Hello Everyone! In this video, you will learn about vulnerability assessment and the tools to perform this activity.

Vulnerability assessment is the process of identifying and quantifying known security vulnerabilities in an environment. It indicates the weaknesses as well as provides the appropriate mitigation procedures required to either eliminate those weaknesses or reduce them to an acceptable level of risk.

Vulnerability Assessment is a step-by-step process. It starts with Identifying Vulnerabilities using open-source or commercial tools such as Nmap, OpenVAS, NESSUS, etc.
After this, the Vulnerabilities are evaluated to estimate the risks posed by them. Vulnerability management solutions will provide different risk ratings and scores for vulnerabilities, such as Common Vulnerability Scoring System (CVSS) scores.
Once a vulnerability has been validated and deemed a risk, the next step is to treat that vulnerability. There are different ways to treat vulnerabilities, including remediation, mitigation, or acceptance. The vulnerabilities which have no known adverse effects may be accepted sometimes.
At last, the vulnerabilities are reported for protecting other systems by resolving the vulnerabilities in a similar way.

Let's discuss some popular vulnerability assessment tools. Nmap or (Network Mapper) is one such open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications. Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.

One of the greatest features of Nmap is "The Nmap Scripting Engine" (known as NSE). Using NSE is crucial in order to automate system and vulnerability scans. Script option is used with the Nmap command for using the Nmap scripting engine, as shown here.

Nmap – sV –Pn –T5 – – script vulscan <target ip>

Here V, P and T options have their usual meaning and they are optional. Vulscan is a script used for vulnerability scanning. There are many Vulcan scripts are available on GitHub. Target ip represents the machine to be scanned.

For example, if the user wants to run a full vulnerability test against his target **192.168.45.130**, he can use the following parameters with the Nmap command:

Nmap --script vuln 192.168.45.130

Here vuln is a script with known vulnerability databases included.

The vulscan script is available of GitHub and can be copied from there using gitclone command, as shown here. After cloning, it is linked to NSE directory using LN command to be directly used for vulnerability scanning.

after this step run the Nmap command as shown.

Google Hacking is mainly referred to pulling the sensitive information from Google using advanced search terms that help users to search the index of a specific website, specific file type and some interesting information from insecure Websites.

Google "**Dorking**" is the practice of using **Google** to find vulnerable web applications and servers by using native **Google** search engine capabilities. Unless you block specific resources from your website using a robot. txt file, **Google** indexes all the information that is present on any website.

You can find very important data such as Admin login pages, Username and passwords, Vulnerable entities, Sensitive documents, Govt/military data, Email lists, Bank account details and lots more using Google dorks, if not controlled.

Nikto is another tool for vulnerability scanning . It is an Open Source web server scanner that performs comprehensive tests for multiple items.
It also checks for server configuration items such as the presence of multiple index files, HTTP server options and also attempts to identify installed web servers and software.
Nikto is free to use, and frequently updated. It Can be used to scan any web server (Apache, Nginx, Lighted, Litespeed, etc.)

Let's see how Nikto can be setup on Kali Linux. Check the vulnerability analysis category tools within Kali Linux to see if it is there; otherwise, being an open source tool you can get Nikto from GitHub, you can use apt install command in Kali Linux, if not available by default, as shown here.

You can use –Help option to see a detailed guide on all the inputs Nikto can take and what each input does, as shown

Here is an example of using Nikto for scanning a website. h option is used to scan any hostname as shown. Substitute the default IP or hostname with a hostname of your choice:

To scan an SSL website, use ssl option as shown.

nikto -h <website ip/url> -ssl

The website ip/url represents the target to be scanned, such as linuxhunt.com.

OpenVAS is a GUI-based vulnerability scanner. It is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning/management solution. Its capabilities include unauthenticated testing, authenticated testing, various high-level and low-level Internet and industrial protocols, performance tuning for large-scale scans, and a powerful internal programming language to implement any type of vulnerability test. It is open source and free. The scanner is developed by Greenbone Networks and has been

maintained by it since 2009. it has an easy to use GUI and scan dashboard.

NESSUS is an another popular and proprietary vulnerability scanner developed by Tenable, Inc. It is a commercial tool. But a free version is available with a limited set of capabilities to scan a maximum of 16 machines per user.

Thank You.