Software & Installatie

Wireshark

Enabling Non-root Capture

- Stap 1: Install setcap

setcap is part of the libcap2-bin package.

```
stretch@Sandbox:~$ sudo apt-get install libcap2-bin
```

- Stap 2: Maak een Wireshark Group (Optioneel)

Since the application we'll be granting heightened capabilities can by default be executed by all users, you may wish to add a designated group for the Wireshark family of utilities (and similar applications) and restrict their execution to users within that group. However, this step isn't strictly necessary.

```
root@Sandbox# groupadd wireshark
root@Sandbox# usermod -a -G wireshark gebruikersnaam
```

After adding yourself to the group, your normal user may have to log out and back in. Or, you can run newgrp to force the effect of the new group (you'll have to launch Wireshark from this same terminal environment in step 3):

```
stretch@Sandbox$ newgrp wireshark
```

We assign the dumpcap executable to this group instead of Wireshark itself, as dumpcap is responsible for all the low-level capture work. Changing its mode to 750 ensures only users belonging to its group can execute the file.

```
root@Sandbox# chgrp wireshark /usr/bin/dumpcap
root@Sandbox# chmod 750 /usr/bin/dumpcap
```

- Step 3: Grant Capabilities

Granting capabilities with setcap is a simple matter:

```
root@Sandbox# setcap cap_net_raw,cap_net_admin=eip /usr/bin/dumpcap
```

In case you're wondering, that =eip bit after the capabilities list grants them in the effective, inheritable, and permitted bitmaps, respectively. A more thorough explanation is provided in section 2 of this FAQ

To verify our change, we can use getcap:

```
root@Sandbox# getcap /usr/bin/dumpcap
```

de output moet zijn : /usr/bin/dumpcap = cap_net_admin,cap_net_raw+eip

You may need to log out and back in for the new group assignment to take effect. Now, as the user who we added to the wireshark group in step 2, execute Wireshark. You should now see the full list of available adapters and can begin sniffing. (If not, double-check that the wireshark group is listed in the output of groups.)

Links

[http://packetlife.net/blog/2010/mar/19/sniffing-wireshark-non-root-user/ sniffing-wireshark-non-root-user]

Timidity / Tuxguitar

Geen geluid in Tuxguitar

* Start op de cli timidity met de volgende parameters:

```
pvi@laptop-pvi ~ $ timidity -iA -Os
Requested buffer size 32768, fragment size 8192
ALSA pcm 'default' set buffer size 32768, period size 8192 bytes
TiMidity starting in ALSA server mode
Opening sequencer port: 129:0 129:1 129:2 129:3
```

* Wijzig nu de geluidsinstelling van Tuxguitar, zet midi op port 129:0 (of anders)

Extra

Follow these steps:

```
  Install the TiMidity++ midi sequencer (apt://timidity-interfaces-extra).
  Make sure you have tuxguitar-alsa (apt://tuxguitar-alsa),
                     tuxguitar-oss (apt://tuxguitar-oss), and
                     tuxguitar-jsa (apt://tuxguitar-jsa) installed.
  Launch TuxGuitar, open Tools/Settings/Sound, and under Midi Port
  choose Gervill or TiMidity Port [x] (128:[x])
  (where x is a number in the range of the available midi ports - usually
0..3).
```

You're good to go!

Extra2

In a terminal window, use these two commands to install the Fluid Soundfonts:

```
sudo apt-get install fluid-soundfont-gm
sudo apt-get install fluid-soundfont-gs
```

Next, we need to open the timidity config file (use 'ubuntu software center' to install 'Timidity++ Midi sequencer' if you haven't already):

```
sudo nano /etc/timidity/timidity.cfg
```

Comment out this line by placing a # at the front of the line, like so:

```
#source /etc/timidity/freepats.cfg
```

Then uncomment (or add this new line) to the timidity config file:

```
source /etc/timidity/fluidr3_gm.cfg
```

Save the changes to the config file, then restart timidity with this terminal command:

```
sudo /etc/init.d/timidity restart
```