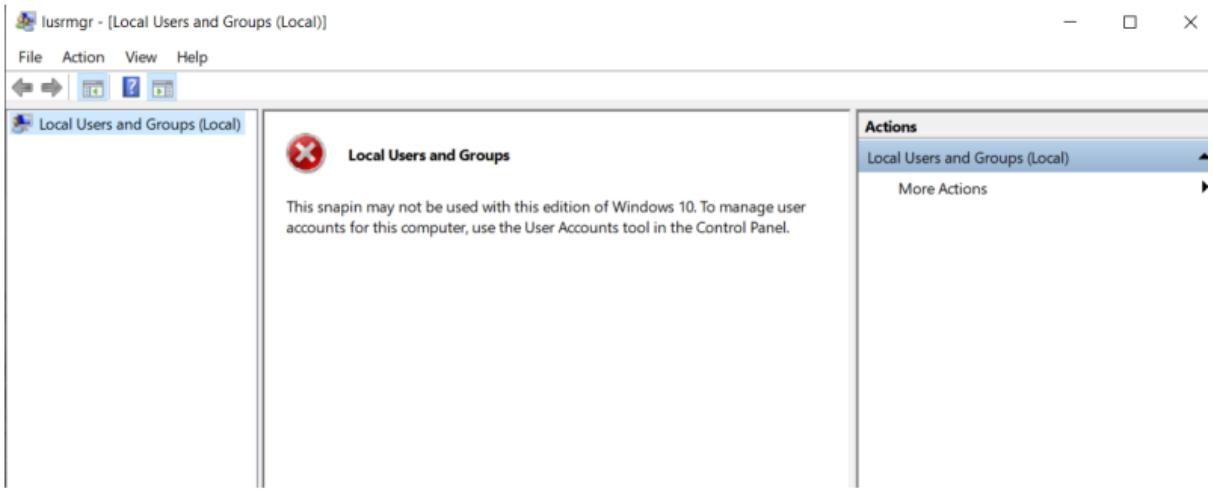
I. Firstly, we can use NIST checklist to complete three phases of incident management. Once all the steps are completed the system is incident free.
II. For the detection phase I will use DOS and powershell. The first step in this phase is to check for the list of users. This can be done by typing lusrmgr.msr command in run window.
III. It can also do this by typing net user command in command prompt.
IV. Next step is to manage local user groups in a system using net local group administrators.
V. Next I will use powershell to get local users details.
VI. To display all the process running on the system I will use task Manager.
VII. To get all the active process running on the computer use command get-process on the powershell.
VIII.To get the process details such as parent process id, name and it's process id use command wmic process get name, parentprocessid, processid.
IX. To display the services offered by the operating system, type services.msc in run window.
X. To display the current services I will use command net start in command prompt. To get the details of the services I will use sc query | more.
XI. Now I will use Task Scheduler to enable or disable any task and to check for incidents.
XII. To get all the scheduled task type schtasks in command prompt.
XIII.To display all startup application, type wmic startup get caption, command in powershell.

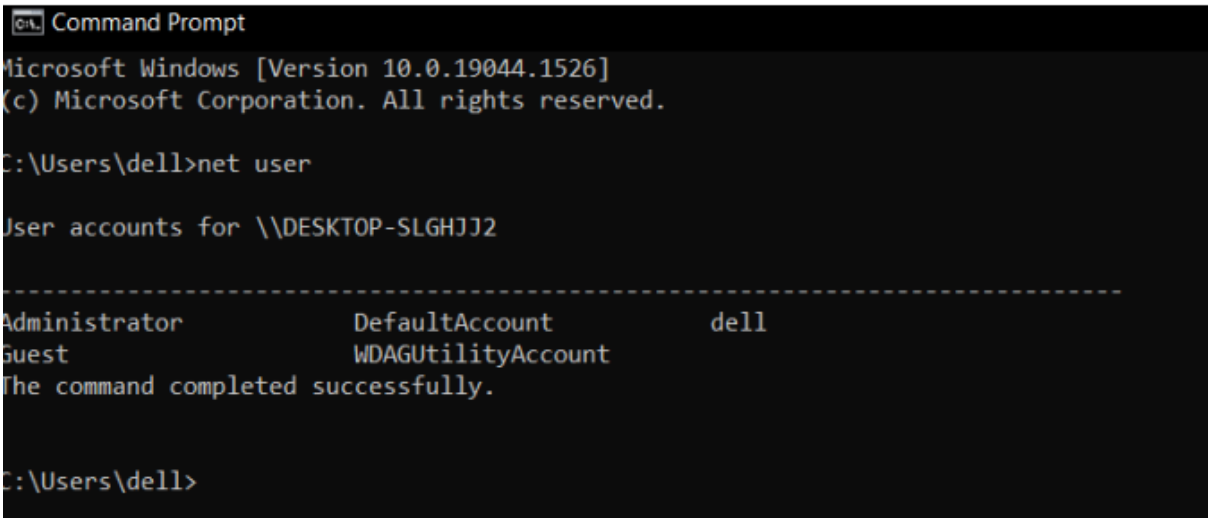
XIV.Now I will verify all the ports for incident, using netstat ano command. XV. Next I will verify the configuration settings, using the command netsh firewall show config in command prompt. To view the current profile settings use command netsh advfirewall show currentprofile. XVI.To display the session details that are created with other systems, use command net use. XVII.To view open session of the system, use command net session. XVIII.For log entries I will use the tool event viewer, it can open using eventvwr.msc in run window.

