Alright, let's break this down into simpler terms:

**What is Port- and Vulnerability Scanning ?**

* **Scanning for Open Ports**: This is like checking the doors and windows of a house to see which ones are open. In computer networks, 'ports' are virtual doors through which network communications can pass. If a port is 'open', it means there's a program running on your computer that is waiting to talk or listen through that port.
* **Vulnerability Scanning**: This is like checking for weak spots in a house where a thief might break in. In computers, this means looking for weaknesses in the network or in the software that can be exploited.

**Tools Used:**

* **Nmap (Network Mapper)**: This is a tool that helps you discover what's connected to your network(hosts), what services they're offering, their operating system, and other details. It's like a high-tech way of mapping out all the devices and services on a network.
* **Zenmap**: This is a more user-friendly version of Nmap. It has a graphical interface, making it easier to use, especially if you're not too familiar with command-line tools.

**How to Use Them:**

* **Starting Zenmap**: If you're using a Linux system, type 'zenmap-kbx' in the terminal. If you're not logged in as the main user (root), use 'sudo zenmap-kbx'.
* **Using Zenmap**: In Zenmap, you can enter the names or IP addresses of the computers you want to scan in the 'Target' field. There are different types of scans you can do, like 'Ping Scan', which is like sending a signal to see if the other computer responds.
* **Scanning an IP Range**: You can scan a range of IP addresses (like '10.11.202.0/24') to find out which computers are connected and what services they're offering.

**Advanced Scans:**

* **Using Command-Line Nmap**: For more advanced options, you can use Nmap in the command line. This lets you do more detailed and specific scans.
* **Scanning Virtual Machines**: You can scan different types of virtual machines (like Windows or Linux) to see which ports are open and what services they are running.
* **Differences Between Windows and Linux Scans**: When scanning, you might notice differences in the open ports and services between Windows and Linux machines.
* **Scanning for Vulnerabilities**: You can also scan machines with known vulnerabilities, like a Windows computer running a Trojan horse (like NetBus) or a backdoor (like 'nc.exe').

**Why Do This?**

* **Learning and Security Testing**: These scans help you understand network security and how to protect your own network. It's like learning the weak points in your own digital 'house' so you can make it safer.

Remember, it's important to only scan networks and computers you have permission to test. Unauthorized scanning can be illegal and unethical.

Top of Form