Lab 08 –Python / SenseHat (5)

1 Security hardening – the continuing saga

1.1 Certainly something

This isn't directly a security hardening issue, but it may be nice for us to have a tool to see what's inside the certificates used on the web.

"Certainly something" is an addon to the Firefox browser.

It's up to you if you want to install it, but it is a nice little utility.

1.2 Clam AV[1]

This is an anti-virus/malware package for Linux.

https://www.clamav.net/

http://www.clamav.net/documents/installing-clamav

```
$ sudo apt-get update
$ sudo apt-get install clamav
```

Previously, it was necessary to run `$ sudo freshclam` to update the definitions. This is **not** necessary anymore, and in fact it may trigger an error.

You probably also want to install **clamtk**.

```
$ sudo apt-get install clamtk
```

You may also use the `Add/Remove software` menu utility.

[1] It works, but it is not a great package ☹

1.3 Rootkit detection & Lynis

1.3.1 The **chkrootkit** is a software package that scan for rootkits

```
$ sudo apt-get install chkrootkit
```

Then you want to run the utility

```
$ sudo chkrootkit
```

1.3.2 The **Lynis** package

More info at: https://cisofy.com/documentation/lynis/get-started/

```
$ sudo apt-get install lynis
$ sudo lynis
```

The last command just list usage info. Simple usage:

```
$ sudo lynis audit system
```

There will be a long list of suggestions!

You should consider the suggestions – and remember this for the last lab's.

1.4 Passwords – yet again

Do we have good quality passwords in our system? Well, there are tools that can help us with our password policy and make sure that users have "good" passwords. One of the suggestions from Lynis is to install PAM (Pluggable Authentication Module) / pwquality.

```
$ sudo apt-get install libpam-pwquality
$ sudo leafpad /etc/security/pwquality.conf
```

You can freely change the settings but be careful. I suggest enabling the **minlen** option. Also, check out the "credit" system: https://www.systutorials.com/docs/linux/man/5-pwquality.conf

2 The events that we shall log (WORK TO DO)

2.1 SenseLogger.py

The attached **SenseLogger** module (a separate python file) defines the interface[2].

What you need to do is to write the missing functions.

Then you try it out on the attached **JoystickLogger.py** programs.

Of course, to try it out you need to write the **JoystickReplay.py** program. You can base this program on the **Joysticklogger.py** program.

```
$ cp JoystickLogger.py JoystickReplay.py
```

- Run JoystickLogger and capture the event (saved to a log file).
- Then re-run the captured event stream with JoystickReplay.
- Make sure that the replay is replayed at the same speed as the capture.

[2] Attached with Lab 4. Continue with that version.