**Vulnerability scans using Kali Linux**

Vulnerability scanning is a process of inspecting a system to identify any loopholes that may expose it to attacks. Security holes that can be used to compromise the system are pointed out in vulnerability scans. Vulnerability scans are used to detect and classify system weaknesses in computers, networks, and communications equipment. After successful scans, predictions are made on the effectiveness of the system, and countermeasures are taken to reduce vulnerability.

There are several steps followed in conducting a vulnerability scan. Before conducting a vulnerability scan, one needs to have an asset inventory in the scanning environment. It’s a requirement to do a network sweep to identify live assets before starting. After identifying the assets, the vulnerability scanning process begins by aiming a scanner at them.

The first step involves information gathering. During this step, hosts and restricted hosts are identified; that is, systems and devices that need not be tested are put aside.

The next step is the actual discovering vulnerability scanning. After successful information gathering, extensive scanning of ports and fingerprinting services and applications are done. Automated scanning tools and technologies are utilized in this stage.

The last stage in vulnerability scanning is to draft an executive summary explaining the overall environment state.

In Kali Linux, vulnerability scans are done using a vulnerability scanner to test a computer application's vulnerability. The scanner creates a directory for each of the processes that are connected to the system. These processes include firewalls, networks, servers, e.t.c First, the vulnerabilities are identified by the scanner then the analysis is done on the risks of the vulnerabilities found. During the analysis, the easiness of exploiting the vulnerability is identified, the impact on the system is identified, that's if the vulnerability will be exploited, and it’s also investigated whether measures are in place to reduce vulnerability.

Lastly, any operations against the vulnerabilities are identified. The vulnerabilities identified need to be fixed or patched to ensure the system is secure and cannot be exploited by an attack. This phase involves two options which include ignoring the vulnerability, that is, if the risk is low and the other option being that the vulnerable system can be ceased or added to security measures to prevent the vulnerability from being exploited.

There are four types of scans used in Kali Linux names: External vulnerability scanning, which is done outside the network of the organization. It targets applications used needed to be used by external users or customers. The second one is internal vulnerability scanning which is carried out inside the organization and targets vulnerabilities that can be exploited by an attacker who can gain access to the organization’s sensitive information. The third scan is unauthorized scanning which searches for vulnerabilities within the organization's network. The last type of scan is authorized scanning, which involves giving out credentials to vulnerabilities scanners to check the network and system for weak passwords, misconfigurations, and applications with flaws.

**Issues one might encounter during vulnerability scanning**

During vulnerability scanning, there are some issues that can be identified by the scanners, which include: External vulnerability scanning identifies known weaknesses in a network. Internal vulnerability scanning looks at other hosts in the same network to identify internal vulnerabilities.

**How to overcome vulnerability issues**

Overcoming vulnerability issues can be done by using breach and attack simulation technology which runs various scans and attacks to check whether it's capable of preventing, detecting, and provide a defense to the targeted network.

Application security testing can also be done to make sure that the application at risk is working correctly and also to prevent exposure of the application to external threats. It also checks misconfigurations in the code of the application. It also checks the application on matters of securities, identifies its weaknesses, and vulnerabilities and helps to identify and prevent vulnerabilities exploitation.

**Results comparison with the initial evaluation**

Penetration testing is basically a cyberattack carried out against a computer system to evaluate its security and check for exportable vulnerabilities. In web applications, penetration testing is used together with a web application firewall.

Penetration testing is done in five stages, namely: the planning stage, where the scope and goals of the test are stated and information is gathered, including domain and network names. The next stage is the scanning stage which aims at understanding the response from the target applications when intrusion attacks are made. The next step is actually gaining access to the application to try and exploit vulnerabilities. The fourth step is maintaining the gained access to determine how long an attacker can access the application without being noticed. The last step is the analysis step, where results of the penetration tests are compiled to make a general report.

Penetration testing is, however, done by tools known as penetration tools. My initial evaluation of the tools goes hand in hand with the study to compare penetration tools done by Bhingardeve and Franklin in 2018. That's derived from their journal titled "A Comparison Study of Open Source Penetration Testing Tools."

**Opinion about the criteria used in the evaluation**

Their criteria of extensive study of one tool at a time are recommendable. There are many penetration testing tools used for penetration testing. It was necessary for them to do extensive research from various sources, including journals, articles, internet sites, archive sources, and blogs.

However, in order to recommend some testing tools over others, it was necessary to come up with various features to check across. Some of the features they came up with were: flexibility, powerfulness, portability, ease of use, availability (free), their documentation for use, whether it's powerful or not, the support provided by the owners, and popularity.

**pros and cons of using Kali Linux vs. Nessus**

Nessus is a tool used to scan vulnerabilities in a system. It works by raising an alert in case of any vulnerabilities, which hackers can use to access any computer connected to a network.

Though Kali is used for penetration testing, Nessus tool is highly recommended to be used hand in hand with Kali Linux as an operating system.

Nessus is available are a very low price; hence it's affordable to use.

It is easy to use and report vulnerabilities using Nessus, which one can customize in his/her own way.

Nessus works well in scanning ipv4 and ipv6 networks.

Nessus can be used for scanning in all companies’ network devices, all company platforms, and across all operating systems.

It is easy to schedule target devices for scanning.

Nessus has a high level of accuracy and with fewer errors.

However, it has its own disadvantages, including:

sometimes scanning takes a long time than expected.

Integrating it with some other third-party tools is hectic at times.

When performing a scan on the same system twice, different results may be obtained.

For large application scanning, it becomes buggy. When working with large data sets, this tool becomes slaggy and slows down.

Its graphical user interface is a bit intuitive; hence finding features becomes hard at times.

Though it's easy to use, it assumes that a user has a certain level of knowledge, thus making it hard for inexperienced users to use it.

**Evaluation score**

The initial evaluation score of Kali Linux has increased on the outlined factors above. This is because after gaining some knowledge on penetration testing and the tools to be used, it's easier to achieve the goal while using kali Linux other than other Linux distros.