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.

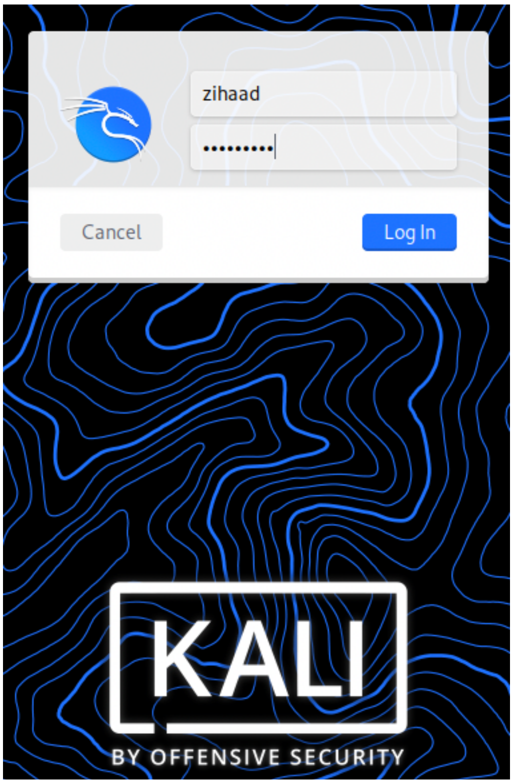
- What does the article teach you about carrying out vulnerability scans using Kali?
- What issues might you encounter?
- How would you overcome them?

Kali Linux Review

Leroux (2020) mentions that Kali Linux is a “Penetration Testing and Ethical Hacking Linux Distribution”, further supported by the official Kali Linux website (www.kali.org) updated by g0tmi1k (2022).

(g0tmi1k, 2022) states that “misuse of security and penetration testing tools within a network, particularly without specific authorization, may cause irreparable damage and result in significant consequences, personal and/or legal.”

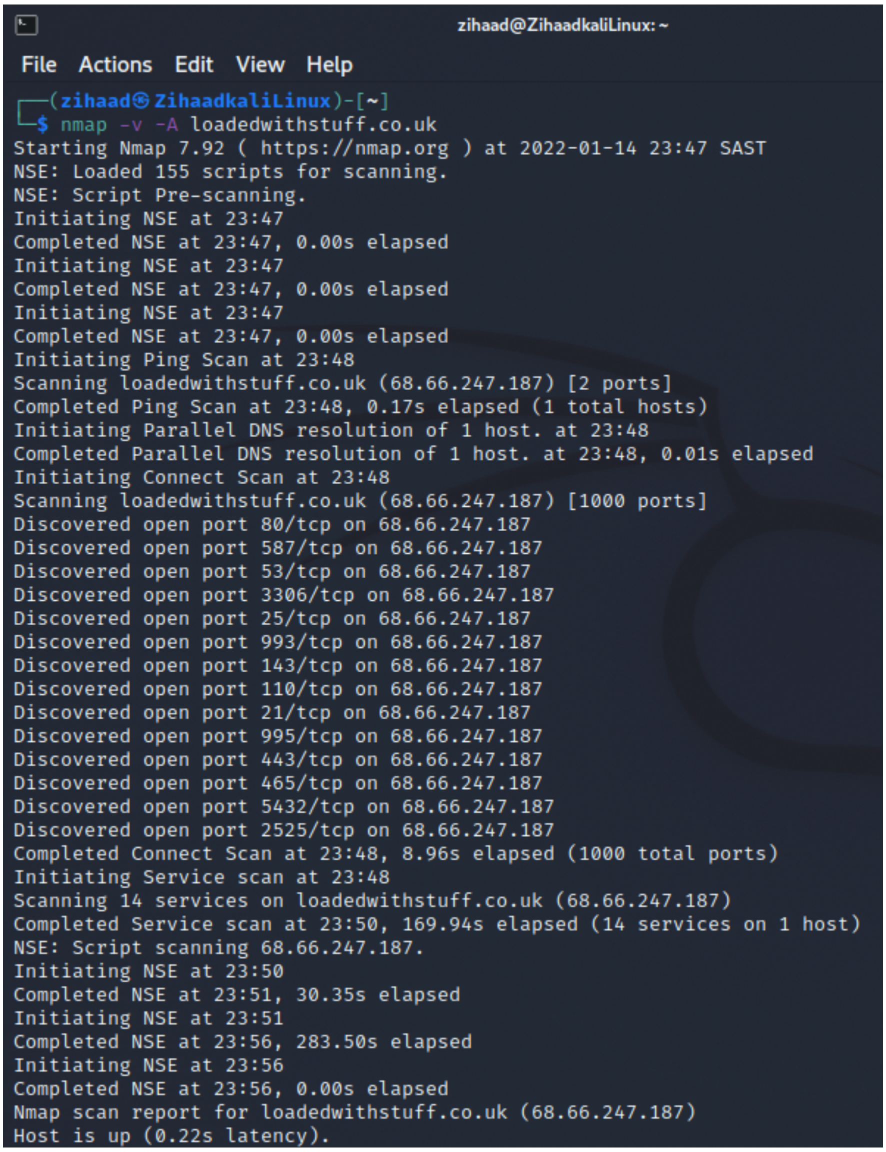
The article mentions the following: “on a default Kali Linux system, the *only* installed user *is* root and you have to work under that identity *all the time*”. This is not entirely true as the author installed Kali Linux on a VirtualBox environment using a MacBook, screenshot below:



