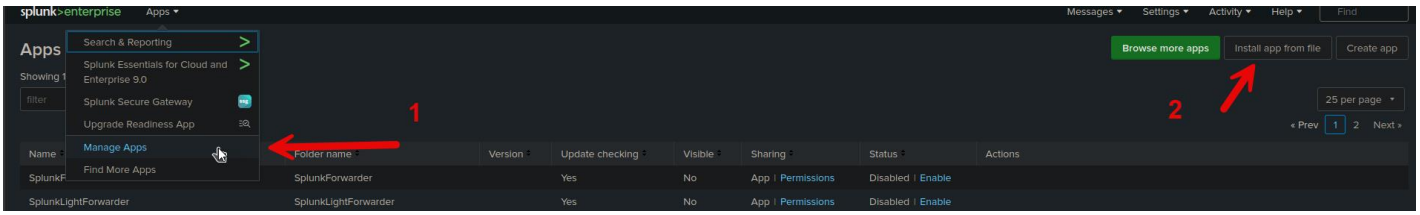
Utilizing Sysmon App for Splunk in HTB

For this lab, I'm utilizing a Splunk Enterprise instance from Hack the Box's SOC Analyst course. During the lab I will be downloading and installing Sysmon App for Splunk first. Afterwards I will load a dashboard to display different security related tables and graphs.

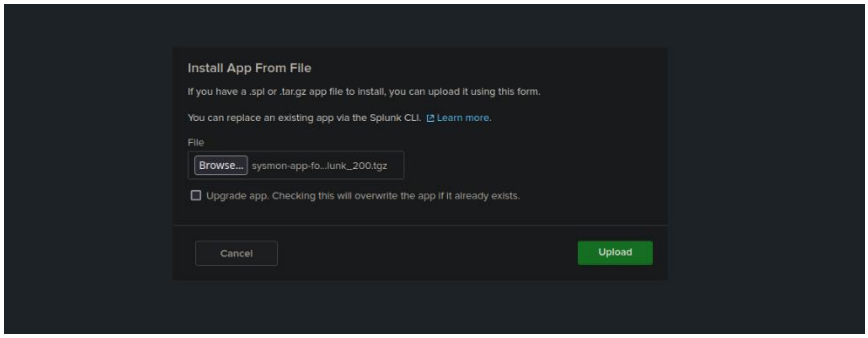
Downloading and Installing Sysmon for Splunk

Navigating to https://splunkbase.splunk.com/app/3544 to find the Sysmon for Splunk Application. After downloading, a SHA256 hash value is provided in case your installation is corrupted.

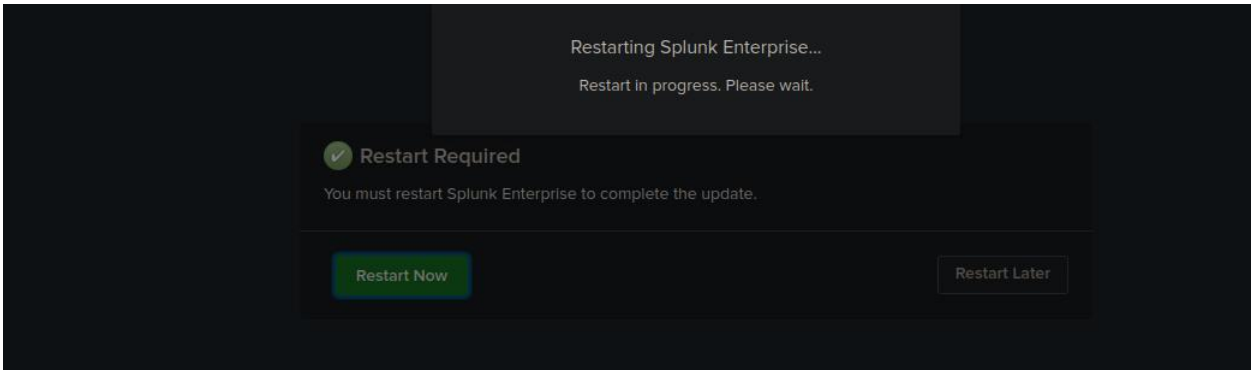
Go into the Splunk Enterprise instance and click these two buttons to install the application:



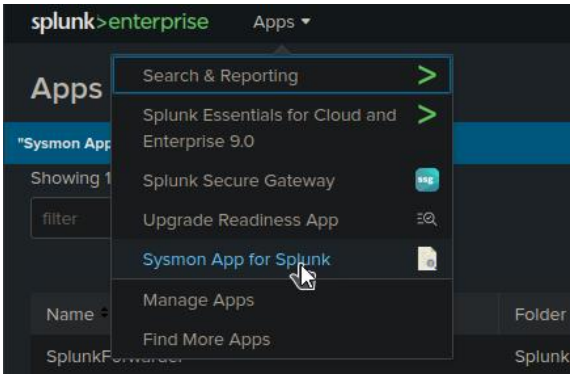
Now you can click browse and navigate to the directory where the application was downloaded to:



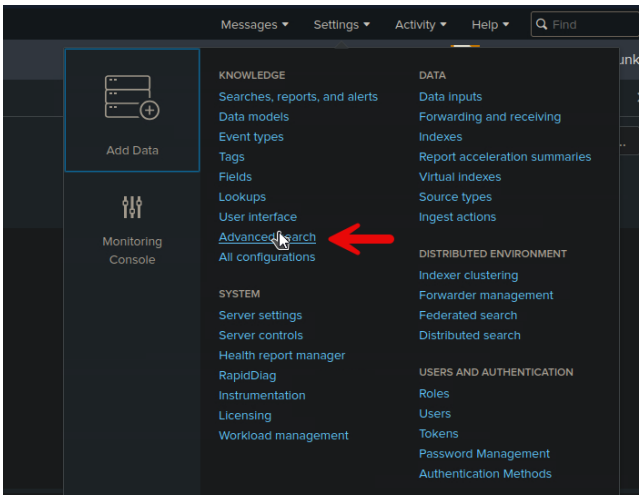
After uploading, Splunk will restart



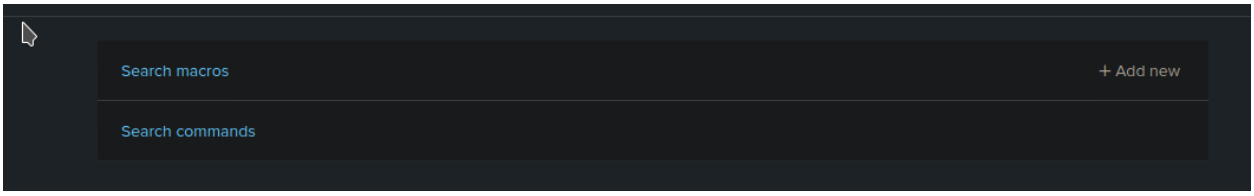
After restarting, we can now load the Sysmon App for Splunk application:

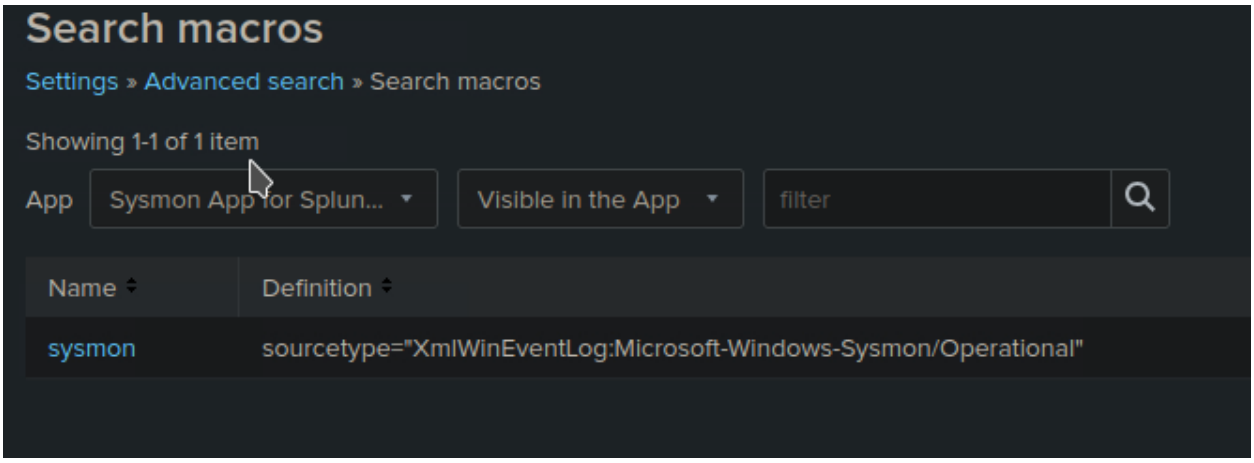


Then click settings and load the Advanced Search option:

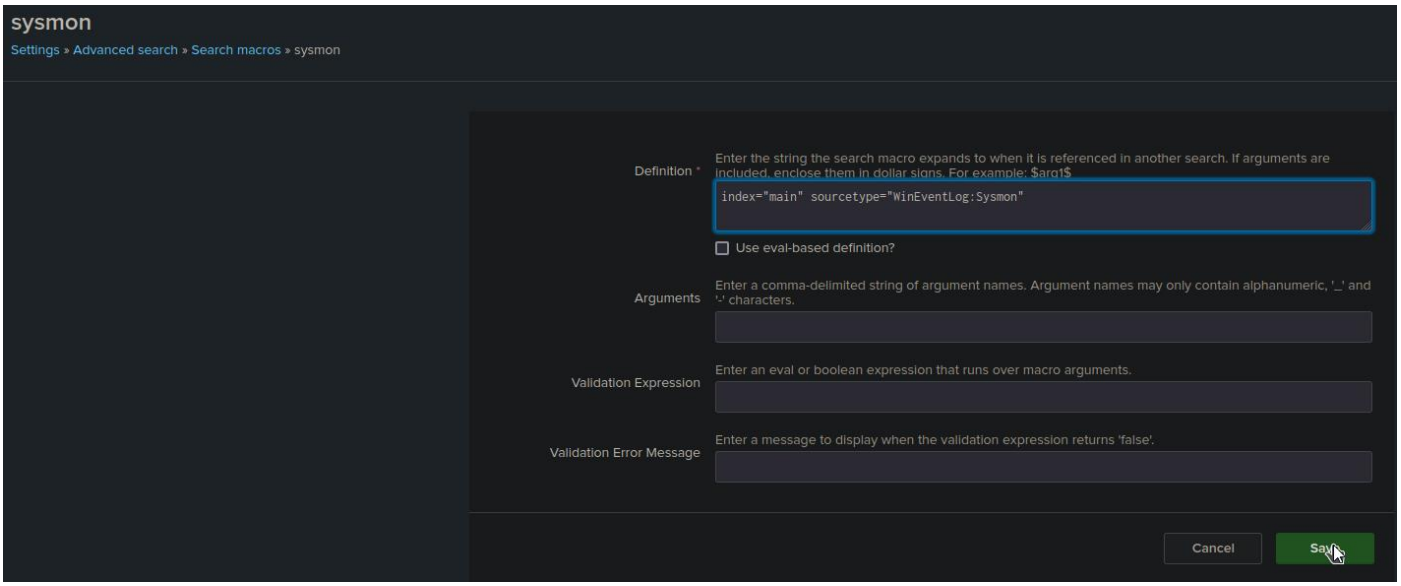


Then click search macros and sysmon:

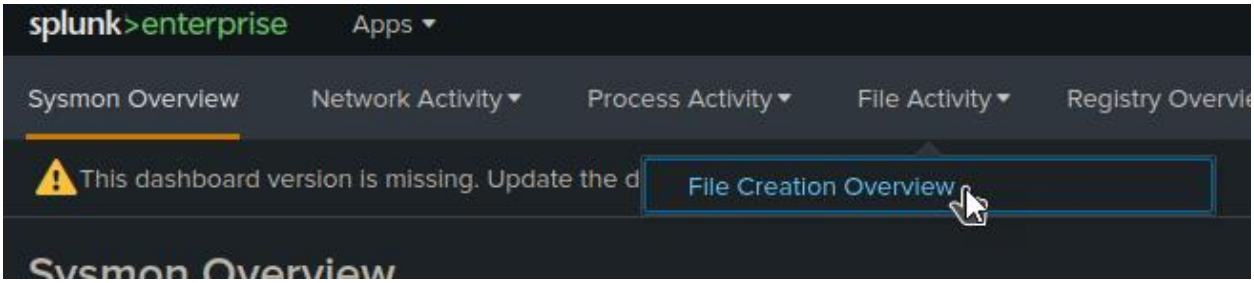




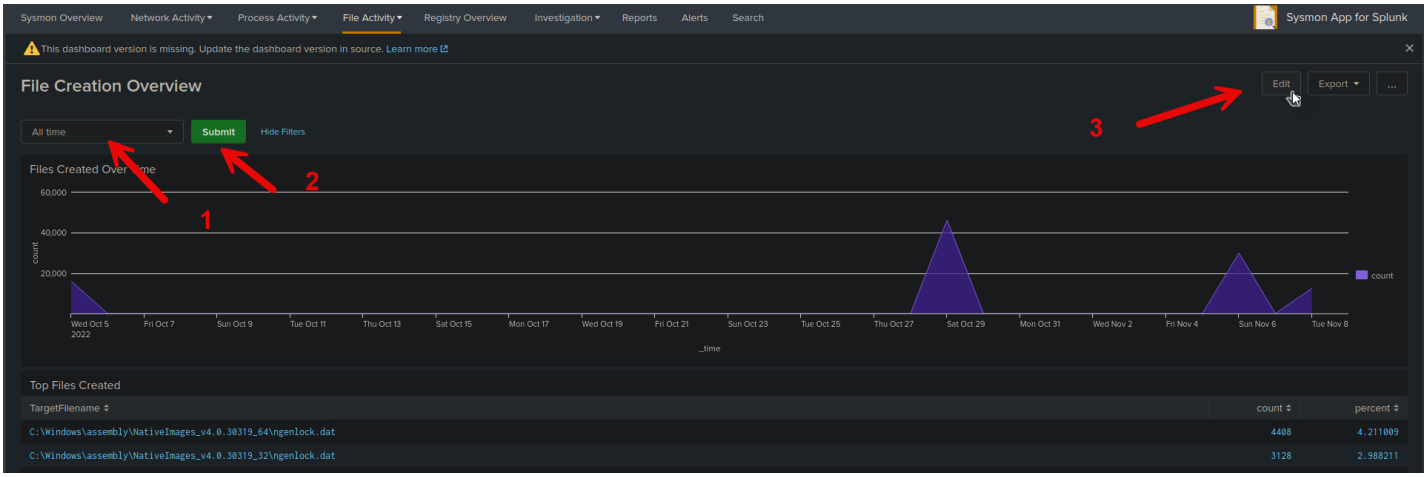
I filled out the following in the definiton box and clicked save:



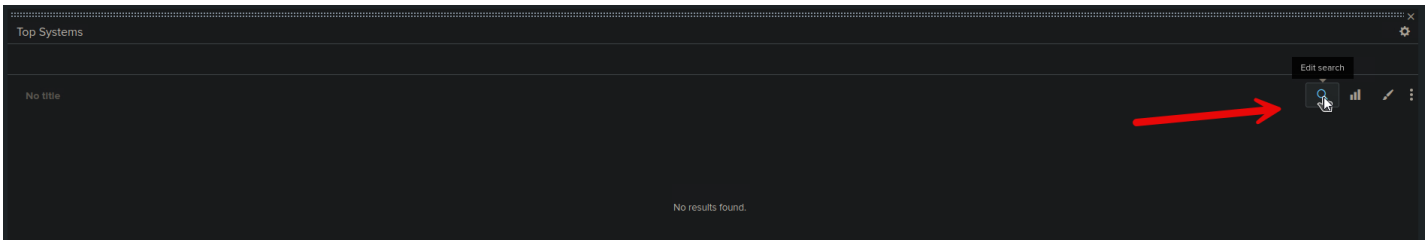
Then head back into the Sysmon App for Splunk and click the following in the File Activity tab:

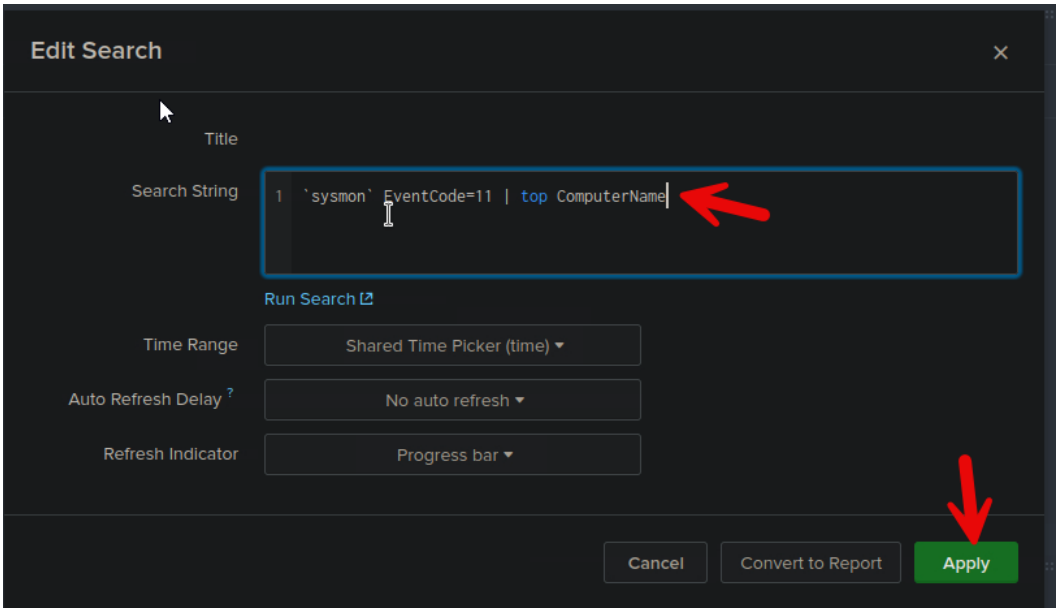


Make sure the following is set to all time, click submit, then click edit (To fill out top systems):