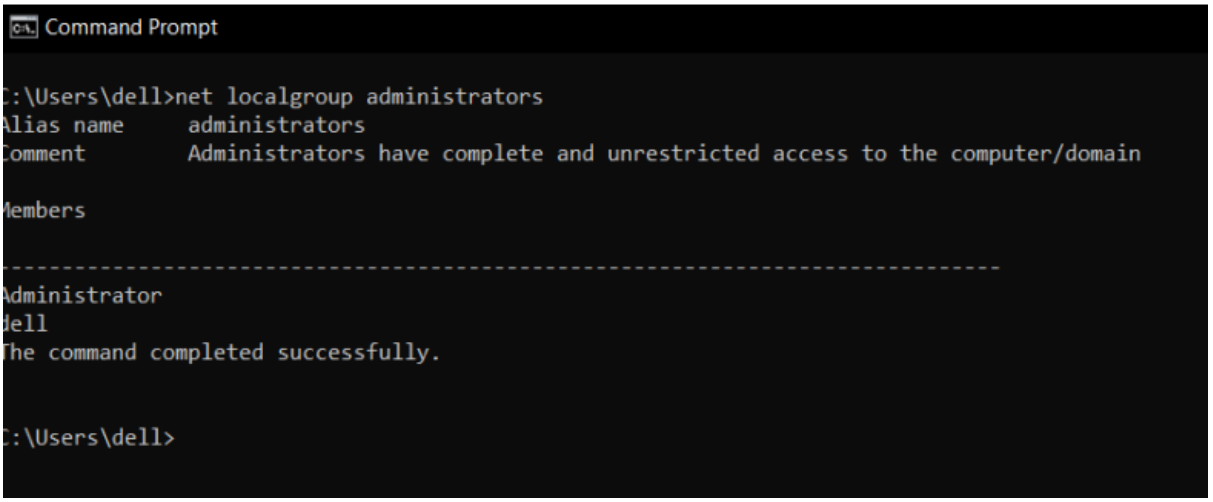
OUPUT:

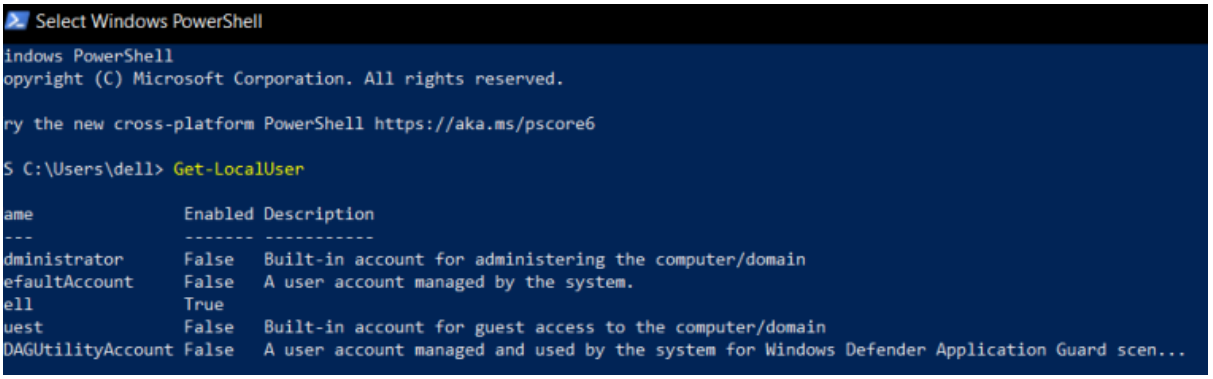
	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

