Splunk4Ninjas - Custom Commands

Hands-On Guide

This guide contains all the commands needed to participate in the session, and its highly recommended to copy and paste them to save time

The below table of contents link to each lab:

Lab 0 - Prerequisites

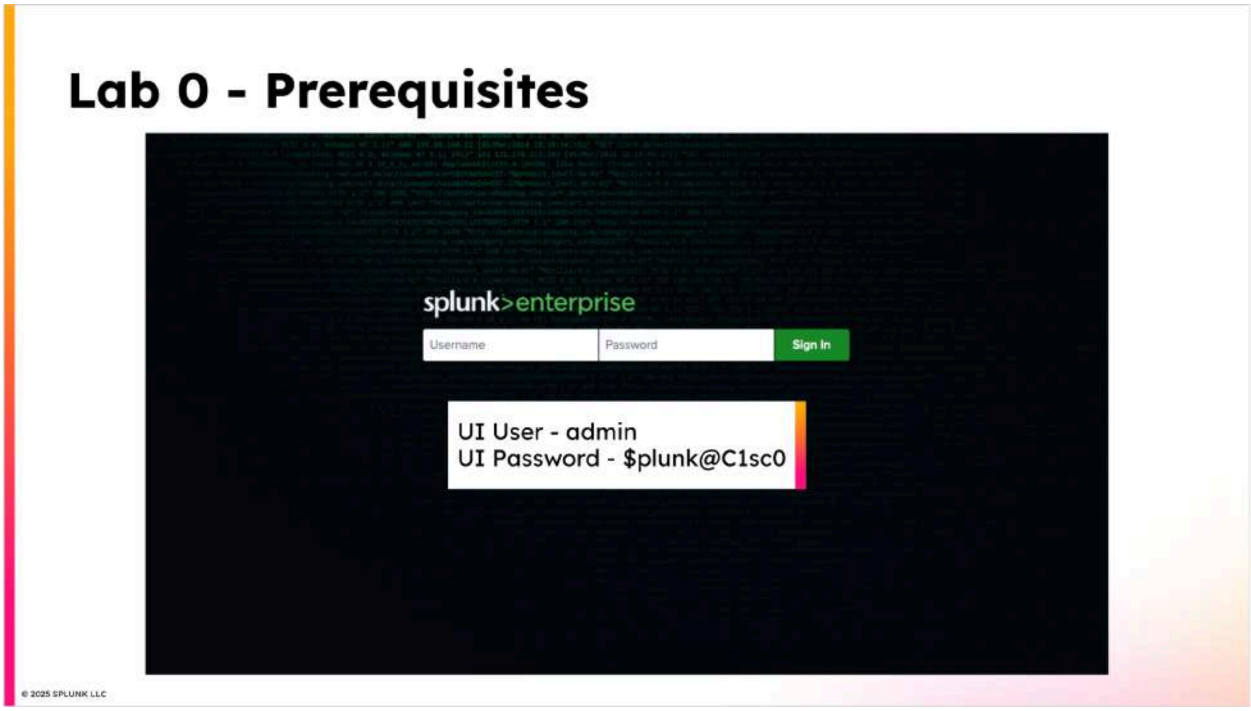
Credentials

Splunk Web:

UI Username - admin
UI Password - $plunk@C1sc0

SSH:

SSH Username - splunk
SSH Password - Sp1unkH00di3
SSH Port - 2222



Lab 0 - Prerequisites

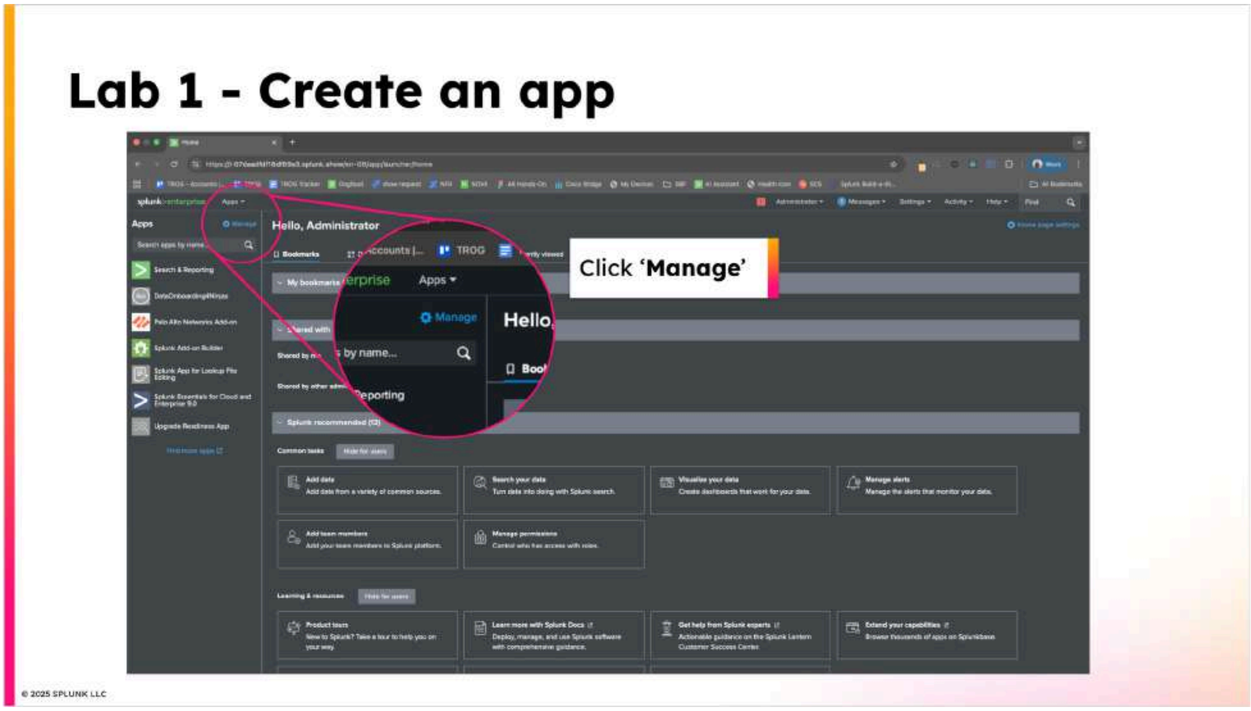
UI User - admin
UI Password - $plunk@C1sc0

© 2025 SPLUNK LLC

Lab 1 - Create an app

Log into Splunk web:

Click ‘Manage’

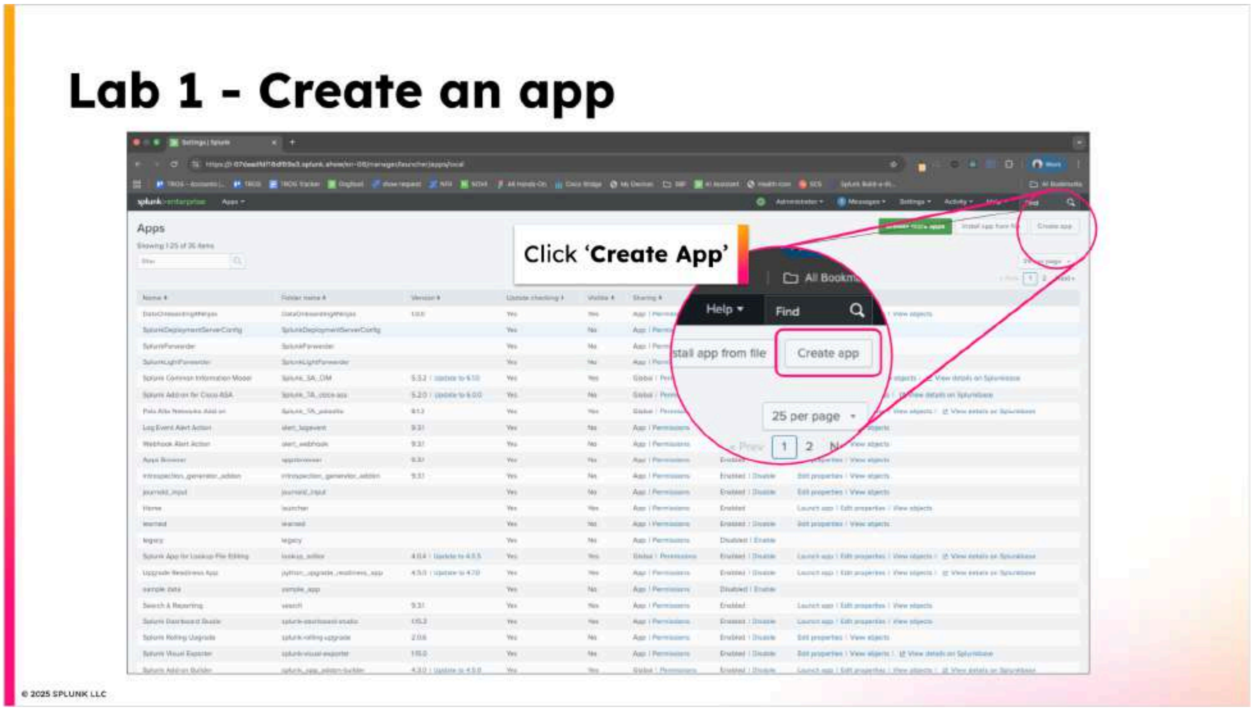


Lab 1 - Create an app

Click ‘**Manage**’

© 2025 SPLUNK LLC

Create app:

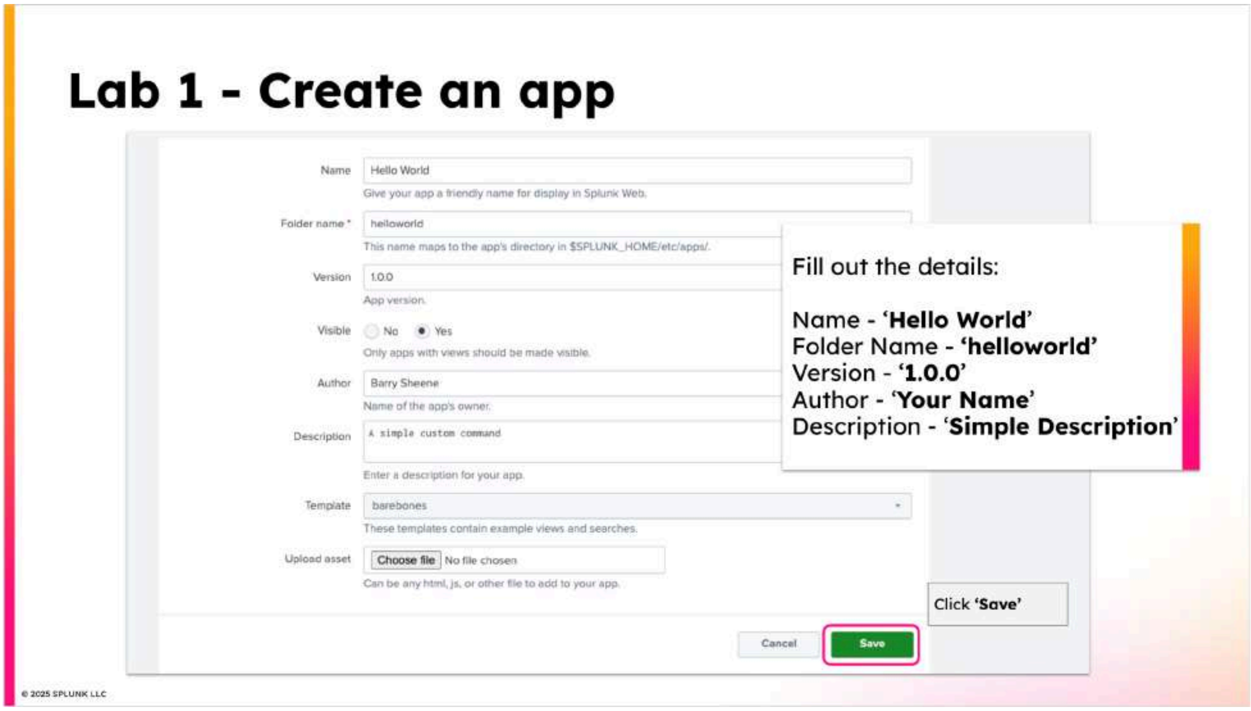


Lab 1 - Create an app

Click ‘**Create App**’

