Splunk Installation

Before we install splunk we need to change some settings.

First we remove the "virbr0" network interface as it's useless for our project. Virbr0 is used for virtualization purposes and acts as a switch you can connect your guests and your host if you are virtualizing.

```
virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
        ether 52:54:00:d1:2f:c2  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

To do this enter following commands:

`systemctl stop libvirtd.service`

`systemctl status libvirtd.service -> make sure service is innactive`

`systemctl disable libvirtd.service`

`reboot`

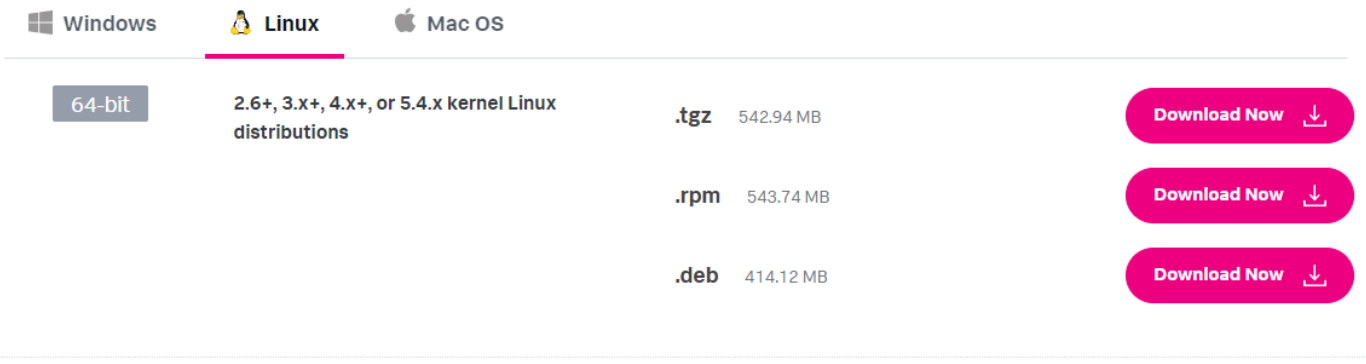
After reboot the interface is removed.

```
[togo@localhost ~]$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.233  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe7b:c4fd  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:7b:c4:fd  txqueuelen 1000  (Ethernet)
        RX packets 344  bytes 32416 (31.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 95  bytes 12671 (12.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[togo@localhost ~]$
```

Install Splunk

Now we are one step closer to the Splunk CTF. First we need to install Splunk Enterprise.

Splunk Enterprise is free for 60 days and afterwards you'll need to provide a license anyway we download Splunk enterprise from the homepage https://www.splunk.com/de_de/download/splunk-enterprise.html
Probably you need to log in yourself to have access.



I followed the guide of Splunk
https://docs.splunk.com/Documentation/Splunk/7.0.3/Installation/InstallonLinux

We are downloading the RPM package. Once downloaded we can start with the installation.

```
[togo@localhost ~]$ cd Downloads/
[togo@localhost Downloads]$ ls
splunk-8.2.2.1-ae6821b7c64b-linux-2.6-x86_64.rpm
```

Confirm that the RPM package you want is available locally on the target host.

Verify that the Splunk Enterprise user account that will run the Splunk services can read and access the file.

If needed, change permissions on the file.

`chmod 744 splunk_splunk-8.2.2.1-ae6821b7c64b-linux-2.6-x86_64.rpm`

```
[root@localhost Downloads]# ls
splunk-8.2.2.1-ae6821b7c64b-linux-2.6-x86_64.rpm
```

Invoke the following command to install the Splunk Enterprise RPM in the default directory /opt/splunk.

`rpm -i splunk-8.2.2.1-ae6821b7c64b-linux-2.6-x86_64.rpm`

```
[togo@localhost Downloads]$ sudo rpm -i splunk-8.2.2.1-ae6821b7c64b-linux-2.6-x86_64.rpm
warning: splunk-8.2.2.1-ae6821b7c64b-linux-2.6-x86_64.rpm: Header V4 RSA/SHA512 Signature, key ID b3cd4420: NOKEY
useradd: cannot create directory /opt/splunk
complete
[togo@localhost Downloads]$
```

```
[togo@localhost opt]$ pwd
/opt
[togo@localhost opt]$ ls
splunk
[togo@localhost opt]$
```

Now as Splunk is installed we need to set the admin password.

Go to the directory: /opt/splunk/bin