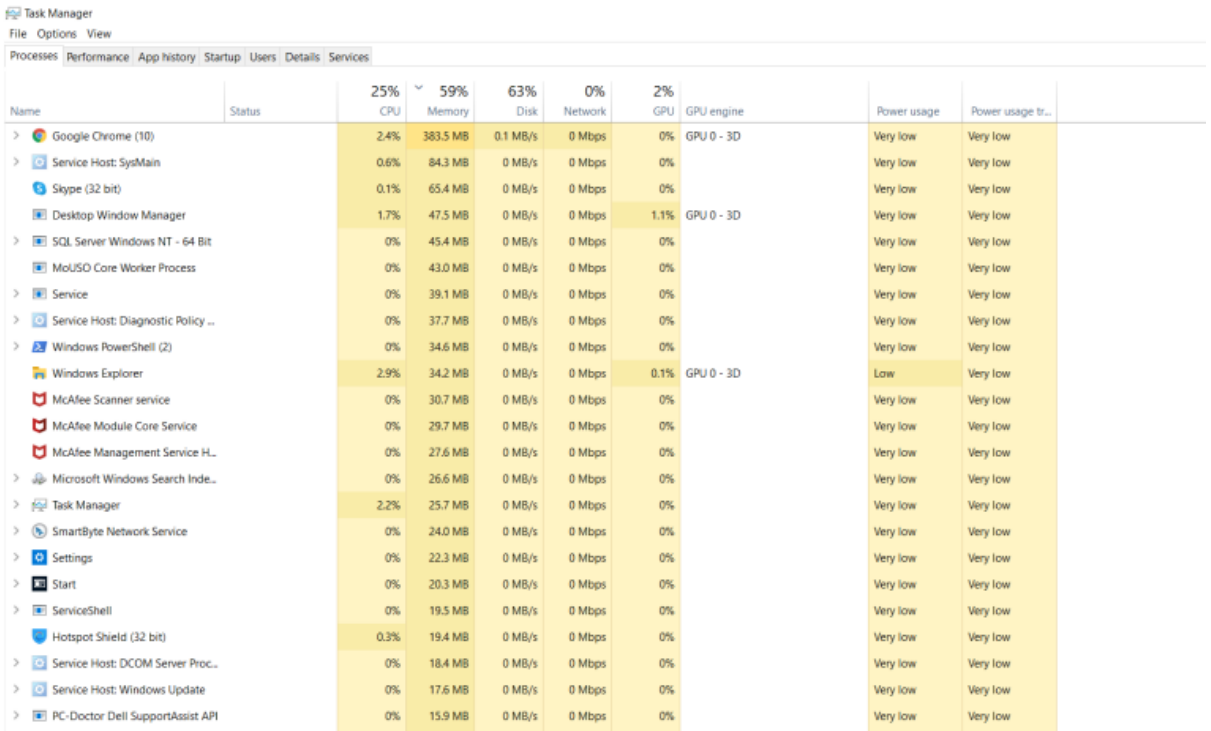

Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
lusrmgr.msc
OK
Cancel
Browse...


lusrmgr - [Local Users and Groups (Local)]
File Action View Help
Local Users and Groups (Local)
Local Users and Groups
This snapin may not be used with this edition of Windows 10. To manage user accounts for this computer, use the User Accounts tool in the Control Panel.
Actions
Local Users and Groups (Local)
More Actions


Command Prompt
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.
C:\Users\dell>net user
User accounts for \\DESKTOP-SLGHJJ2
Administrator DefaultAccount dell
Guest WDAGUtilityAccount
The command completed successfully.
C:\Users\dell>


Command Prompt
C:\Users\dell>net localgroup administrators
Alias name administrators
Comment Administrators have complete and unrestricted access to the computer/domain
Members
Administrator
dell
The command completed successfully.
C:\Users\dell>

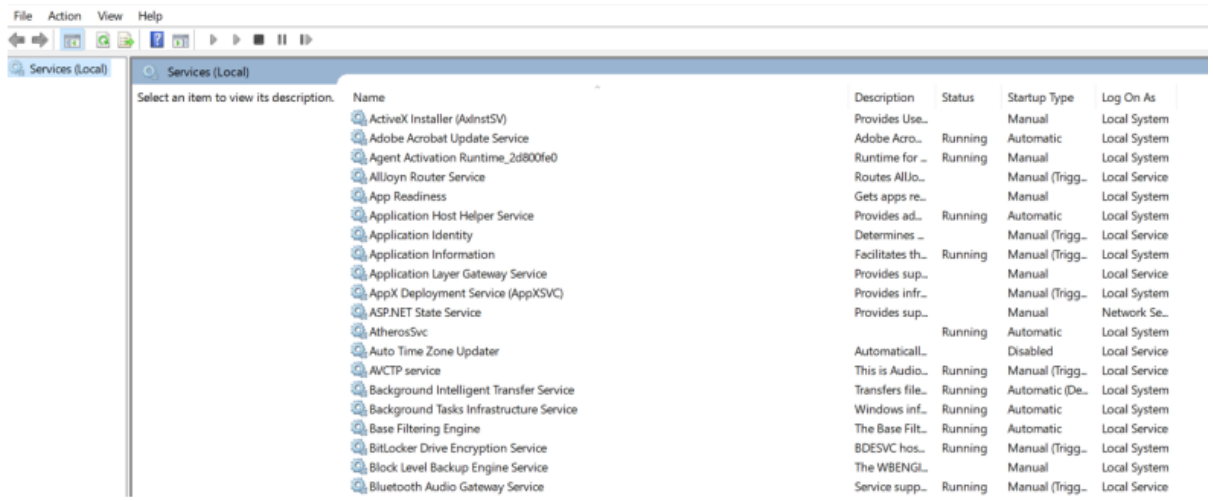

Select Windows PowerShell
indows PowerShell
opyright (C) Microsoft Corporation. All rights reserved.
ry the new cross-platform PowerShell https://aka.ms/pscore6
S C:\Users\dell> Get-LocalUser
ame Enabled Description
dministrator False Built-in account for administering the computer/domain
efaultAccount False A user account managed by the system.
ell True
uest False Built-in account for guest access to the computer/domain
DAGUtilityAccount False A user account managed and used by the system for Windows Defender Application Guard scen...