© 2025 SPLUNK LLC

Complete the form:



Lab 1 - Create an app

Name	Hello World Give your app a friendly name for display in Splunk Web.
Folder name *	helloworld This name maps to the app's directory in $SPLUNK_HOME/etc/apps/.
Version	1.0.0 App version.
Visible	○ No ● Yes Only apps with views should be made visible.
Author	Barry Sheene Name of the app's owner.
Description	A simple custom command Enter a description for your app.
Template	barebones 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.

Fill out the details:

Name - ‘**Hello World**’
Folder Name - **‘helloworld’**
Version - **‘1.0.0’**
Author - **‘Your Name’**
Description - ‘**Simple Description**’

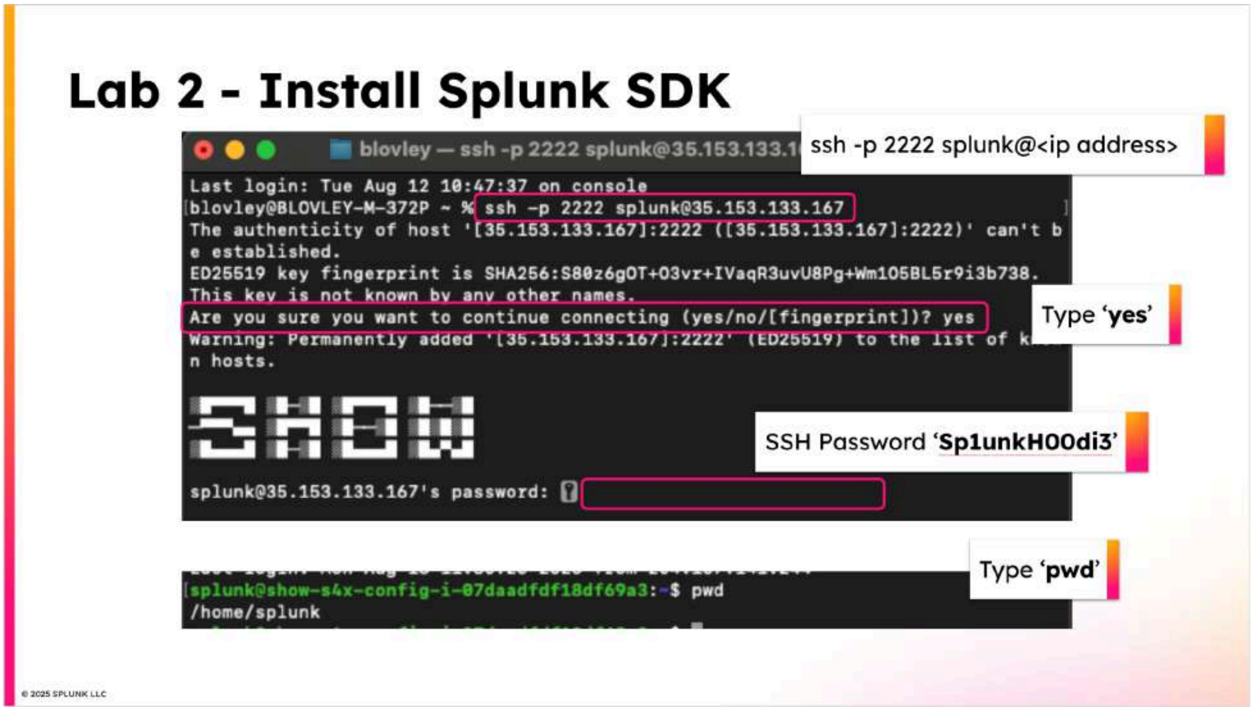
Click **‘Save’**

Name **-** ‘**Hello World**’
Folder Name **- ‘helloworld’**
Version **- ‘1.0.0’**
Author **- ‘Your Name’**
Description **- ‘Simple Description**

Intentionally Blank

Lab 2 - Install Splunk SDK

SSH into Splunk:



Lab 2 - Install Splunk SDK

blovley — ssh -p 2222 splunk@35.153.133.1

```
Last login: Tue Aug 12 10:47:37 on console
blovley@BLOVLEY-M-372P ~ % ssh -p 2222 splunk@35.153.133.167
The authenticity of host '[35.153.133.167]:2222 ([35.153.133.167]:2222)' can't b
e established.
ED25519 key fingerprint is SHA256:S80z6gOT+O3vr+IVaqR3uvU8Pg+Wm1O5BL5r9i3b738.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[35.153.133.167]:2222' (ED25519) to the list of k
n hosts.

SHOW

splunk@35.153.133.167's password:
```

ssh -p 2222 splunk@<ip address>

Type '**yes**'

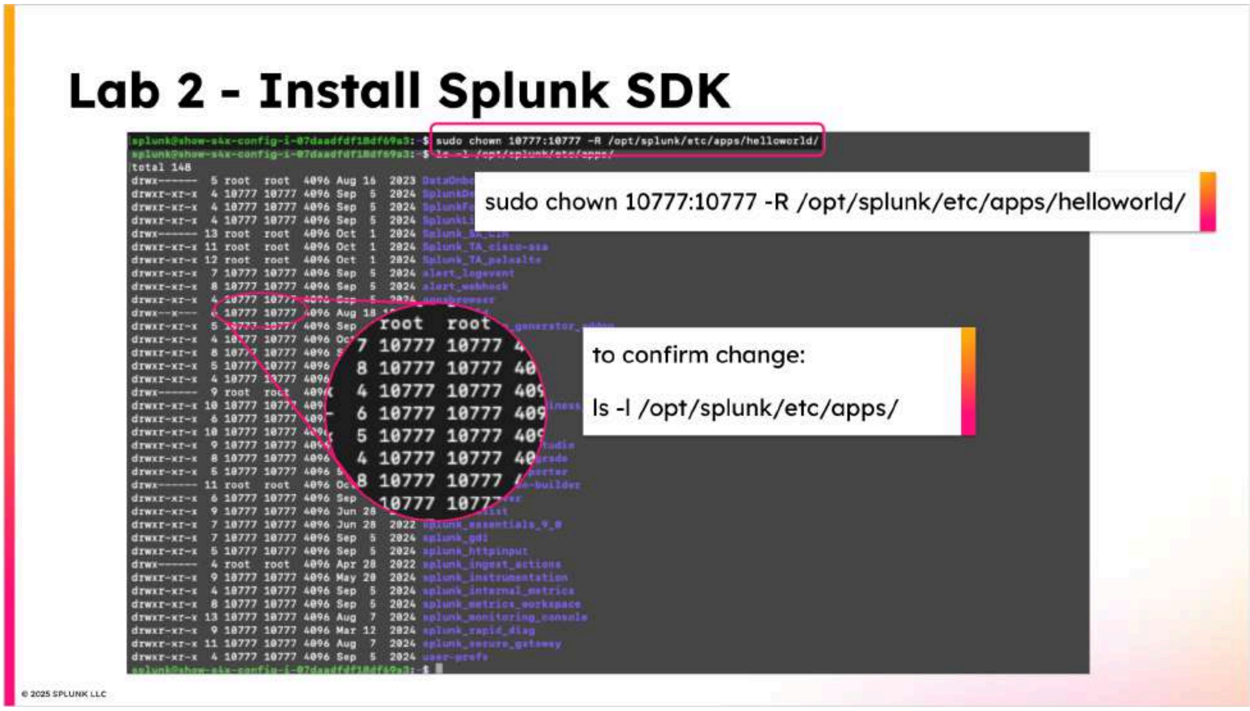
SSH Password '**Sp1unkH00di3**'

Type '**pwd**'

```
splunk@show-s4x-config-i-07daadfdf18df69a3:~$ pwd
/home/splunk
```

```
Shell
ssh -p 2222 splunk@XXX.XXX.XXX.XXX

yes

Sp1unkH00di3

pwd
```

Intentionally Blank



Lab 2 - Install Splunk SDK

```
splunk@show-s4x-config-i-07daadfdf18df69a3:~$ sudo chown 10777:10777 -R /opt/splunk/etc/apps/helloworld/
splunk@show-s4x-config-i-07daadfdf18df69a3:~$ ls -l /opt/splunk/etc/apps/
total 148
```

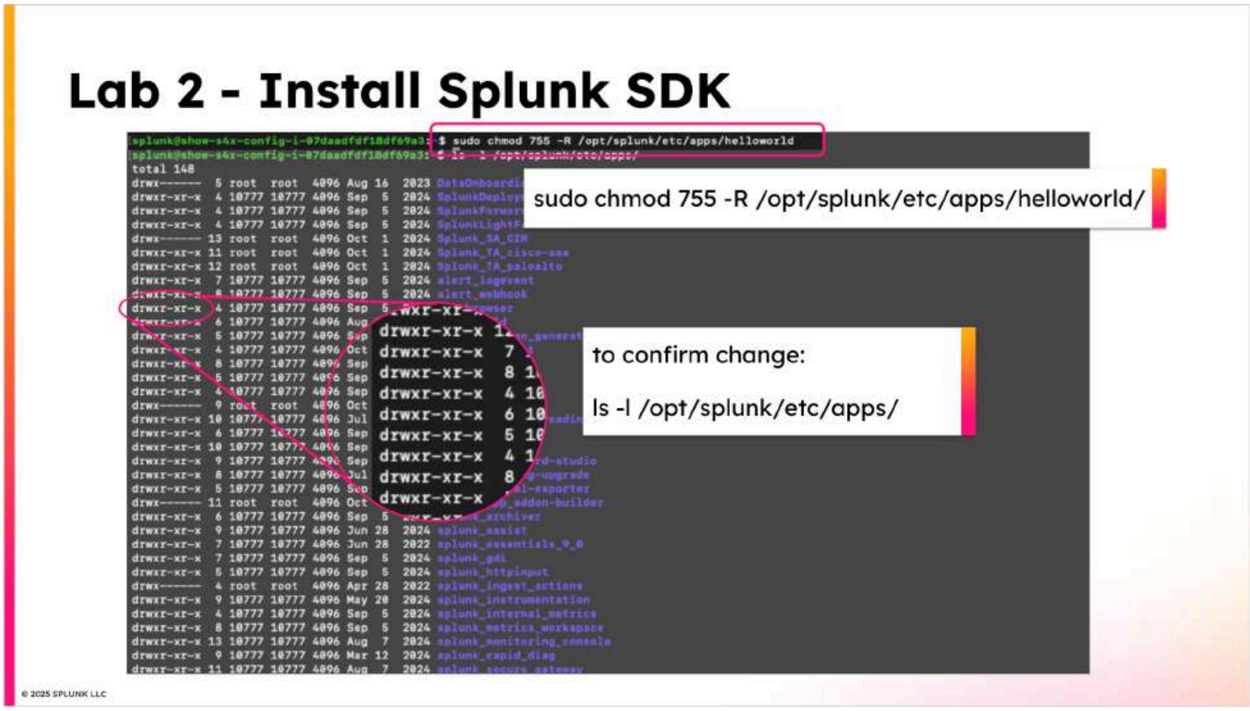
sudo chown 10777:10777 -R /opt/splunk/etc/apps/helloworld/

to confirm change:

ls -l /opt/splunk/etc/apps/

Shell

```
sudo chown 10777:10777 -R /opt/splunk/etc/apps/helloworld/

ls -l /opt/splunk/etc/apps/
```



