KGiSL Educational Institutions,cbe.

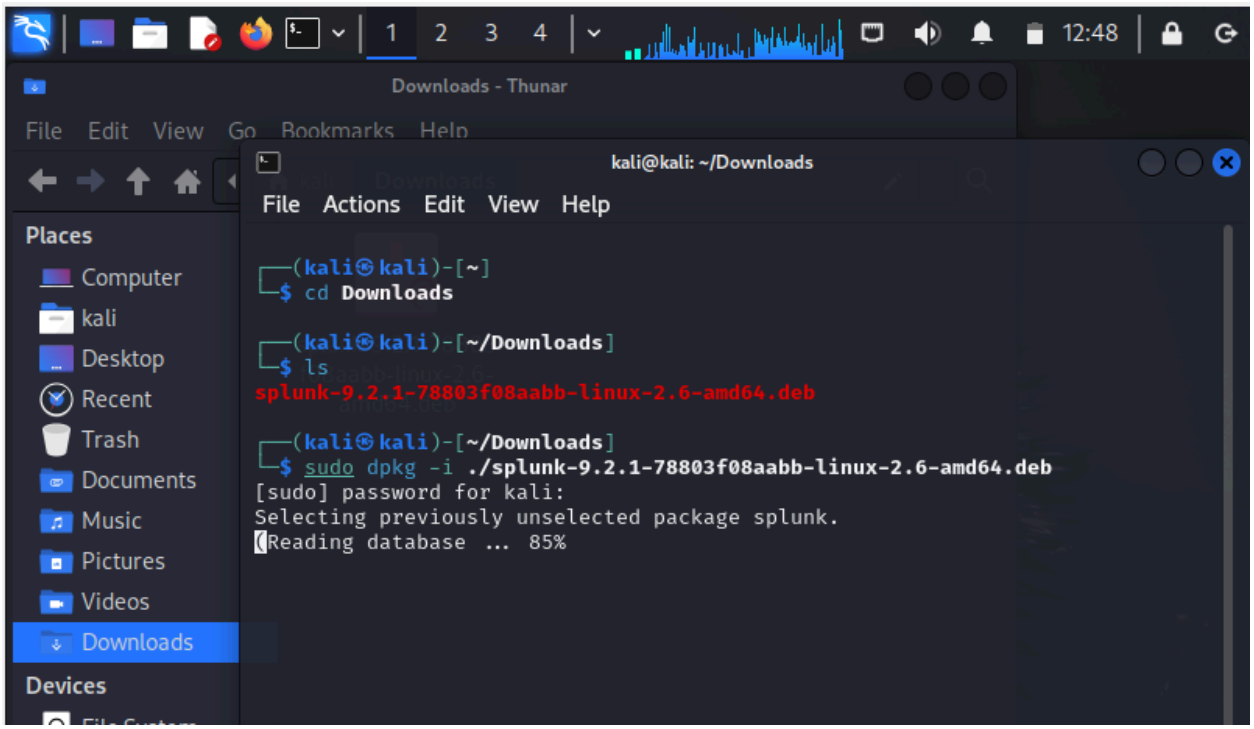
How to Download & Install Splunk in Kali Linux?

Step 1: Prerequisite ,to download splunk for linux .deb from the splunk website
Step 2: Open a terminal, and goto downloads and check its availability.

Cd Downloads
ls

Step 3: To install Splunk suing the command

Sudo dpkg -i ./splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb



```
┌──(kali㉿kali)-[~]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo dpkg -i ./splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb
[sudo] password for kali:
Selecting previously unselected package splunk.
(Reading database ... 404048 files and directories currently installed.)
Preparing to unpack .../splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb ...
Unpacking splunk (9.2.1+78803f08aabb) ...
Setting up splunk (9.2.1+78803f08aabb) ...
complete
```

