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

Conducting penetration testing should be carried out in an ethical manner (white hat hacking). Caution needs to be practised at all times to ensure that there are no unintended activities that can cause unintended and unforeseen outcomes as a result of ignorance or negligence. The best practice would be to utilise an isolated environment from the production environment when utilising Kali. The setting can be on a virtual computing platform with no direct access to the production network environment. Kali has been designed with security professionals in mind. Thus, a great list of tools pre-installed on Kali to conduct vulnerability testing, such as information gathering, vulnerability analysis, password attacks, and wireless network attacks.

What issues might you encounter?

Firstly, you might download a compromised version of Kali loaded with malware.

While conducting a vulnerability scan, there is a possibility that the activities might impact the production environment and result in unintended outcomes.

How would you overcome them?

Always run a hashing checksum result verification to ensure that you have downloaded the uncompromised version of the operating system to ensure that you are not introducing malware in the environment.

Request permission and obtain approval to conduct a vulnerability scanning. Communicate to the relevant stakeholders inform them of the activities you are about to carry out and the possible disruption that may be encountered. Clear and transparent communication with the stakeholders will ensure that they can make balanced risk-based decisions.

How do their results compare with your initial evaluation?

Nmap, Wireshark and Metasploit were rated higher because they are the tools I use most compared to the rest.

What do you think of their criteria?

Although the list contains tools with specific functions, I believe that the list could have included comprehensive tools such as Pentestbox (pentestbox.org), which has the following tools included :

- Web Vulnerability Scanners
- Web Applications Proxies
- CMS Vulnerability Scanners
- Web Crawlers
- Information Gathering
- Exploitation Tools
- Password Attacks
- Android Security
- Reverse Engineering
- Stress Testing
- Sniffing
- Forensic Tools
- Wireless Attacks
- Text Editors
- Linux Utilities
- Browser

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

Pros:

- Kali is free of cost, whereas Nessus is now commercial.
- Kali is customisable with the on-demand installation of tools.

Cons:

- Nessus has policy management, whereas Kali doesn't have policy management.
- There is no customer support for Kali Linux.