Unit 7 Task: Jonathan Callaghan 15-01-2022

Read the following articles on Kali Linux:

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/***

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.

- *What does the article teach you about carrying out vulnerability scans using Kali?*
- *What issues might you encounter?*
- *How would you overcome them?*

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.

- *How do their results compare with your initial evaluation?*
- *What do you think of their criteria?*

"Kali Linux is a well-respected collection of open source pen testing tools, including metasploit, nmap, wireshark and sqlmap amongst many others. It has the benefit of being available as a 'live distro' which means that there is no requirement to install it – it will run from a DVD or a USB/ thumb drive. For these reasons, we recommend that Kali Linux is the tool of choice for this assignment." (UoEO Computing Team, 2020.)

Based on your evaluation in the previous session and the articles above, consider the recommendation given above:

- *What are the pros and cons of using Kali Linux vs. Nessus?*
- *Has this changed your original evaluation score?*

Discuss your answers within your team and then record your answers and team discussions in your e-portfolio.

- What does the article teach you about carrying out vulnerability scans using Kali?
- What issues might you encounter?
- How would you overcome them?

When considering Kali Linux, Leroux (2020) suggests that first time users may be cautious in their approach when using Kali unless they have specific needs. Kali Linux is not necessarily anything new or unique since the penetration testing tools available could be installed on any Linux distribution. However, what sets it apart is the ease of use for the user as tools are preinstalled even though some tasks maybe be found challenging due to this. Leroux (2020) continues to suggest there is a risk of using Kali from the onset as it is essential to verify you are not installed a compromised package; the fingerprint of the file checking the SHA-256 can support this verify the checksum. Another issue to consider is that you would need to run from root to use most tools. This could be risky if any files get deleted/edited accidentally or if the user shares the computer with others and there are no basic permissions on the machine, which could cause your system to be unusable. The orientation of applications is geared to security which means that large office applications are not part of the standard installation. The positive is that you can do anything as a root user, which means you could set your unprivileged accounts on the system. A key benefit of Kali is that its 'required to hide its presence on a network and harden itself from potential attacks' (Leroux, 2020). After installing packages, Kali may offer messages regarding concerns which is also a positive. A critical problem for installations is not becoming a FrankenDebian that can break the system. It is essential to use trusted sources and use Debian Stable.

A more practical solution is to run Kali Linux in a virtual machine. This can allow you to practice your skills without causing harm to your system or activities.

Whilst reviewing Bhatt (2018), we can infer the importance of the usefulness and flexibility of Kali Linux. The wide array of pen-testing utilities and the benefit of applying

skills in a virtualised environment (Bhatt, 2018) supports Leroux (2020) findings. A concern without a virtual lab would be that test scans and data could flow out to the internet, and the snapshot tools can recover lab work whilst eliminating footprints of malicious activity. Kali offers an adaptable framework to personalise peoples needs. The applications submitted are extensive and can be configured with applications such as Metasploit. The assessment tools can be carried out on anti-virus systems and firewalls so that results are accurate and useful. The challenge is that users could leave themselves vulnerable, as mentioned in the first article.

- *How do their results compare with your initial evaluation?*
- *What do you think of their criteria?*

After reviewing Bhingardeve & Franklin (2018), when comparing my initial evaluation, the first enlightenment has more tools than I had expected. This offers far greater scope to assess and test defensive and offensive security capabilities (Bhingardeve & Franklin, 2018). I was only aware of four of the six tools, and it was surprising to see that Nmap topped the list. From the list of tools and research, I would have considered Metasploit to top that list. Concerning the criteria used, there are many aspects the same; however, this evaluation focuses on social interaction such as popularity, acclamation, support, and documentation. In the initial assessment, popularity was an extra addition considered in the research. The limitation of the criteria would be regarded as when some requirements are vague such as 'Easy' and 'Free' (Bhingardeve & Franklin, 2018). The 'Easy' does not give us an insight into whether this is easy to install or ease of use, making the initial evaluation stronger in comparison. The 'Free' aspect does not consider whether it is a community edition, open-source, completely free, or a paid version of the tools. Overall the comparison

table is helpful as it offers a slightly different perspective and variation of tools however parts could be made more explicit in defining criterion key terminology.

"Kali Linux is a well-respected collection of open source pen testing tools, including metasploit, nmap, wireshark and sqlmap amongst many others. It has the benefit of being available as a 'live distro' which means that there is no requirement to install it – it will run from a DVD or a USB/ thumb drive. For these reasons, we recommend that Kali Linux is the tool of choice for this assignment." (UoEO Computing Team, 2020.)

Based on your evaluation in the previous session and the articles above, consider the recommendation given above:

- *What are the pros and cons of using Kali Linux vs. Nessus?*
- *Has this changed your original evaluation score?*

When evaluating Kali Linux and Nessus, there are valid arguments for both. The benefits for Nessus are that it is incredibly accurate with the industry's lowest false positive rate, broad coverage concerning CVE's and plug-ins and is very popular amongst organisations globally (Tenable, 2021). Nessus can quickly transfer licenses between computers, providing clients with customisable reports after each complete assessment. Reports can provide detailed feedback that can priortitse risk and vulnerabilties whilst providing pre-built policies and templates to maximise the efficiency and time of the security practitioners offering a comprehensive service. The limitations of Nessus are that to have this complete package, there is a significant expense.

Tenable (2021) suggests that 50% of the Fortune 500 and 30% of the Global 200 companies rely on Nessus technology. Therefore security practitioners will require some form of knowledge and understanding of using this tool. Furthermore there are additional costs should you need expertise and traning on how to maximise the performance of Nessus. Therefore for small to medium-sized companies, this expense

may not be on their priority budget list and may price business out of the market for this tool.

Kali Linux offers a different perspective. The first benefit would be the pre-packaged solution offering a platform with numerous tools to complete practical penetration testing assessments. Furthermore, the pre-packaged approach offers open-sourced community editions which means that most services are free, providing access to all. Kali Linux will provide an excellent platform for students to learn and develop skills and, through the use of a virtual box, can practice without the risk of doing irreparable damage to the computer system. The limitations of this are that inexperienced users will take more time to become accustomed to the tools and will not have the time-saving options of customisable reports generated by Nessus. Kali Linux may not have the convenience and and well organised interface that Nessus offers but it be a great solution for security practicioners to learn and assess security policies and practices. The UoEo Computing Team (2020) recommends Kali Linux as the chosen tool, a reasonable assumption.

This did change my evaluation score as I would rate Kali Linux higher now due to understanding the benefits and practicalities of using the all in one platform.

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.

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.

Leroux, S. (2020). The Kali Linux Review You Must Read Before You Start Using It. It's FOSS. . Available: https://itsfoss.com/kali-linux-review/ [Accessed 15 January 2022].

Tenable. (2021). Nessus Professional. Available: https://static.tenable.com/marketing/datasheets/DataSheet-Nessus_Professional.pdf [Accessed 16 January 2022].

Team discussion and responses: