High Level Design (HLD)

Vulnerb

Date :- 05/11/2022

By

Abhijeet Adani

**Table of Contents                                                                    Page No**

**ABSTRACT**

**1. INTRODUCTION                                                                                                                                  1**

**1.1 Introduction**

**1.2 Purpose                                                                                                                                         1**

**1.3 Scope                                                                                                                                         2**

**2. LITERATURE SURVEY 3**

**2.1 Fyodor.             3**

**2.2 Marco de Vivo, Eddy Carrasco, Germinal Isern and Gabriela O. 3**

**2.3 Pete Herzog.**

**2.4 Roger Christopher. 4**

**2.5 Brenden Claypool. 4**

**2.6 Harry Anderson. 4**

**2.7 Nazar El-Nazeer and Kevin Daimi. 4**

**2.8 Gadge, J. Patil. 5**

**2.9 Zhang and Fang. 5**

**2.10 Monowar H Bhuyan, D K Bhattacharyya and J K Kalita. 5**

**2.11 Mehiar Dabbagh, Ali J. Ghandour, Kassem Fawaz, Wassim El Hajj and Hazem Hajj. 5**

**3. REFERENCES 6**

**ACKNOWLEDGEMENT 7**

**ABSTRACT**

Rising technologies overall the world is increasing day by day. The Internet is a massive interconnection that connects the global wide area network throughout the world. The network connection is used for various activities such as emails, downloading files, etc., and also new techniques propages through different filed in different activities.

With the increasing concern for security in the network, many approaches are laid out that try to protect the network from unauthorized access. New methods have been adopted in order to find the potential discrepancies that may damage the network. Most commonly used approach is the vulnerability assessment. By vulnerability, we mean, the potential flaws in the system that make it prone to the attack. Assessment of these system vulnerabilities provide a means to identify and develop new strategies so as to protect the system from the risk of being damaged.

Keywords:- Vulnerability scanner , web application penetration testing, WAP , OWASP Top 10, Port scanner, Hacking web Application, DevSecOps.

**1 Introduction**

**1.1 Introduction**

Vulnerb (Vulnerability/Port Scanner) is a free utility for network exploration and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts.

**1.1** **Purpose**

                  Port scanning is a method of determining which ports on a network are open and could be receiving or sending data.

   It is also a process for sending packets to specific ports on a host and analysing responses to

   identify vulnerabilities.

This scanning can’t take place without first identifying a list of active hosts and mapping those hosts to their IP addresses. This activity, called host discovery, starts by doing a network scan.

The goal behind port and network scanning is to identify the organization of IP addresses, hosts, and ports to properly determine open or vulnerable server locations and diagnose security levels. Both network and port scanning can reveal the presence of security measures in place such as a firewall between the server and the user’s device.

After a thorough network scan is complete and a list of active hosts is compiled, port scanning can take place to identify open ports on a network that may enable unauthorized access.

It’s important to note that network and port scanning can be used by both IT administrators and cybercriminals to verify or check the security policies of a network and identify vulnerabilities — and in the attackers’ case, to exploit any potential weak entry points. In fact, the host discovery element in network scanning is often the first step used by attackers before they execute an attack.

As both scans continue to be used as key tools for attackers, the results of network and port scanning can provide important indications of network security levels for IT administrators trying to keep networks safe from attacks.

**1.2 Scope**

      Port scanning is a popular reconnaissance technique which is used to discover the open ports and services available on a particular host. It can be used by the network administrator to check the open ports; it can be used by penetration tester during the security audit to check for vulnerabilities or it can be used by an attacker or a hacker to discover vulnerable service that they can exploit to break into the system. Every host connected to the LAN or internet run many services that listen on some port. By running the port scan, we can get the information like what all ports are open, what service is running on each port, what is the OS and MAC address of the target host, etc. We can configure the port scanner according to our requirement to get the maximum information from the target system.

Port scanners send a request to connect to each port sequentially and based on the response it decides whether the port is open, closed or filtered.

