**Unit 7 ePortfolio Activity**

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?**

Kali Linux is a purpose-built penetration testing toolkit with diverse uses, from vulnerability scanning to digital forensics. Whilst it does not contain unique tools, it does come with over 600 tools by default. The tools include a range of both general user interface (GUI) and command line (CLI) interfaces to suit security professionals of varying technical capabilities.

This operating system can be used to secure a wide range of devices, from servers to mobile phones. Many standard services are disabled in an attempt to hide its presence on a network and stop it becoming the target of an attack. It is highly recommended to run Kali Linux on a virtual machine (VM) in order to segregate any testing from other activities. This is also advisable as Kali Linux was not designed for everyday use and therefore does not feature common office or productivity applications.

**What issues might you encounter?**

As Kali Linux is not designed for general purpose use, root access is used as the default. This level of access can lead to inadvertent damage to the system as access to key files is unrestricted. Furthermore, some of the tools can damage the system or home network if not used carefully. Some tools could also contravene the law if used without consent.

In addition, there is a risk that adversaries may attempt to compromise the Kali Linux VM image and ISO downloads.

**How would you overcome them?**

In order to address the risks of using the root account as standard, it is possible to create an unprivileged account to use instead of root. If privileges are required then the ‘sudo’ command can be used. With regards to addressing the risks of network damage and attracting negative attention, it is important to understand the tools before utilising them.

Finally, to address the risk of running a compromised Kali Linux download, the downloaded file should be verified against the checksum provided on the official site.

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?**

Compared with my initial evaluation, this was a more in-depth study based on a range of secondary sources. On the one hand, some of the same tools were featured in both studies. On the other hand, Bhingardeve and Franklin (2018) only featured open source tools and did not cover certain key tools, such as Nessus.

In spite of the differences between the studies, Nmap was considered to be the strongest tool featured in both.

**What do you think of their criteria?**

The criteria in the study is not made clear and appears to be subjective. For example, the criterion ‘powerful’ is not defined and it is not clear how this is measured. In addition, there are criteria that could have overlap, for example ‘acclaimed’ and ‘popular’.

‘Well-documented’ is a helpful criterion to use and this was one factor that influenced my scores for ‘ease of use’. It is worth noting that ‘free’ is an unnecessary criterion when measuring open source tools only.

“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?**

The pros of Kali Linux over Nessus include that it is open source and therefore free. Although, for the purpose of the exercises in this module, the free Nessus package would likely suffice. Kali Linux is effectively a toolbox comprising of a wide range of tools. Nessus is one of the tools that can be installed on Kali Linux.

There are no cons of Kali Linux against Nessus as you can install Nessus on Kali Linux. These software packages cannot be practically compared as one is an operating system and the other is a vulnerability assessment tool.

**Has this changed your original evaluation score?**

This exercise would lead me to adjust the scores given for Kali Linux in the following ways:

* Ease of install: This would now be a 5 as there are many ways to install this programme. My original score was skewed by the challenges I experienced in setting up Kali Linux at the beginning of the module.
* Flexibility: This would now be a 5 because it is possible to download the majority of other tools and use them within Kali Linux, with some even being there by default.

These changes would bring Kali Linux up to an average score of 4.67 in line with OWASP ZAP and joint second place in the tools. Whilst Nmap is on Kali Linux as default, I would still argue that it is easier to use, especially for beginners, so it will retain first place in the tools.