Using Splunk Applications

Splunk Applications

Splunk applications, or apps, are packages that we add to our Splunk Enterprise or Splunk Cloud deployments to extend capabilities and manage specific types of operational data. Each application is tailored to handle data from specific technologies or use cases, effectively acting as a pre-built knowledge package for that data. Apps can provide capabilities ranging from custom data inputs, custom visualizations, dashboards, alerts, reports, and more.

Splunk Apps enable the coexistence of multiple workspaces on a single Splunk instance, catering to different use cases and user roles. These ready-made apps can be found on Splunkbase.

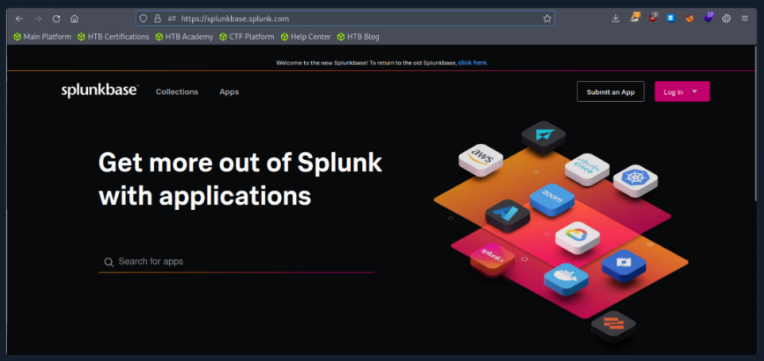
As an integral part of our cybersecurity operations, the Splunk apps designed for Security Information and Event Management (SIEM) purposes provide a range of capabilities to enhance our ability to detect, investigate, and respond to threats. They are designed to ingest, analyze, and visualize security-related data, enabling us to detect complex threats and perform in-depth investigations.

When using these apps in our Splunk environment, we need to consider factors such as data volume, hardware requirements, and licensing. Many apps can be resource-intensive, so we must ensure our Splunk deployment is sized correctly to handle the additional workload. Further, it's also important to ensure we have the correct licenses for any premium apps, and that we are aware of the potential for increased license usage due to the added data inputs.

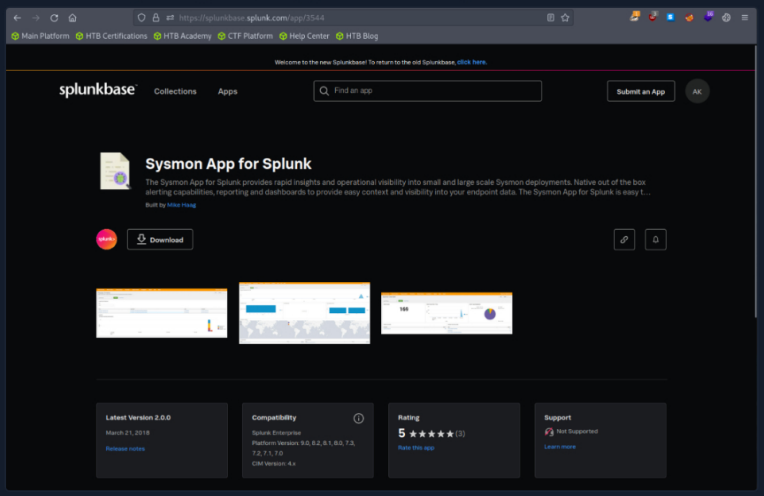
In this segment, we'll be leveraging the `Sysmon App for Splunk` developed by Mike Haag.

To download, add, and use this application, follow the steps delineated below:

1. Sign up for a free account at splunkbase



2. Once registered, log into your account
3. Head over to the Sysmon App for Splunk page to download the application.



4. Add the application as follows to your search head.

? Go to Questions

Table of Contents

Splunk Fundamentals

Introduction To Splunk & SPL

Using Splunk Applications

Investigating With Splunk

Intrusion Detection With Splunk (Real-world Scenario)