Lab 2 - Install Splunk SDK

```
splunk@show-s4x-config-i-07daadfdf18df69a3:~$ sudo chmod 755 -R /opt/splunk/etc/apps/helloworld
splunk@show-s4x-config-i-07daadfdf18df69a3:~$ ls -l /opt/splunk/etc/apps/
total 148
```

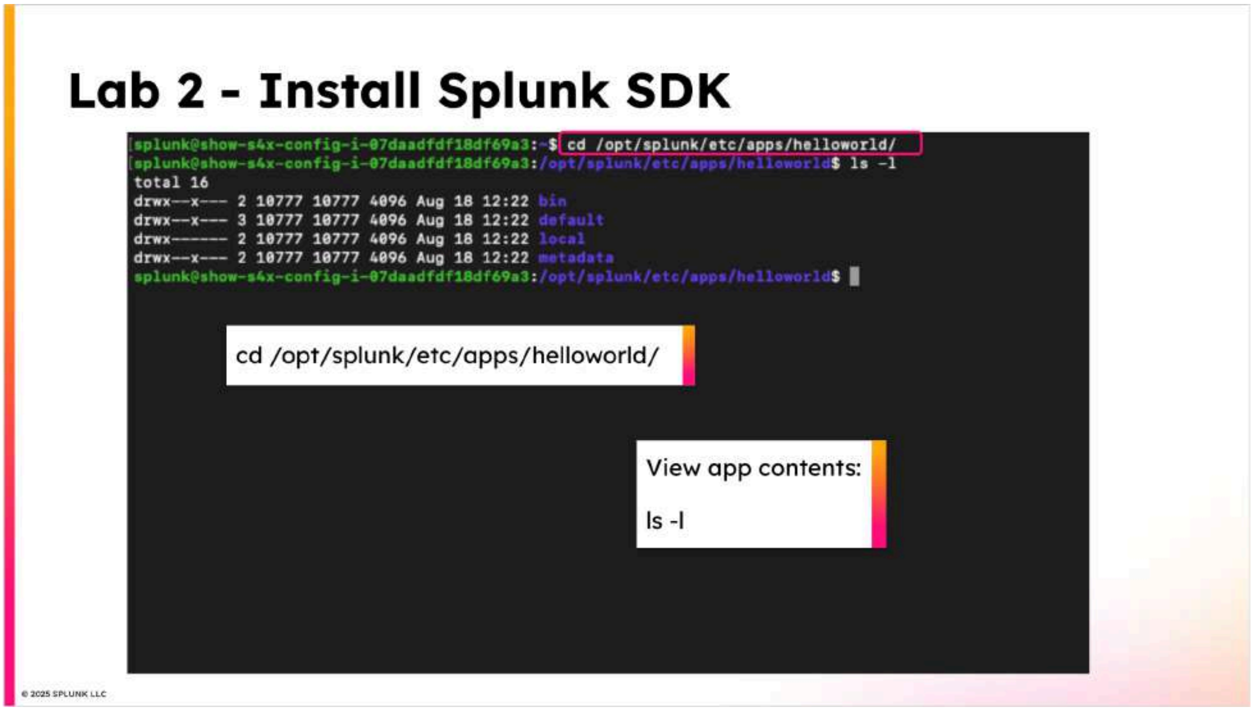
sudo chmod 755 -R /opt/splunk/etc/apps/helloworld/

to confirm change:

ls -l /opt/splunk/etc/apps/

Shell

```
sudo chmod 755 -R /opt/splunk/etc/apps/helloworld/

ls -l /opt/splunk/etc/apps/
```



Lab 2 - Install Splunk SDK

```
splunk@show-s4x-config-i-07daadfdf18df69a3:~$ cd /opt/splunk/etc/apps/helloworld/
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld$ ls -l
total 16
drwx--x--- 2 10777 10777 4096 Aug 18 12:22 bin
drwx--x--- 3 10777 10777 4096 Aug 18 12:22 default
drwx------ 2 10777 10777 4096 Aug 18 12:22 local
drwx--x--- 2 10777 10777 4096 Aug 18 12:22 metadata
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld$
```

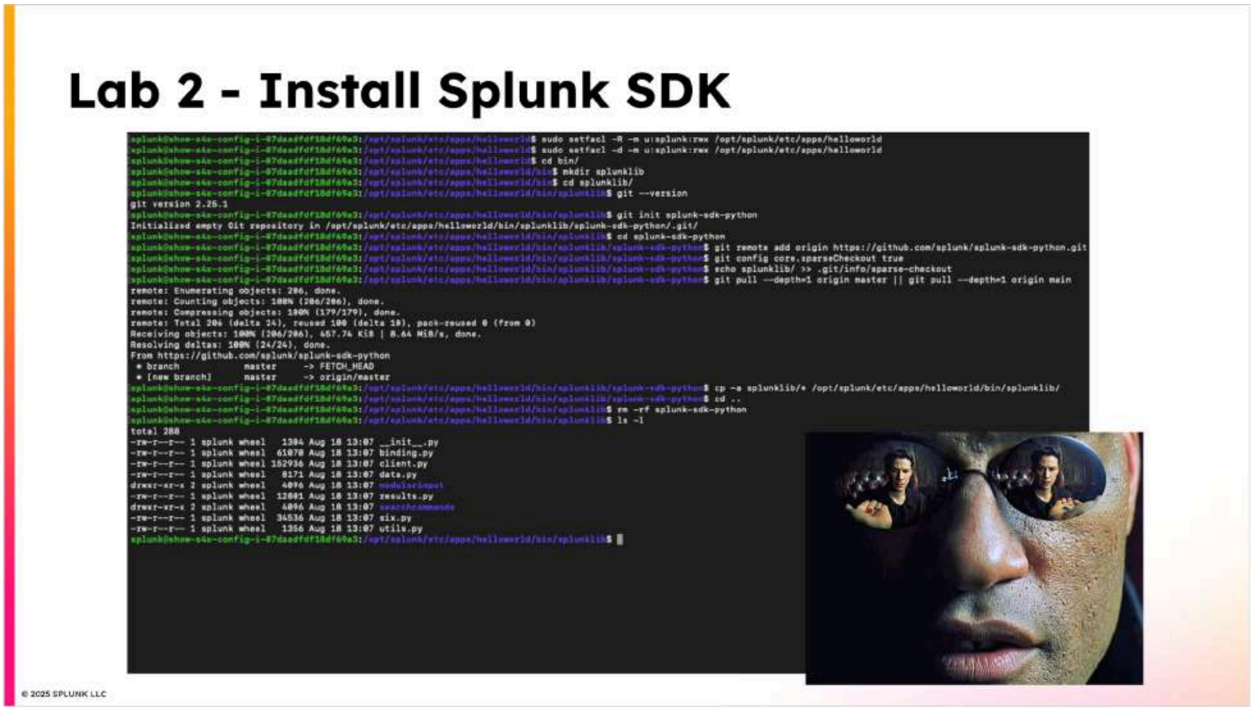
cd /opt/splunk/etc/apps/helloworld/

View app contents:

