Unit 7: e-Portfolio Activity

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?

  Bhatt (2018) mentions tha Kali Linux is an advanced penetration testing tool that has a wide range of applications including information gathering, vulnerability analysis, web application analysis, database assessment, password and wireless attacks and reverse engineering.

- What issues might you encounter?

  Leroux (2020) remarks that using kali linux might be harmful to your home network if you execute the wrong commands so it is important to know what you are doing especially when you are working as a root user.

- How would you overcome them?

  By conducting proper research, and understanding the purpose of the tools. Also by learning the appropriate commands for the task you wish to carry out.

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?

Our evaluation and the one done by Bhingardeve, N. & Franklin, S. (2018) had only three tools in common: SQLMap, Metasploit and Nmap . The results are mostly the same except for NMap that we feel is not flexible.

	Flexibility		Easy		Free		Reputation	
	Team B	Authors	Team B	Authors	Team B	Authors	Team B	Authors
SQLMap	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Nmap	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Metasploit	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

What do you think of their criteria?

They had some other criterias such as power, portability, documentation, support which are important factors to also consider when making a choice of pen test tools.

"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?

  Kali Linux is free.

  Nessus comes at a fee (esecurityplanet, 2019)

- Has this changed your original evaluation score?

  Not at all. Kali Linux still remains a top tool and the resources mentioned above also prove that

<u>References</u>

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.

Esecurityplanet (2019) Best Penetration Testing Tools for 2021 Available from: https://www.esecurityplanet.com/products/best-penetration-testing/ [Accessed 14 September 2021]

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 20 September, 2021]