Detecting Attacker Behavior With Splunk Based On TTPs

Detecting Attacker Behavior With Splunk Based On Analytics

Skills Assessment

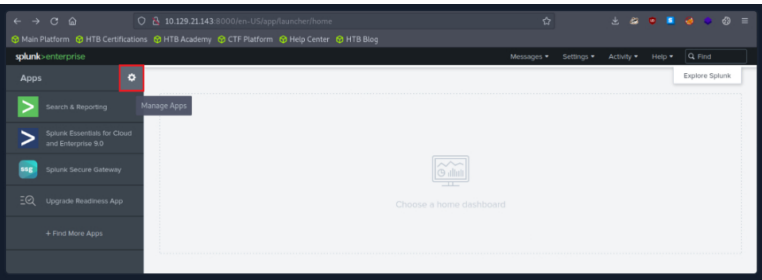
Skills Assessment

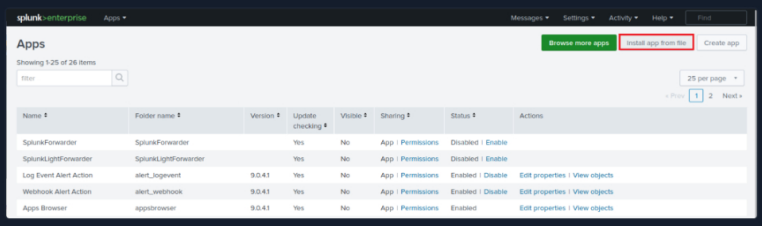
My Workstation

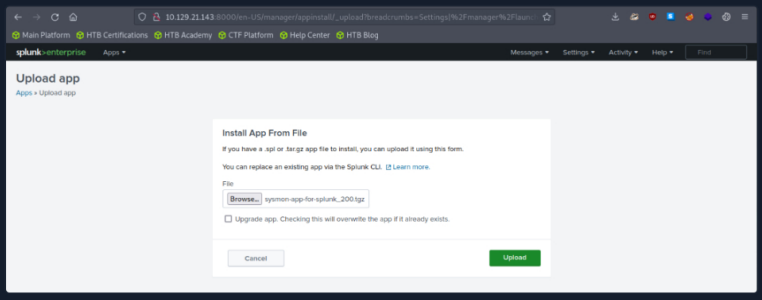
OFFLINE

Start Instance

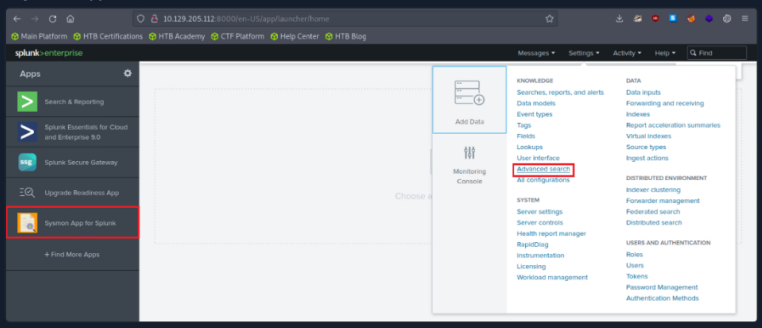
∞ / 1 spawns left

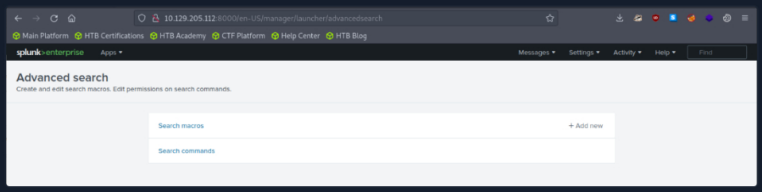


