Unit 7 E-Portfolio Group 3 Team Discussion Responses

Ying:

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

Gathering and understanding the target information

Dmitry is a deep magic information gathering tool used to identify

Test on the exploits and other attacks

- What issues might you encounter?

The assessment needs to be carried out on anti-virus and firewalls systems to get the precise final result.

Security system might prevent the penetration testing of WAF

- How would you overcome them?

Clone the system and test it without a security system

- How do their results compare with your initial evaluation?

Mostly the same

- What do you think of their criteria?

Better to quantify the criteria instead of Yes/ No.

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

Kali Linux pros: It is capable of running it “live” from a USB drive / DVD, including most of the common free tools.

Kali Linux cons: Required Linux and system knowledge.

Nessus pros: Provided plugins for most of the vulnerabilities. It is easy to use and can run the scan in a large scale by scheduling.

Nessus cons: It is not actively prevented attacks but a tool that checks your computers to find vulnerabilities that are exploited.

- Has this changed your original evaluation score?

Kali Linux should be the most powerful tool to cover the penetration testing process. The initial evaluation was based on different criteria, which balanced from the typical user point of view. It should include accuracy, exploit discovered rate, etc., which had most common free tools and the capability to install and customise.

Haseeb:

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

It understands 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 to gather information, such as system analysis and exploitation tools.

What issues might you encounter?

Using root user may damage the system if altered critical files or the system become unstable. Some commands maybe harm the network if not understood the implications.
Some actions may be turn out to be unlawful.

How would you overcome them?

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

How do their results compare with your initial evaluation?

Netcat is a super powerful tool that can discover network hosts, scan ports, get operating system details, and application name and version.
Open VAS and Nikto are complete, where open VAS is used to explore

network vulnerabilities while Nikto performs web server penetration tests.

What do you think of their criteria?

Enlisting the potential vulnerabilities or threats, then list tools as per priority and criticality those from their side of view; therefore, they missed a minor or straightforward threat which may cause harm to the system.
It is good to do a general weakness assessment alongside the purpose assessment. Otherwise, they need to use more tools to guarantee that the result is valid.

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

Pros:
Free
Kali can run from DVD or flash desk without being installed
Pre-installed package with more than 600 tools.

Cons:
The root user could be a potential threat if the Kali is connected to an 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?
🤔