QRadar 7.3.1 Community Edition

Installation Manual by David Krasnitsky

- Some of the steps in the official manual aren't complete or have errors in them, thus I've created this manual.
- Here is what I did to make it work on VirtualBox:
- Create a new Machine for Linux: Red Hat 64-bit.
- Allocate it 16GB RAM, 4 Cores (8 is better if your system allows it) and 150GB's for a virtual Hard Drive.
- Insert the file 'CentOS-7-x86_64-Minimal-1804.iso' to the virtual CD/DVD-ROM.
  - The file you are inserting is CentOS 7.5 which is the only version QRadar CE installs with.
  - Keep that file close because it wasn't a simple process to get it now that 7.6 is out and there are no 7.5 images anymore.
- Follow the next steps from the official manual ('b_qradar_community_edition.pdf'):

  Page 3: Step 2 to step 3.d

  - Make sure hostname has a dot (.) in at as QRadar installations requires a fully qualified domain name.
- On step 3.e:
  - They kinda forgot to mention..
  - Since QRadar is going to be installed under the root parition ("/"), make sure the root parition has at least 130GBs allocated and the swap partition has 8GBs and only then go on with the rest of the paritions.
- Keep on through steps 3.f to step 4
- Step 5: Disabling SELinux (https://linuxize.com/post/how-to-disable-selinux-on-centos-7/):
  1. Run the next commands as root (if you're running as non-root user, just use 'sudo' at the beginning of each command):
     a. Run the command:

        vi /etc/selinux/config

     b. Press the 'insert' button on the keyboard to the edit.

     c. Go to: SELINUX=

     d. Update the SELINUX value to 'disabled':

        SELINUX=disabled

     e. Press the ESC button to stop 'INSERT' mode and then enter the following line:

        :wx

     :wq - This will write(w) to file and quit(q) VI

     a. Reset the virtual machine with the command:

        shutdown -r now

     b. When the machine is running again and you're logged, make sure SELinux is disabled by running the command:

        sestatus
- Mounting the QRadar CE ISO file:

  a. Insert into the virtual machine CD-DVD ROM the ISO file: 'QRadarCE7_3_1.GA.iso'

  b. Run the following command:

     mkdir /media/cdrom

  c. Mount the ISO with the following command:

     mount /dev/cdrom /media/cdrom
- Run QRadar CE Installation (First Run):

```
/media/cdrom/setup
```

- Accept all questions to processed with the Installation.
- At the end you will get a message telling you to restart the machine. Use the command:

```
shutdown -r now
```

- When you are logged in again, repeat step 8.c and then run the setup again (repeat step 9)
- Let it install.
- Continue with step 8 in page 4.