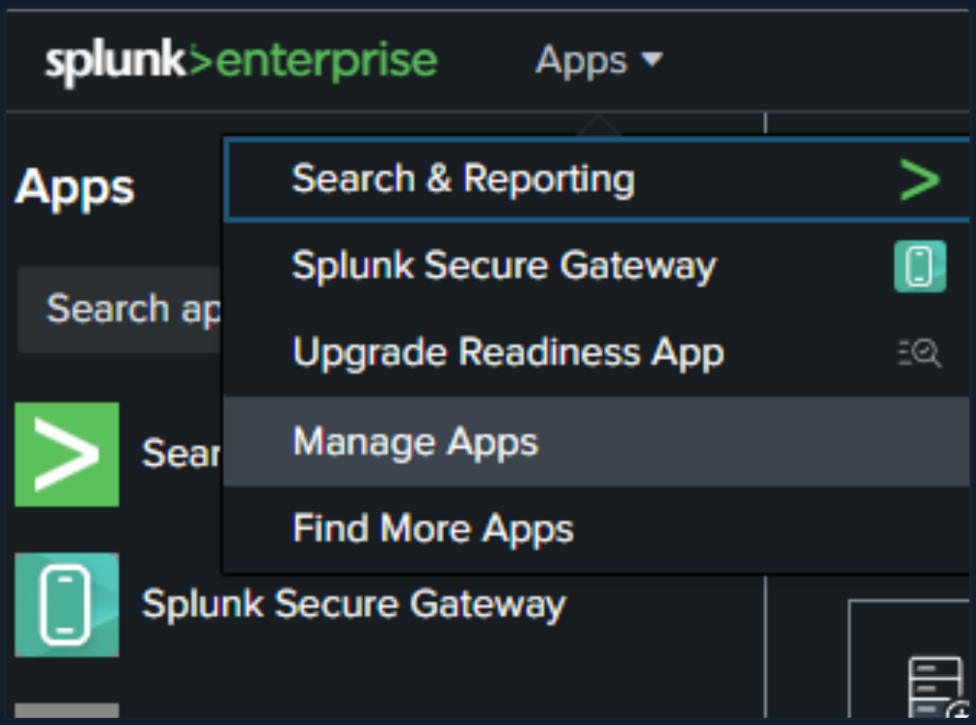
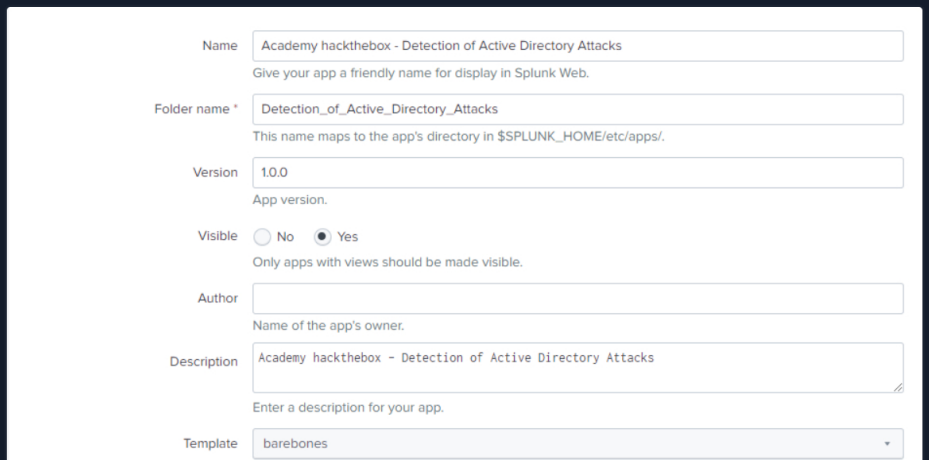
Creating Custom Splunk Applications

