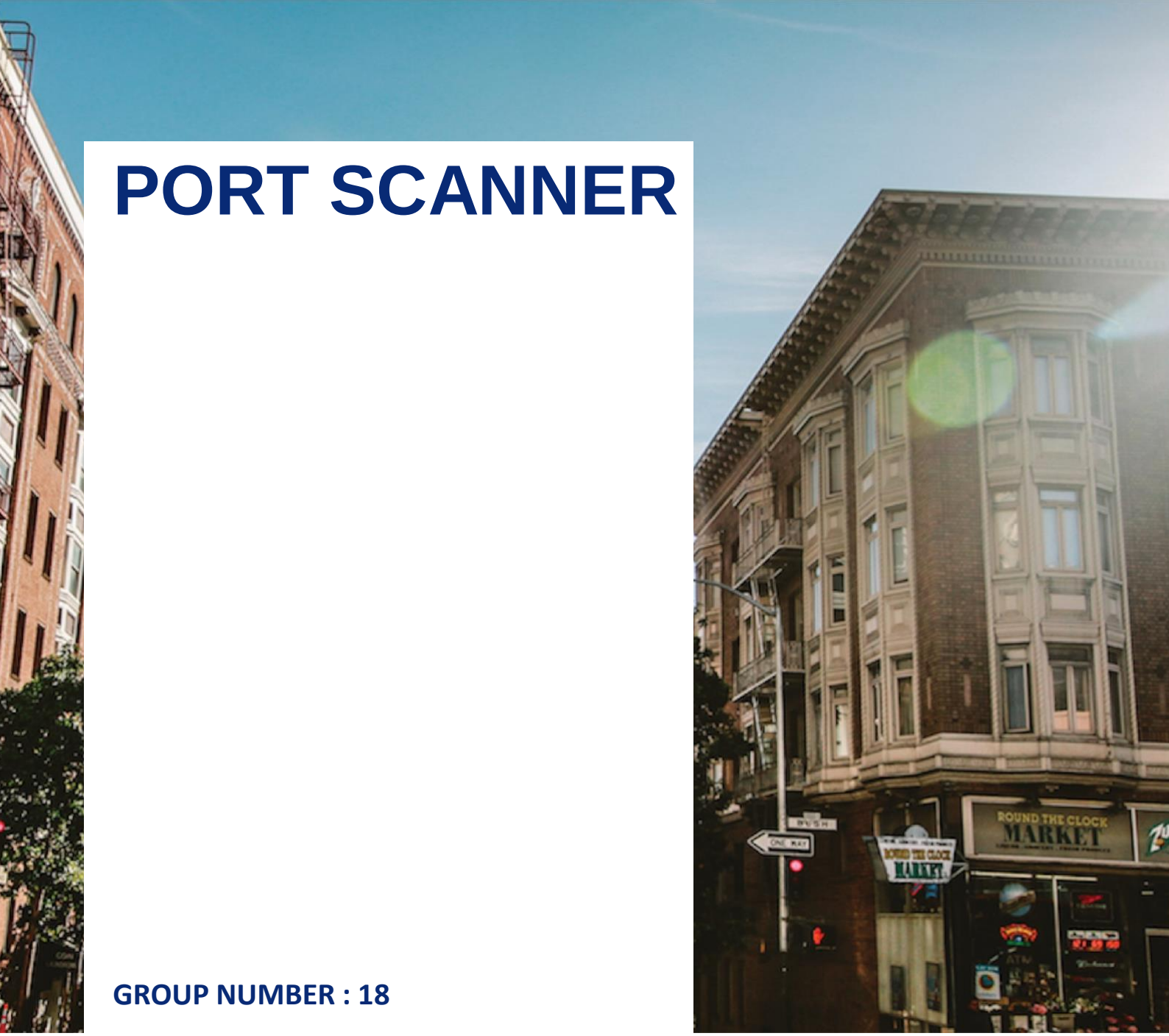
PORT SCANNER



GROUP NUMBER : 18

COMPUTER NETWORKS ASSIGNMENT

Authored by: ARSHIYA KHAN(16116010)

BALRAM CHOUDHARY(16116015)

SHREY AGGARWAL(16116064)

SAURABH UDAI(16114061)

ABSTRACT

The main aim of this project is to implement a legitimate technique of extract the information about what goes in and what goes out of various interconnected computers i.e., Port Scanning.