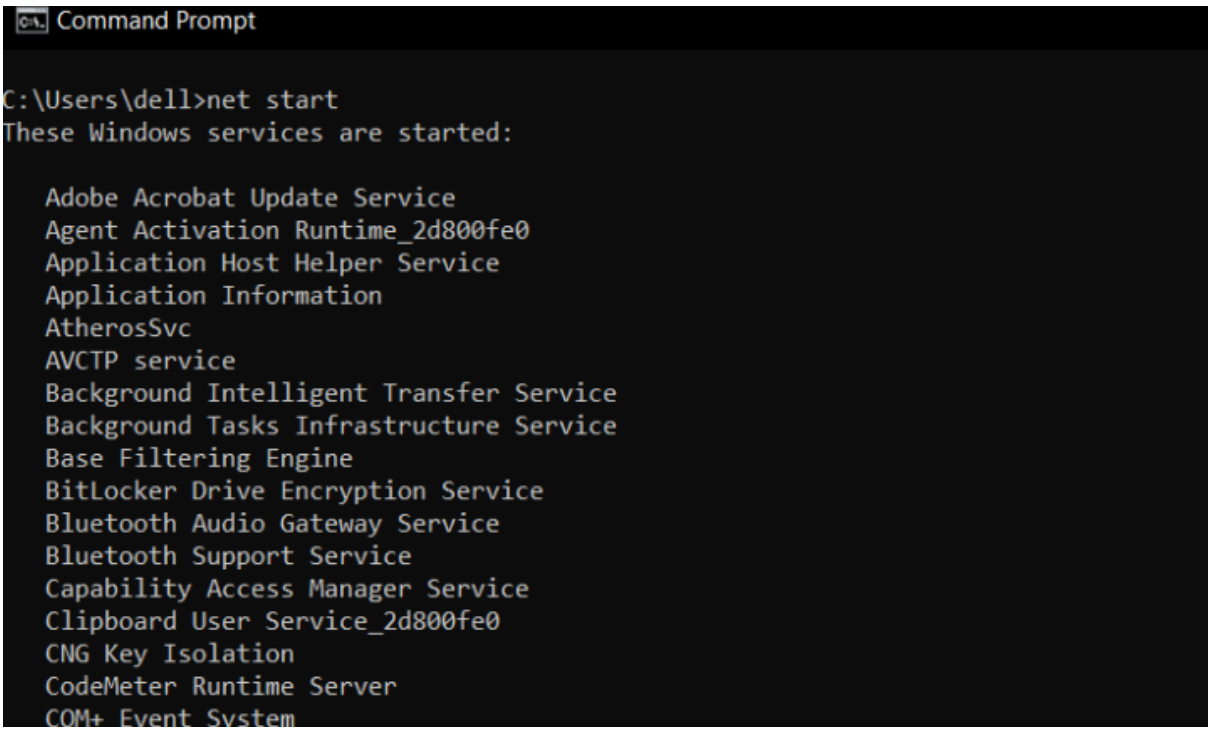

Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Name Status 25% CPU 59% Memory 63% Disk 0% Network 2% GPU GPU engine Power usage Power usage tr...
Google Chrome (10) 2.4% 383.5 MB 0.1 MB/s 0 Mbps 0% GPU 0 - 3D Very low Very low
Service Host: SysMain 0.6% 84.3 MB 0 MB/s 0 Mbps 0% Very low Very low
Skype (32 bit) 0.1% 65.4 MB 0 MB/s 0 Mbps 0% Very low Very low
Desktop Window Manager 1.7% 47.5 MB 0 MB/s 0 Mbps 1.1% GPU 0 - 3D Very low Very low
SQL Server Windows NT - 64 Bit 0% 45.4 MB 0 MB/s 0 Mbps 0% Very low Very low
MoUSO Core Worker Process 0% 43.0 MB 0 MB/s 0 Mbps 0% Very low Very low
Service 0% 39.1 MB 0 MB/s 0 Mbps 0% Very low Very low
Service Host: Diagnostic Policy ... 0% 37.7 MB 0 MB/s 0 Mbps 0% Very low Very low
Windows PowerShell (2) 0% 34.6 MB 0 MB/s 0 Mbps 0% Very low Very low
Windows Explorer 2.9% 34.2 MB 0 MB/s 0 Mbps 0.1% GPU 0 - 3D Low Very low
McAfee Scanner service 0% 30.7 MB 0 MB/s 0 Mbps 0% Very low Very low
McAfee Module Core Service 0% 29.7 MB 0 MB/s 0 Mbps 0% Very low Very low
McAfee Management Service H... 0% 27.6 MB 0 MB/s 0 Mbps 0% Very low Very low
Microsoft Windows Search Inde... 0% 26.6 MB 0 MB/s 0 Mbps 0% Very low Very low
Task Manager 2.2% 25.7 MB 0 MB/s 0 Mbps 0% Very low Very low
SmartByte Network Service 0% 24.0 MB 0 MB/s 0 Mbps 0% Very low Very low
Settings 0% 22.3 MB 0 MB/s 0 Mbps 0% Very low Very low
Start 0% 20.3 MB 0 MB/s 0 Mbps 0% Very low Very low
ServiceShell 0% 19.5 MB 0 MB/s 0 Mbps 0% Very low Very low
Hotspot Shield (32 bit) 0.3% 19.4 MB 0 MB/s 0 Mbps 0% Very low Very low
Service Host: DCOM Server Proc... 0% 18.4 MB 0 MB/s 0 Mbps 0% Very low Very low
Service Host: Windows Update 0% 17.6 MB 0 MB/s 0 Mbps 0% Very low Very low
PC-Doctor Dell SupportAssist API 0% 15.9 MB 0 MB/s 0 Mbps 0% Very low Very low