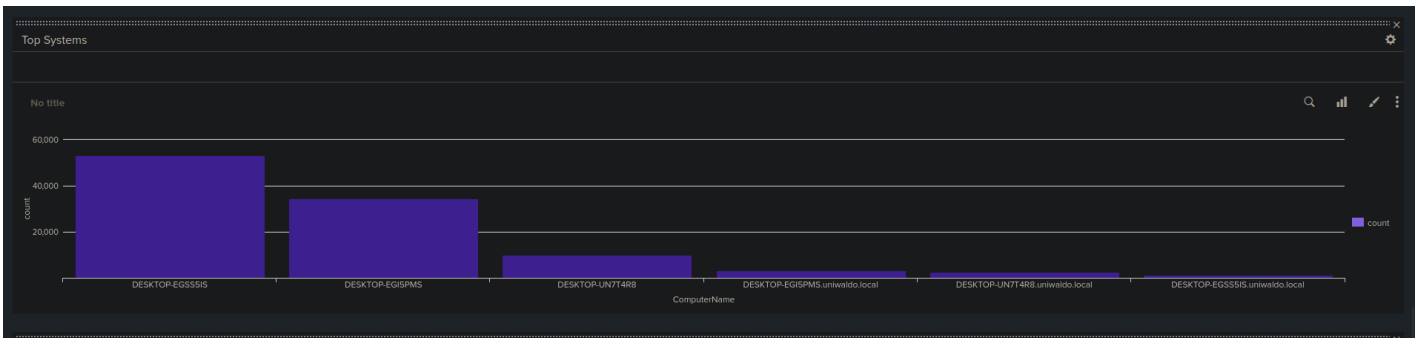


Scroll down to top systems and click edit search, then change “Computer” to “ComputerName”. This needs to be done becaue Sysmon 11 ID events have the ComputerName field and not the Computer field. Afterwards click apply:





After clicking apply, the computers with the largest numbers of Sysmon 11 ID events will display on a graph:



Other graphs/tables shown on this dashboard include Files Created Over Time, Top Files Created, and Top File Creation Processes:

Top File Creation Processes

No title

Image	count	percent
C:\Windows\system32\svchost.exe	31933	30.505932
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe	14797	14.135731
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe	9810	9.371597
C:\Windows\System32\svchost.exe	8722	8.332219
C:\Windows\SoftwareDistribution\Download\Install\updateplatform.exe	6856	6.549609
C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	4137	3.952120
C:\Windows\system32\wuauclt.exe	3798	3.628270
C:\Program Files\Microsoft Office\Root\Office16\SDXHelper.exe	3107	2.968150
C:\Windows\System32\poqexec.exe	2746	2.623283
C:\Windows\System32\mousocoreworker.exe	2349	2.244025

Top Files Created

No title

TargetFilename	count	percent
C:\Windows\assembly\NativeImages_v4.0.30319_64\ngenlock.dat	4408	4.211009
C:\Windows\assembly\NativeImages_v4.0.30319_32\ngenlock.dat	3128	2.988211
C:\Windows\SoftwareDistribution\Download\a1b907e9fd357c397a8703aa58cc5a63\Metadata\dpx.tmp	1778	1.698542
C:\Windows\SoftwareDistribution\Download\61dc5311e95a2b591ffb66a67c6561e6\Metadata\dpx.tmp	1530	1.461625
C:\Windows\Prefetch\MSCORSVW.EXE-16B291C4.pf	1068	1.020272
C:\Windows\Microsoft.NET\ngennicupdatelock.dat	919	0.877930
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngenrootstorelock.dat	674	0.643879
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\InstallService\{24A2C2C9-889B-43E9-B20C-774D6FEBA5E4}.checkpoint	486	0.464281
C:\Windows\System32\sru\SRUtmp.log	422	0.403141
C:\Windows\Prefetch\TASKHOSTW.EXE-2E5D4B75.pf	422	0.403141

Files Created Over Time