First, we are checking whether the port is reachable or not and then we are checking whether it is in use or not. We have used java language for the same.

OBJECTIVE

Port scan is an act of systematically scanning a computer's ports. As ports on a computer are the place where information is sent and received, port scanning is analogous to knocking on doors to see if someone is home. Port scanning has legitimate uses in managing networks, but port scanning also can be malicious in nature if someone is looking for a weakened access point to break into your computer. System and network administrators use port scans to identify open ports to a system so that they may be able to limit access to those ports, or shut them off entirely. Port scans represent a sizable portion of today’s Internet traffic. The aim of this project is to analyze sample network traces to discover and classify properties of port scans. It helps to generate better network intrusion detection systems and increase general network security. It can also be used for revealing the presence of security devices such as

firewalls that are present between the sender and the target. This technique is known as fingerprinting.

The vertical scan is a port scan that targets several destination ports on a single host. Single detection mechanisms are required in this scan. On the other hand a horizontal scan is a port scan that targets the same port on several hosts. Most often the attackers are aware of a particular vulnerability and wishes to find susceptible machines.

We are going to implement block scans, a combination of vertical and horizontal scanning styles over some well known ports which are:

Port 20: FTP | Data port
Port 21: FTP | Control (Command) port
Port 22: SSH| Secure logins and file transfer
Port 23: Telnet | Unencrypted text communications
Port 25: SMTP | Used for e-mail routing between mail servers
Port 80: HTTP | Hypertext Transfer Protocol
Port 135: TCP | Microsoft Remote Procedure Call (RPC) service.
Port 139: TCP | NetBIOS
Port 445: UDP | Microsoft-DS (Active Directory, Windows shares)

PROCEDURE

First, we are using testing the reachability of a host on a IP network. For this we are using ping. It finds out the time taken for round trip for the messages send to a destination computer from the originating host which are echoed back to the source.

If it is reachable, then port scanning starts.

The simplest port scan sends a carefully constructed packet with a chosen 32 bit destination IP address to each of the ports from 0 to 65535 to find out the ports that user is using. But as we are implementing block scan we will run this process for a number of users which are interconnected through a local area network (LAN). We have used SYN scan technique to detect whether an IP is using a port or not.

SYN scan:

This technique is also called half-open scanning, because a TCP connection is not completed. A SYN packet is sent (as if we are going to open a connection), and the target host responds with a SYN+ACK, this indicates the port is listening, and an RST indicates a non- listener. The server process is never informed by the TCP layer because the connection did not complete.