ls -l

Shell
```
cd /opt/splunk/etc/apps/helloworld/

ls -l
```

Intentionally Blank



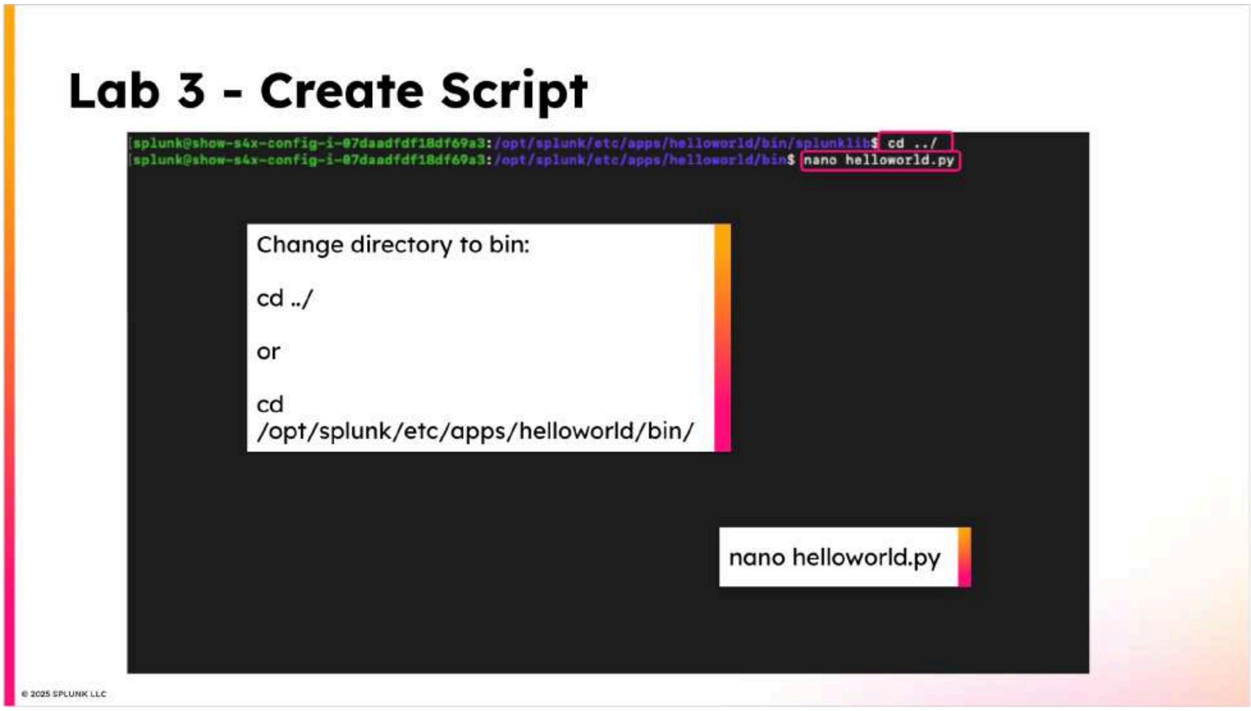
Lab 2 - Install Splunk SDK

```
splunk@show-s4e-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld$ sudo setfacl -R -m u:splunk:rwx /opt/splunk/etc/apps/helloworld
splunk@show-s4e-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld$ sudo setfacl -d -m u:splunk:rwx /opt/splunk/etc/apps/helloworld
splunk@show-s4e-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld$ cd bin/
splunk@show-s4e-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin$ mkdir splunklib
splunk@show-s4e-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin$ cd splunklib/
splunk@show-s4e-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib$ git --version
git version 2.25.1
splunk@show-s4e-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib$ git init splunk-sdk-python
Initialized empty Git repository in /opt/splunk/etc/apps/helloworld/bin/splunklib/splunk-sdk-python/.git/
splunk@show-s4e-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib$ cd splunk-sdk-python
splunk@show-s4e-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib/splunk-sdk-python$ git remote add origin https://github.com/splunk/splunk-sdk-python.git
splunk@show-s4e-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib/splunk-sdk-python$ git config core.sparseCheckout true
splunk@show-s4e-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib/splunk-sdk-python$ echo splunklib/ >> .git/info/sparse-checkout
splunk@show-s4e-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib/splunk-sdk-python$ git pull --depth=1 origin master || git pull --depth=1 origin main
remote: Enumerating objects: 206, done.
remote: Counting objects: 100% (206/206), done.
remote: Compressing objects: 100% (179/179), done.
remote: Total 206 (delta 24), reused 100 (delta 10), pack-reused 0 (from 0)
Receiving objects: 100% (206/206), 457.74 KiB | 8.64 MiB/s, done.
Resolving deltas: 100% (24/24), done.
From https://github.com/splunk/splunk-sdk-python
 * branch            master     -> FETCH_HEAD
 * [new branch]      master     -> origin/master
splunk@show-s4e-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib/splunk-sdk-python$ cp -a splunklib/* /opt/splunk/etc/apps/helloworld/bin/splunklib/
splunk@show-s4e-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib/splunk-sdk-python$ cd ..
splunk@show-s4e-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib$ rm -rf splunk-sdk-python
splunk@show-s4e-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib$ ls -l
total 288
-rw-r--r-- 1 splunk wheel   1304 Aug 18 13:07 __init__.py
-rw-r--r-- 1 splunk wheel  61070 Aug 18 13:07 binding.py
-rw-r--r-- 1 splunk wheel 152936 Aug 18 13:07 client.py
-rw-r--r-- 1 splunk wheel   8171 Aug 18 13:07 data.py
drwxr-xr-x 2 splunk wheel   4096 Aug 18 13:07 modularinput
-rw-r--r-- 1 splunk wheel  12801 Aug 18 13:07 results.py
drwxr-xr-x 2 splunk wheel   4096 Aug 18 13:07 searchcommands
-rw-r--r-- 1 splunk wheel  34536 Aug 18 13:07 six.py
-rw-r--r-- 1 splunk wheel   1356 Aug 18 13:07 utils.py
splunk@show-s4e-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib$ 
```

Shell

```
sudo setfacl -R -m u:splunk:rwx /opt/splunk/etc/apps/helloworld
sudo setfacl -d -m u:splunk:rwx /opt/splunk/etc/apps/helloworld
cd bin/
mkdir splunklib
cd splunklib/
git --version
git init splunk-sdk-python
cd splunk-sdk-python
git remote add origin https://github.com/splunk/splunk-sdk-python.git
git config core.sparseCheckout true
echo splunklib/ >> .git/info/sparse-checkout
git pull --depth=1 origin master || git pull --depth=1 origin main

cp -a splunklib/* /opt/splunk/etc/apps/helloworld/bin/splunklib/
cd ..
rm -rf splunk-sdk-python
```

Lab 3 - Create Script



Lab 3 - Create Script

```
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib$ cd ../
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin$ nano helloworld.py
```

Change directory to bin:

cd ../

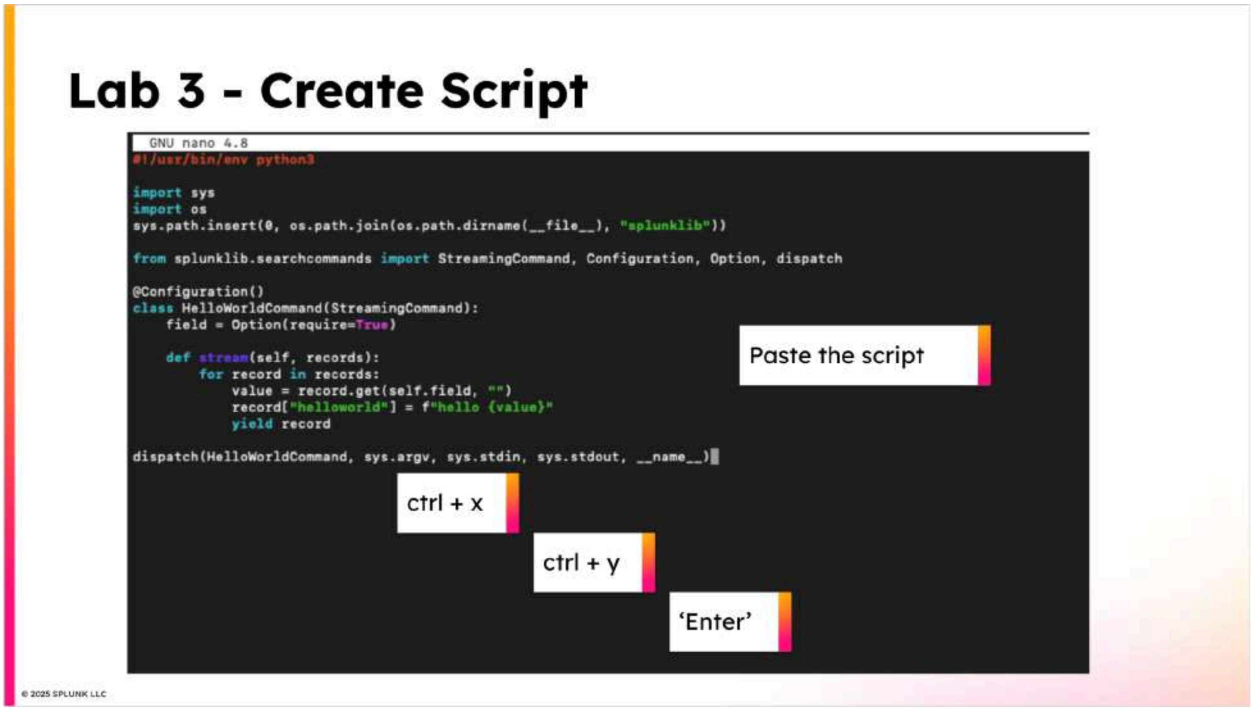
or

cd /opt/splunk/etc/apps/helloworld/bin/

nano helloworld.py

Shell

```
cd /opt/splunk/etc/apps/helloworld/bin/

nano helloworld.py
```



Lab 3 - Create Script

```
  GNU nano 4.8
#!/usr/bin/env python3

import sys
import os
sys.path.insert(0, os.path.join(os.path.dirname(__file__), "splunklib"))

from splunklib.searchcommands import StreamingCommand, Configuration, Option, dispatch

@Configuration()
class HelloWorldCommand(StreamingCommand):
    field = Option(require=True)

    def stream(self, records):
        for record in records:
            value = record.get(self.field, "")
            record["helloworld"] = f"hello {value}"
            yield record

dispatch(HelloWorldCommand, sys.argv, sys.stdin, sys.stdout, __name__)
```

Paste the script

ctrl + x

ctrl + y

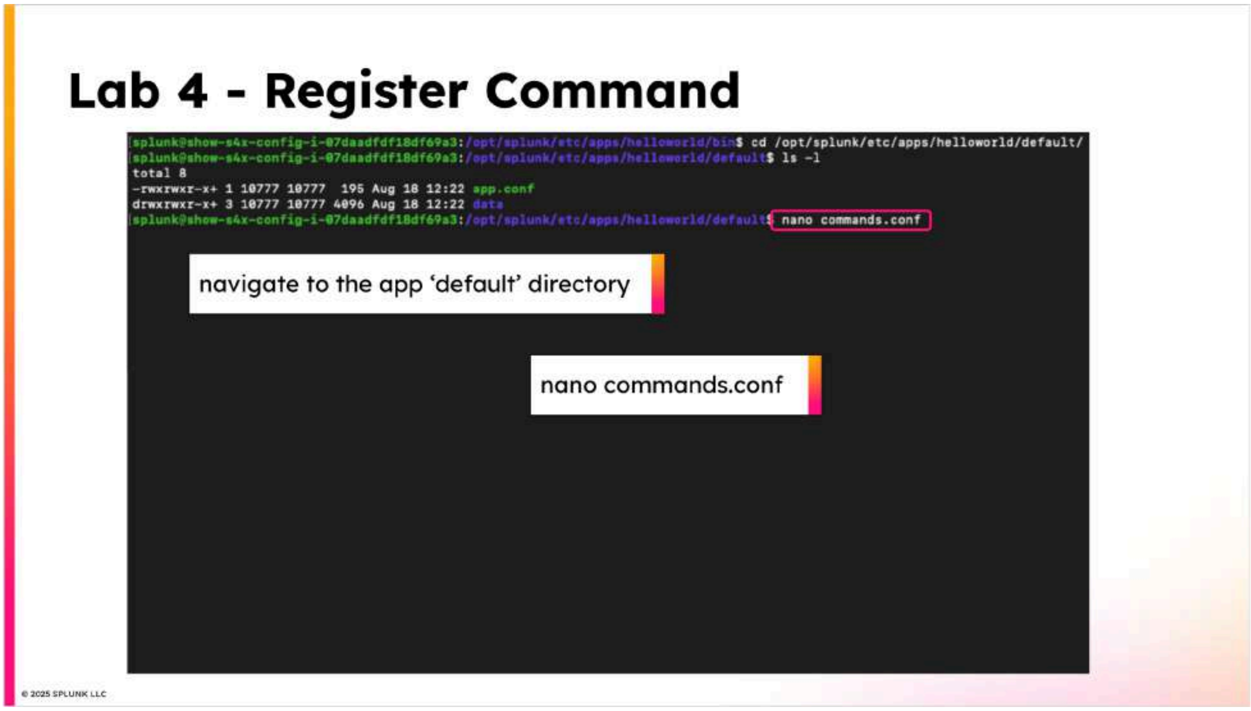
'Enter'