* Open port: The remote host sends a response to accept the connection.
* Closed port: The remote host sends a response indicating the connection is denied.
* Filtered port: There is no reply from the remote host.
* There are total 65536 ports each for TCP and UDP protocol which are divided into three ranges:
* Well known ports: These ports are in the range of 0-1023.
* Registered ports: These ports are associated with certain protocols or application. These ports lie in the range of 1024-49151.
* Dynamic /private ports: Ports>49151

**2. LITERATURE SURVEY**

Port scanning permits a hacker to deduce what services are running on the systems that have been pointed out. If vulnerable or insecure services are tracked down, the hacker may be able to exploit these to gain unauthorized access. We have a total of 65,535 \* 2 ports (TCP & UDP). While a complete scan of all these ports may not be feasible, analysis of popular ports should be performed. By port scanning, one is able to find out which ports are accessible. Factually, a port scan consists of sending a message to each port, one at a time and analyzing the response received. If the port is in use, it can then be examined further for weakness. Port Scanning is one of the most favoured reconnaissance techniques which attackers use. By port scanning, one discovers which ports are available (i.e. being listened to by a service). Essentially, a port scan consists of sending a message to each port, one at a time and examining the response received. If the port is in use, it can then be probed further for weakness. Port Scanning is one of the most popular among the reconnaissance techniques attackers use.

In [1] Fyodor has suggested many techniques used to discover what ports (or similar protocol abstraction) of a host are listening for connections. These ports typify potential communication channels. Mapping their existence smooth`s the exchange of information with the host, and thus it is very useful for anyone who wants to investigate their networked environment, including hackers.

 In [2] Marco de Vivo, Eddy Carrasco, Germinal Isern and Gabriela O. de Vivo have set forth that TCP port scanners are distinctive programs used to discover what TCP ports of a host have processes listening on them for viable connections. Since these ports specify, in part, the amount of manifestation of the hosts to potential external attacks, knowing their existence is a elementary matter for network and/or security administrators.

In [3] Pete Herzog has suggested that Port scanning is an invasive examining of system ports on the transport and network level. The paper also includes the validation of system reception to encapsulated, tunneled or routing protocols. This parameter is to calculate live or accessible Internet services as well as penetrating the firewall to discover additional live systems. Testing for different protocols will depend on the system type and services it provides.

In [4] Roger Christopher has described that Port Scanning is one of the most favorable techniques attackers use to find services that they can enslave to break into systems. All systems connected to a LAN or the Internet with a modem run services that listen to the ports which are well-known and not so well-known. By port scanning, the attacker can gather the following information about the targeted systems: what services are executing, under what users those services run, whether anonymous logins are supported or not, and whether certain network services require authentication or not.

In [5] Brenden Claypool have described that Port scanning is a skillful and efficient way which is used by attackers, curious individuals, and administrators to gather information from computers on a network. System and network administrators take the help of port scans to find out open ports to a system so that they may be able to access those ports, or shut them off fully. The way attackers and administrators use port scanning is the same but the only difference lies in their purpose. The attackers use port scanning for malicious purpose. There are many techniques which are used in stealth scanning, ranging from those that prevent their detection by logging systems, identity concealment, to confusing the server with invalid information. All of these techniques are interesting in their implementation and execution.

In [6] Harry Anderson has described that Port scanning appears simple on the surface but is actually a very complicate subject. One factor which makes port scanning tough is the response system. Accuracy, stealth and speed are the principal factors to stabilize when scanning the ports. The factors which affect these are timeouts, the type of scan and what ports to scan. The two most often used types of scans are the SYN scans and connect (). There is disparity of both in Nessus and in the optional NMap component.

In [7] Nazar El-Nazeer and Kevin Daimi have put the light on network port scanning tools. A port is an application noticeable software construct acting as an endpoint in many communications. The Transmission Control Protocol (TCP) and the User Diagram Protocol(UDP) of the Transport Layer mainly uses the ports. Ports are recognized by numbers. For example, Port 25 is used for Simple Mail Transfer, and port 80 is reserved by HTTP. A port scan is an attack that tries to discover known vulnerabilities of a service running on active ports. Both network administrators and attackers use port scanner tools to examine servers/hosts for open ports, but with different purposes.