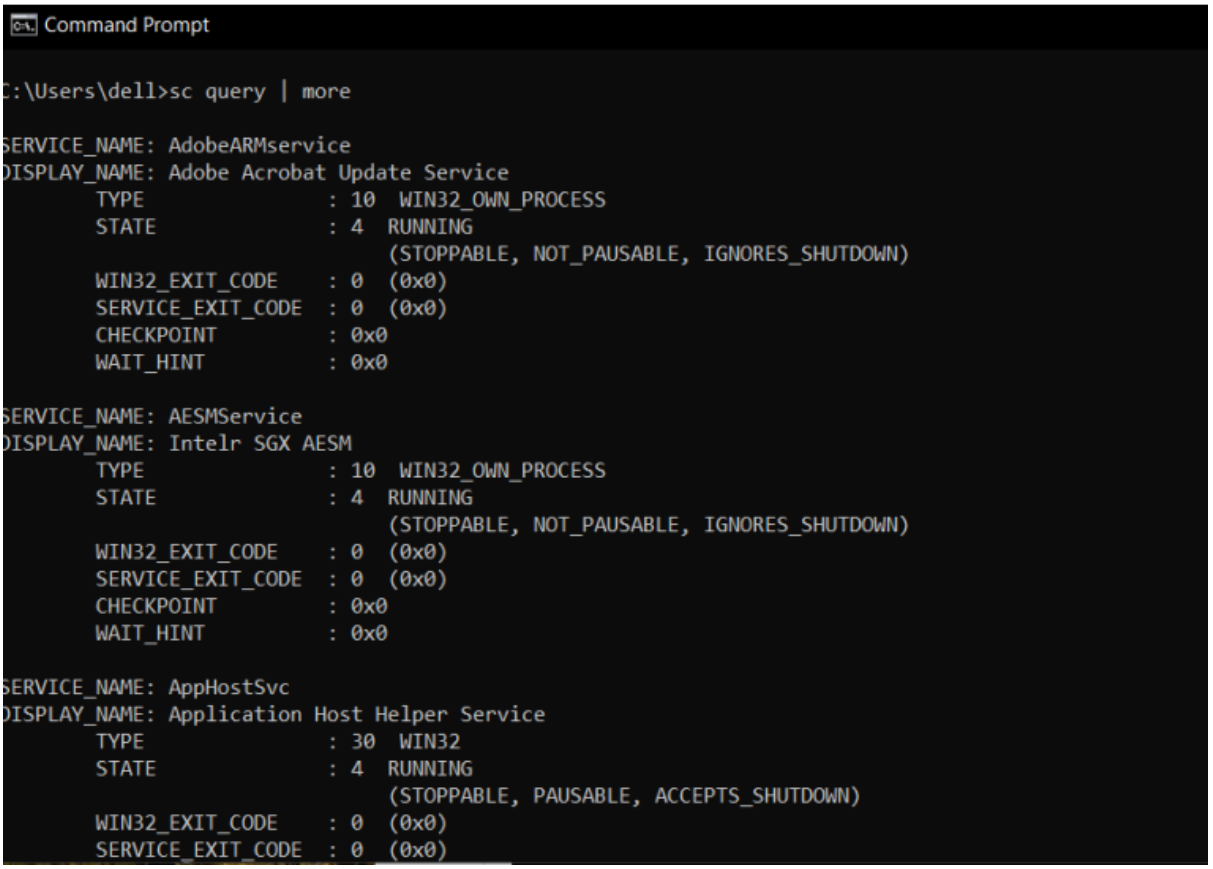
```
PS C:\Users\dell> get-process

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
    163       9     2524       3712               3544   0 AdminService
    178      10     2736       2784               9840   0 aesm_service
    494      26    13528      34560       1.41   27288   4 ApplicationFrameHost
    136       8     1276       1680               3536   0 armsvc
    298      17    24896      48876       1.06   5204   4 chrome
    310      17    21468      54100       2.41  10224   4 chrome
    217      13    12044      27264       0.23  11248   4 chrome
    376      30    12788      34040      15.05  12476   4 chrome
    557      28   135108     155560      55.75  17592   4 chrome
    177       9     2000       7880       0.08  18324   4 chrome
   1448      53    91840     165528      56.42  23960   4 chrome
    529      21   169944     242116     106.14  26092   4 chrome
    280      17     7356      20556       0.36  26844   4 chrome
    218      13     6972      17160       0.16  27196   4 chrome
     73       5     2484       4564       0.05  10844   4 cmd
   1195      84    96144      42688               3676   0 cmw_srv
    351      22    12756      15664              11240   0 CodeMeter
    155      10     6712       2584               6904   0 conhost
    275      14     6148      17960       0.84  10652   4 conhost
    270      14     7524      19832       0.52  16944   4 conhost
    106       7     6356       5776       0.05  17296   4 conhost
    103       7     6264       5584              23520   0 conhost
    529      45    32820      54908      15.25  14164   4 Cortana
    993      30     2244       3412                768   0 csrss
    768      23     2736       6940              13772   4 csrss
    533      17     5200      22216      22.03  12416   4 ctfmon
    420      19     5704       8960               4448   0 dasHost
    168       9     2184       2088               9288   0 DDVCollectorSvcApi
    370      21    25544      17644              14780   0 DDVDataCollector
    275      17    17768       7176               5832   0 DDVRulesProcessor
    676      35    31420      26548              14308   0 DeliveryService
   1501      77    94940      41828               8368   0 DellSupportAssistRemedationService
    212      17     3988       6624               5976   0 dllhost
    253      16     4156      12604       1.20  13460   4 dllhost
    137       8     1920       8748       0.36  16744   4 dllhost
     54       6     1372       4248       1.08  26120   4 dptf_helper
    829      67   113696      46408              11912   0 Dsapi
   1426      47    77020      96592              10520   4 dwm
    129       8     1824       2872               3908   0 esif_uf
    539      33    18936      52396       4.03   5020   4 explorer
   3039     106    98748     177744     142.39  30436   4 explorer
```

