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

As we know that Kali Linux is Debian-based open-source Linux system, intended for advanced penetration testing and security audits. The Kali Linux distribution includes a wide range of tools for penetration testing, security research, and computer forensics.

There are lot of tools in kali linux which is used for the vulnerability scans because kali linux is used for the offensive security. This article teaches us that by using kali linux tools we can find out the vulnerability of each platform like web, waf, endpoint and phishing awareness etc. Because of its open-source nature different people are always trying to contribute in it to make it more powerful. There are lot of vulnerability scanners in it like nuclei, nikto and many other tools.

I also learnt about the following things that we can do using kali linux are vulnerability analysis, web application analysis, Database assessment, Password attack, Wireless attacks, reverse engineering, and exploitation.

**What issues might you encounter?**

The issues that I encountered is given below in details:

1. While installing kali linux, it is taking time to install in VM, and it slow down the pc.
2. I face some issue while making my machine root user or simple user.
3. I tried different tools, but some was running and some of them was not running because of python version.
4. While starting Metasploit framework I was not understanding that how to set payload which payload I have to set how to set Rhost and Lhost etc.

**How would you overcome them?**

I overcome all the issues by learning different platforms like I solved the first issue by installing my VM in SSD drive and give more CPU to Kali Linux VM which is shown in Figure 1 and increase its base memory to 4gb which is shown in figure 2.

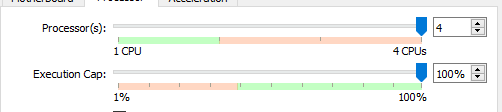


Figure 1. CPU Assigned

Timeline

Description automatically generated

Figure 2. Base Memory

I resolved the second issue by making a new user instead of using the root user because I learnt that how to use root user with sudo command. I read that we can change our local user to root user at any time that’s why I make new user.

I resolved third issue by installing python version 3.9.2 because some of the tools are not running on it firstly the version is 2.7 which is shown below.

Text

Description automatically generated

Figure 3. Python Version before updating

Then I changed the version and install new python version which is 3.9.2

Text

Description automatically generated

Figure 4. Python Version after updating

After updating versions of python, tools were executing successfully.

After reading some article about the kali linux Metasploit framework I done with all the difficulties and hurdles and check all the configuration and their working process and understood about how to set payload and all that. I used help menu to understand the whole process.

Text

Description automatically generated

Figure 5. MSF Console Help Menu

**How do their results compare with your initial evaluation?**

In their results they are making comparison of different tools and there are some constraints defined to evaluate them. I installed and run all the tools in my kali linux machine all the screen shot are given below. I feel that this is not a big deal to run all the tool and my observation is also according to their results.

Text

Description automatically generated

Figure 6. Nmap Results

A screenshot of a computer

Description automatically generated with medium confidence

Figure 7. MSF Console Running

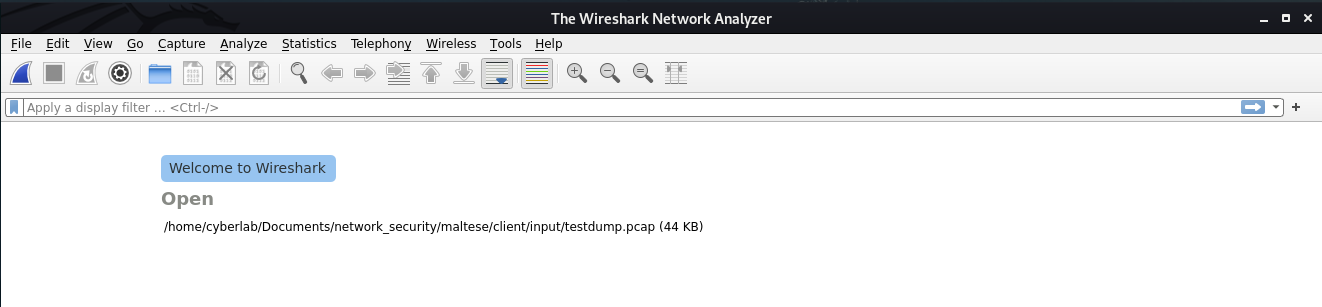


Figure 8. Wireshark’s Menu



Figure 9. SQL map Menu

Hence after running all the tools, I analyzed that all the features are correct. We also visit GitHub for checking all the documentation, some of the tool’s documentations are available and well explained and some of the tool documentation was not available. I also checked rest of all the features of all the tools.

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

Their criteria were just about checking the tool features, it will be good if they add some of screenshot as a result and they also can add some of more features in it. They just simply define the tools and make comparison based on that definition they must run it and explain in detail that how we can perform assessment how to analyze and what type of functionalities these specific tools can perform instead of making comparison on the basis of definition.

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

|  |  |
| --- | --- |
| **PROS and CONS** | |
| **Kali Linux** | **Nessus** |
| Linux distribution developed exclusively for penetration testing. Many pen test tools are pre-installed in Kali Linux. | With the help of Nessus, a penetration tester may identify both local and remote vulnerabilities and exploit them. Compliance and configuration audits |
| Open Source | Its Paid tool |
| Vulnerability Scanning and exploitation framework | Only Provide scanning |
| Its Operating System | Its Just Software |
| Large no of Tools in it | Single software |
| Provide penetration testing of endpoint, web, waf, phishing awareness | Just network vulnerability scanner |
| Automated and Manual | Automated |
| Perform exploitation on run time | No runtime exploitation |
| Reporting | Better Reporting |
| Only Debian based | Can be use on any OS |