**CHAPTER- 4: Vulnerability Scanner**

**4.1) DEFINITION:**

Vulnerability scanner is an automated tool that identifies and creates an inventory of all IT assets (including servers, desktops, laptops, virtual machines, containers, firewalls, switches, and printers) connected to a network.

For each asset, it also attempts to identify operational details such as the operating system it runs and the software installed on it, along with other attributes such as open ports and user accounts. A vulnerability scanner enables organizations to monitor their networks, systems, and applications for security vulnerabilities.

**Tools Required:**

* Kali Linux
* Python3
* Pycharm (optional)

**Dependencies:**

* socket Library
* Ipy Library
* Threading module
* Vulnerable Banners

**Step 1:**

Import all modules needed

Text

Description automatically generated

**Step 2:**

Also create two arrays for storing the ports and banners and iterate through them.

Text

Description automatically generated

**Step 3:**

We create the port scanner class which checks all the ports for vulnerabilities using the banner grabbing technique and will append the vulnerabilities found

**Text

Description automatically generated**

**Step 4:**

Defining the banner class which receives banners from the target

Text

Description automatically generated

**Step 5:**

We specify the target by taking input from the command line

Text

Description automatically generated

**Step 6:**

We then specify the ports to be scanned by taking input from the command line

Text

Description automatically generated

**Step 7:**

We finally create a function to open the vunerable\_banners.txt and use it to compare banners

This text file is to be updated based on the present vulnerabilities discovered

Text

Description automatically generated

Now our script is ready

**Step 8:**

Create the vulnerable\_banners.txt and append the present vulnerable Banners

Text

Description automatically generated with low confidence

**Step 9:**

put both the script and the vulnerability scanner script and the vulnerable\_banners.txt in the same folder

Graphical user interface, website

Description automatically generated

Now the tool is ready for use

**Execution and Usage :**

In the directory of the tool, execute python3 portsc.py which is the vulnerability scanner

A screenshot of a computer

Description automatically generated with medium confidence

We give the target as input

A picture containing text, indoor, computer, dark

Description automatically generated

Also the number of ports to be scanned

A screenshot of a video game

Description automatically generated

As there are no vulnerabilities we can see no issues

Text

Description automatically generated