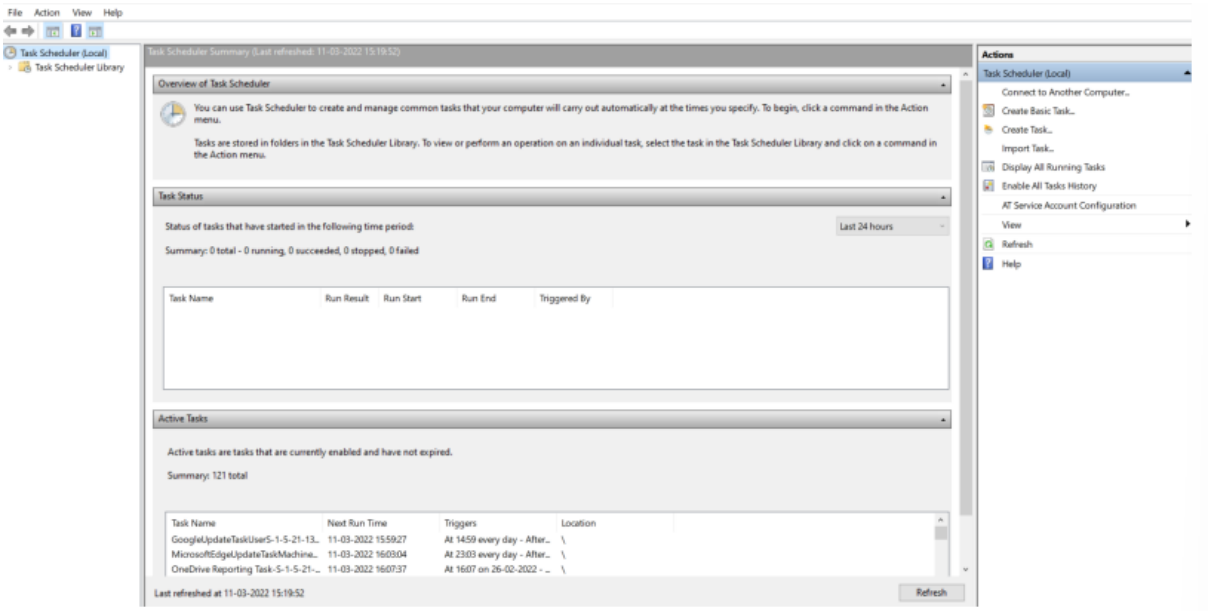
Windows PowerShell

```
S C:\Users\dell> wmic process get name,parentprocessid,processid
lame                                  ParentProcessId  ProcessId
ystem Idle Process                    0                0
ystem                                 0                4
egistry                               4                100
mss.exe                               4                504
srss.exe                              752              768
ininit.exe                            752              852
ervices.exe                           852              992
sass.exe                              852              1012
vchost.exe                            992              688
ontdrvhost.exe                        852              724
UDFHost.exe                           992              1048
vchost.exe                            992              1092
vchost.exe                            992              1156
vchost.exe                            992              1304
vchost.exe                            992              1336
vchost.exe                            992              1464
vchost.exe                            992              1504
```




Command Prompt
C:\Users\dell>net start
These Windows services are started:
Adobe Acrobat Update Service
Agent Activation Runtime_2d800fe0
Application Host Helper Service
Application Information
AtherosSvc
AVCTP service
Background Intelligent Transfer Service
Background Tasks Infrastructure Service
Base Filtering Engine
BitLocker Drive Encryption Service
Bluetooth Audio Gateway Service
Bluetooth Support Service
Capability Access Manager Service
Clipboard User Service_2d800fe0
CNG Key Isolation
CodeMeter Runtime Server
COM+ Event System


Command Prompt
C:\Users\dell>sc query | more
SERVICE_NAME: AdobeARMservice
DISPLAY_NAME: Adobe Acrobat Update Service
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: AESMService
DISPLAY_NAME: Intelr SGX AESM
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: AppHostSvc
DISPLAY_NAME: Application Host Helper Service
TYPE : 30 WIN32
STATE : 4 RUNNING
(STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)




```
Command Prompt
perable program or batch file.

:\Users\dell>schtasks

Folder: \
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
BlueStacksHelper_nxt                     11-03-2022 19:39:42    Ready
Dell SupportAssistAgent AutoUpdate       14-03-2022 09:10:55    Ready
GoogleUpdateTaskUserS-1-5-21-1323162510- 12-03-2022 14:59:27    Ready
GoogleUpdateTaskUserS-1-5-21-1323162510- 11-03-2022 15:59:27    Ready
McAfeeLogon                              N/A                    Ready
OneDrive Reporting Task-S-1-5-21-1323162 11-03-2022 16:07:37    Ready
OneDrive Standalone Update Task-S-1-5-21 12-03-2022 16:09:37    Ready
SmartByte Telemetry                      N/A                    Running
User_Feed_Synchronization-{7FAA3BC6-9B7A 11-03-2022 20:02:49    Ready

Folder: \Agent Activation Runtime
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
S-1-5-21-1323162510-1186768033-154788936 N/A                    Disabled

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
======================================== ====================== ===============
```

