



# MANUAL DE LABORATORIO

SC-203 FUNDAMENTOS DE SISTEMAS  
OPERATIVOS

## Contents

Laboratorio #7 - Clase 11.....	2
Tema .....	2
Tiempo estimado .....	2
Objetivo.....	2
Requerimientos Previos .....	2
Procedimiento.....	2
Paso 1 - Uso del Resource Monitor.....	2
Paso 2 - Descarga Sysinternals desde el sitio <a href="https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite">https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite</a> haciendo clic en el link Download Sysinternals Suite (41.4MB) ...	4
Paso 3 - Comando Autoruns.exe .....	5
Paso 5 - Ejecute el comando Process Explorer - procexp.exe .....	5
Paso 6 - Ejecute el comando TCPView .....	6

# Laboratorio #7 – Clase 11

## Tema

Opciones avanzadas en Windows 10.

## Tiempo estimado

Se estima que el estudiante requerirá **60 minutos** para completar el laboratorio.

## Objetivo

Aprender sobre el uso de opciones avanzadas de monitoreo del rendimiento e información del hardware y aplicaciones en ejecución.

## Requerimientos Previos

Ejecutar desde Windows 10.

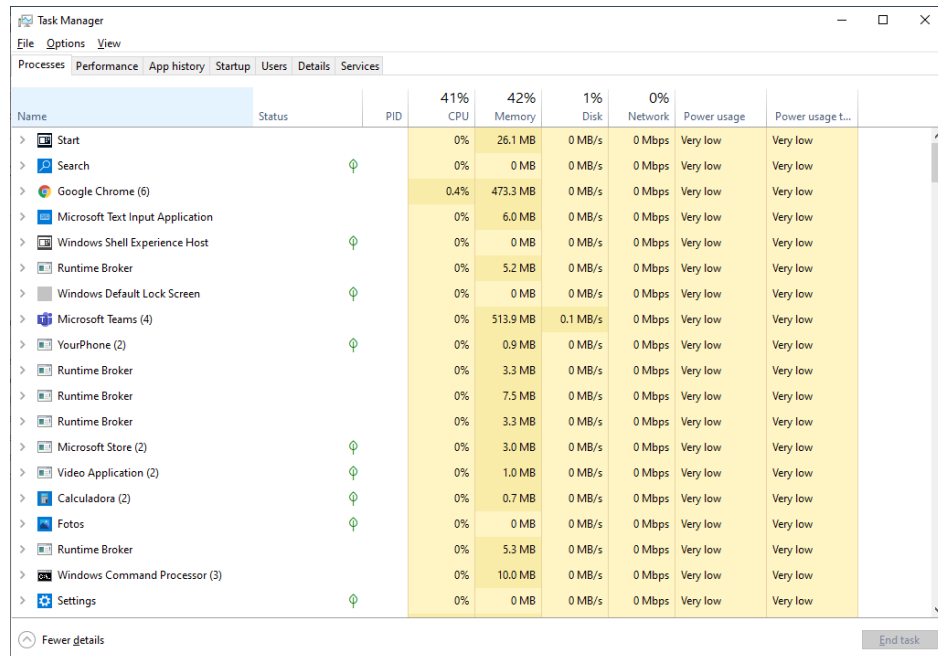
## Entregable

En un documento guarde las evidencias, 1 por cada paso. Cargue el documento en la actividad correspondiente del Campus Virtual.

## Procedimiento

### Paso 1 – Uso del Resource Monitor

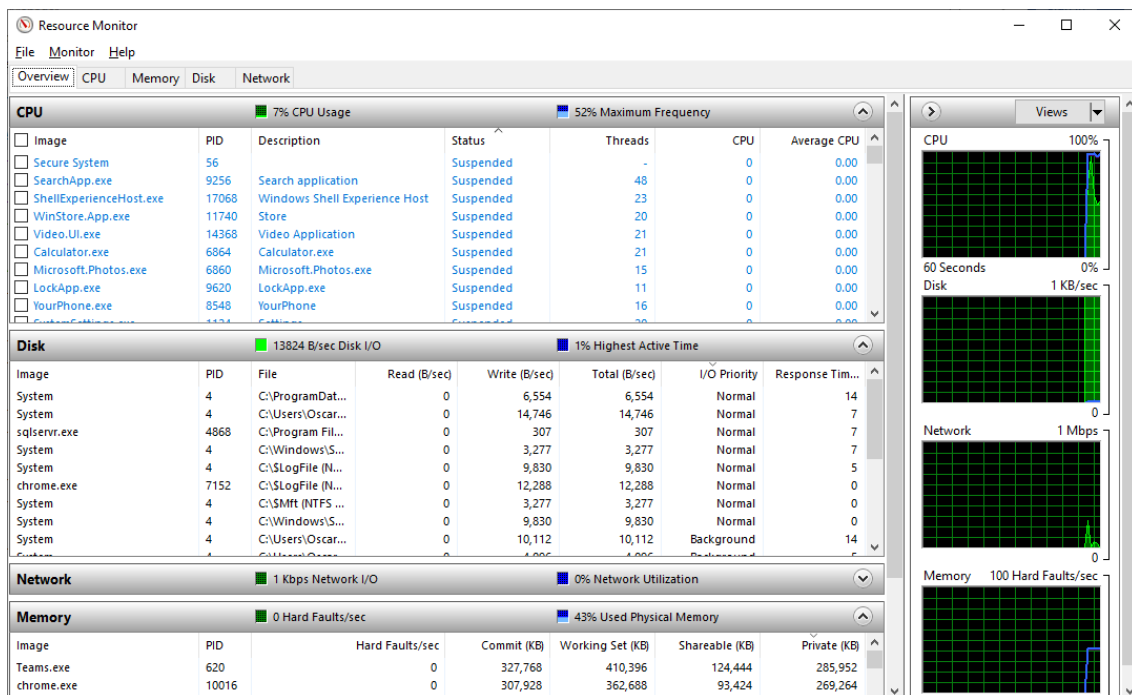
En la barra de tareas, haga clic con el botón derecho y escoja la opción “Task Manager”.



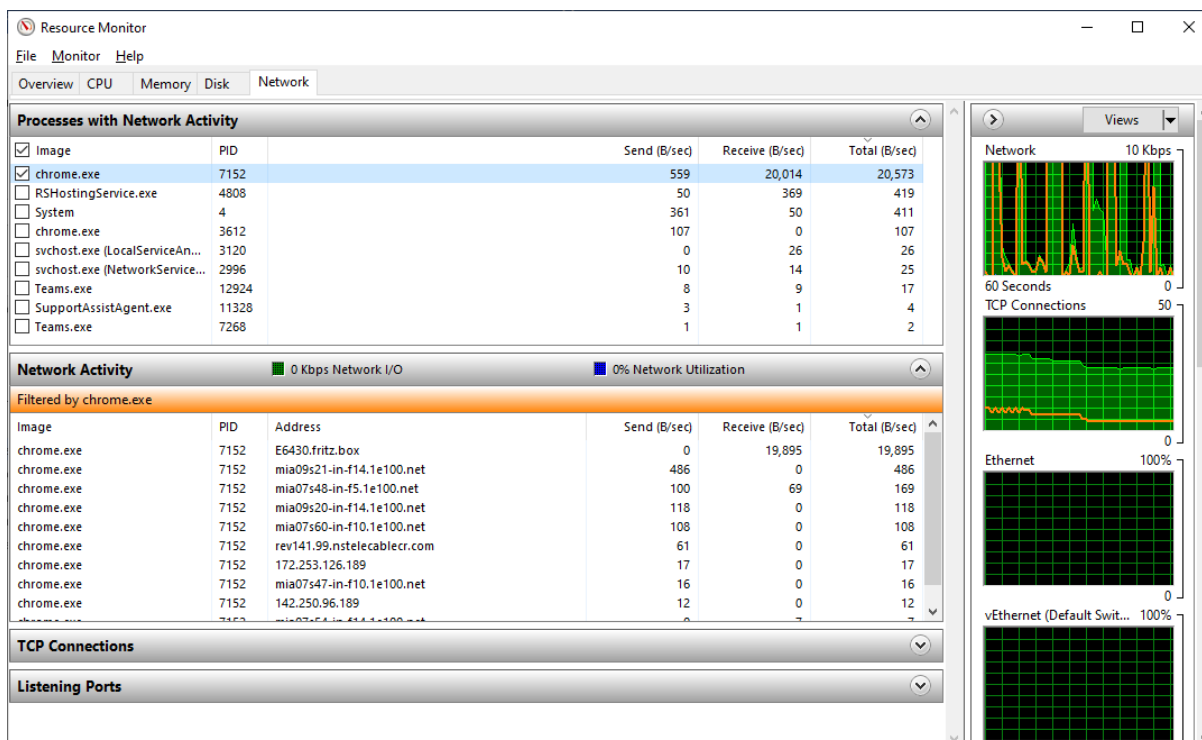
The screenshot shows the Windows Task Manager window with the 'Performance' tab selected. The window title is 'Task Manager'. The menu bar includes 'File', 'Options', and 'View'. The tabs at the top are 'Processes', 'Performance', 'App history', 'Startup', 'Users', 'Details', and 'Services'. The 'Performance' tab is active, displaying a table of resource usage for various processes. The table has columns for Name, Status, PID, CPU, Memory, Disk, Network, Power usage, and Power usage t... (truncated). The processes listed include Start, Search, Google Chrome (6), Microsoft Text Input Application, Windows Shell Experience Host, Runtime Broker, Windows Default Lock Screen, Microsoft Teams (4), YourPhone (2), Runtime Broker, Runtime Broker, Runtime Broker, Microsoft Store (2), Video Application (2), Calculadora (2), Fotos, Runtime Broker, Windows Command Processor (3), and Settings. The CPU usage is 41%, Memory is 42%, Disk is 1%, and Network is 0%. Power usage is Very low for all processes.