Step 4: Check whether its installed

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls /opt
microsoft  splunk
```

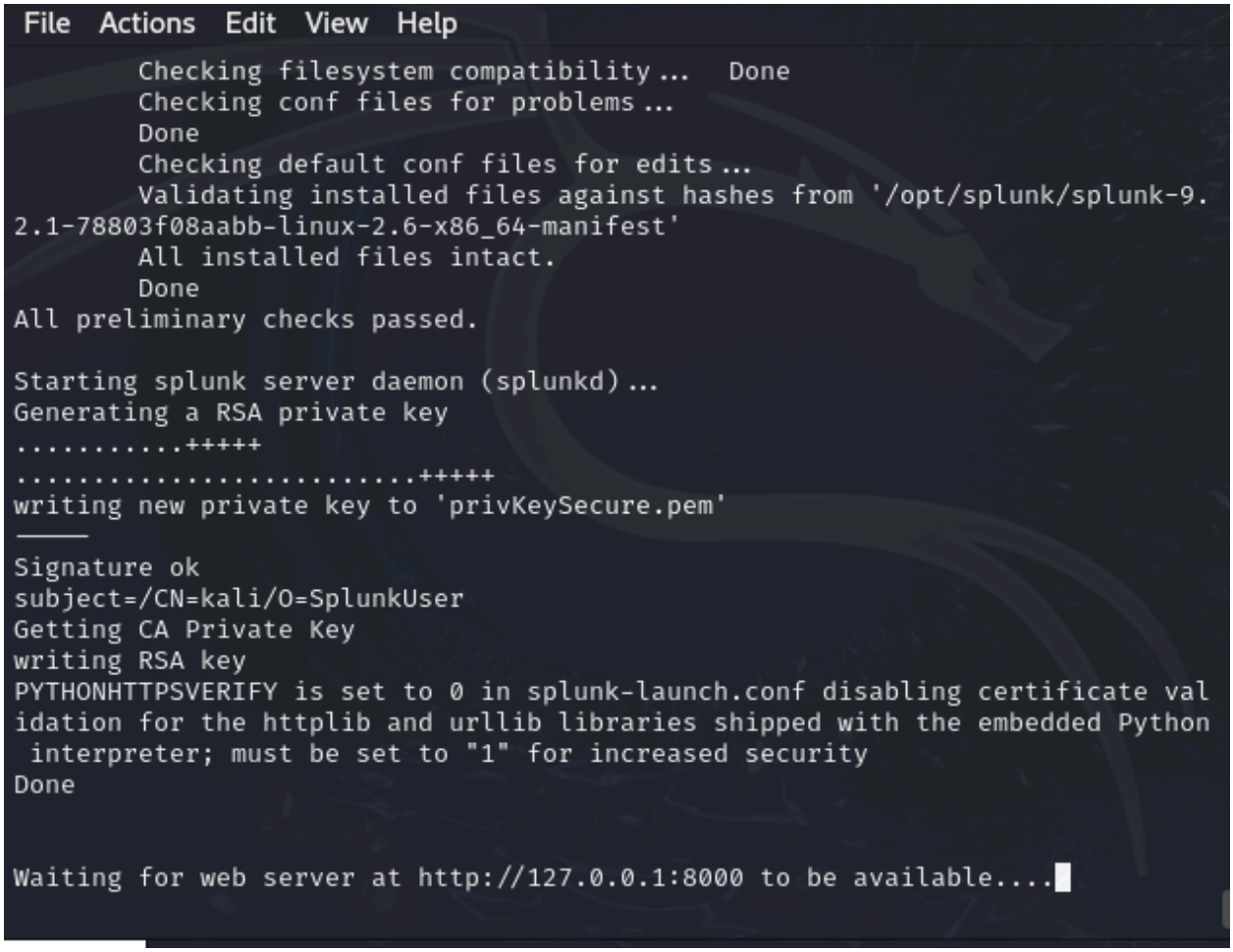
Start : To start Splunk server

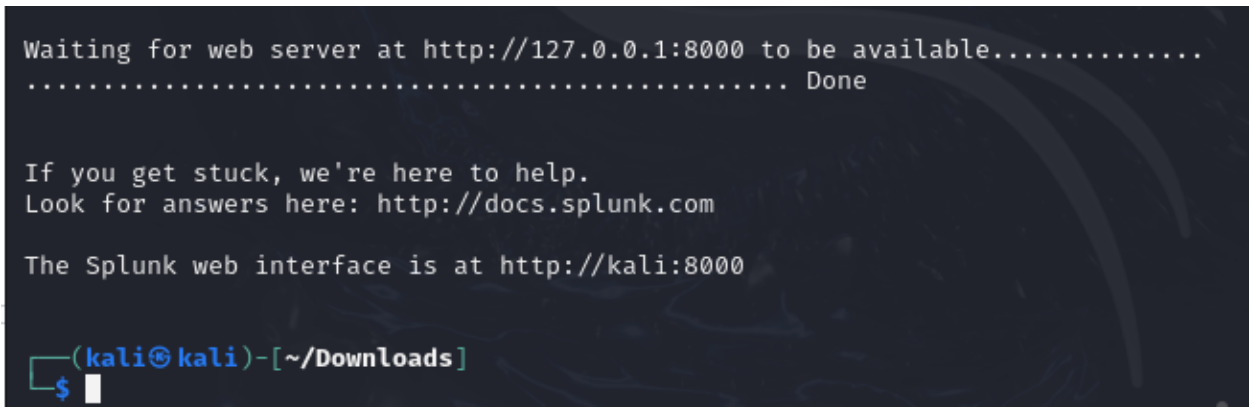
```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls /opt
microsoft  splunk

