

Creating Custom Splunk Applications

How To Create A Custom Splunk Application

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

The screenshot shows the Splunk Enterprise dashboard with the 'splunk>enterprise' logo. On the left, there's a sidebar with 'Apps' and search functions. The main area has several cards: 'Search & Reporting' (highlighted), 'Splunk Secure Gateway', 'Upgrade Readiness App', 'Manage Apps' (selected), 'Find More Apps', and another 'Splunk Secure Gateway' card. The 'Manage Apps' card contains sub-options like 'Create New App', 'Edit Existing App', and 'Delete App'.

- Create a New App:** On the **Apps** page, click on **Create app**.
- 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.

The form fields are as follows:

- Name:** Academy hackthebox - Detection of Active Directory Attacks
- Folder name ***: Detection_of_Active_Directory_Attacks
- Version**: 1.0.0
- Visible**: No Yes
- Author**: (empty)
- Description**: Academy hackthebox - Detection of Active Directory Attacks
- Template**: barebones

Resources

Table of Contents

Leveraging Windows Event Logs

- Detecting Common User/Domain Recon
- Detecting Password Spraying
- Detecting Responder-like Attacks
- Detecting Kerberoasting/AS-REProasting
- Detecting Pass-the-Hash
- Detecting Pass-the-Ticket
- Detecting Overpass-the-Hash
- Detecting Golden Tickets/Silver Tickets
- Detecting Unconstrained Delegation/Constrained Delegation Attacks
- Detecting DCSync/DCShadow

Leveraging Splunk's Application Capabilities

- Creating Custom Splunk Applications

Leveraging Zeek Logs

- Detecting RDP Brute Force Attacks
- Detecting Beacons Malware
- Detecting Nmap Port Scanning
- Detecting Kerberos Brute Force Attacks
- Detecting Kerberoasting
- Detecting Golden Tickets
- Detecting Cobalt Strike's PSEExec
- Detecting Zerologon
- Detecting Exfiltration (HTTP)
- Detecting Exfiltration (DNS)
- Detecting Ransomware

Skills Assessment

- Skills Assessment

These templates contain example views and searches.

Upload asset

Choose File

No file chosen

Can be any html, js, or other file to add to your app.

Cancel

Save

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

The screenshot shows the Splunk Enterprise interface. In the top right corner, there's a "My Workstation" section indicating "OFFLINE". Below it, a green button says "Start Instance" and "∞ / 1 spawns left". The main area is titled "splunk>enterprise" and has a "Apps" dropdown menu. A modal window is open over the page, showing the "Search & Reporting" category selected. Inside this category, the "Academy hackthebox - Detection of Active Directory Attacks" app is listed. Other items in the category include "Splunk Secure Gateway" and "Upgrade Readiness App". Below the category list are links for "Manage Apps" and "Find More Apps". On the left side of the main page, there's a sidebar with a "Successfully" status message, a "Showing 1" count, a "filter" button, and a "Name" dropdown. The overall theme is dark with blue and white text.

This screenshot shows the same Splunk Enterprise interface as the previous one, but with a different view. It features a search bar at the top with the placeholder "Search apps by name..." and a magnifying glass icon. Below the search bar, there's a large green button with a white right-pointing arrow and the text "Search & Reporting". Underneath this, there's another card for the "Academy hackthebox - Detection of Active Directory..." app, which includes an "App" icon. The overall layout is clean and modern, with a white background and blue text.

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:

Code: **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**.

The screenshot shows the Splunk interface with the 'Dashboards' tab selected. The top navigation bar includes 'splunk>enterprise', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. The main content area has a heading 'Dashboards' and a sub-instruction: 'Dashboards include searches, visualizations, and input controls that capture and present available data.' Below this is a 'Latest Resources' section with three cards: 'Examples for Dashboard Studio', 'Intro to Dashboard Studio', and 'Intro to Classic Dashboards'. At the bottom, there's a table-like structure for managing dashboards with columns for 'Title', 'Actions', 'Owner', 'App', 'Sharing', and 'Type'. A prominent green 'Create New Dashboard' button is located at the top right of the dashboard list.

Create New Dashboard

Dashboard Title

Domain Reconnaissance

domain_reconnaissance

Edit ID

Description

Optional

Permissions

Shared in App

How do you want to build your dashboard?

[What's this?](#)

Classic Dashboards

The traditional Splunk dashboard builder

Dashboard Studio NEW

A new builder to create visually-rich, customizable dashboards

[Cancel](#)

[Create](#)

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.