In [8] Gadge, J. Patil, and A.A. have proposed that Port scanning is a phase in foot printing and scanning; this comes in reconnaissance which is regarded as the first phase of a computer attack. Port scanning aims at finding open ports in a system. These open ports are taken as an advantage by attackers to carry out attacks and exploits. There are a number of tools which are used for scanning open ports. However, very few tools are present to detect port scanning attempts.

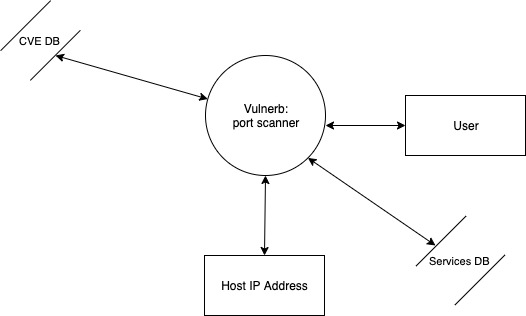
 In [9] Zhang and Fang have proposed a new port scan detection approach known as time-based flow size distribution sequential hypothesis testing (TFDS) for transit networks which are having high speed where only unidirectional flow information is available. TFDS makes use of the foremost ideas of sequential hypothesis testing to detect scanners that exhibit abnormal access patterns in terms of flow size distribution entropy.

In [10] Monowar H Bhuyan, D K Bhattacharyya and J K Kalita, have described that the Scanning of ports on a computer occur habitually on the Internet. An attacker conducts port scans of IP addresses to discover vulnerable hosts so as to compromise them. However, it is also helpful for system administrators and other network defenders to discover port scans as possible preparatory measures to more serious attacks. It is a very tough task to recognize instances of malicious port scanning. Port scanning is designed to examine a network host for open ports and other services accessible. From the attacker‟s viewpoint, a port scan is helpful for collecting relevant information for initiating a successful attack. Thus it is of appreciable interest to attackers to determine whether or not the defenders of a network are scanning ports frequently. Defenders do not often conceal their identity during port scanning while attackers do.

