Unit 7 - e-Portfolio 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?
  - Virtualization is useful for mitigating data and network outflow to the internet
  - Use virtualization for ideal environment as Kali is designed to be run in a virtual machine (VM)
  - Less fingerprint and ability to break your system. Making network changes or running untested scripts that may affect the stability or overall function of an operating system are much safer to run in lab or sandbox environments. Using a virtual machine is a safe way to make changes without damaging the primary, host environment.
  - Kali effectively categorizes tools based on their application and intended use. This makes finding relevant tools for the relatively intuitive. The flip side of this is that there are a lot of tools available in the distribution and finding the correct tool for the task can be challenging when given so many choices. Some of the tools included may no longer be well regarded, or only work on vulnerabilities or systems that have long since been patched.
  - (Bhatt, 2018) outlines the importance of workflow in pentesting by outlining the information gathering stage prior to any actual exploit.
- What issues might you encounter and how would you overcome them?
  - Because Kali is an operating system, some enthusiastic newcomers might be tempted to run the distribution as their primary operating system. (Leroux, 2020) advises against this, however, emphasizing the importance of running Kali within a VM. Kali has a very niche use case, geared specifically towards penetration testing and security. Many useful everyday applications are missing from this OS and while it’s not impossible to install them, a prospective user would be better off installing Windows or a more user-centric Linux distribution, running Kali inside a VM.

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?

Many of the tools covered throughout (Bhingardeve, Franklin, 2018) study were not evaluated during our tool evaluation exercise. Tools such as John the Ripper and Aircrack have been touched on, but not actively tested or used throughout this module. Overall, I agree with the evaluation of tools and while our results don't totally mirror each other, they reflect similar trends in overall perceived usefulness, reputation and support.

- What do you think of their criteria?

The criteria for this report, like many of these tool comparison studies, seems arbitrary. Comparing distinct tools, with very little overlap in application doesn't seem productive. SQLMap is a specialized tool capable of SQL injection and even database takeover. This software is unrelated to NMap, which is used in information gathering via a powerful range of network scanning functions. To compare the two is like trying to compare an MRI machine to an ultrasound machine. They don't compete because they complement each other in their specific use cases. Until NMap is capable of replacing SQLMap in its ability to perform a SQL Injection attack the two shouldn't share a table comparing their merits against each other.

"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 and cons of using Kali vs other tools (in this case Nessus) has been widely debated throughout this module. This however is an arbitrary question, not dissimilar to comparing an intelligent toolbox to the tools held within. I wouldn't make a comparative argument on the pros and cons of Windows operating system vs VLC when trying to

decide on what is the best to choose for viewing media. Kali is not a pentest tool in and of itself and there is no Kali linux branded scanning tool. Kali is a distribution of linux that has a suite of tools, including many of the tools we're asked to compare it to.

Some of the pros of Kali are that it's widely available and can be easily and safely installed or used in a variety of ways. Users are free to use live CDs at the cost of performance, or install it on a virtual machine and assign whatever resources are available. Users can also install Kali as a primary system, but this is not recommended as the distribution is not designed to be a general use, primary operating system.

If we're to compare Kali to Nessus, I would say that Kali is by default quieter than Nessus; this is because Kali doesn't actually scan anything and can be run quietly and somewhat autonomously within a virtual machine. Nessus however, is a noisier solution for vulnerability scanning. Nessus is better compared to similar vulnerability scanners, such as Qualys or Trustwave (Tenable, 2019) that are designed to scan IPs and networks within an organization.

- Has this changed your original evaluation score?

Given further evaluation, the score remains unchanged. These two products are distinct and have different use cases. A pentester will likely use both of these tools simultaneously if they're launching Nessus scans from within Kali.

Pentest Tools

Tool	Install	Use	Flexibility	Licensing	Privacy	Reputation	Totals
Metasploit	4	2	5	3	2	5	21
Nessus	4	4	5	2	2	4	21
Burp Suite	2	3	4	5	2	5	21
Nmap	4	4	4	5	3	5	25
OWASP Zap	5	3	3	5	3	4	23
SQLMap	5	5	3	5	2	4	24
Kali	5	4	5	5	5	5	29
Jawfish	3	4	2	5	2	1	17

Figure 1: ranking of penetration tools

References:

Tenable (2019). *Nessus Product Family*. Tenable®. Available at: https://www.tenable.com/products/nessus. [Accessed June 19, 2021]

Bhatt, D. (2018). Modern Day Penetration Testing Distribution Open Source Platform -Kali Linux -Study Paper. *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, 7. Available at: https://www.ijstr.org/final-print/apr2018/Modern-Day-Penetration-Testing-Distribution-Open-Source-Platform-Kali-Linux-Study-Paper.pdf. [Accessed June19, 2021]

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. [Accessed June 19, 2021]