Name	Status	PID	CPU	Memory	Disk	Network	Power usage	Power usage t...
Start			0%	26.1 MB	0 MB/s	0 Mbps	Very low	Very low
Search			0%	0 MB	0 MB/s	0 Mbps	Very low	Very low
Google Chrome (6)			0.4%	473.3 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Text Input Application			0%	6.0 MB	0 MB/s	0 Mbps	Very low	Very low
Windows Shell Experience Host			0%	0 MB	0 MB/s	0 Mbps	Very low	Very low
Runtime Broker			0%	5.2 MB	0 MB/s	0 Mbps	Very low	Very low
Windows Default Lock Screen			0%	0 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Teams (4)			0%	513.9 MB	0.1 MB/s	0 Mbps	Very low	Very low
YourPhone (2)			0%	0.9 MB	0 MB/s	0 Mbps	Very low	Very low
Runtime Broker			0%	3.3 MB	0 MB/s	0 Mbps	Very low	Very low
Runtime Broker			0%	7.5 MB	0 MB/s	0 Mbps	Very low	Very low
Runtime Broker			0%	3.3 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Store (2)			0%	3.0 MB	0 MB/s	0 Mbps	Very low	Very low
Video Application (2)			0%	1.0 MB	0 MB/s	0 Mbps	Very low	Very low
Calculadora (2)			0%	0.7 MB	0 MB/s	0 Mbps	Very low	Very low
Fotos			0%	0 MB	0 MB/s	0 Mbps	Very low	Very low
Runtime Broker			0%	5.3 MB	0 MB/s	0 Mbps	Very low	Very low
Windows Command Processor (3)			0%	10.0 MB	0 MB/s	0 Mbps	Very low	Very low
Settings			0%	0 MB	0 MB/s	0 Mbps	Very low	Very low

Haga clic en la pestaña “Performance” y luego en la opción “Open Resource Monitor”