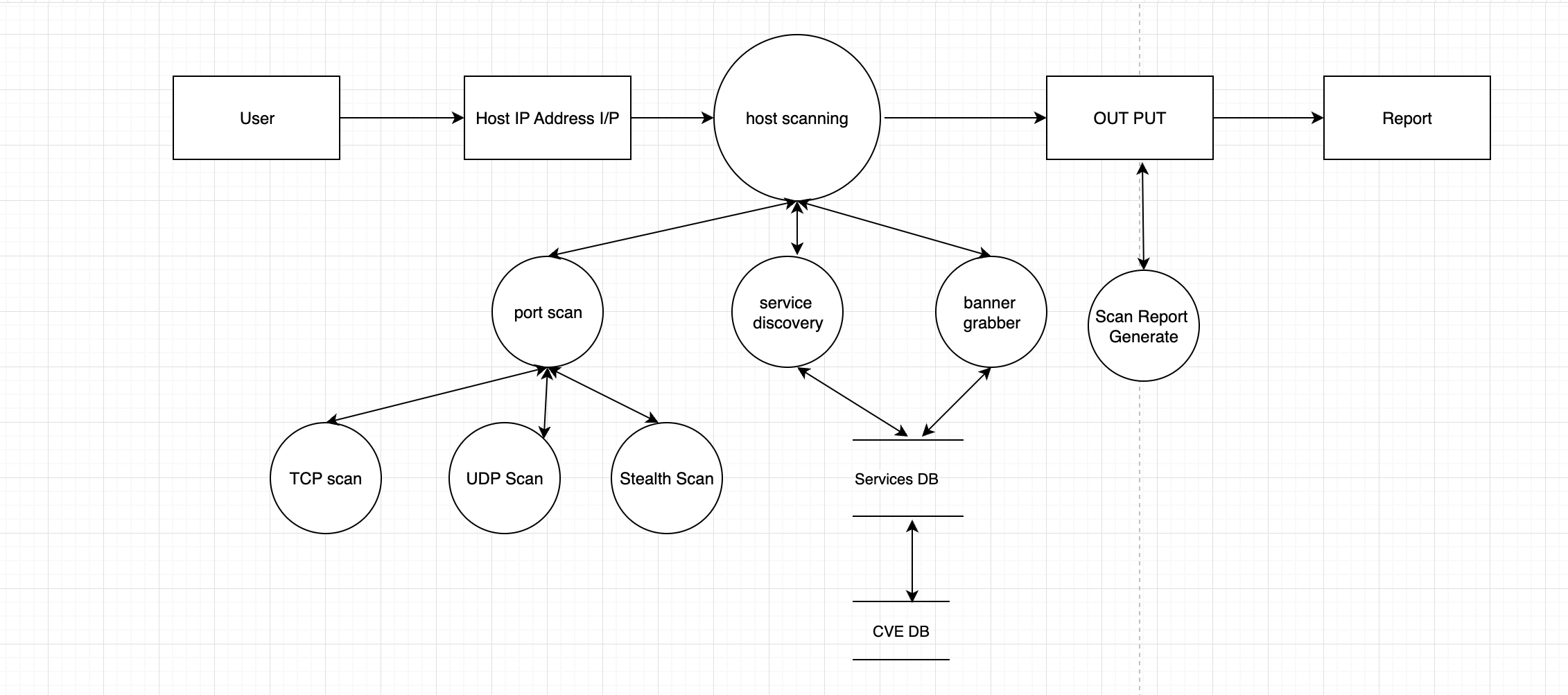
 In [11] Mehiar Dabbagh, Ali J. Ghandour, Kassem Fawaz, Wassim El Hajj and Hazem Hajj have suggested that port scanning is generally divided into two main parts, horizontal and vertical. In horizontal scans, the same port is scanned on the multiple hosts. This is helpful for attackers who want to gain access on victim hosts by exploiting a known vulnerability of a definite service running on that port. While in vertical attacks, multiple ports are scanned over the same host. This is common for attackers who are collecting information to attack a particular target host. Port scanning is the most favorable reconnaissance technique which attackers use to determine services they can exploit. Port scanning detection has got a lot of attention by researchers.Nevertheless, a slow port scan attack can defraud most of the existing Intrusion Detection Systems (IDS).