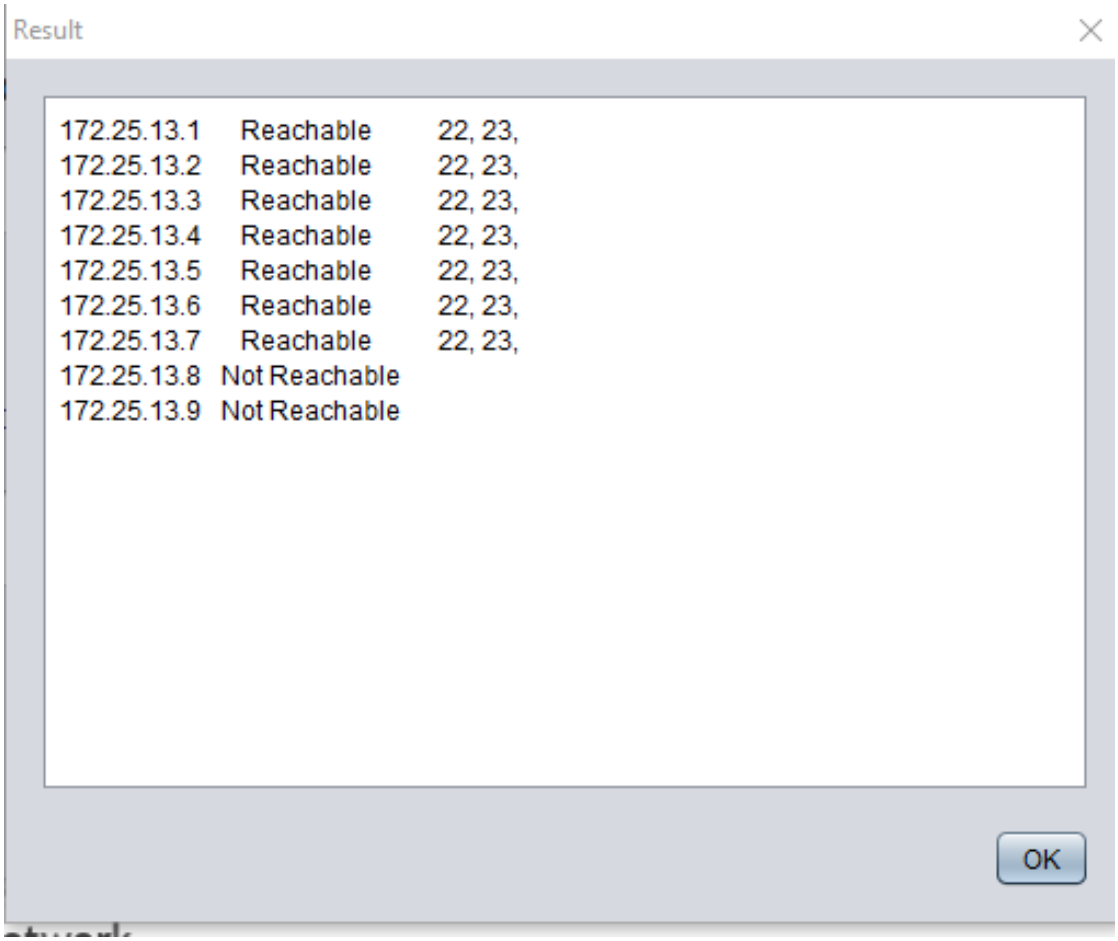
This process is repeated for all the IP addresses in the network range.

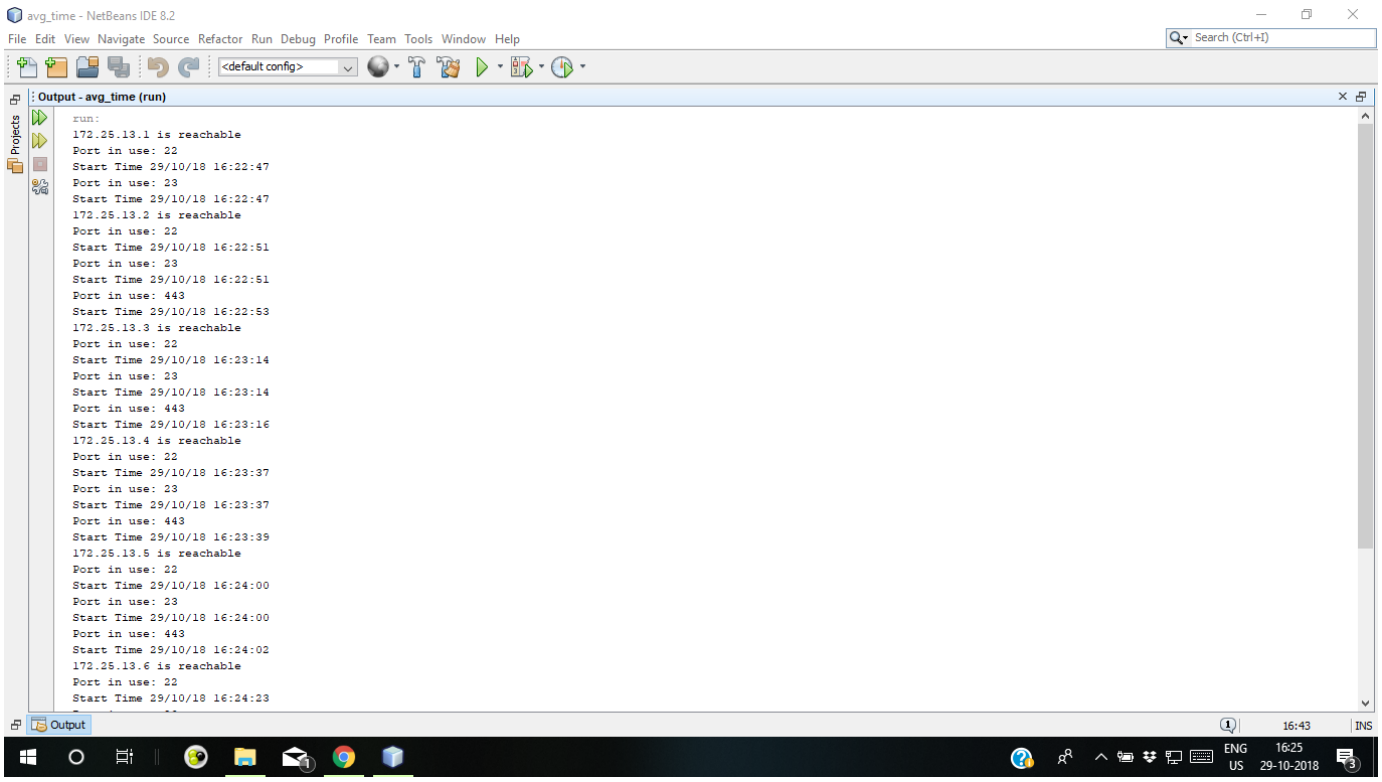
While checking the ports, we have stored the time at which the user starts and stops using that port in a text file. This is done by using the “Date” class.