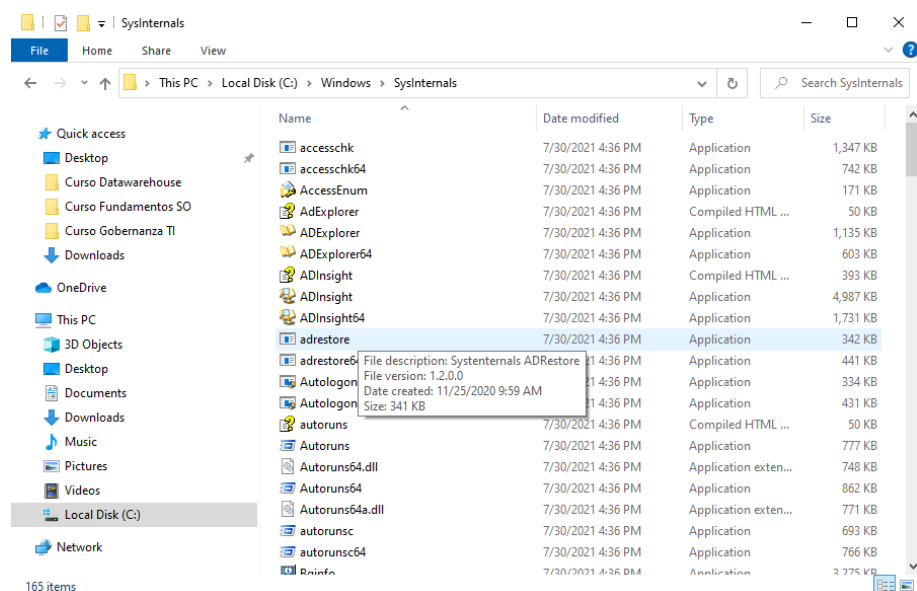


Seleccione la pestaña “Network” y expanda la sección “Network Activity”. De un vistazo general a la información en general al consumo de las columnas Send y Receive, así como los gráficos de consumo “Network” y “TCP Connections”.

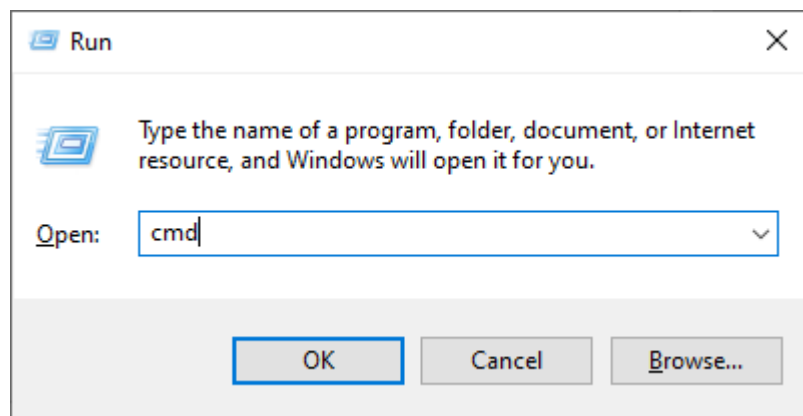


Paso 2 – Descarga Sysinternals desde el sitio <https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite> haciendo clic en el link Download Sysinternals Suite (41.4MB)

Utilizando el Windows Explorer, de doble clic al archivo descargado y copie el contenido en una nueva carpeta con nombre “c:\windows\SysInternals”.



Presione la tecla Windows + R para ejecutar el siguiente comando “CMD”. Vaya a la carpeta creada mediante el comando “cd \windows\SysInternals”.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19042.1110]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Oscar>cd \windows\sysinternals