zihaad

••••••••••

A user is created during the initial install, a sample nmap scan was initiated as indicated in the screenshot below, however superuser access may still be required to execute various scanning exercises.



```
┌──(zihaad㉿ZihaadkaliLinux)-[~]
└─$ nmap -v -A loadedwithstuff.co.uk
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-14 23:47 SAST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 23:47
Completed NSE at 23:47, 0.00s elapsed
Initiating NSE at 23:47
Completed NSE at 23:47, 0.00s elapsed
Initiating NSE at 23:47
Completed NSE at 23:47, 0.00s elapsed
Initiating Ping Scan at 23:48
Scanning loadedwithstuff.co.uk (68.66.247.187) [2 ports]
Completed Ping Scan at 23:48, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:48
Completed Parallel DNS resolution of 1 host. at 23:48, 0.01s elapsed
Initiating Connect Scan at 23:48
Scanning loadedwithstuff.co.uk (68.66.247.187) [1000 ports]
Discovered open port 80/tcp on 68.66.247.187
Discovered open port 587/tcp on 68.66.247.187
Discovered open port 53/tcp on 68.66.247.187
Discovered open port 3306/tcp on 68.66.247.187
Discovered open port 25/tcp on 68.66.247.187
Discovered open port 993/tcp on 68.66.247.187
Discovered open port 143/tcp on 68.66.247.187
Discovered open port 110/tcp on 68.66.247.187
Discovered open port 21/tcp on 68.66.247.187
Discovered open port 995/tcp on 68.66.247.187
Discovered open port 443/tcp on 68.66.247.187
Discovered open port 465/tcp on 68.66.247.187
Discovered open port 5432/tcp on 68.66.247.187
Discovered open port 2525/tcp on 68.66.247.187
Completed Connect Scan at 23:48, 8.96s elapsed (1000 total ports)
Initiating Service scan at 23:48
Scanning 14 services on loadedwithstuff.co.uk (68.66.247.187)
Completed Service scan at 23:50, 169.94s elapsed (14 services on 1 host)
NSE: Script scanning 68.66.247.187.
Initiating NSE at 23:50
Completed NSE at 23:51, 30.35s elapsed
Initiating NSE at 23:51
Completed NSE at 23:56, 283.50s elapsed
Initiating NSE at 23:56
Completed NSE at 23:56, 0.00s elapsed
Nmap scan report for loadedwithstuff.co.uk (68.66.247.187)
Host is up (0.22s latency).
```

The paper 'Modern Day Penetration Testing Distribution Open Source Platform' by Bhatt (2018) describes white hat hacker techniques of penetration testing.

Kali Linux has many built in tools commonly used for vulnerability scanning such as:

- Information Gathering
- Vulnerability Analysis
- Web Application Analysis
- Database Assessment
- Password Attacks
- Wireless Attacks
- Reverse Engineering

- Exploitation tools

According to Bhatt (2018) “Kali Linux has not been developed to be a easy range of tools, but instead a adaptable framework that specialized penetration testers, security enthusiasts, students, and newbie can personalize to match their particular needs.”

According to Bhatt (2018) “Kali Linux distribution has over six hundred security testing tools and graphical interfaces to make those tools to use very easy for newbie as well.”

What issues might you encounter?

- Kali Linux is not a recommended for everyday use and may affect the normal functioning if installed on a general purpose computer (g0tmi1k, 2022). It is therefore recommended to be installed on a Virtual machine to perform any scanning and/or penetration tasks (Leroux, 2020).

- Kali Linux may not be hardware compatible and “might not work as expected or not work at all” (g0tmi1k, 2022). Researching hardware capability is required before installation.

- New users to Linux may not find Kali Linux user friendly

- When performing scans it is important that they do not outflow to the internet as mentioned by Bhatt (2018), this could constitute as hacking and have legal and criminal implications.

How would you overcome them?

- Do not use Kali Linux for everyday use
- Researching hardware capability is required before installation.
- Isolate local networks so that scans do not overflow to the internet

How do their results compare with your initial evaluation?

What do you think of their criteria?

Common tools evaluated includes:

- Nmap
- Metasploit
- sqlmap

Our nmap ease of install, ease of use and flexible criteria differ slightly as this is operating system specific, for example it was easier to install nmap on a Linux/MAC OS distribution rather than a Windows OS.

Our Metasploit criteria is more aligned with the results in the paper – ‘A Comparison Study of Open Source Penetration Testing Tools’

The SQLMap flexibility criteria differ from the results mentioned by Bhingardeve & Franklin, 2018). Group 1 argues that sqlmap is not flexible as it only detects and exploits SQL injection flaws. The remaining criteria are aligned, for example Bhingardeve & Franklin (2018) mention that sqlmap is not well documented which aligns with Group 1’s reputation score.

Bhingardeve & Franklin (2018) criteria is more descriptive and specific than the criteria used in the module, the criteria used in the module can have different meanings based on ones interpretation. For example features such as ‘free’ and “well-documented’ rules out ambiguity.

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?**

According to Babincev & Vuletic (2016): “Nessus is a free tool for scanning and finding vulnerabilities in computer systems. Nessus supports over 50,000 plugins for detection of various types of vulnerabilities. A plugin typically contains information about the vulnerabilities, guides the user to confirm the existence of certain vulnerabilities and gives instructions for their removal. Using the Nessus tool on the Kali Linux operating system requires an additional installation of Nessus, because Nessus does not belong to the set of tools contained in Kali Linux.”

According to Jenik (2016): “Nessus is, by design, a manual testing tool for network vulnerabilities.” It is potentially intrusive and produces a high number of false positives. The Graphical User Interface of the tool is not very intuitive.

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

Evaluation score remains unchanged as they align with the research above.

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. Available from: https://www.ijstr.org/final-print/apr2018/Modern-Day-Penetration-Testing-Distribution-Open-Source-Platform-Kali-Linux-Study-Paper.pdf [Accessed 14 January 2022].

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. Available from: https://www.ijtsrd.com/computer-science/computer-security/15662/a-comparison-study-of-open-source-penetration-testing-tools/nilesh-bhingardeve [Accessed 14 January 2022].

Babincev, I.M. and Vuletić, D.V. (2016) 'Web application security analysis using the Kali Linux operating system', Vojnotehnički glasnik, 64(2): 513-531. Available from: https://aseestant.ceon.rs/index.php/vtg/article/download/9231/4110/ [Accessed 14 January 2022].

Jenik A (2016) What are the drawbacks of nessus as a network security tool? Available from: https://www.quora.com/Have-you-used-Nessus-What-were-the-pros-and-cons-of-using-the-tool [Accessed 14 January 2022]

g0tmi1k (2022). Should I Use Kali Linux? Available from: https://www.kali.org/docs/introduction/should-i-use-kali-linux/. [Accessed 14 January 2022].

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 14 January 2022].