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

Understanding the target by gathering information about the targets such as hosts, domains, sub-domains, operating system, application version, and open ports.

Kali Linux has many tools which are used to gathering information, vulnerabilities as system analysis, and exploitation tools.

What issues might you encounter?

With using root user may damage system if altered a critical files or system become unstable. Some commands maybe harm the network if not understand the implications.

Some actions maybe turn out to be unlawful.

How would you overcome them?

Using test environment in virtual lab by using virtualization technique to guarantee that all tests done inside the lab not outside.

-------------------------------------------------------------------------------------------------------------------------

How do their results compare with your initial evaluation?

, netcat is a super powerful tool, which can be used to discover network hosts, scan ports, get operating system details, and application name and version.

Open VAS and Nikto are complete each other where open VAS used to explore network vulnerabilities, while Nikto used to perform web server penetration test.

What do you think of their criteria?

Enlisting the potentials vulnerabilities or threats, then list tools as per priority and criticality those from their side of view, therefore, maybe they missed a small or simple threat which may cause bad harm to the system.

It is good to do general weakness assessment along side with the purpose assessment. Otherwise, they need to use more tools to guarantee that the result is valid.

------------------------------------------------------------------------------------------------------------------------------

“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?

Pros:

Free

Kali can run from DVD or flash desk without be installed

Pre-installed package with more than 600 tools.

Cons:

Root user can be a potential threat if the Kali connected to exposed environment.

Some Kali commands can cause damage to your home network

Need training because of many tools especially command tools.

Nessus Cons:

Commercial using

Has this changed your original evaluation score?

🤔

------------------------------------------------------------------------------------------------------------------------------------