C:\Windows\SysInternals>
```

Paso 3 – Comando Autoruns.exe

Ejecute el comando “Autoruns.exe”

Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

Filter:

AppInitKnownDLLsWinlogonWinsock ProvidersPrint MonitorsLSA ProvidersNetwork ProvidersWMIOffice

EverythingLogonExplorerInternet ExplorerScheduled TasksServicesDriversCodecsBoot ExecuteImage Hijacks

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
<input checked="" type="checkbox"/> HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				12/7/2019 3:15 AM	
<input checked="" type="checkbox"/> cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	12/10/1953 8:58 PM	
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				7/15/2021 11:29 AM	
<input checked="" type="checkbox"/> Apoint	Alps Pointing-device Driver	(Verified) ALPS ELECTRIC CO...	c:\program files\dellpad\apoin...	12/26/2018 7:57 AM	
<input checked="" type="checkbox"/> Launch LCore	Logitech Gaming Framework	(Verified) Logitech Inc	c:\program files\logitech gamin...	12/19/2016 5:44 PM	
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				7/28/2021 6:10 PM	
<input checked="" type="checkbox"/> IDProtect Monitor	IDProtect Monitor	(Verified) NXP Semiconductors...	c:\program files (x86)\nxp semi...	5/13/2019 3:29 AM	
<input checked="" type="checkbox"/> SunJavaUpdateS...	Java Update Scheduler	(Verified) Oracle America, Inc.	c:\program files (x86)\common ...	6/9/2021 8:56 AM	
<input checked="" type="checkbox"/> HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				7/28/2021 4:31 PM	
<input checked="" type="checkbox"/> CiscoMeetingDae...	Cisco Webex Meetings	(Verified) Cisco WebEx LLC	c:\users\oscar\appdata\local\...	4/8/2021 8:59 PM	
<input checked="" type="checkbox"/> Fimador BCCR			c:\users\oscar\appdata\roami...	8/28/2020 6:43 PM	
<input checked="" type="checkbox"/> GoogleDriveFS	Google Drive	(Verified) Google LLC	c:\program files\google\drive fi...	7/27/2021 9:04 AM	
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				8/11/2020 8:43 PM	
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer	(Verified) Google LLC	c:\program files (x86)\google\c...	7/17/2021 6:07 PM	
<input checked="" type="checkbox"/> Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft...	7/20/2021 8:13 PM	
<input checked="" type="checkbox"/> n/a	Windows host process (Rundl...	(Verified)	c:\windows\system32\windll32...	7/1/1967 10:25 AM	
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				8/11/2020 8:43 PM	
<input checked="" type="checkbox"/> n/a	Windows host process (Rundl...	(Verified)	c:\windows\syswow64\windll3...	8/26/2026 10:58 AM	
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Classes\Protocols\Filter				10/2/2020 7:42 PM	
<input checked="" type="checkbox"/> text/xml	Microsoft Office XML MIME Filter	(Verified) Microsoft Corporation	c:\program files\microsoft offic...	8/15/2020 11:38 AM	
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Classes\Protocols\Handler				10/2/2020 7:42 PM	
<input checked="" type="checkbox"/> mso-minsb-roamin...	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft offic...	9/7/2020 11:29 PM	
<input checked="" type="checkbox"/> mso-minsb.16	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft offic...	9/7/2020 11:29 PM	
<input checked="" type="checkbox"/> osf-roaming.16	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft offic...	9/7/2020 11:29 PM	
<input checked="" type="checkbox"/> osf.16	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft offic...	9/7/2020 11:29 PM	
<input checked="" type="checkbox"/> HKLM\Software\Classes\ShellEx\ContextMenuHandlers				2/13/2021 12:00 PM	

(Escape to cancel) Scanning... Signed Windows Entries Hidden.

Paso 4 – Ejecute el comando Process Explorer – procexp.exe

Desde el Comand Prompt, ejecute el comando “procexp.exe”.

Process Explorer - Sysinternals: www.sysinternals.com [E6430\Oscar]

File Options View Process Find Users Help

