Improve smbcmp, the capture diff tool

Rufus

Table of Contents

1. Introduction

At present, the smbcmp tool can view single capture or diff 2 captures side by side with a diff on the bottom pane but smbcmp has a very little user base a is nothing more finally than a script, at first my reflex was to verify if it's available on the main repository of my distro but I think this is such a great program which deserves more than git clone && chmod +x, instead, regular updates and improvements.

2. Project Goals

The aim of this project is (as stated in the title) to improve the tool by adding some features, the first are the ideas took on the idea list, then some of my ideas to actually improve the tooling

2.1. Use or combine current tshark output with the XML output

This is for doing better and deeper diffs by ignoring indentation differences, adding ways to let users add/ignore rules, etc. The XML output is known in the Wireshark world as PDML (Product Data Markup Language) after some researches, I found a resource explaining the specifications http://xml.coverpages.org/pdml.html I think that in order to do that, I'll use the **-Tpdml** option of tshark and use the output to apply filters (add/ignore rules).

2.1.1. Add an html output

According to https://wiki.wireshark.org/PDML, make an html output from the xml one is pretty easy, with **xsltproc** from the xslt library with a simple call, then style the webpage to render a pretty thus more readable output.

2.1.2. Deliverable

A pull request containing all the changes ready for review.

2.2. Make smbcmpp highlight diffs from the packet summary listing

The current implementation of this is satisfying (at least for me) but one thing I think I can add is a descriptive text stating that white packets are the same, it may be confusing at first for newbies who doesn't really know the structure of a samba packet.

2.2.1. Deliverable

A pull request

2.3. Automate the creation of .smbcmp file

For now, we need to manually copy the settings from the sample in the readme then paste it and tweak to our desires, first i want to automate the process of a config file, and maybe add a frontend for configuration.

2.3.1. Deliverable

A pull request

2.4. Make a proper delivery way

By packaging as flatpak, appimage or snap or at least creating an "install/configure" script

2.4.1. Deliverable

It depends on what will be chosen, but at this point, the Readme of the repos should be updated with the new delivery method.

2.5. Correct soome flaws of the tool

2.5.1. smbcmp throws an error if there is no samba packet in the pcap file

this is already listed on this issue https://github.com/aaptel/smbcmp/issues/3, I plan to tackle it in my work.

2.5.2. smbcmp close unexpectedly after resizing to critical values

3. Timeline

The breakdown structure here is just as the program announce it and as an approximative indication on what I will be working on.

3.1. Community Bonding Period[May 6 - May 26]

Since I have exams starting in this period, I'll need a little break of maximum 3 weeks but during that time I won't be idle as I can start prototyping the html page output and get insight and advices about my weak areas + a better understanding on how the core samba protocol works, I will talk regurlarly to my mentor(s) about any specifications on various functionnalities.

3.2. Coding officially begins [May 27]

I will be able to work full time on the project after the end of my exams (around the 7th of June). The classes restart by the 9th of September.

3.2.1. June 7 - June 28 (First second and third Weeks)

I will be working on the use and combination of xml output for better overview of results + the implementation of the html view and diff highlighting, on the official timeline it's stated that from 24 to 28 of June there are evaluations it's also included in my planning

3.2.2. June 28 - July 26 (Weeks 4 - 7)

Automate the creation of .smbcmp file and correct some flaws of the tools, including those that I would have eventually added. This phase is also marked by and evaluation.

3.2.3. July 26 - August 19 (Week 7 - end)

Work on the delivery process of the application, here I will make the final decision on how I should distribute it.

4. About Me

4.1. Name

Mairo Paul Rufus

4.2. Email

akoudanilo@gmail.com

4.3. Github

https://github.com/RMPR

4.4. Phone Number

+237 690823108

4.5. Summary

Currently I'm pursuing a Bachelor degree in computer engineering (2015-2020) in National Advanced School of Engineering of Yaounde, Cameroon. I'm a selft taught considering python since we are most working with JAVA. As for my work experience, last year we implemented a recommender system hosted at http://52.23.196.12 on an AWS machine and the years before that, I used to do "IT-hoping" (test many IT fields in order to see what suits me the most, hence many contributions in web development).

4.6. Contributions to OSS :

4.6.1. Merged PR

1. Powerline

   https://github.com/powerline/fonts/pull/293

2. Telegram Desktop

   https://github.com/telegramdesktop/tdesktop/pull/5502

3. Awesome design tools

   https://github.com/LisaDziuba/Awesome-Design-Tools/pull/114
   https://github.com/LisaDziuba/Awesome-Design-Tools/pull/149

4. Smbcmp

   https://github.com/aaptel/smbcmp/pull/2

5. Source code pro

https://github.com/adobe-fonts/source-code-pro/pull/216

4.6.2. Unmerged PR

1. Daily Coding Problem

   https://github.com/r1cc4rdo/daily_coding_problem/pull/7

2. yii2-user-extended

   https://github.com/cinghie/yii2-user-extended/pull/13

3. Typescript react starter

   https://github.com/Microsoft/TypeScript-React-Starter/pull/230

4. Polybar

   https://github.com/jaagr/polybar/pull/1712