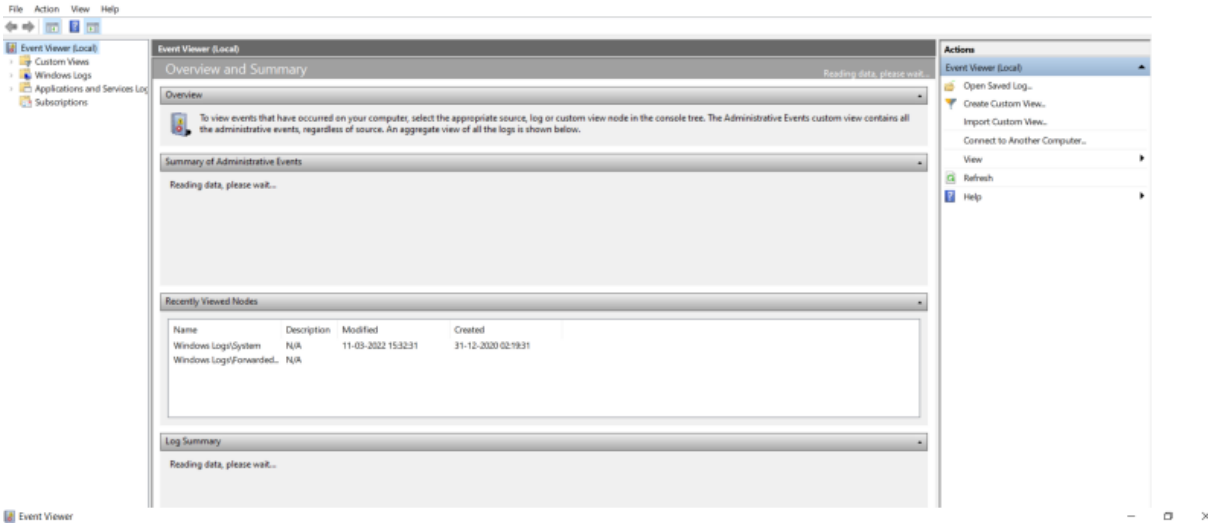
```
PS C:\Users\dell> wmic startup get caption,command
Caption                  Command

OneDrive                 "C:\Users\dell\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background

Google Update            "C:\Users\dell\AppData\Local\Google\Update\1.3.36.122\GoogleUpdateCore.exe"

com.squirrel.Teams.Teams  C:\Users\dell\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe" --process-start-args "--system-
initiated"
Figma Agent              "C:\Users\dell\AppData\Local\FigmaAgent\figma_agent.exe"

Skype for Desktop        C:\Program Files (x86)\Microsoft\Skype for Desktop\Skype.exe

Spotify                  C:\Users\dell\AppData\Roaming\Spotify\Spotify.exe --autostart --minimized

SecurityHealth           %windir%\system32\SecurityHealthSystray.exe

DellMobileConnectWelcome  "C:\Program Files\Dell\DellMobileConnectDrivers\DellMobileConnectWStartup.exe"

IAStorIcon               "C:\Program Files\Intel\Intel(R) Rapid Storage Technology\IAStorIconLaunch.exe" "C:\Program Files\Intel\Intel(R)
Rapid Storage Technology\IAStorIcon.exe" 60
QuickSet                 c:\Program Files\Dell\QuickSet\QuickSet.exe

RTHDVCPL                 "C:\Program Files\Realtek\Audio\HDA\RtkNGUI64.exe" -s

RtHDVBg_PushButton       "C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe" /IM

WavesSvc                 "C:\Program Files\Waves\MaxxAudio\WavesSvc64.exe" -Jack
```