Python

```python
#!/usr/bin/env python3

import sys
import os
sys.path.insert(0, os.path.join(os.path.dirname(__file__), "splunklib"))

from splunklib.searchcommands import StreamingCommand, Configuration, Option, dispatch

@Configuration()
class HelloWorldCommand(StreamingCommand):
    field = Option(require=True)

    def stream(self, records):
        for record in records:
            value = record.get(self.field, "")
            record["helloworld"] = f"hello {value}"
            yield record

dispatch(HelloWorldCommand, sys.argv, sys.stdin, sys.stdout, __name__)
```

Intentionally Blank

Lab 4 - Register Command



Lab 4 - Register Command

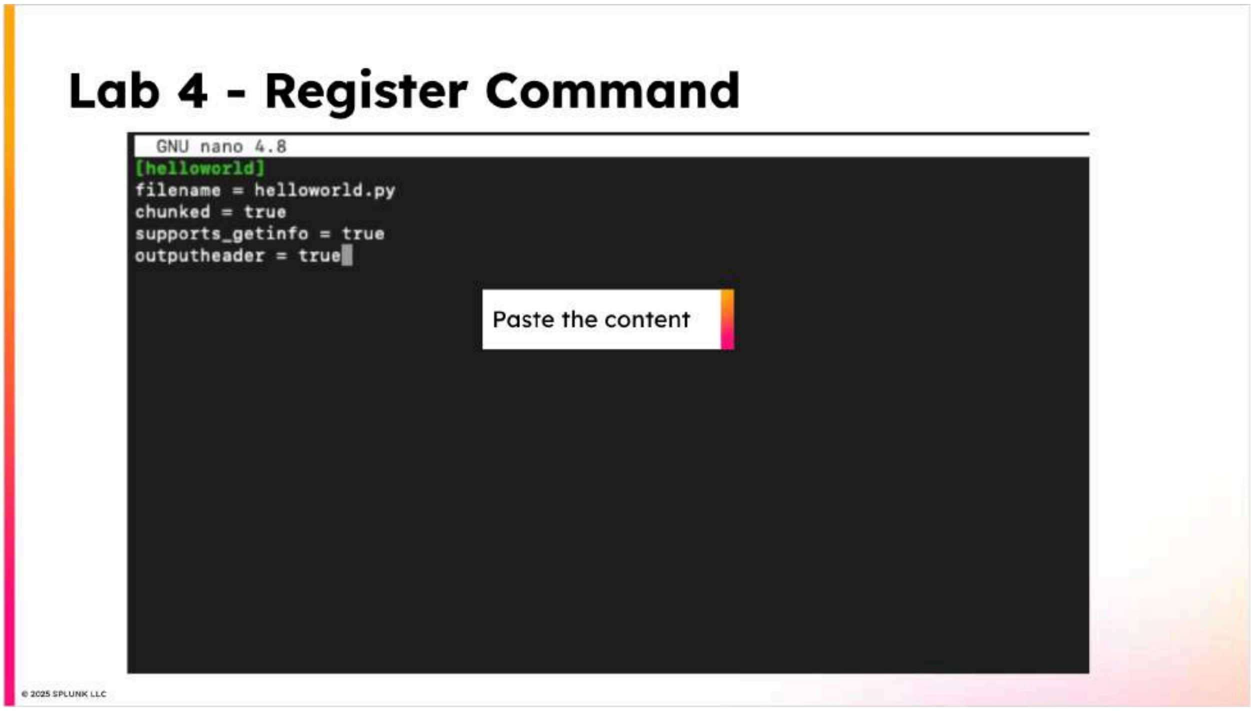
```
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin$ cd /opt/splunk/etc/apps/helloworld/default/
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/default$ ls -l
total 8
-rwxrwxr-x+ 1 10777 10777  195 Aug 18 12:22 app.conf
drwxrwxr-x+ 3 10777 10777 4096 Aug 18 12:22 data
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/default$ nano commands.conf
```

navigate to the app 'default' directory

nano commands.conf

Shell
```
nano commands.conf
```

Intentionally Blank



Lab 4 - Register Command

```
  GNU nano 4.8
[helloworld]
filename = helloworld.py
chunked = true
supports_getinfo = true
outputheader = true
```

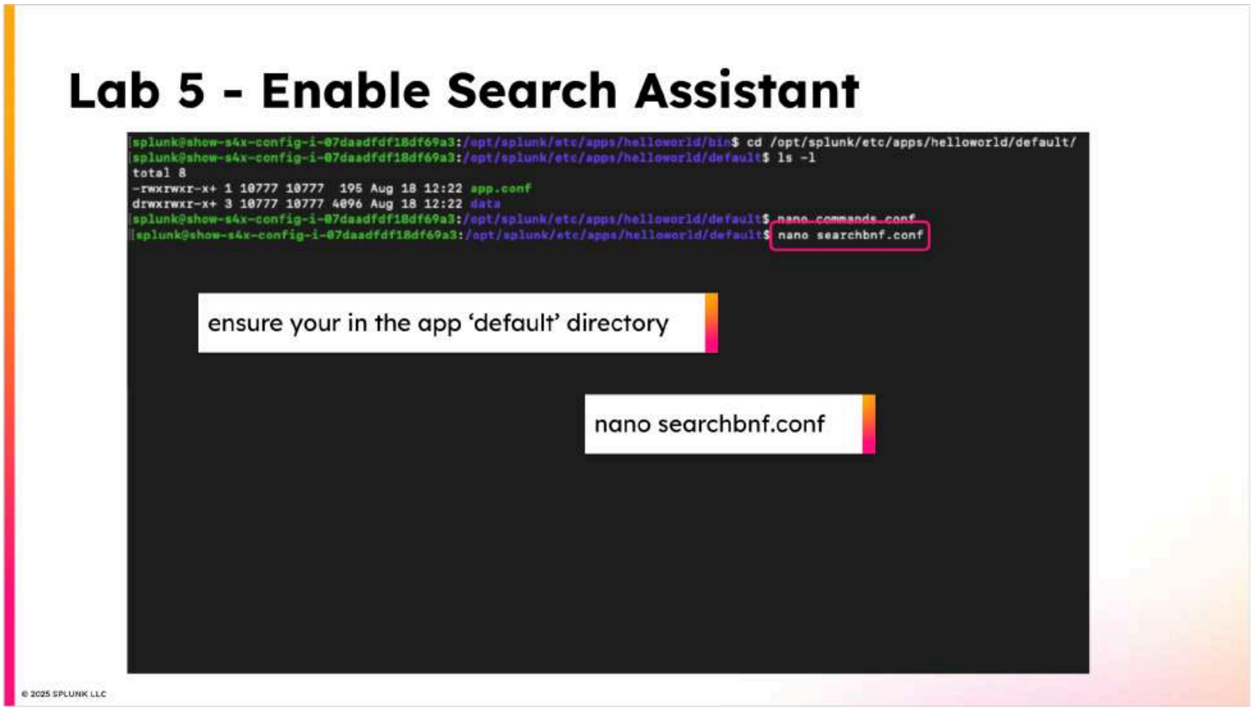
Paste the content

© 2025 SPLUNK LLC

```
None
[helloworld]
filename = helloworld.py
chunked = true
supports_getinfo = true
outputheader = true
```

Intentionally Blank

Lab 5 - Enable Search Assistant



Lab 5 - Enable Search Assistant

```
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin$ cd /opt/splunk/etc/apps/helloworld/default/
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/default$ ls -l
total 8
-rwxrwxr-x+ 1 10777 10777  195 Aug 18 12:22 app.conf
drwxrwxr-x+ 3 10777 10777 4096 Aug 18 12:22 data
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/default$ ~~nano commands.conf~~
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/default$ nano searchbnf.conf
```

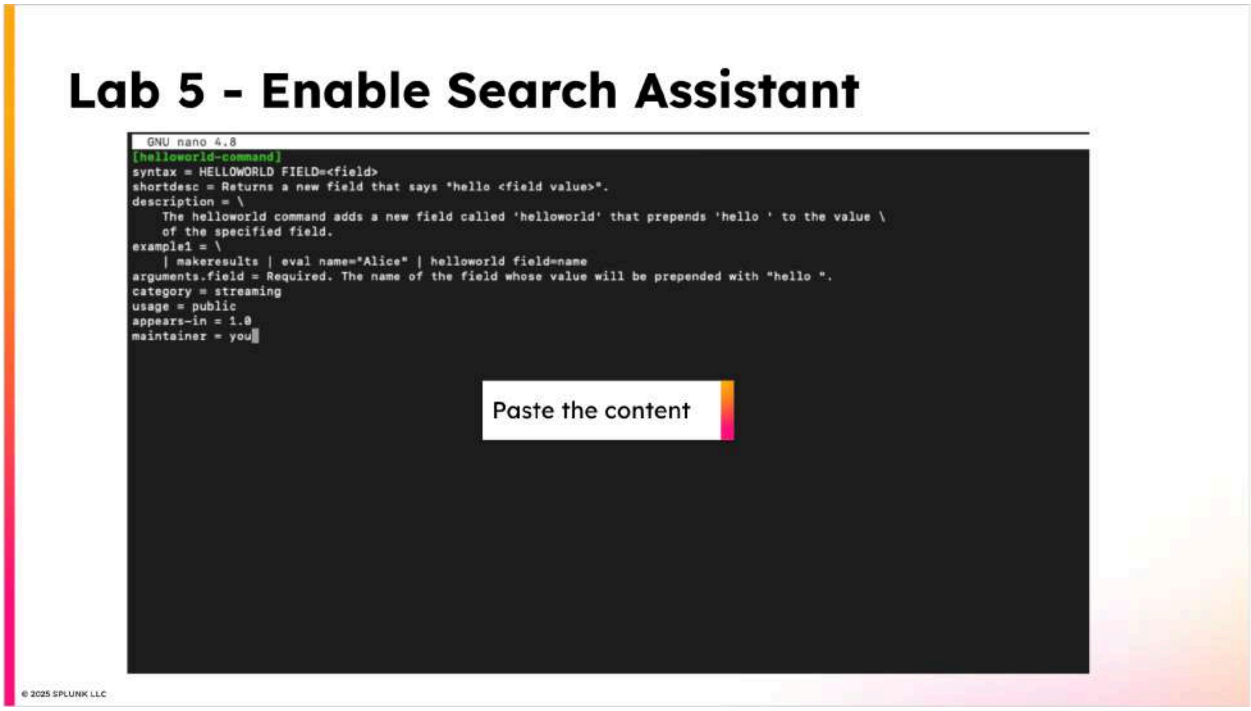
ensure your in the app 'default' directory