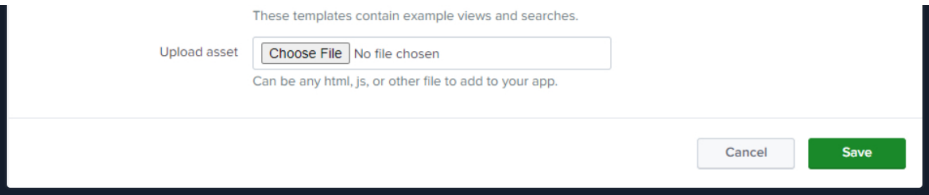
How To Create A Custom Splunk Application

1. `Access Splunk Web`: Open your web browser and navigate to Splunk Web.
2. `Go to Manage Apps`: From the menu bar at the top, select `Apps` and then choose `Manage Apps`.

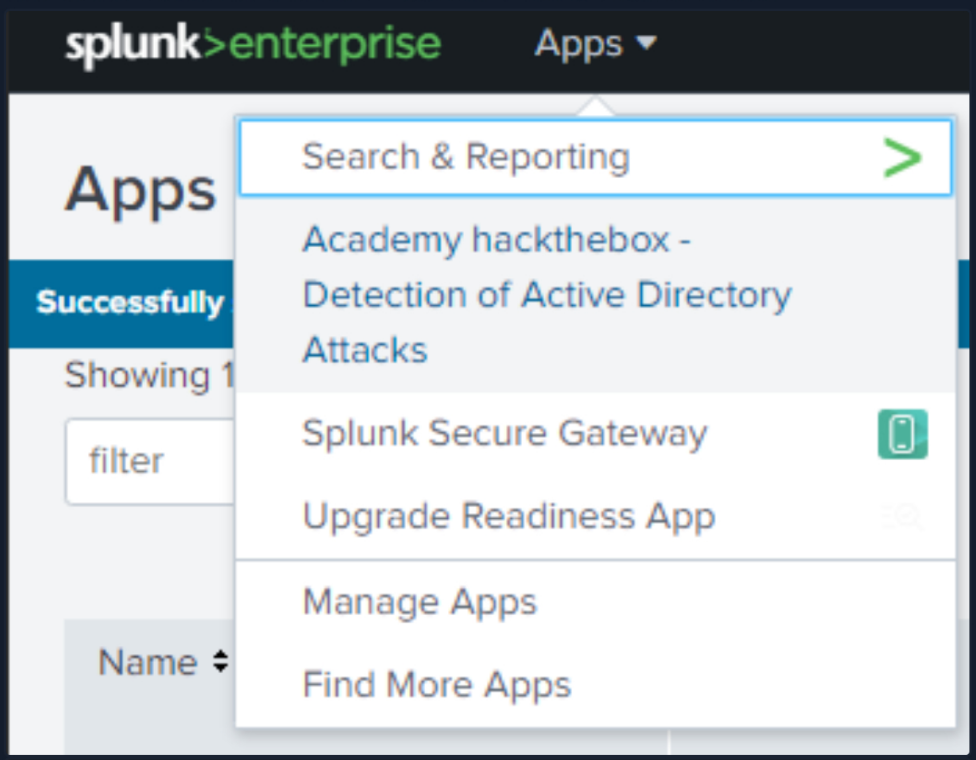


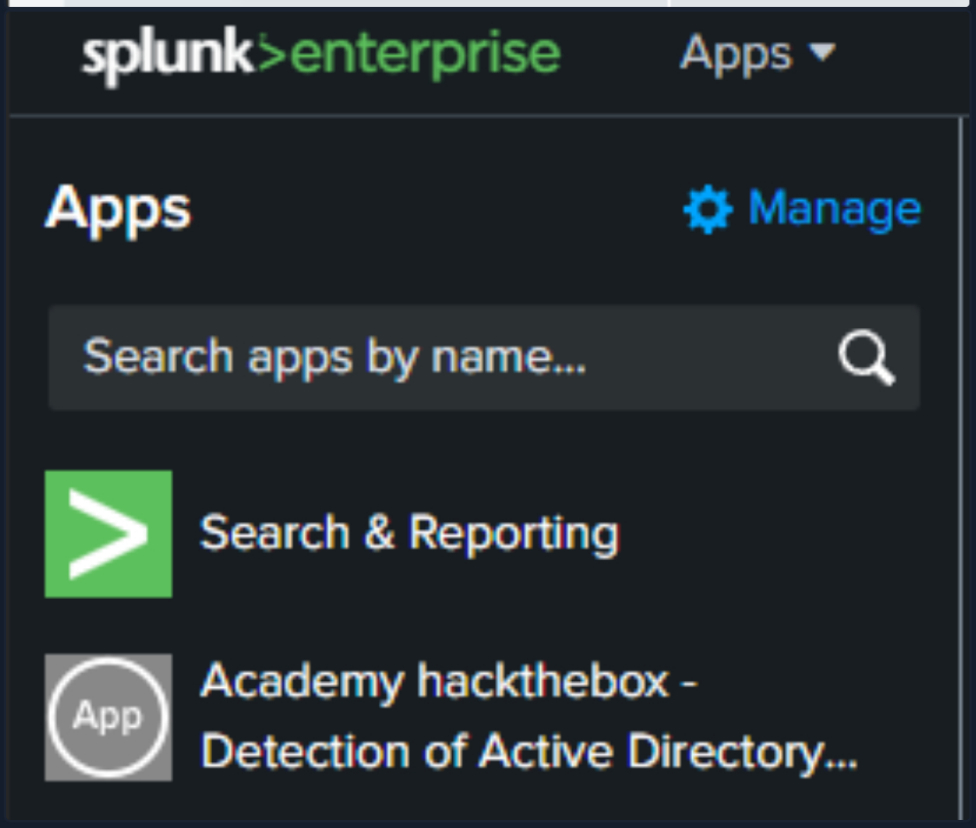
3. `Create a New App`: On the `Apps` page, click on `Create app`.
4. `Enter App Details`: On the `Add new` page, complete the properties for your new app:
   - `Name`: Enter the name for your app, for example, `<Your app name>`.
   - `Folder name`: Specify the folder name, which should be similar to `<App_name>`. This will correspond to the app's directory under `$SPLUNK_HOME/etc/apps/`.
   - `Version`: Input "1.0.0".
   - `Description`: Provide a description for your app, for instance, `<App description>`.
   - `Template`: Choose `barebones` from the drop-down menu.





5. `Save the App`: Click on `Save`. You can verify that your app has been created by going to the `Apps` menu. Your new app should now be listed there. Also, if you navigate to the Splunk Web home page, you'll find your app listed under the `Apps` list as `Academy hackthebox - Detection of Active Directory Attacks`.





6. `Explore the Directory Structure`: Use a file browser to navigate to `$SPLUNK_HOME/etc/apps`. Here you'll find your app directory, which includes the following folders:
   - `/bin`: This is where scripts are stored.

- `/default`: This directory holds files for configuration, views, dashboards, and app navigation.
- `/local`: This directory contains user-modified versions of files for configuration, views, dashboards, and app navigation.
- `/metadata`: This directory holds permissions files.