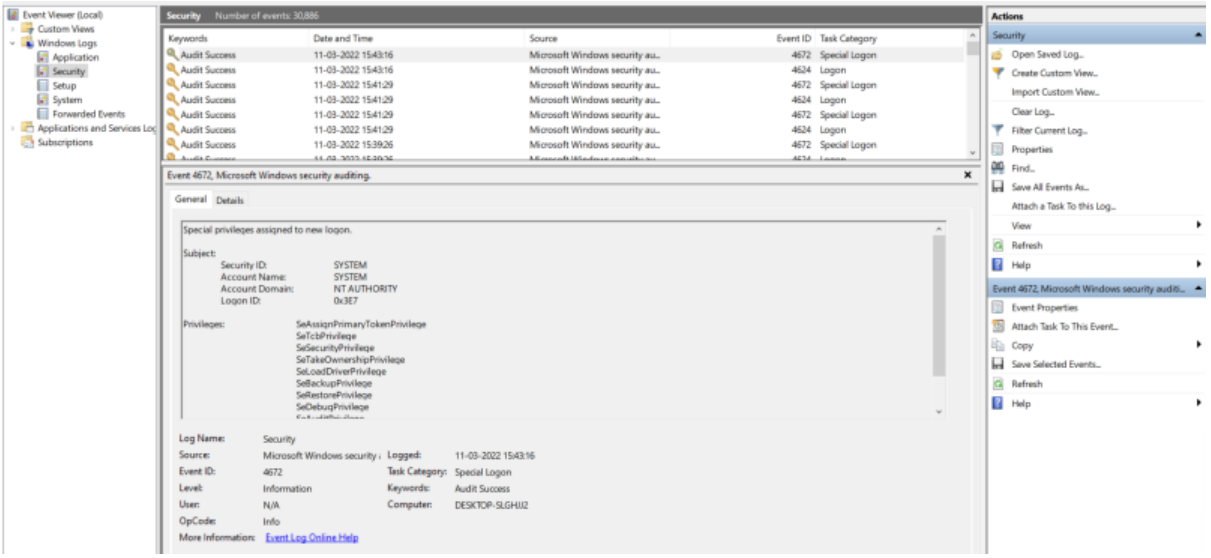
Command Prompt

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

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1092
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING       4736
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING       4736
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       9140
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5700           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:6646           0.0.0.0:0              LISTENING       22376
  TCP    0.0.0.0:22350          0.0.0.0:0              LISTENING       11240
  TCP    0.0.0.0:26060          0.0.0.0:0              LISTENING       3308
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       1012
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       852
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1464
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       1632
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       1348
  TCP    0.0.0.0:49692          0.0.0.0:0              LISTENING       992
  TCP    127.0.0.1:7335         0.0.0.0:0              LISTENING       24040
```

```
Command Prompt

C:\Users\dell>netsh firewall show config

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

IMPORTANT: "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at https://go.microsoft.com/fwlink/?linkid=121488 .
```

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

There are no entries in the list.


C:\Users\dell>net session
System error 5 has occurred.

Access is denied.
```

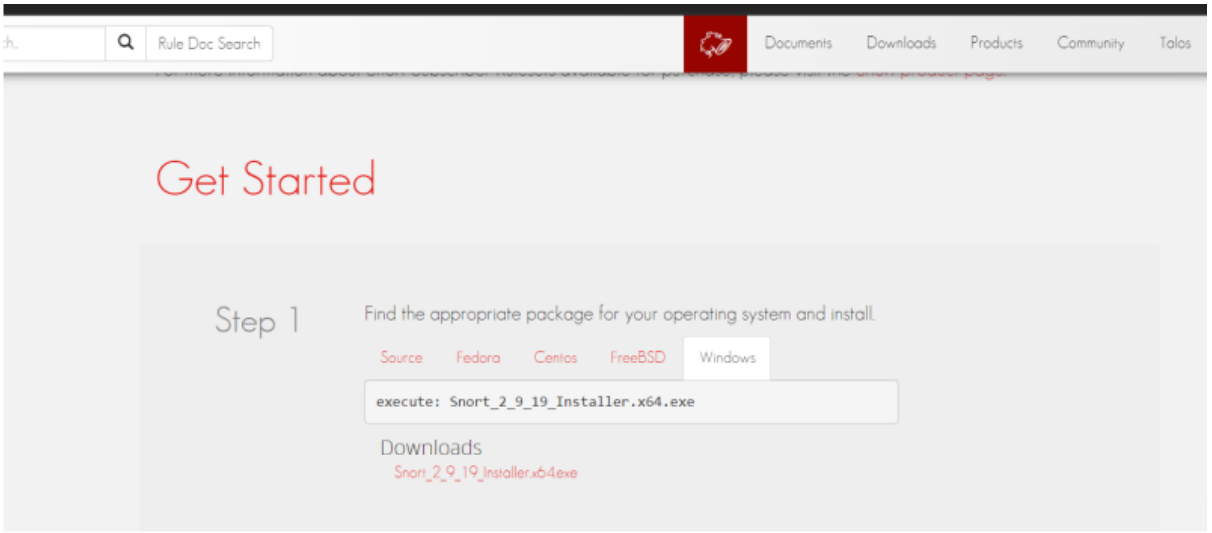





```
PS C:\Users\dell> Get-EventLog -List

  Max(K) Retain OverflowAction       Entries Log
  ------ ------ --------------       ------- ---
  20,480      0 OverwriteAsNeeded     38,978 Application
     512      7 OverwriteOlder            57 Dell
  20,480      0 OverwriteAsNeeded           0 HardwareEvents
     512      7 OverwriteOlder              0 IntelAudioServiceLog
     512      7 OverwriteOlder              0 Internet Explorer
  20,480      0 OverwriteAsNeeded           0 Key Management Service
  16,384      0 OverwriteAsNeeded           0 ODiag
  16,384      0 OverwriteAsNeeded         587 OSession
                                              Security
  20,480      0 OverwriteAsNeeded     29,679 System
     512      7 OverwriteOlder           742 Thycotic Management Server
     512      0 OverwriteAsNeeded         55 Veeam Agent
  15,360      0 OverwriteAsNeeded      2,376 Windows PowerShell
```

Q2) Implementation of Intrusion Detection/Prevention using SNORT

OUTPUT:



Downloading and Installing Npcap Free Edition

```
Select Command Prompt - snort.exe
C:\Users\dell>cd ..

C:\Users>cd ..

C:\>cd snort

C:\Snort>cd bin

C:\Snort\bin>snort.exe
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{4DE2D76D-5117-4503-B5AD-D0BFA50F0BD8}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.19-WIN64 GRE (Build 85)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

Commencing packet processing (pid=10652)
```