The screenshot shows the Splunk dashboard editor interface. At the top, there are navigation links: Search, Analytics, Datasets, Reports, Alerts, and Dashboards. Below that is a toolbar with buttons for Edit Dashboard, UI, Source, + Add Panel, + Add Input, Dark Theme, Cancel, Save as..., and Save. The main area is titled 'Domain Reconnaissance' and has a note 'No description'. A message at the bottom says 'Click Add Panel to start.'

The screenshot shows the configuration of a 'Time' input panel. On the left is a sidebar with options: Text, Radio, Dropdown, Checkbox, Multiselect, Link List, and Time. The 'Time' option is selected and highlighted with a blue border. The main panel shows the 'General' tab with fields for 'Label' (set to 'Time'), 'Search on Change' (checked), and 'Token Options' (set to 'time'). The 'Default' dropdown shows a range from '9:52:29 AM – 10:38:07 ...'. At the bottom are 'Cancel' and 'Apply' buttons.

The screenshot shows the 'Add Panel' dialog. It includes a search bar, a list of categories: New (15), Events, Statistics Table (which is selected and highlighted in blue), and Line Chart. To the right, the 'New Statistics Table' dialog is open, showing a 'Time Range' set to 'Shared Time Picker (time)' and a 'Content Title' field containing 'System Process events'. There is also a 'Add to Dashboard' button.

The screenshot shows the Splunk interface with a search bar containing the following query:

```
index=main source="XmlWinEventLog:Microsoft-Windows-Sysmon
    /Operational" EventID=1
| table _time, process, process_id, parent_process,
  parent_process_id, dest, user
```

Below the search bar is a "Run Search" button. The main area displays a table titled "Domain Reconnaissance" with the following columns: _time, process, process_id, parent_process_id, dest, and user. The table contains several rows of log entries from the Sysmon Process events index.

_time	process	process_id	parent_process_id	dest	user
2023-07-27 10:19:12	C:\Windows\system32\sc.exe start wuauserv	7056	C:\Windows\system32\svchost.exe -k netsvcs -p	356	BLUE.corp.local SYSTEM
2023-07-27 10:19:11	C:\Windows\system32\sc.exe start pushinstall registration	3028	C:\Windows\system32\svchost.exe -k netsvcs -p	356	BLUE.corp.local SYSTEM
2023-07-27 10:18:03	whoami /upn	4948	C:\Windows\system32\cmd.exe /C whoami /upn	2676	BLUE.corp.local JOLENE_MCGEE
2023-07-27 10:18:03	C:\Windows\system32\cmd.exe /C whoami	2676	C:\Windows\system32\rundll32.exe	5040	BLUE.corp.local JOLENE_MCGEE
2023-07-27 10:18:00	whoami	1472	C:\Windows\system32\cmd.exe /C whoami	4028	BLUE.corp.local JOLENE_MCGEE
2023-07-27 10:18:00	C:\Windows\system32\cmd.exe /C whoami	4028	C:\Windows\system32\rundll32.exe	5040	BLUE.corp.local JOLENE_MCGEE
2023-07-27 10:17:57	C:\Windows\system32\wbem\wmprvse.exe -secured -Embedding	4928	-	764	BLUE.corp.local LOCAL SERVICE
2023-07-27 10:17:56	systeminfo	5628	C:\Windows\system32\cmd.exe /C systeminfo	4556	BLUE.corp.local JOLENE_MCGEE
2023-07-27 10:17:56	C:\Windows\system32\cmd.exe /C systeminfo	4556	C:\Windows\system32\rundll32.exe	5040	BLUE.corp.local JOLENE_MCGEE
2023-07-27 10:17:53	nltest /domain_trusts /all_trusts	1952	C:\Windows\system32\cmd.exe /C nltest /domain_trusts /all_trusts	3940	BLUE.corp.local JOLENE_MCGEE

At the bottom of the table, there are navigation links for "Prev" and "Next" and a search bar with a magnifying glass icon.

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`".

The screenshot shows a terminal window with the title "GNU nano 4.8". The file content is the XML configuration for the navigation bar:

```
<nav search_view="search">
  <view name="search" default='true' />
  <view name="domain_reconnaissance" />
  <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.

The screenshot shows the Splunk interface with the "Domain Reconnaissance" dashboard selected in the navigation bar. The dashboard title is "Academy hackthebox - Detection of Active Directory Attacks".

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' />
```

```
<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

