**IOSR Journal of Engineering (IOSRJEN)** **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 61-62

# Application on Securing System Ports

Ankita lohkare[#1], Ruchika bangade[*2], Vaishnavi rokde[#3]
Aditya khnate, Abhishek shukla
*Information Technology RTM University India*

***Abstract***— *Gathering, an attacker uses to create a profile of the target organization.Our application will determine what host are available on the network, the services that are enabled.Devices get hacked in the network, if they have open ports.Basically, majority of attacks performed on system is performed by scanning ports.So, It is good to make an application which will scan for ports and tell user that which port is open Network scanning refers to a set of procedures for identifying host, ports and services on a device in a network.*
***Keyword –****PORT, WHOIS, CVE*

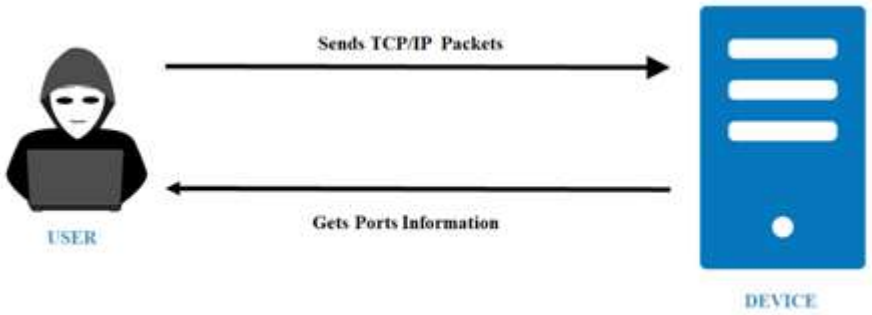
## I. Introduction

Network scanning refers to a set of procedures for identifying host, ports and services on a device in a network.

Network scanning is one of the components of intelligence gathering, an attacker uses to create a profile of the target organization. Our application will determine what host are available on the network, the services that are enabled.

With an increase in computer literacy people are becoming aware about the loopholes present in the Operating Systems, networking protocols, software applications which are used on a daily basis. Many easy-to-use tools are freely available on the Internet which can take advantage of these loopholes to gain unauthorized access to a system. To further complicate the things most of us do not follow good security practices, making the job of computer criminals even easier. Computer crimes have increased over the years. They are not limited to trivial acts such as guessing the login password of a system, they are much more dangerous. Studies indicate that the first stage of an attack is reconnaissance [5]. In this stage the prime objective is to get information about the target system. One critical piece of information is the list of open ports of the system. Open ports of a system can be exploited in a number of ways. To identify open ports a number of tools are available [4].

network scanning process




Currently a number of solutions are in place to deal with attacks. However, most of the solutions such as Antivirus and Intrusion Detection Systems indicate occurrence of an attack or an un-authorized activity when it happens. Having a system which predicts occurrence of attacks in the near future is advantageous. As port scans are usually performed before an actual attack, identification of port scan attempts gives precautionary indication that attacks might follow in the near future. The goal of this project is to identify port scan attempts. This would make it possible to take precautionary steps to strengthen the defenses of the system. It would be very useful to have information about the machine from where the scans are coming. Information such as the Operating System being used, the possible location from where the scan came, information from WHOIS database and Traceroute would help in providing clues about the scanner. This information can be used against him if an attack takes place in future. Brute force scanners essentially perform scans in an aggressive manner by scanning one port after another for the specified range. They establish a full connection to the target machine and inspect whether the port is open. Owing to the full connection establishment, it is possible to detect their

presence. Thus when a large number of SYN packets arrive to request for a connection from a single IP address at multiple ports of the target machine, it indicates that a brute force scanner is being used to look for open ports. Stealth scanners get their name from their pattern of not establishing a full connection with the target. They send a single packet with a particular flag set at the target, based on the response it can be understoo

SYN Scans In this scan a large number of packets with only the SYN flag set arrive at the destination. This scan does not complete the 3-way TCP connection establishment handshake and tears down the connection after the victim replies with a SYN/ACK indicating an open port.

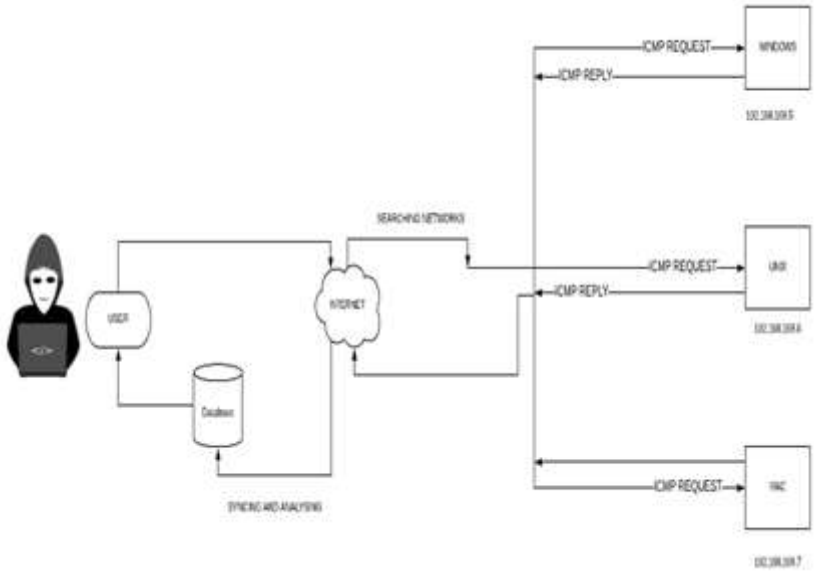
TCP Connect Scan In this scan a large number of connections are established with the victim at different ports. Establishment of a connection at a port indicates that the corresponding port is open. Once the connection is established and the open ports identified, the connection is closed

ACK Scan In this scan a large number of packets with only the ACK flag set arrive at the destination. This scan does not complete the 3-way TCP connection establishment handshake and tears down the connection after the victim replies with a SYN/ACK indicating an open port.

FIN Scan In this scan a large number of packets with only the FIN flag set arrive at the destination. If the victim replies with a RST it indicates that the port is closed, open ports simply ignore these packets. This scan can be easily identified if there are a large number of packets with the FIN flag set in them come from a single host.

XMAS Scan In this scan the flags FIN, PSH and URG are set. Open ports ignore these packets whereas closed ports reply with a RST. This scan can be easily identified if there are a large number of packets with the FIN, PSH and URG flag set in them coming from a single host.

Model Architecture




Scan Detection Using the information provided by the sniffer about the incoming packets, in particular the TCP flags present, patterns similar to general and stealth scans are found within the incoming packets. If a pattern is identified it will be marked. If the number of marked entries reaches a pre-specified threshold, it indicates that a scan is being performed. Filters are used to filter out the unnecessary traffic and concentrate only on packets which might

indicate a port scan attempt. For instance, a filter ' tcp[tcpflags] (tcp-syn|tcp-fin|tcpack) !=0 ' captures data about packets which have Ack, Syn and Fin flags set. Thus, using appropriate filters enables capturing of relevant packets with regards to different types of scans. Packets may be coming from many different sources; every packet is associated with the machine from which it is coming with the help of IP address. Online activities such as checking the E-mail, internet messengers and surfing web-pages generate packets which might be captured by the filters used. But the number of packets captured within a short span of time for these activities are very few compared to those captured when a scan is coming from a port scanner.

NULL Scan In this scan a large number of packets with no flags set arrive at the destination. The open ports ignore these packets whereas closed ports reply back with a RST.

ICMP Scan This includes sending ICMP echo request to the specified IP addresses to see if they are alive.

,