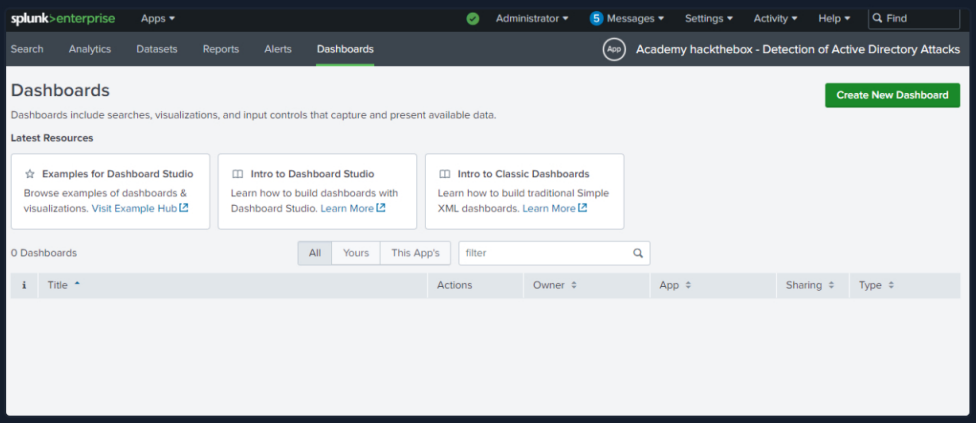
```
ubuntu@ubuntu-virtual-machine:/opt/splunk/etc/apps$ sudo su
root@ubuntu-virtual-machine:/opt/splunk/etc/apps# cd Detection_of_Active_Directory_Attacks/
root@ubuntu-virtual-machine:/opt/splunk/etc/apps/Detection_of_Active_Directory_Attacks# ls -la
total 24
drwx--x---  6 root   root   4096 Jul 30 09:15 .
drwxr-xr-x 32 splunk splunk 4096 Jul 30 09:15 ..
drwx--x---  2 root   root   4096 Jul 30 09:15 bin
drwx--x---  3 root   root   4096 Jul 30 09:15 default
drwx------  2 root   root   4096 Jul 30 09:15 local
drwx--x---  2 root   root   4096 Jul 30 09:15 metadata
root@ubuntu-virtual-machine:/opt/splunk/etc/apps/Detection_of_Active_Directory_Attacks#
```

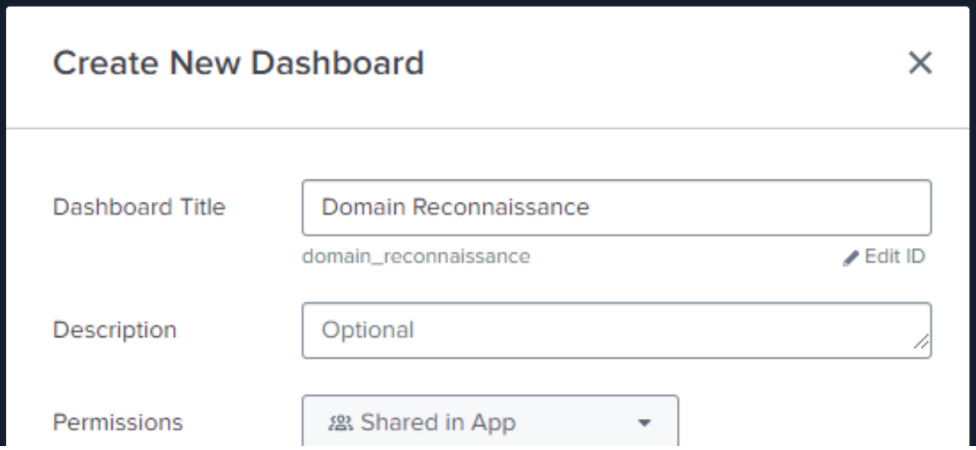
7. `View the Navigation File`: The navigation configuration file is an XML file. Using a text editor, open `$SPLUNK_HOME/etc/apps/<your app>/default/data/ui/nav/default.xml`. Here you'll find the default navigation definition for an app:

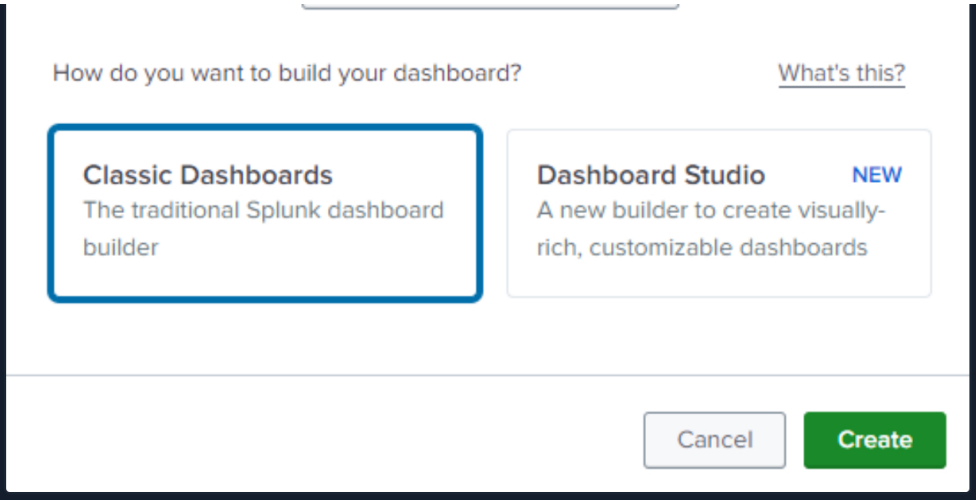
```xml
<nav search_view="search">
<view name="search" default='true' />
<view name="analytics_workspace" />
<view name="datasets" />
<view name="reports" />
<view name="alerts" />
<view name="dashboards" />
</nav>
```

In this XML, the top-level nav tag acts as the parent. The `search_view` attribute designates the default view for searches. In this case, the `search` view is employed, which is inherited from the `Search & Reporting` app. The next level in the XML hierarchy corresponds to items displayed on the app bar. The list of view tags denotes different views to show. Each of the views corresponds to a view from the Search & Reporting app. The attribute `default='true'` indicates the view to use as the app home page – here, the `search` view serves as the home page.

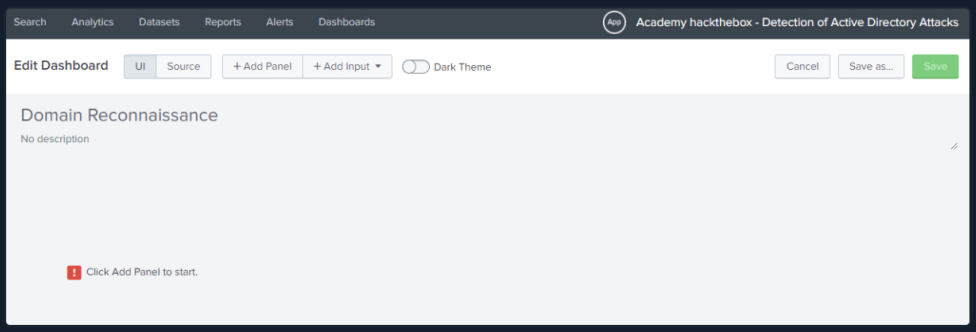
8. `Create Your First Dashboard`: Go to `dashboards` and click on `Create New Dashboard`. Enter the dashboard name, provide a description if necessary, set permissions, and select `Classic Dashboards`.