DFD Diagram:-

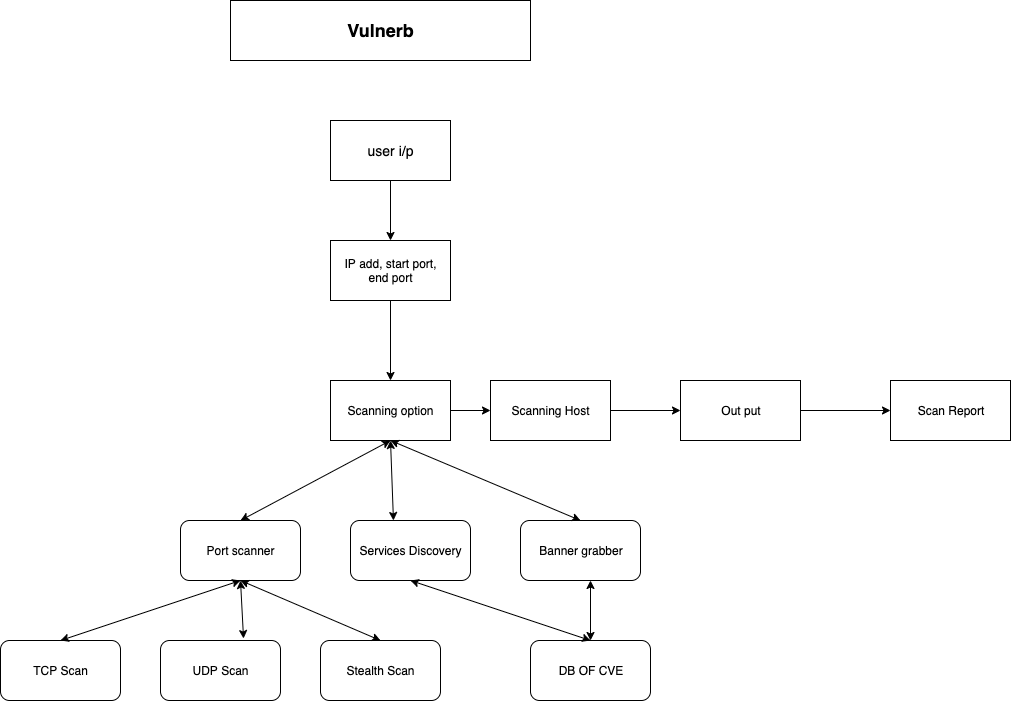
Level 0 :-



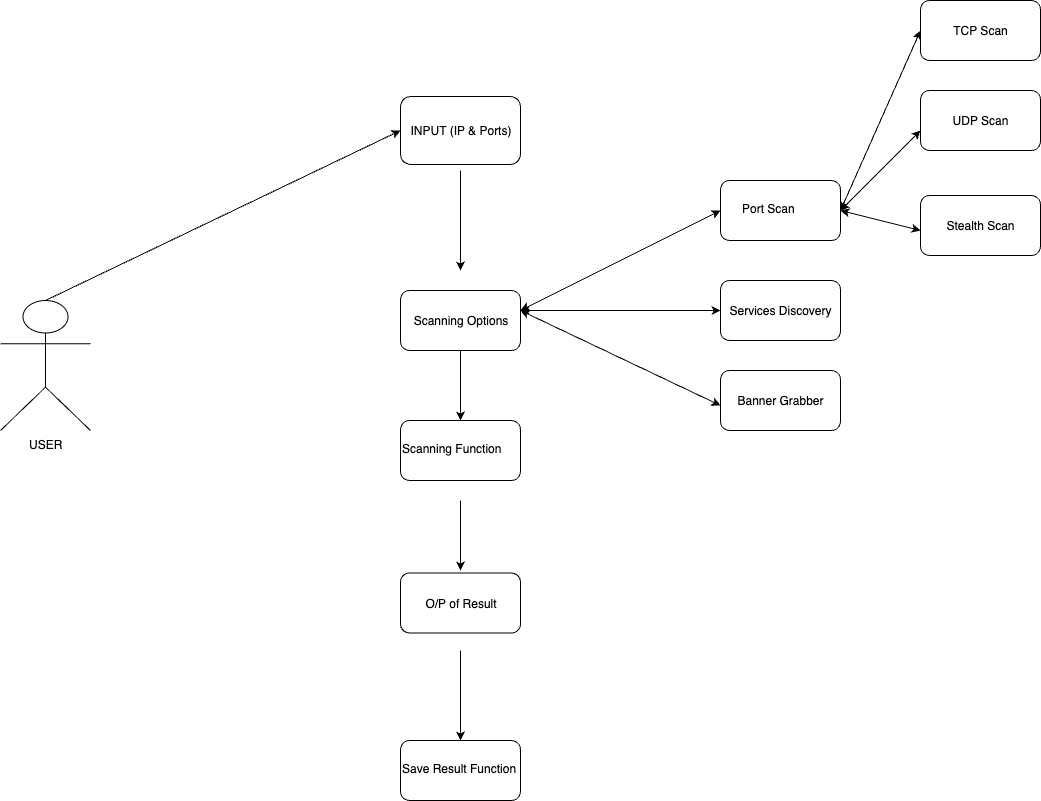
Level 1:-



State Transition Diagram :-

****

Use Case Diagram :-



**References**

**Internet Sources:**

**[1]**[**https://nmap.org/**](https://nmap.org/)

**[2]**[**https://www.sciencedirect.com/**](https://www.sciencedirect.com/)

**[3]**[**https://www.techopedia.com/**](https://www.techopedia.com/)

**[4]**[**https://www.python.org/doc/essays/blurb/**](https://www.python.org/doc/essays/blurb/)

**[5] https://www.tenable.com**