nano searchbnf.conf

Shell

```
nano searchbnf.conf
```

Intentionally Blank



Lab 5 - Enable Search Assistant

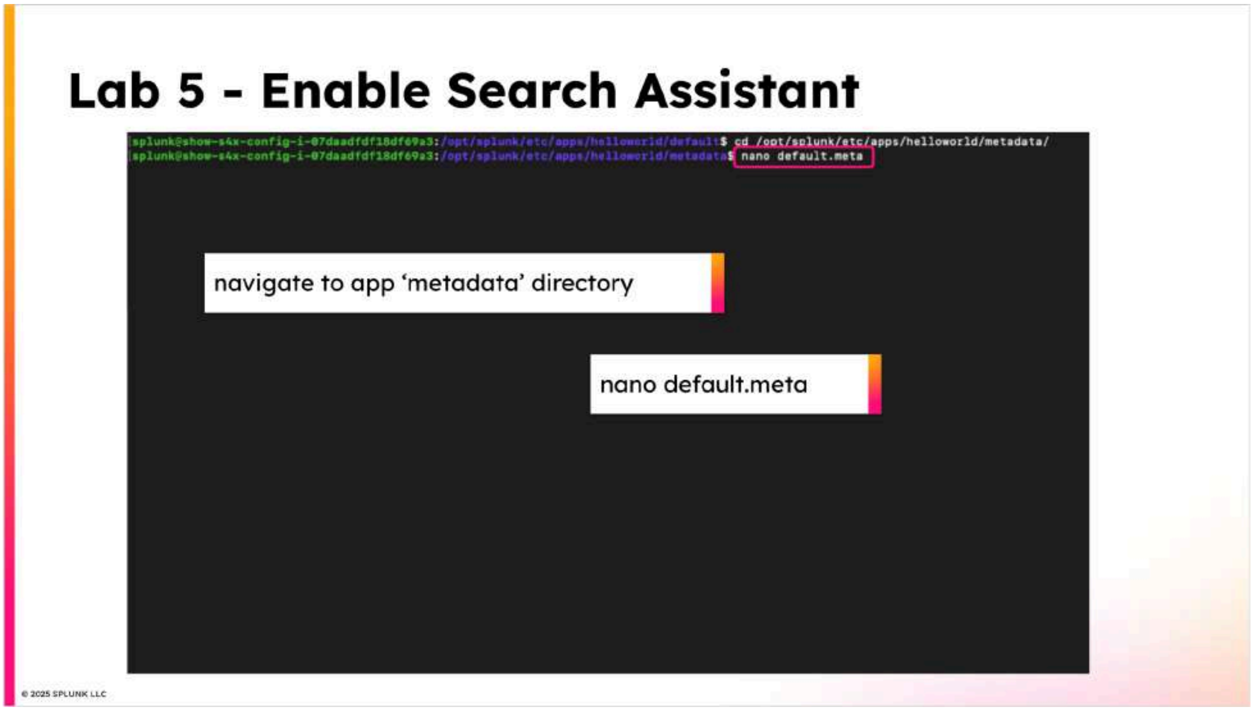
```
[helloworld-command]
syntax = HELLOWORLD FIELD=<field>
shortdesc = Returns a new field that says "hello <field value>".
description = \
    The helloworld command adds a new field called 'helloworld' that prepends 'hello ' to the value \
    of the specified field.
example1 = \
    | makeresults | eval name="Alice" | helloworld field=name
arguments.field = Required. The name of the field whose value will be prepended with "hello ".
category = streaming
usage = public
appears-in = 1.0
maintainer = you
```

Paste the content

None

```
[helloworld-command]
syntax = HELLOWORLD FIELD=<field>
shortdesc = Returns a new field that says "hello <field value>".
description = \
    The helloworld command adds a new field called 'helloworld' that prepends
'hello ' to the value \
    of the specified field.
example1 = \
    | makeresults | eval name="Alice" | helloworld field=name
arguments.field = Required. The name of the field whose value will be prepended
with "hello ".
category = streaming
usage = public
appears-in = 1.0
maintainer = you
```

Intentionally Blank



Lab 5 - Enable Search Assistant

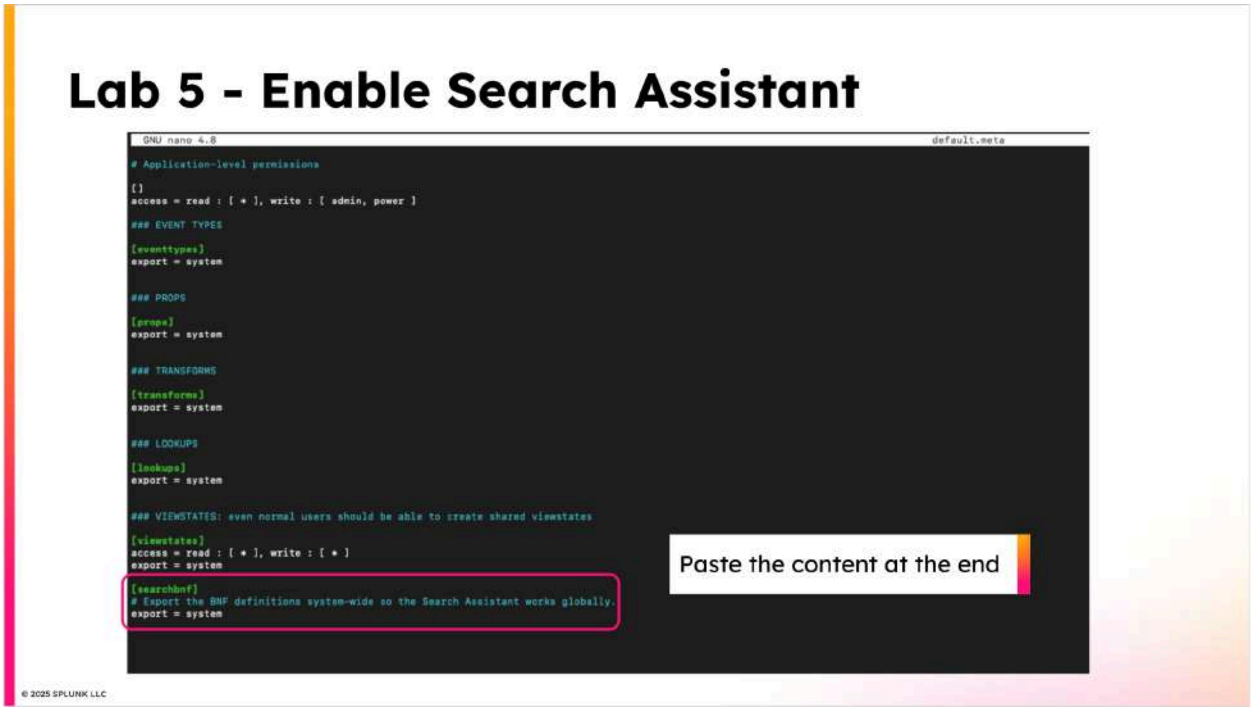
```
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/default$ cd /opt/splunk/etc/apps/helloworld/metadata/
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/metadata$ nano default.meta
```

navigate to app ‘metadata’ directory

nano default.meta

Shell

```
nano default.meta
```



Lab 5 - Enable Search Assistant

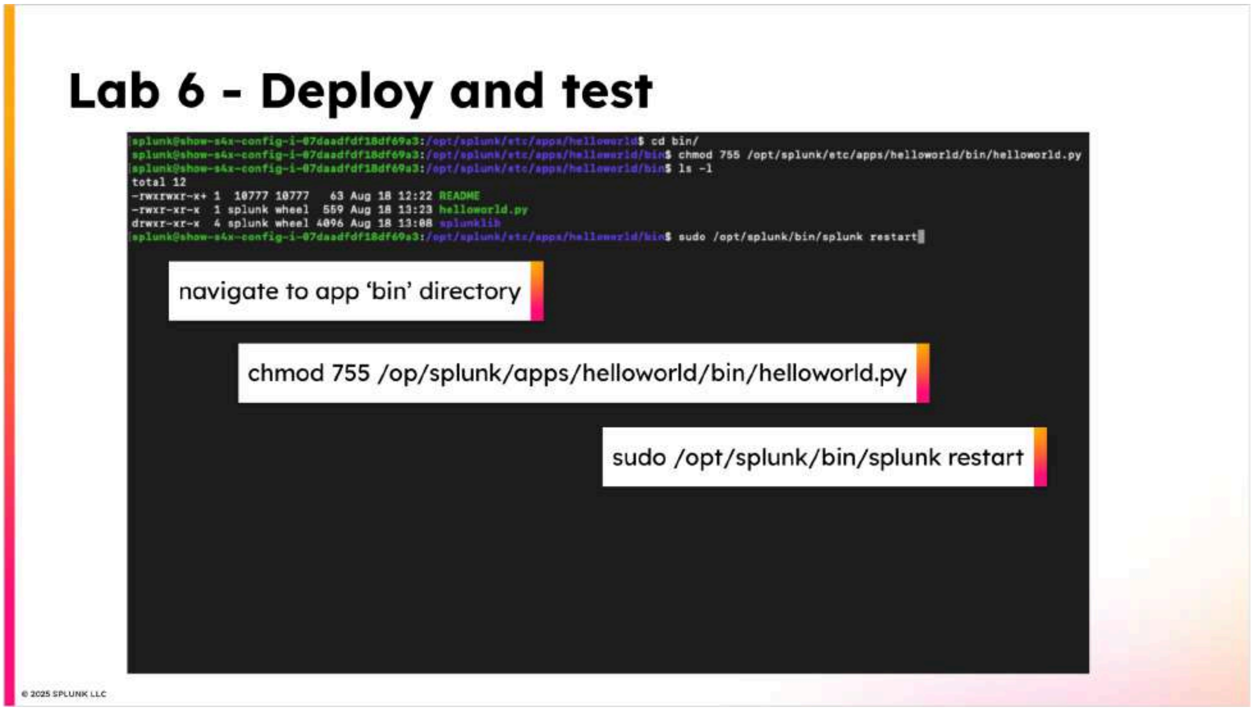
```
  GNU nano 4.8                                                                                    default.meta

# Application-level permissions

[]
access = read : [ * ], write : [ admin, power ]

### EVENT TYPES

[eventtypes]
export = system


### PROPS

[props]
export = system


### TRANSFORMS

[transforms]
export = system


### LOOKUPS

[lookups]
export = system


### VIEWSTATES: even normal users should be able to create shared viewstates

[viewstates]
access = read : [ * ], write : [ * ]
export = system

[searchbnf]
# Export the BNF definitions system-wide so the Search Assistant works globally.
export = system
```