```
[togo@localhost bin]$ sudo ./splunk start
[sudo] password for togo:
```

Afterwards you are prompted to accept the license. Accept it and go on.

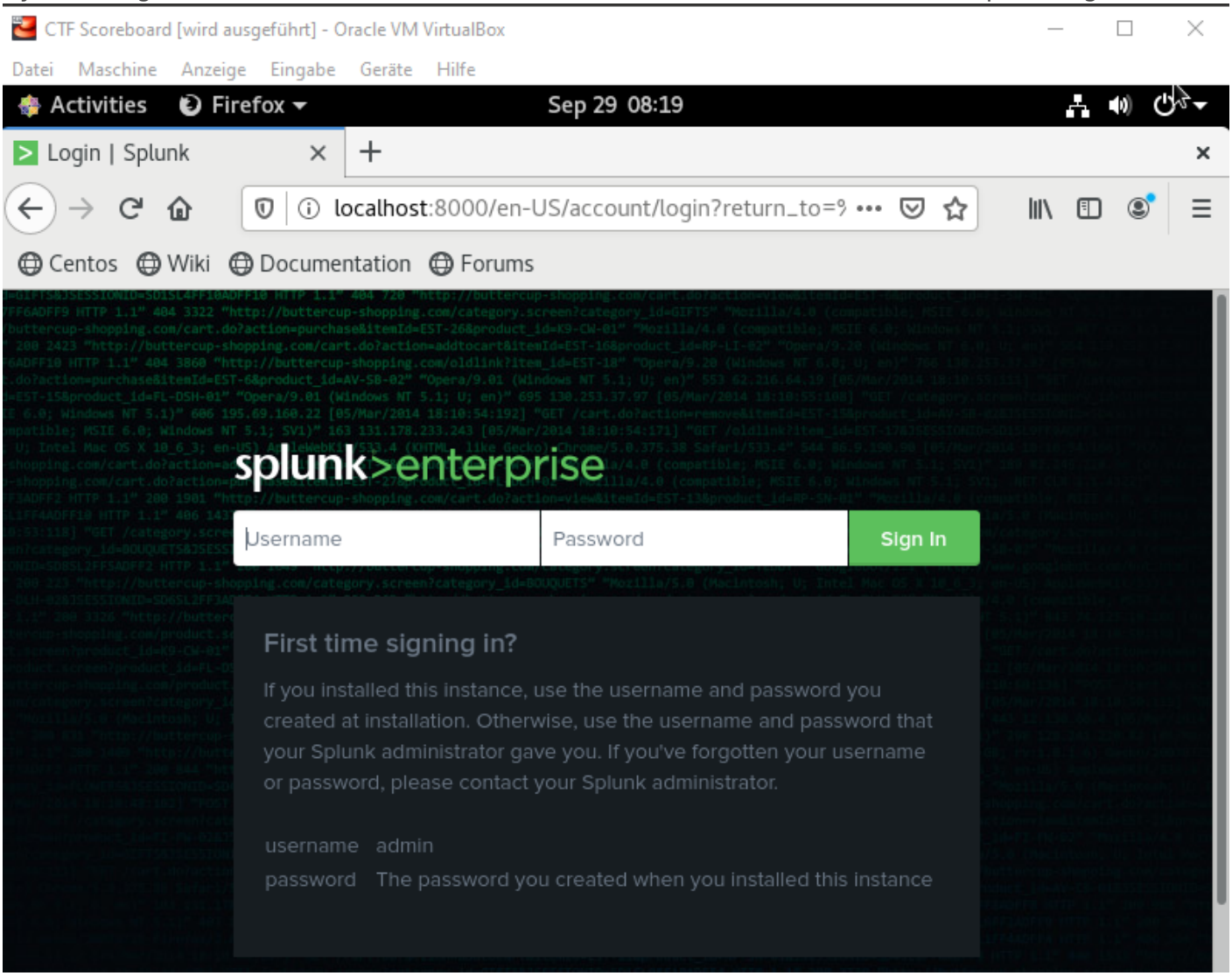
Choose and administrator username:

```
This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: admin
```

Provide a password and splunk will get started.

```
Signature ok
subject=/CN=localhost.localdomain/O=SplunkUser
Getting CA Private Key
writing RSA key
Done
                                                           [  OK  ]

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://127.0.0.1:8000

[togo@localhost bin]$
```

By checking on the browser in the CentOS VM localhost:8000 we should see a Splunk login screen:



Revision #2
Created 9 July 2022 07:55:04 by Togoboi
Updated 10 July 2022 08:32:18 by Togoboi