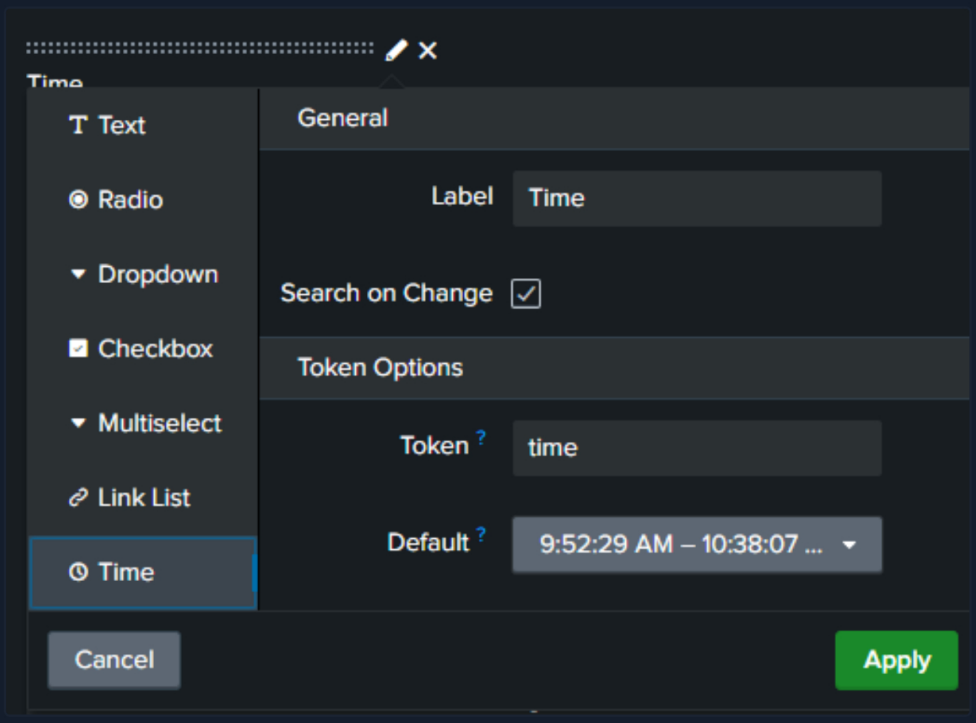


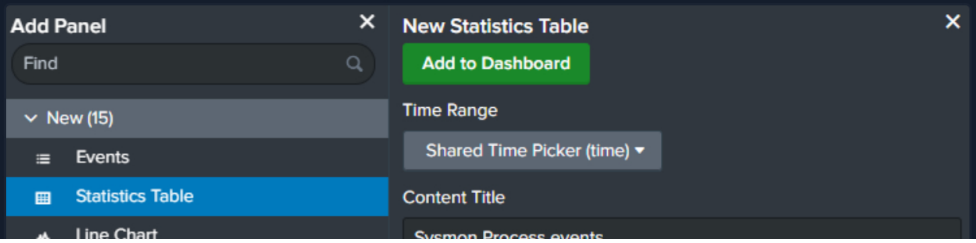


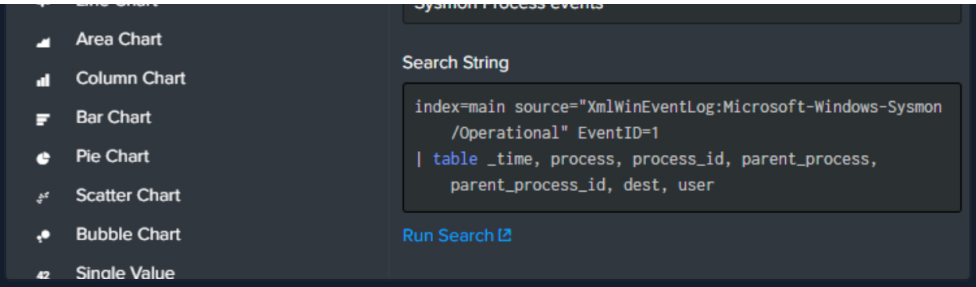


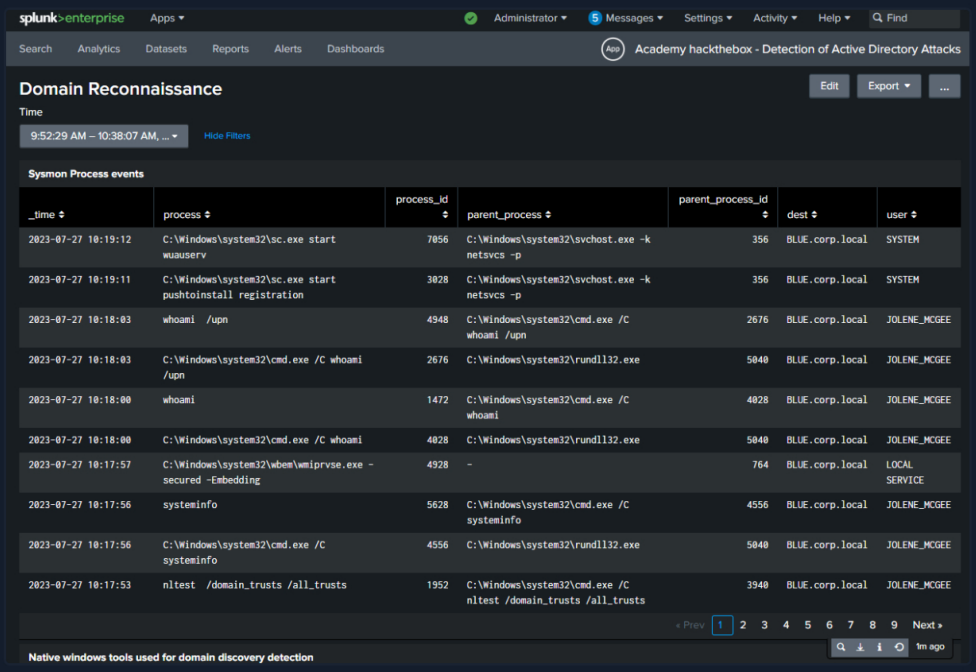
9. `Configure the Dashboard`: You'll now see the dashboard editor page, where you can configure panels, inputs, etc., to facilitate your monitoring process. Add time input for the dashboard and adjust the default time range to suit your needs. Next, add a statistical table panel, select a time range for the Shared Time Picker, add the Content Title (e.g., `"<Panel name>"`), and input the Search String. To use input in searches, enclose the input token with dollar signs, like `$user$`. Click `Add to Dashboard` when ready. Save your changes.







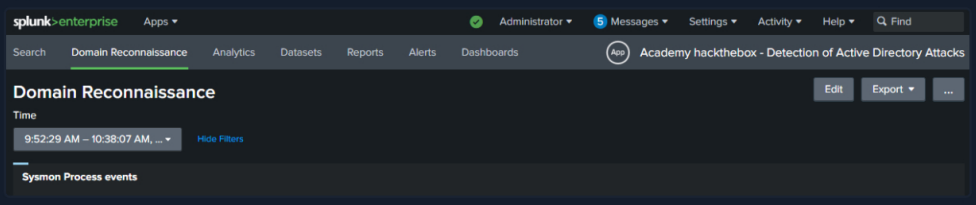




10. `Dashboard Storage`: All dashboards you've created in your app are stored at "`<AppPath>/local/data/ui/views/dashboard_title.xml`". To add your dashboard to the navigation bar, simply append the dashboard title to the navigation default page XML: "`<AppPath>/local/data/ui/nav/default.xml`".

```
  GNU nano 4.8
<nav search_view="search">
  <view name="search" default='true' />
  <view name="domain_reconnaissance" />S
  <view name="analytics_workspace" />
  <view name="datasets" />
  <view name="reports" />
  <view name="alerts" />
  <view name="dashboards" />
</nav>
```

11. `Restart Splunk`: Reboot your Splunk instance. Once restarted, you should see your dashboard in the navigation bar.



12. `Grouping Dashboards`: If you wish to group multiple dashboards under a single entry in the navigation bar, use the collection tag.

```
<nav search_view="search" color="#5cc05c">
    <view name="search" default='true' />
```

```
<collection label="Command and Control">
    <view name="c2_investigator" />
    <view name="c2_investigator_zeek" />
```

Updating & Exploring The "Academy hackthebox - Detection of Active Directory Attacks" Splunk Application

`Detection-of-Active-Directory-Attacks.tar.gz.tar` can be downloaded from the `Resources` section of this module (upper right corner) and used to update the existing `Academy hackthebox - Detection of Active Directory Attacks` Splunk Application by clicking `Apps` -> `Manage Apps` -> `Install app from file` -> `Browse` -> ✓ `Upgrade app. Checking this will overwrite the app if it already exists.` -> `Upload`.

Now, take some time to explore this custom Splunk application and see how it can significantly improve our monitoring capabilities.

← Previous Next →

Mark Complete & Next

Powered by HACKTHEBOX