Option 1: Security analysis and tool usability

- What other ways there are to obtain information security tools?
- How can I install them individually into my own computer? Could there be problems with "just getting them to work"?
    - Can you install them also on embedded devices or mobile phones?
    - Why don't we see much Windows in this context?

Security analysis-oriented Linux distributions, like Black Arch and Parrot OS are quite convenient and a common way to access information security tools. However, this is not the only way to access information security tools, one other option is to install tools individually. This installation can be done from the tools' official websites and repositories or by using different package managers (Pacman, APT which are for Linux systems). It is true that there could be problems with "just getting the tool to work" since some of the tools may be optimized for Linux environments and getting those kinds of tools to work on Windows or macOS could be nearly impossible if not impossible. Although there are possibilities to make those tools work for other OS: s than Linux, for example by using Virtual machines or WSL on Windows. Other issue that may pop up when installing these information security tools is different dependencies, because many of the tools may require specific libraries etc. in order to work.

It is also possible but maybe a bit difficult to install these information security tools on some embedded devices and mobile phones. For example, the Raspberry Pi can run Linux distributions, like the Raspbian OS which is based on Debian [1]. Other example is Termux which allows Android devices to run a Linux environment [2]. However, it is important to notice that there may be restrictions due to hardware constraints and compatibility.

Since many of the information security tools are developed for Linux due to its great features, Windows is left on the background on this topic. The features that the Linux OS offers, for example it's open-source nature, flexibility and well-supported environment are much more suitable for information security tools than Windows with its closed-source OS and own security features like Windows Defender that may cause issues with penetration testing.

- How do these other ways, and for example, the above distributions compare in terms of usability, tool amount, and popularity?
- Select one or two tools that are *new for you*, and can be used in different ways (such as pre-installed insecurity-focused Linux distributions, or standalone installation by the user)
    - Compare the official documentation of the tools, manual pages of the tools, and possible operating-system-provided documentation. How good it is?

If we compare the above-mentioned distributions (Black Arch, etc.) and the other ways there are to use information security tools, we notice a large gap between them in terms of usability, tool amount and popularity. The distributions provide environments that are ready to use and already have almost everything that is needed, and therefore the usability of it, is excellent. on the other hand, the manual installation of different tools requires much more effort from the user. And when it comes to the number of tools, the distributions have hundreds of different tools rather than the one specific or a few that comes with the manual installation and other ways. Popularity is high with the distributions since they have established communities and that way, they can also offer documentation and support. Popularity with the manual installation and other tools is not so high because of the raise in effort that comes with just installing them and getting them to work and also, sometimes not so great documentation.

Wireshark and John the Ripper, [3] & [4]

I selected two new information security tools for me, Wireshark and John the Ripper. The documentation of Wireshark is good: there is everything you need to know about the tool and its usage, there are even a bunch of YouTube -tutorials, a FAQ -forum and a blog about the tool. The documentation and manual are available on Wireshark's websites and also as a PDF file. John the Ripper has also great documentation on its primary website that is hosted by Openwall, however it is not as impressive as the Wiresharks documentation. Both official documentations have operating-system-provided documentation, which is also good.

- For the same tools, try to look for information on what they are and how to use them, by using some new LLM services below. You can also test them to generate some commands for CLI applications and explain them.
- Compare the accuracy of the official sources and LLM. Without actually using the tools, could you tell the difference?
- Could you get started with little effort by using LLMs? Is the information correct enough? Could they boost your productivity and help you to reach the actual testing goals?

I used OpenAI:s ChatGPT to generate information about the tools [5]. The ChatGPT generated information and examples of the commands for CLI seemed to match the information provided on the official websites and documentation. It is very hard to tell the difference without actually using the tools. The ChatGPT generated information is more overall and not as precise as it is on the official documentation, for both tool examples. Without actually using the tools, it is in my opinion only a tiny bit hard to tell the difference between the ChatGPT generated information and the information on the official documentation. But perhaps for me, it is easier to notice AI generated text since I have seen it so much.

From what I marked from the ChatGPT generated information and CLI commands, I would think that it could be possible to get started just by that little effort. The information was correct enough to get started, but I am sure at some point, when the usage of the tools evolves, there will definitely be a point where ChatGPT will provide false information and then at last it is a must to check out the official documentation. The ChatGPT generated information could boost my productivity since it gives the information in step-by-step and easy tutorial that I can just follow and maybe in that way, yes, it could help me reach the actual testing goal.

Word count: 805

Sources:

[1] Raspbian. (n.d.). Raspbian official website. Retrieved January 14, 2025, from https://www.raspbian.org/

[2] Termux. (n.d.). Termux: Linux terminal emulator for Android. Retrieved January 14, 2025, from https://termux.dev/en/

[3] Wireshark Foundation. (n.d.). Wireshark user's guide. Retrieved January 14, 2025, from https://www.wireshark.org/docs/wsug_html_chunked/

[4] Openwall Project. (n.d.). John the Ripper password cracker. Retrieved January 14, 2025, from https://www.openwall.com/john/

[5] ChatGPT. (n.d.). ChatGPT: AI language model. Retrieved January 14, 2025, from https://chatgpt.com/

Usage of AI:

In this essay, I have used AI to rephrase my text, to check my grammar and to check the format of the APA -style references.