<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Secure System	Suspended	184 K	38,604 K	56		
Registry		13,400 K	66,672 K	104		
System Idle Process	94.25	60 K	8 K	0		
System	0.73	204 K	3,332 K	4		
Interrupts	0.37	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,076 K	1,020 K	508		
Memory Compression		1,328 K	167,364 K	2644		
csrss.exe		2,208 K	4,348 K	612		
wininit.exe		1,748 K	4,460 K	720		
services.exe		9,732 K	11,820 K	880		
svchost.exe		30,088 K	40,960 K	532	Host Process for Windows Services	Microsoft Corporation
dllhost.exe		3,252 K	5,148 K	9036		
MoUsCoreWorker.exe		179,348 K	168,784 K	11636		
LockApp.exe	Suspended	15,068 K	50,948 K	9620	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		10,044 K	36,956 K	6763	Runtime Broker	Microsoft Corporation
StartMenuExperienceHost.exe		36,360 K	84,884 K	10544		
RuntimeBroker.exe		6,824 K	27,844 K	15524	Runtime Broker	Microsoft Corporation
SearchApp.exe	Suspended	124,976 K	196,052 K	9256	Search application	Microsoft Corporation
RuntimeBroker.exe		16,480 K	47,320 K	17260	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		6,276 K	25,540 K	13060	Runtime Broker	Microsoft Corporation
SettingSyncHost.exe		2,404 K	6,904 K	16576	Host Process for Setting Synchronization	Microsoft Corporation
TextInputHost.exe		14,800 K	42,208 K	6792		
ShellExperienceHost.exe	Suspended	27,148 K	78,580 K	17068	Windows Shell Experience Host	Microsoft Corporation
RuntimeBroker.exe		7,412 K	31,948 K	17380	Runtime Broker	Microsoft Corporation
ApplicationFrameHost.exe		15,908 K	36,684 K	3236	Application Frame Host	Microsoft Corporation
WinStore.App.exe	Suspended	48,452 K	3,464 K	11740	Store	Microsoft Corporation
RuntimeBroker.exe		6,448 K	26,280 K	1384	Runtime Broker	Microsoft Corporation
Video.UI.exe	Suspended	21,416 K	11,704 K	14368		
RuntimeBroker.exe		2,184 K	10,364 K	17592	Runtime Broker	Microsoft Corporation
UserOOBEBroker.exe		2,196 K	10,352 K	8908	User OOBEBroker	Microsoft Corporation
Calculator.exe	Suspended	24,036 K	3,036 K	6864		

CPU Usage: 5.50% Commit Charge: 52.88% Processes: 239 Physical Usage: 44.50%

## Paso 5 – Ejecute el comando TCPView

Desde el Comand Prompt, ejecute el comando “tcpview.exe”.

TCPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

4 TCP v4 6 TCP v6 4 UDP v4 6 UDP v6

Search

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create
svchost.exe	996	TCP	Listen	0.0.0.0	135	0.0.0.0	0	7/15/2021 11:28:...
System	4	TCP	Listen	172.27.128.1	139	0.0.0.0	0	7/30/2021 2:52:...
System	4	TCP	Listen	192.168.1.56	139	0.0.0.0	0	7/30/2021 2:52:...
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	7/30/2021 2:51:...
System	4	TCP	Listen	192.168.240.1	139	0.0.0.0	0	7/30/2021 2:52:...
LMS.exe	8412	TCP	Listen	0.0.0.0	623	0.0.0.0	0	7/30/2021 2:52:...
sqlservr.exe	4868	TCP	Listen	127.0.0.1	1434	0.0.0.0	0	7/15/2021 11:29:...
vmms.exe	2344	TCP	Listen	0.0.0.0	2179	0.0.0.0	0	7/15/2021 11:28:...
msmdsrv.exe	4928	TCP	Listen	0.0.0.0	2383	0.0.0.0	0	7/15/2021 11:29:...
svchost.exe	2860	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	7/30/2021 2:51:...
TeamViewer_Service.exe	4740	TCP	Listen	127.0.0.1	5939	0.0.0.0	0	7/15/2021 11:29:...
System	4	TCP	Listen	127.0.0.1	8884	0.0.0.0	0	7/15/2021 11:32:...
SupportAssistAgent.exe	11328	TCP	Listen	127.0.0.1	9012	0.0.0.0	0	7/15/2021 11:32:...
Ighub_updater.exe	4504	TCP	Listen	127.0.0.1	9100	0.0.0.0	0	7/15/2021 11:28:...
Ighub_updater.exe	4504	TCP	Listen	127.0.0.1	9180	0.0.0.0	0	7/15/2021 11:28:...
LMS.exe	8412	TCP	Listen	0.0.0.0	16992	0.0.0.0	0	7/30/2021 2:52:...
SearchApp.exe	9256	TCP	Established	192.168.1.56	49441	40.102.35.114	443	7/30/2021 4:27:...
chrome.exe	7152	TCP	Established	192.168.1.56	49604	64.4.54.254	443	7/30/2021 5:30:...
lsass.exe	912	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	7/15/2021 11:28:...

Endpoints: 192 Established: 18 Listening: 51 Time Wait: 19 Close Wait: Update: 2 sec States: (All)