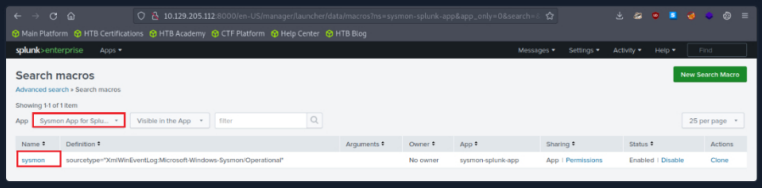


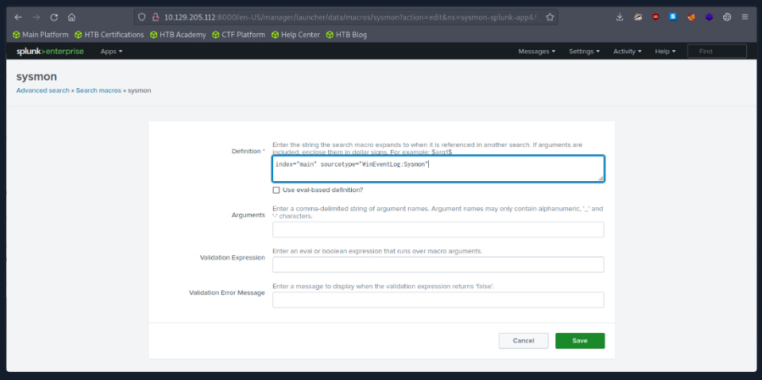


5. Adjust the application's macro so that events are loaded as follows.



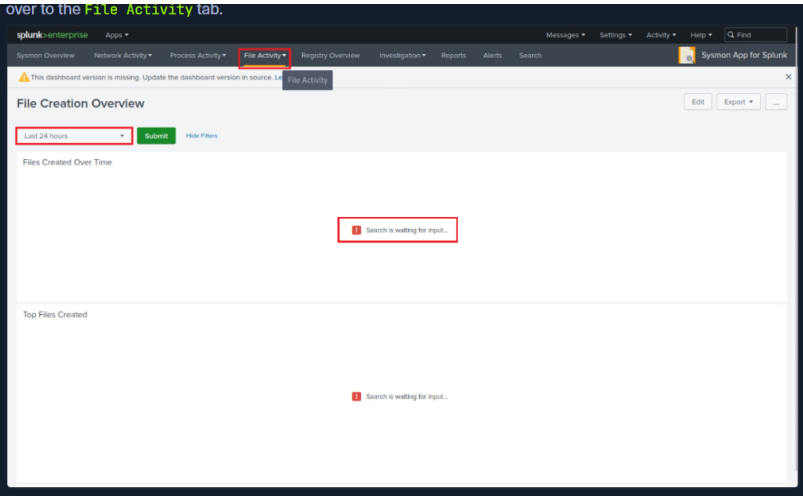




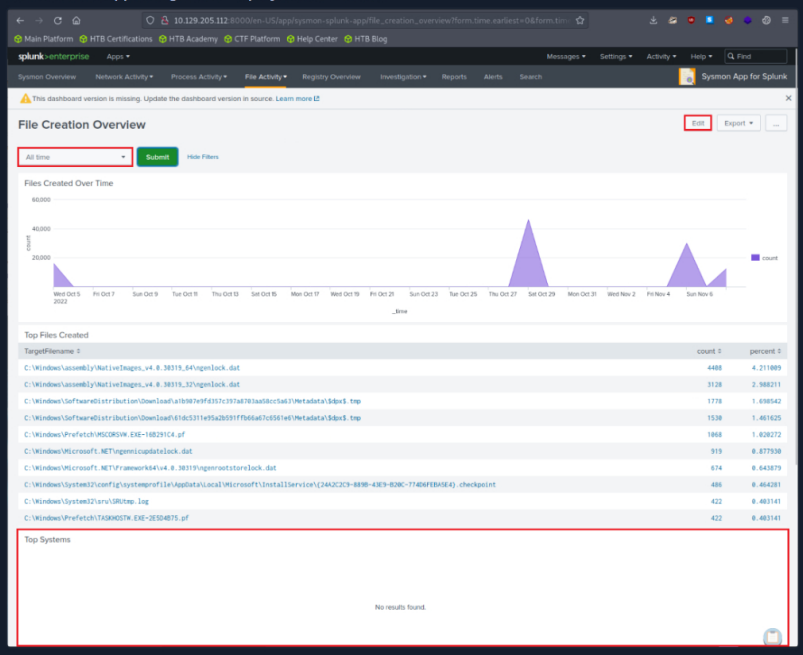


Let's access the Sysmon App for Splunk by locating it in the "Apps" column on the Splunk home page and head

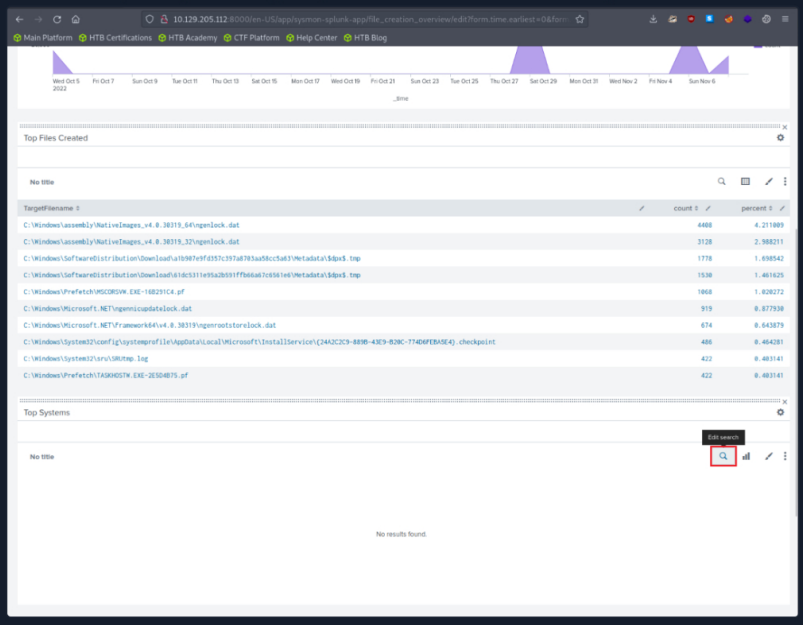
over to the `File Activity` tab.



