E-Portfolio Activity - Kali Linux - Michael Geiger

Kali Linux was developed by the security company Offensive Security and is a Debian-based digital forensic and penetration testing Linux distribution, which emerged from BackTrack. The OS is based on Linux, but offers pre-installed tools for ethical hacking. It is designed to act as quietly as possible in order to disguise the presence in the network and at the same time to offer as little attack surface as possible for external attacks. For this reason, it makes sense to use Kali Linux only for penetration testing and not to run other applications such as a web server on the OS. To make sure that a valid version of Kali Linux is downloaded, it is necessary to compare the SHA-256 fingerprint of the received file with that of the download page (Leroux, 2020).

Since Kali Linux runs as "root" there are no permission checks. This means that all commands can be carried out, including those that are not intended or that could damage the own computer and render the system unusable. A reflective use of the OS is therefore of the highest priority. Kali Linux also offers the software for hacking. Inexperienced users may therefore be tempted to try out the respective tools without hesitation. However, these tools have the potential to cause damage and thus to carry out illegal actions. In order to behave ethically and legally correctly, the individual commands must be used carefully.

In order to work safely with Kali Linux and to minimize dangers on the own computer, it should be used in a virtual machine (Bhatt, 2018). There is a free and compatible VM for the Windows 10 OS, the Virtual-Box. Nevertheless, oneself must be clear about the commands that are used. A playful, blind use of Kali Linux must be discouraged, as although the VM minimizes a lot of potential damage, unlawful actions can still be carried out.

The results of the comparative study of penetration testing tools achieved by Bhingardeve & Franklin (2018) reveal results that are similar to their own study. In terms of quality, the results of the comparative study generally correspond to those of our own study. Only in Nmap and Metasploit can other evaluations be seen in comparison with regard to individual aspects. Nmap was rated less well

in our own research in terms of simplicity. However, it must be noted here that the aspect of simplicity in our investigation was divided into two categories, installation and use. With regard to the installation, we found out that under the Windows OS it was a bit more complex compared to other tools. The support from Metasploit was also rated better than Nmap. To our knowledge, Metasploit offers more information and tutorials on its website for use than Nmap. Unfortunately, a quantitative comparison of the respective results is not possible, as the comparative study only differentiates between applicable and not applicable and does not carry out any individual weighting. It is therefore difficult to assess which of the tools is most suitable for carrying out penetration testing. According to the comparative study ranking, Nmap would be the best tool. However, flexible and efficient are not criteria that can be answered satisfactorily with yes or no. According to our knowledge, Metasploit, for example, offers a larger repertoire of examination options such as Nmap. The comparative study therefore offers a good first overview of the penetration testing tools, but is not sufficient, especially with regard to the comparison of various tools, to create a well-founded picture of which of the tools is best for penetration testing. A quantitative evaluation method could have offered a more transparent result here.

Based on the recommendations received, our own assessments could be confirmed. It is therefore not necessary to adjust the original assessment. In a final comparison of the two tools Kali Linux and Nessus Vulnerability Scanner, however, it can be shown that Kali Linux provides a larger repertoire of tools and thus allows potentially more complex investigations. Since the Nessus Vulnerability Scanner is a paid tool and less complex than Kali Linux, it can be assumed that Nessus is more user-friendly for beginners. Kali Linux requires a lot of research and practice to be able to use the full potential of the tool. However, the simpler way is not always the better and the potential that Kali Linux offers with its multitude of tools is enormous. It can therefore be summarized that the Nessus Vulnerability Scanner is definitely useful for users with little knowledge of cyber security and the use of penetration test tools and thus especially for small companies that do not have their own cyber security department, can achieve an overview of the security of the own online presence. Kali Linux,

on the other hand, offers free tools that require prior knowledge in order to be effectively usable. However, Kali Linux offers a wide range of options for experienced users and therefore offers cyber security specialists a powerful tool for ethical hacking and penetration testing.

Discussion results:

During a discussion about the results of the respective e-portfolio activity, some new insights could be gained. With regard to Kali Linux, it was noted that the OS does not necessarily have to be run as "root". When installing in a VM, there is the option to set up a user account right at the beginning. Also many penetration testing commands can be executed without "root" privileges. However, it should be noted that some commands cannot be executed without admin privileges. It was also agreed that Kali Linux should not be used as the standard OS for everyday use. Since Kali Linux should be as quiet as possible, the OS should only be used for penetration testing. Furthermore, it was found that the OS is not very user-friendly compared to others and therefore can be challenging for beginners. Kali Linux cannot run on all hardware, so it is necessary to determine whether the hardware used is compatible for the OS. It should also be noted to isolate the local network so that scans do not overflow to the internet.

In relation to the comparison of the study of open source penetration testing tools by Bhingardeve & Franklin with their own research results, it was found that the respective assessments correspond to each other. A comparison of the qualitative results with the own quantitative results turns out to be difficult. We can confirm the assessments of the study, but it must be noted that the qualitative assessment is rated as unsatisfactory.

Also the discussion about the comparison of Kali Linux with Nessus Vulnerability Scanner brought confirming results. Another important point to note, however, is that a direct comparison between Kali Linux and Nessus is difficult since Nessus is a tool and Kali Linux is an OS with a variety of tools. It is also possible to install Nessus in Kali Linux, where it is not pre-installed.

References:

Bhatt, D. (2018) Modern Day Penetration Testing Distribution Open Source Platform - Kali Linux - Study Paper. *International Journal of Scientific & Technology Research* 7(4): 233-237. Available from: https://www.ijstr.org/final-print/apr2018/Modern-Day-Penetration-Testing-Distribution-Open-Source-Platform-Kali-Linux-Study-Paper.pdf [Accessed: 10.01.2022]

Bhingardeve, N. & Franklin, S. (2018) A Comparison Study of Open Source Penetration Testing Tools. *International Journal of Trend in Scientific Research and Development* 2(4): 2595-2597. Available from: https://www.ijtsrd.com/computer-science/computer-security/15662/a-comparison-study-of-open-source-penetration-testing-tools/nilesh-bhingardeve [Accessed: 11.01.2022]

Leroux, S. (2020) The Kali Linux Review You Must Read Before You Start Using It. It's FOSS. Available from: https://itsfoss.com/kali-linux-review/ [Accessed: 10.01.2022]