Kali Linux

What does the article teach you about carrying out vulnerability scans using Kali?

In general, performing vulnerability scans through a built-in tool like Metasploit is fairly simple. You can first search for a vulnerability by name. With this, you specify which vulnerability you wish to attempt to exploit. Then you can show options that are necessary to run the exploit. Lastly, specify the remote host that you wish to target.

What issues might you encounter?

The biggest issue is most likely the vast number of commands that are built into Metasploit. There's a lot that can be done within the tool and knowing all the commands can be difficult. As well, interpreting the results can also be overwhelming at first depending on the user's experience.

How would you overcome them?

To overcome the issue of knowing commands there are several helpful solutions. The most useful is the built-in help command. It provides information about any command and what it does. As well, official documentation can help with performing commands but also in interpreting what the results mean.

How do their results compare with your initial evaluation?

Their results match up with my initial evaluation. They provide great information about kali Linux and the array of tools that are available in it. It is agreed upon that Metasploit is one of the best tools built into kali Linux. As well there are dozens of other amazing tools that can be used instead of or in conjunction with others.

What do you think of their criteria?

The evaluation criteria provided does a good job of breaking down the tools provided overall. It would be useful when looking for tools to have a general comparison, to help specify which ones to use. However, the tools in the article all have relatively different purposes, as such the comparison in the article isn’t very useful. It would be more beneficial to have a comparison of tools that were made with a similar purpose in mind.

What are the pros and cons of using Kali Linux vs. Nessus?

Both tool kits provide a great set of tools and functions. Kali Linux provides Metasploit, an open-source vulnerability scanner. It provides the ability to perform vulnerability scans and automation. It is also free but does offer a paid pro version. Nessus on the other hand also does vulnerability scanning but also provides more network and risk management tools. It is also premium only and requires to be purchased. However, this does provide more customer support and business level support.

Has this changed your original evaluation score?

It has not changed my original score. Kali Linux is still a great tool with a wide variety of tools. It allows for multiple tools to be used seamlessly in one environment. It is also free and easy to set up. Other great options can be used instead but Kali can generally provide the same thing in one package.

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.

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. Available from: <https://itsfoss.com/kali-linux-review/> [Accessed 15 January 2020].

Tenable. (2021) Available from: <https://www.tenable.com/products/nessus> [Accessed 15 January 2020].