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo /opt/splunk/bin/splunk start
[sudo] password for kali:
```

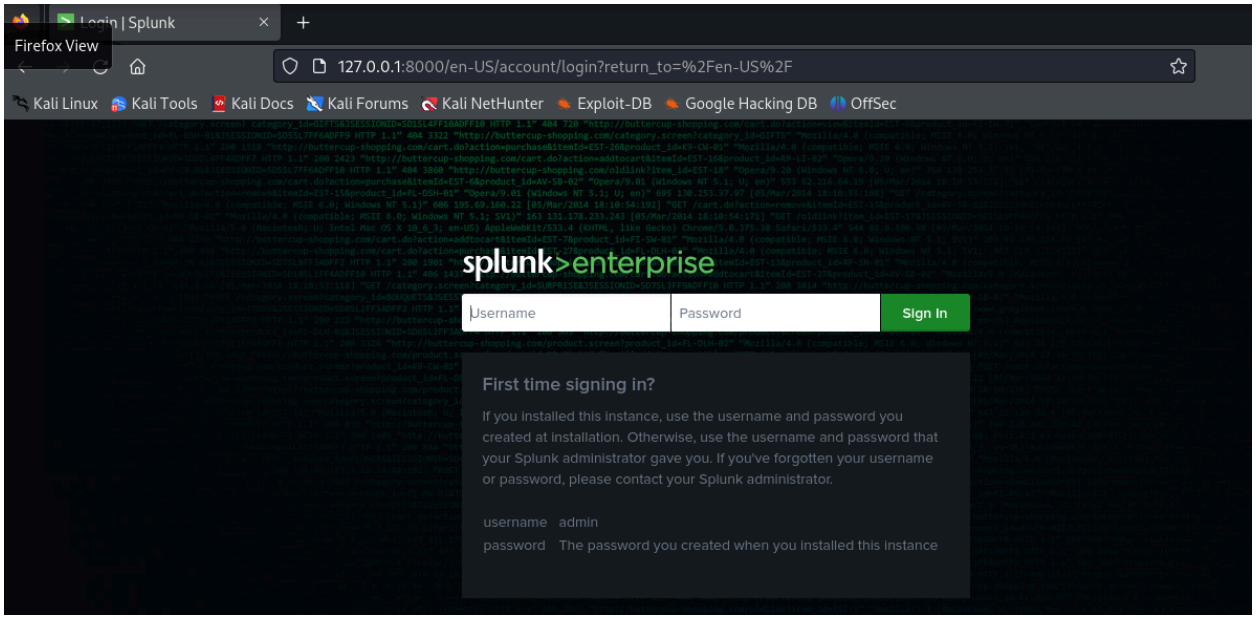
```
your users use any of the Offerings. You certify that you are not on any of
the relevant U.S. government lists of prohibited persons, including the
Treasury Department's List of Specially Designated Nationals and the Commerce
Department's List of Denied Persons or Entity List. You will not export,
re-export, ship, transfer or otherwise use the Offerings in any country
subject to an embargo or other sanction by the United States, including,
without limitation, Iran, Syria, Cuba, the Crimea Region of Ukraine, Sudan an
d
North Korea, and you will not use any Offering for any purpose prohibited by
the Export Laws.

(D) GovCloud Services. If you access or use any Hosted Services in the
specially isolated Amazon Web Services ("AWS") GovCloud (US) region (includin
g
without limitation any Hosted Services that are provisioned in a FedRAMP
authorized environment), you  represent and warrant that users will only
access the Hosted Services in the AWS GovCloud (US) region if users: (i) are
"US Person(s)" as defined under ITAR (see 22 CFR part 120.15); (ii) have and
will maintain a valid Directorate of Defense Trade Controls registration, if
required by ITAR; (iii) are not subject to export control restrictions under
US export control laws and regulations (i.e., users are not denied or debarre
d
parties or otherwise subject to sanctions); and (iv) maintain an effective
compliance program to ensure compliance with applicable US export control law
s
and regulations, including ITAR, as applicable. If you access or use any
--More--(36%)
```

```
"Statement of Work" means the statements of work and/or any and all applicabl
e
Orders, that describe the specific services to be performed by Splunk,
including any materials and deliverables to be delivered by Splunk.
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]: y
```

```
Please enter an administrator username: sakthivel.d@kgcas.com
WARN  ConfMetrics - single_action=BASE_INITIALIZE took wallclock_ms=1449
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
```


File Actions Edit View Help
Checking filesystem compatibility... Done
Checking conf files for problems...
Done
Checking default conf files for edits...
Validating installed files against hashes from '/opt/splunk/splunk-9.2.1-78803f08aabb-linux-2.6-x86_64-manifest'
All installed files intact.
Done
All preliminary checks passed.
Starting splunk server daemon (splunkd)...
Generating a RSA private key
writing new private key to 'privKeySecure.pem'
Signature ok
subject=/CN=kali/O=SplunkUser
Getting CA Private Key
writing RSA key
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done
Waiting for web server at http://127.0.0.1:8000 to be available....


Waiting for web server at http://127.0.0.1:8000 to be available.....
Done
If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com
The Splunk web interface is at http://kali:8000
(kali㉿kali)-[~/Downloads]
$



Goto Settings - Server Setting - General Setting - Enable SSL