Paste the content at the end

None

```
[searchbnf]
export = system
```

Lab 6 - Deploy and test



Lab 6 - Deploy and test

```
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld$ cd bin/
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin$ chmod 755 /opt/splunk/etc/apps/helloworld/bin/helloworld.py
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin$ ls -l
total 12
-rwxrwxr-x+ 1  10777 10777   63 Aug 18 12:22 README
-rwxr-xr-x  1 splunk wheel  559 Aug 18 13:23 helloworld.py
drwxr-xr-x  4 splunk wheel 4096 Aug 18 13:08 splunklib
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin$ sudo /opt/splunk/bin/splunk restart
```

navigate to app ‘bin’ directory

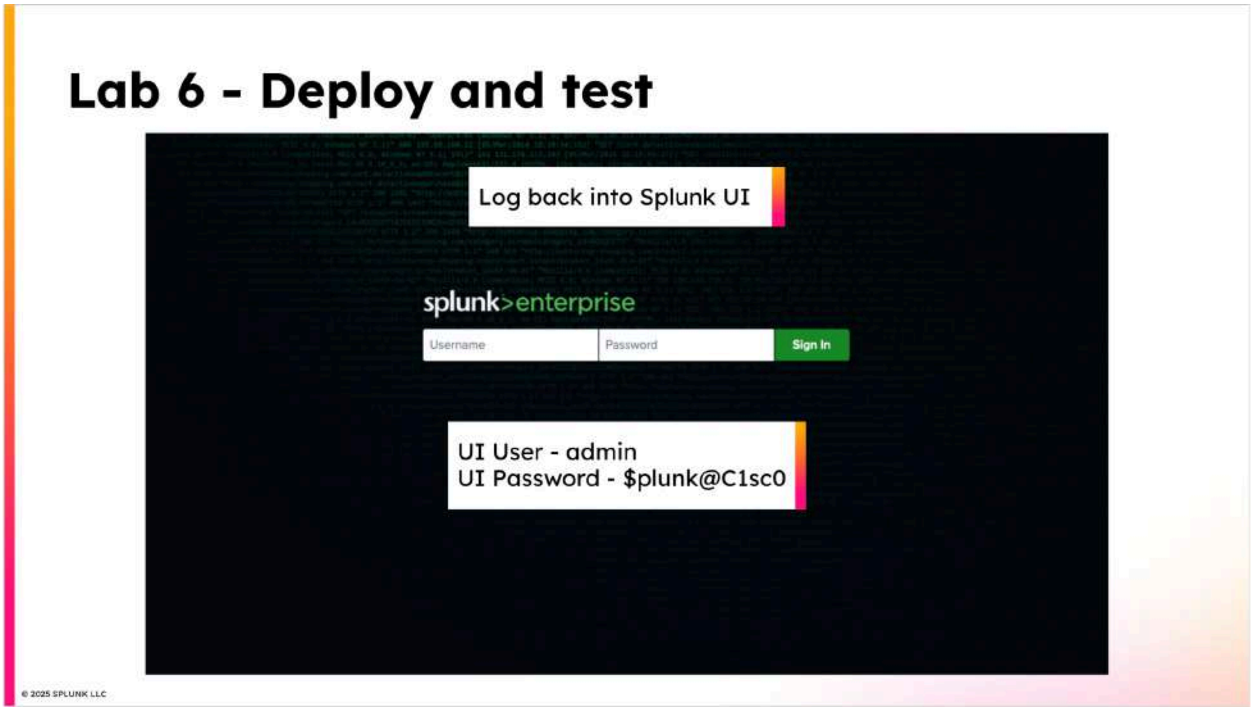
chmod 755 /op/splunk/apps/helloworld/bin/helloworld.py

sudo /opt/splunk/bin/splunk restart

© 2025 SPLUNK LLC

Shell

```
chmod 755 /op/splunk/apps/helloworld/bin/helloworld.py

sudo /opt/splunk/bin/splunk restart
```



Lab 6 - Deploy and test

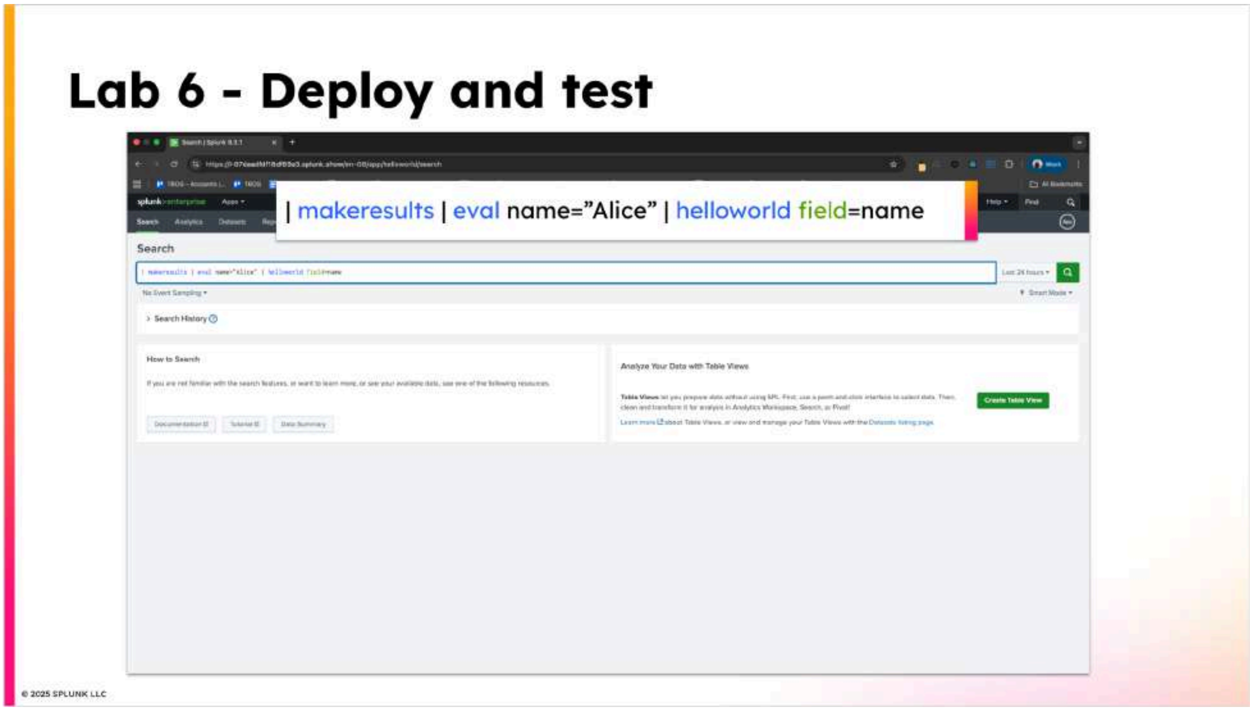
Log back into Splunk UI

UI User - admin
UI Password - $plunk@C1sc0

© 2025 SPLUNK LLC

None

```
admin
$plunk@C1sc0
```



Lab 6 - Deploy and test

| makeresults | eval name="Alice" | helloworld field=name

Search

| makeresults | eval name="Alice" | helloworld field=name

How to Search

If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.

Analyze Your Data with Table Views

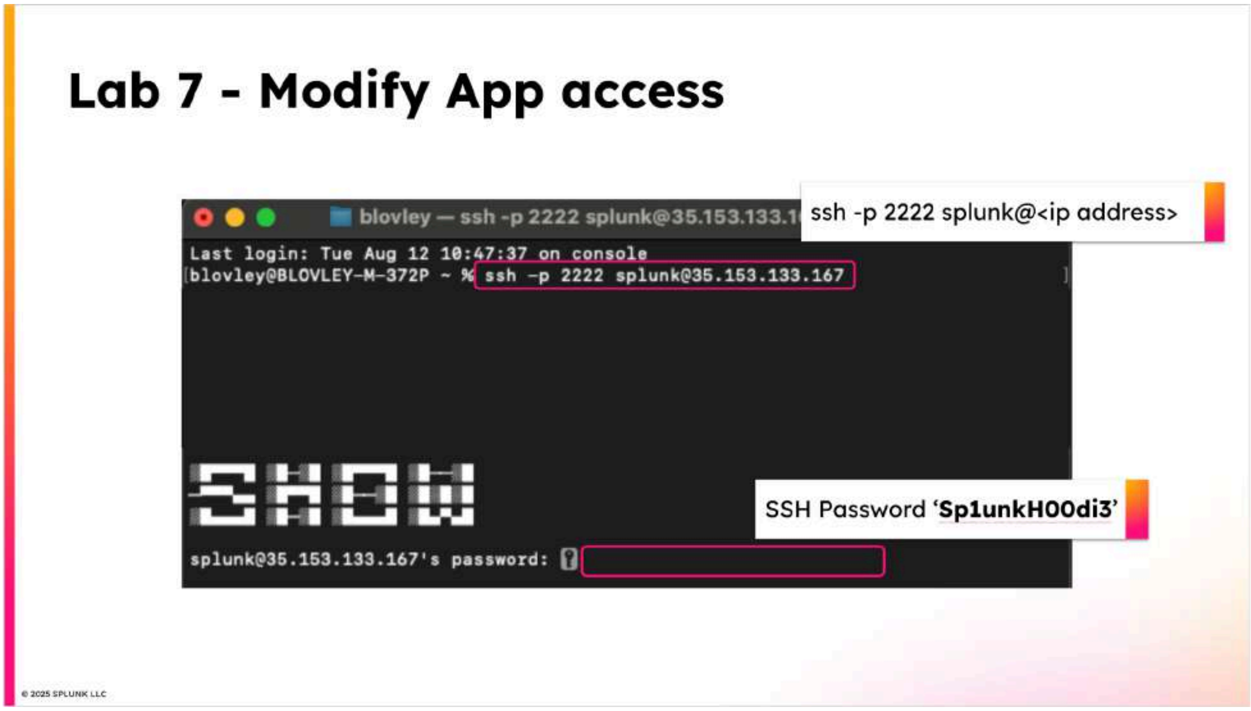
Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for analysis in Analytics Workspace, Search, or Pivot!

Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.

```
None
| makeresults | eval name=”Alice” | helloworld field=name
```

Intentionally Blank

Lab 7 - Modify App access



Lab 7 - Modify App access

```
blovley — ssh -p 2222 splunk@35.153.133.1
Last login: Tue Aug 12 10:47:37 on console
[blovley@BLOVLEY-M-372P ~ % ssh -p 2222 splunk@35.153.133.167

splunk@35.153.133.167's password:
```

