DESIGN AND IMPLEMENTATION OF PORT SCANNER AND SNIFFER

[1]Snehal Dhabarde, [2]Reshma Zade,[3]Nayan Paraswar, [4]Samruddhi Sonak,
Department of Information Technology, Rajiv Gandhi College of Engineering and Research Nagpur
Email:[1]dhabarde.snehal10@gmail.com,[2]zadereshma99@gmail.com,[3]nayanparaswar 1994@gmail.com,[4]sonaksamu@gmail.com

Abstract: A port scanner is a piece of software designed to search a network host for open ports. The only way to track open ports is by using a port scanner, and the most accurate port scanner will be an online port scan. This project aims at the creation of a comprehensive application, which can be used at corporate environments. The port scanner and sniffer software is as simple as possible so that it can be configured even by a nontechnical person. This is often used by administrators to check the security of their networks and by hackers to compromise it. The main objective of this project is to scan the various ports within a specified range. With help of this administrator can easily identify the open ports and warn the clients. Packet sniffing is a technique of monitoring every packet that crosses the network. A packet sniffer is a piece of software that monitors all network traffic. The security threat presented by sniffers is their ability to capture all incoming and outgoing traffic, including clear-text passwords and usernames or other sensitive material.

INTRODUCTION

Port scanning: Port scanning presents a method used to recognize ports for the open network in the computer system that they can break into. Port scanning has different legitimate uses that it performs in a system. It can be used to send a request to connect to the aimed computer and note the ports that responds or appears to open. Port scanning is also used to configure applications for network security to inform the administrators in case they detect some connections across a wide range of ports from a single host. Port scanning may involve all of the 65,535 ports or only the ports that are well-known to provide services vulnerable to different security related exploits. If a port on a remote host is open for incoming connection requests and you send it a SYN packet, the remote host will respond back with a SYN+ACK packet. If a port on a remote host is closed and your computer sends it a SYN packet, the remote host will respond back with a RST packet.

Packet sniffer: A packet sniffer is a tool that plugs into a computer network and monitors all network traffic. It monitors traffic destined to itself as well as to all other hosts on the network. Packet sniffers can be run on both non-switched and switched networks. Packet sniffers are more formally known as network analyzers and protocol analyzers. It monitors hub is called a Switched Ethernet. The switch maintains a table keeping track of each computer's MAC address and delivers packets destined for a particular machine to the port on which that machine is

connected. Packet sniffing is an essential activity for network engineers as well as security experts. If, used in a positive way, it is the most essential tool for network analysis, protocol analysis, network troubleshooting, intrusion detection and hundreds of such other applications.

A packet sniffer works by looking at every packet.

Sniffing methods

There are three types of sniffing methods. Some methods work in non-switched networks while others work in switched networks. The sniffing methods are:

- **IP-based sniffing:** This is the original way of packet sniffing. It works by putting the network card into promiscuous mode and sniffing all packets matching the IP address filter. Normally, the IP address filter isn't set so it can capture all the packets. This method only works in non-switched networks.

- **MAC-based sniffing**: This method works by putting the network card into promiscuous mode and sniffing all packets matching the MAC address filter.

- **ARP-based sniffing:** This method works a little different. It doesn't put the network card into promiscuous mode. This isn't necessary because ARP packets will be sent to us. This happens because the ARP protocol is stateless. Because of this, sniffing can be done on a switched network. To perform this kind of sniffing, you first have to poison the ARP cache1 of the two hosts that you want to sniff, identifying yourself as the other host in the connection. Once the ARP caches are poisoned, the two hosts start their connection, but instead of sending the traffic directly to the other host it gets sent to us. We then log the traffic and forward it to the real intended host on the other side of the connection. This is called a man-in-the-middle attack.

This application is designed into three independent modules which take care of different tasks efficiently:

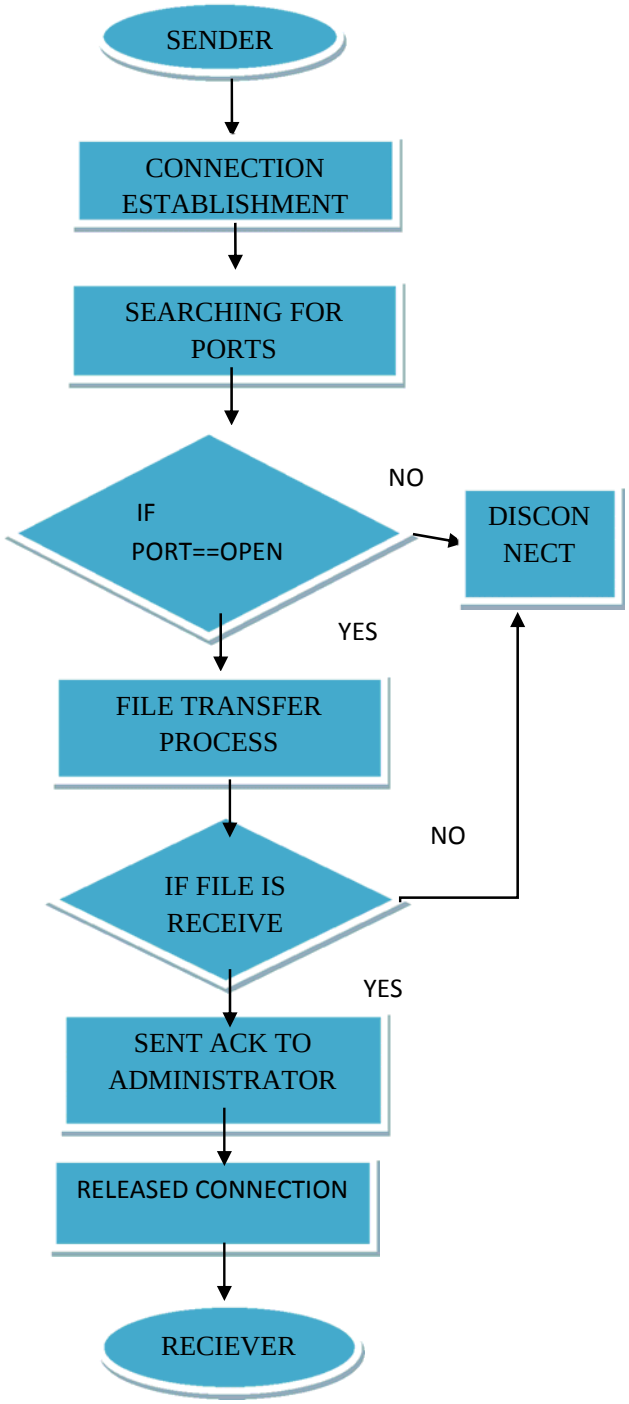
- **Authentication module:** In this module the administrator verifies the username and password. In ms access the administrator creates a database and in that the fields' username and passwords are entered. Whenever a client enters his details the system checks those details by comparing them with the details present in the database. If he is an authorized user he can log onto the system or else the access will be denied.
- **Scanning module:** In this we use the concept called multithreading to scan the multiple ports simultaneously. There are two types of scanning one is TCP scan and other is UDP scan. In TCP scan we send connect () system call to each and every port. If the port is open then connect() will proceed. In UDP scan we send a packet, if the packet is unreachable then we get ICMP port unreachable error. TCP scan is more reliable than UDP scan. In the scan page the admin/clients have to specify the IP address of the target machine, type of scanning and the range of the ports to be scanned.
- **Packet Sniffing Module**: Packet sniffer's, are protocol analyzers meant to capture the packets that are seen by a machine's network interface. When a sniffer runs on a system, it grabs all the packets that come into and goes out of the Network Interface Card (NIC) of the machine on which the sniffer is installed then it will receive all the packets sent to the network if that network is connected by a hub.

PROPOSED SYSTEM

Over time, a number of techniques have been developed for surveying the protocols and ports on which a target machine is listening. We send a blizzard of packets for various protocols, and we deduce which services are listening from the responses we receive (or don't receive). The application creates threads which attempt to connect to the supplied IP address and using the range of port numbers supplied. In this approach the effects of connection timeouts is minimized and the application can process a range of port. In this application it can show the "packet sniffing" concept. In this manner it can show the

captured packets and size of the packet and source and destination machine IP addresses which are involved in the packet transferring.

METHODOLOGY



Methodology: This project works as sender and receiver based application. Firstly client sends request to the admin or server after that server accepts request and connection will be established between client and server. After that the port scanning process starts if the port is open then file transfer process will be started else connection will be disconnected. If file is received then acknowledgement is send by receiver else connection will be disconnected. After the successful file transfer process the connection between sender and receiver is released.

CONCLUSION

The technological benefits of PORT SCANNER are monitor and enhance the performance of the system and provide security to the system. Using port scanner we can scan multiple ports simultaneously by using the concept called multi threading, by this time will be saved. Mainly port scanners are used in firewalls to find the open ports, so that the firewall can protect our system from threats which attack through these open ports. We can scan our own system without any help of a web server and we don't require any additional software to use this.

FUTURE WORK

In future administration will be given rights to close the open ports of the clients.Time limit will be given for each and every open port, if the port is not closed in the specified time it will be closed automatically.It can be extended as online port scanner.

ACKNOWLEDGMENT

We would like to express my special thanks of gratitude to our Guide Prof. Komal Ramteke as well as our Co-guide Mrs. Hemlata Arasade.

REFERENCES

[1] Marco de vivo , "A review of port scanning techniques"ACM SIGCOMM Computer Communication Review Volume 29 Issue 2, April 1999

[2] Ali, F.H.M. Fac. of Comput.& Math.Sci., Univ. Teknol. MARA, Shah Alam, Malaysia , "Simple port knocking method: Against TCP replay attack and port scanning"Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on Date: 26-28 June 2012

[3]http://en.wikipedia.org/wiki/Port_Scanner

[4]http://ieeexplore.ieee.org/search/searchresult.jsp?newsearch=true&queryText=Research+and+Implementation+of+Multithread+Port+Scanning+technology&x=0&SSS

5]http://en.wikipedia.org/wiki/sniffer