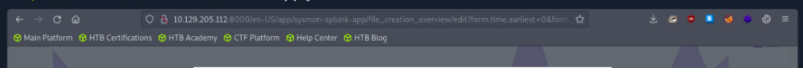
Let's now specify "All time" on the time picker and click "Submit". Results are generated successfully; however, no results are appearing in the "Top Systems" section.

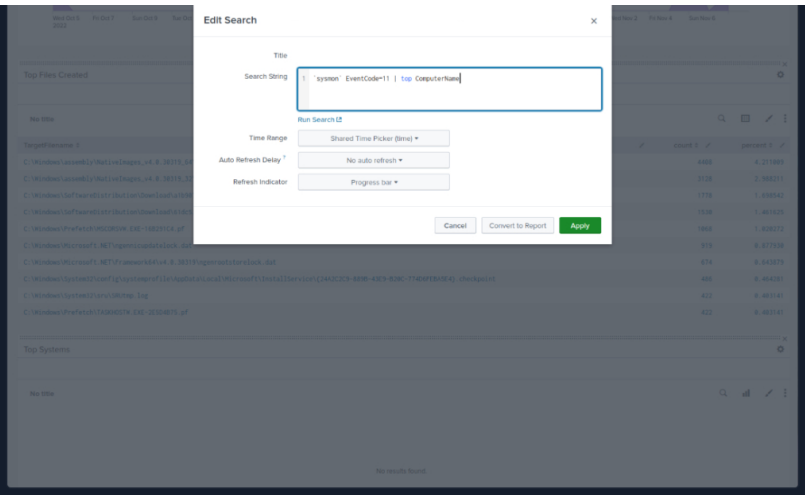


We can fix that by clicking on "Edit" (upper right hand corner of the screen) and editing the search.

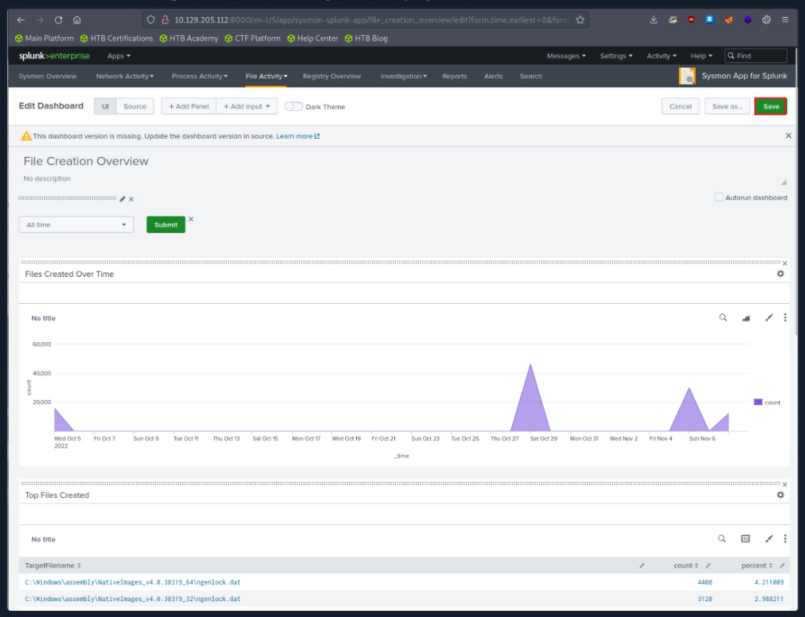


The Sysmon Events with ID 11 do not contain a field named `Computer`, but they do include a field called `ComputerName`. Let's fix that and click "Apply"





Results should now be generated successfully in the "Top Systems" section.



Feel free to explore and experiment with this Splunk application. An excellent exercise is to modify the searches when no results are generated due to non-existent fields being specified, continuing until the desired results are obtained.

Practical Exercises

Navigate to the bottom of this section and click on `Click here to spawn the target system!`

Now, navigate to `http://[Target IP]:8000`, open the `Sysmon App for Splunk` application, and answer the questions below.

VPN Servers

⚠ **Warning:** Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Existing PwnBox instances will automatically switch to the new VPN server.

US Academy 3 — Medium Load

PROTOCOL

UDP 1337 TCP 443

DOWNLOAD VPN CONNECTION FILE

Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK 159ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

Download VPN Connection File

Target(s): Click here to spawn the target system!

+ 1 Access the Sysmon App for Splunk and go to the "Reports" tab. Fix the search associated with the "Net - net view" report and provide the complete executed command as your answer. Answer format: net view /Domain:_.local

net view /DOMAIN:uniwaldo.local

Submit Hint

+ 1 Access the Sysmon App for Splunk, go to the "Network Activity" tab, and choose "Network Connections". Fix the search and provide the number of connections that SharpHound.exe has initiated as your answer.

6

Submit

Previous Next

Mark Complete & Next