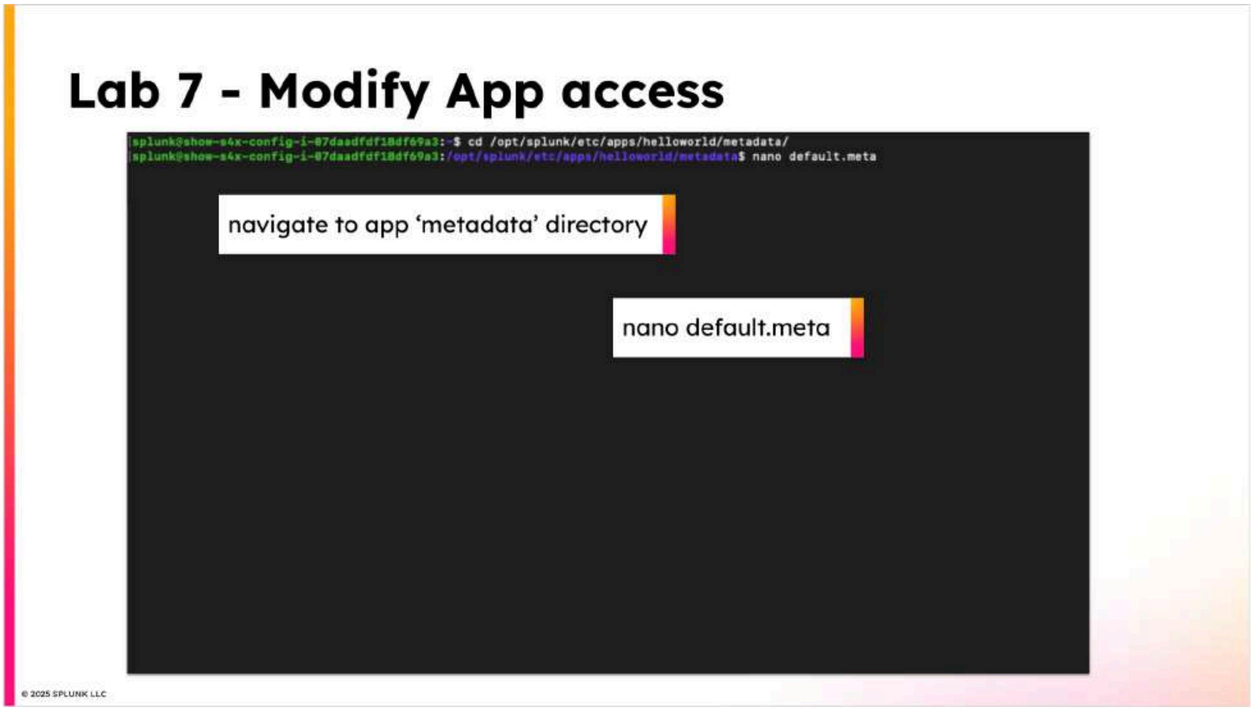
ssh -p 2222 splunk@<ip address>

SSH Password ‘**Sp1unkH00di3**’

Shell

```
ssh -p 2222 splunk@XXX.XXX.XXX.XXX

Sp1unkH00di3
```

Intentionally Blank



Lab 7 - Modify App access

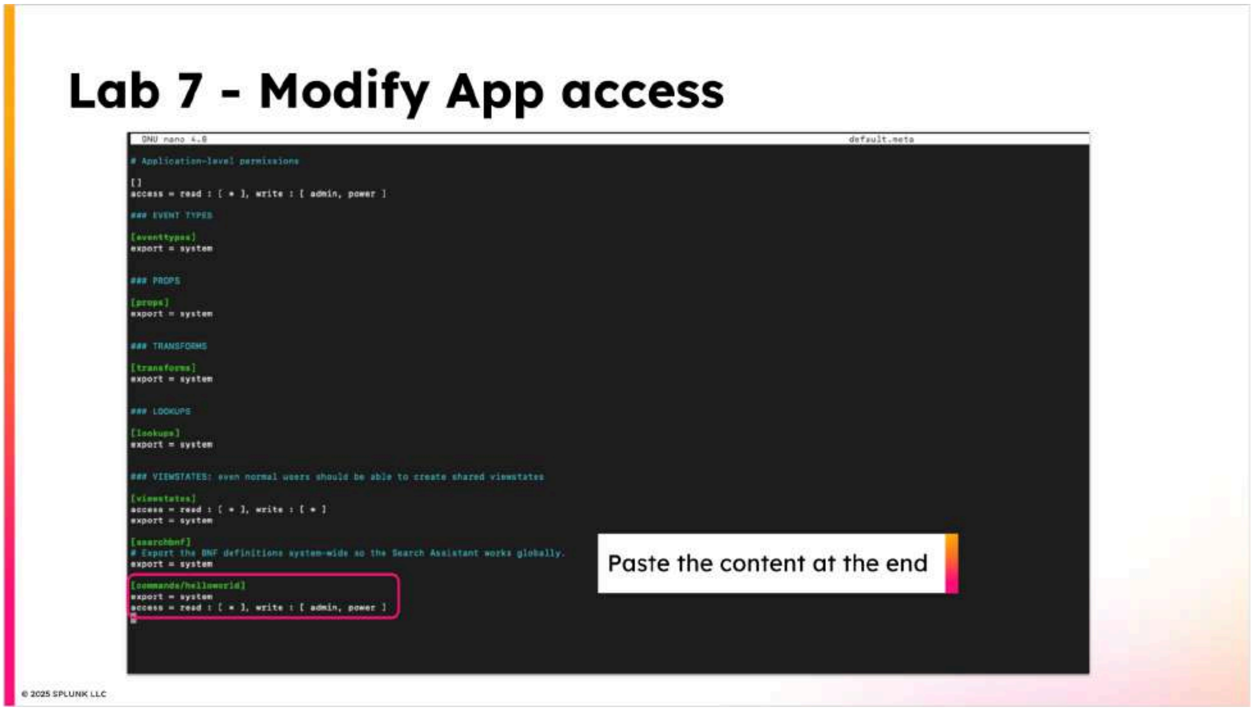
```
splunk@show-s4x-config-i-07daadfdf18df69a3:~$ cd /opt/splunk/etc/apps/helloworld/metadata/
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/metadata$ nano default.meta
```

navigate to app ‘metadata’ directory

nano default.meta

Shell
```
cd /opt/splunk/etc/apps/helloworld/metadata

nano default.meta
```

Intentionally Blank



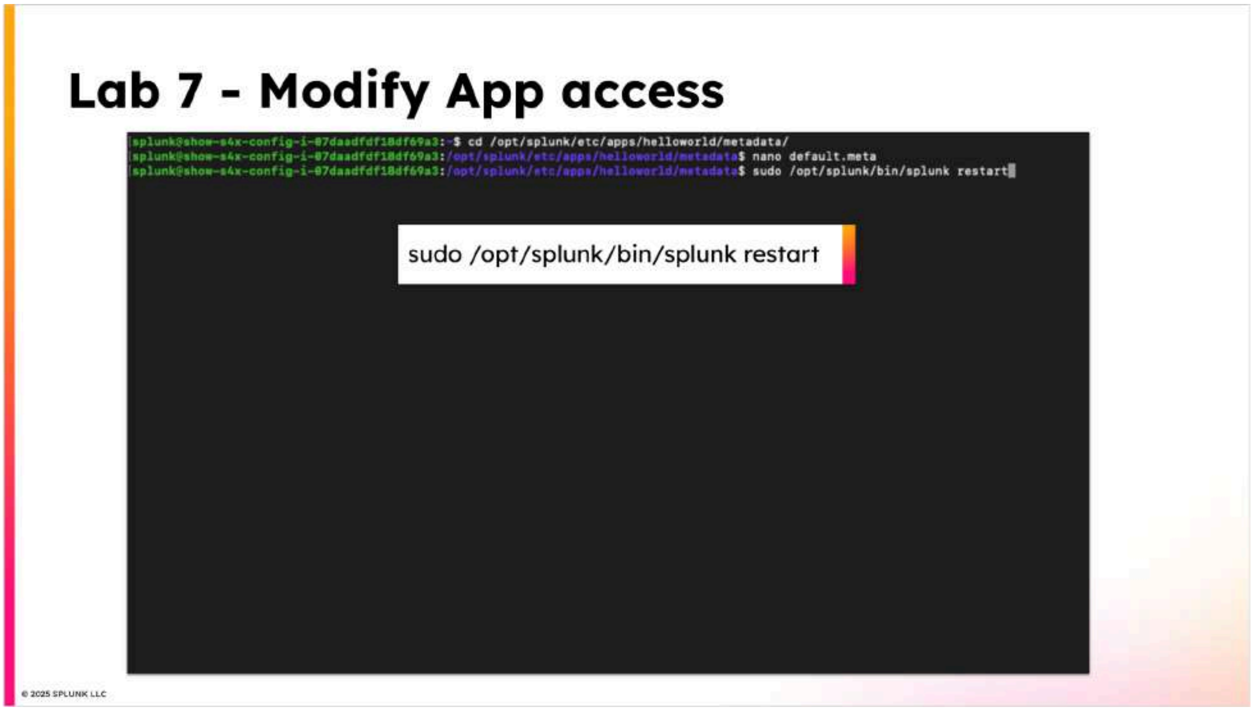
Lab 7 - Modify App access

```
  GNU nano 4.8                                                          default.meta
# Application-level permissions

[]
access = read : [ * ], write : [ admin, power ]

### EVENT TYPES

[eventtypes]
export = system


### PROPS

[props]
export = system


### TRANSFORMS

[transforms]
export = system


### LOOKUPS

[lookups]
export = system


### VIEWSTATES: even normal users should be able to create shared viewstates

[viewstates]
access = read : [ * ], write : [ * ]
export = system

[searchbnf]
# Export the BNF definitions system-wide so the Search Assistant works globally.
export = system

[commands/helloworld]
export = system
access = read : [ * ], write : [ admin, power ]
```

Paste the content at the end

None

```
[commands/helloworld]
export = system
access = read : [ * ], write : [ admin, power ]
```



Lab 7 - Modify App access

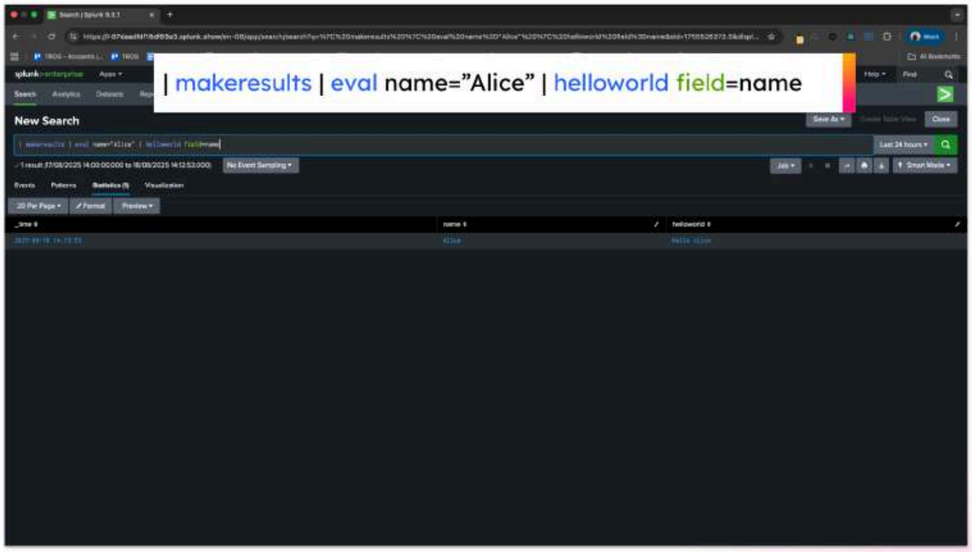
```
splunk@show-s4x-config-i-07daadfdf18df69a3:~$ cd /opt/splunk/etc/apps/helloworld/metadata/
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/metadata$ nano default.meta
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/metadata$ sudo /opt/splunk/bin/splunk restart
```

sudo /opt/splunk/bin/splunk restart

Shell

```
sudo /opt/splunk/bin/splunk restart
```

Lab 7 - Modify App access



| makeresults | eval name=”Alice” | helloworld field=name

_time	name	helloworld
[illegible]	Alice	Hello Alice

```
None
| makeresults | eval name=”Alice” | helloworld field=name
```