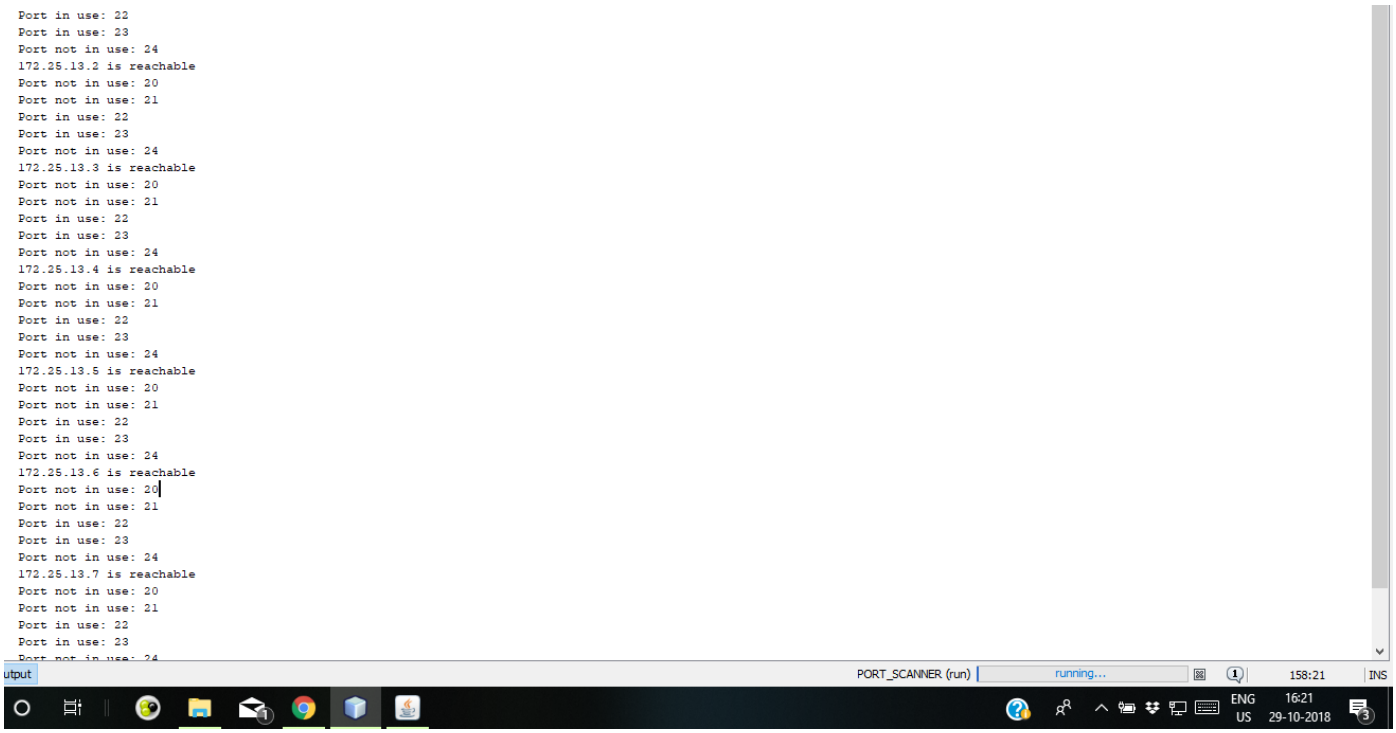
MAC Address Detection:

We have created a jar file from java file which runs the mac_finder.bat(batch file) in the command prompt. We are using arp command for the same.ARP stands for Address Resolution Protocol. This command is used to convert IP address to MAC address. This batch file gets the list of MAC addresses of the active devices present in the network. This list is saved in a file.

RESULTS


Result
172.25.13.1 Reachable 22, 23,
172.25.13.2 Reachable 22, 23,
172.25.13.3 Reachable 22, 23,
172.25.13.4 Reachable 22, 23,
172.25.13.5 Reachable 22, 23,
172.25.13.6 Reachable 22, 23,
172.25.13.7 Reachable 22, 23,
172.25.13.8 Not Reachable
172.25.13.9 Not Reachable
OK


avg_time - NetBeans IDE 8.2
File Edit View Navigate Source Refactor Run Debug Profile Team Tools Window Help
Search (Ctrl+I)
<default config>
Output - avg_time (run)
Projects
run:
172.25.13.1 is reachable
Port in use: 22
Start Time 29/10/18 16:22:47
Port in use: 23
Start Time 29/10/18 16:22:47
172.25.13.2 is reachable
Port in use: 22
Start Time 29/10/18 16:22:51
Port in use: 23
Start Time 29/10/18 16:22:51
Port in use: 443
Start Time 29/10/18 16:22:53
172.25.13.3 is reachable
Port in use: 22
Start Time 29/10/18 16:23:14
Port in use: 23
Start Time 29/10/18 16:23:14
Port in use: 443
Start Time 29/10/18 16:23:16
172.25.13.4 is reachable
Port in use: 22
Start Time 29/10/18 16:23:37
Port in use: 23
Start Time 29/10/18 16:23:37
Port in use: 443
Start Time 29/10/18 16:23:39
172.25.13.5 is reachable
Port in use: 22
Start Time 29/10/18 16:24:00
Port in use: 23
Start Time 29/10/18 16:24:00
Port in use: 443
Start Time 29/10/18 16:24:02
172.25.13.6 is reachable
Port in use: 22
Start Time 29/10/18 16:24:23
Output
16:43
INS
ENG
US
16:25
29-10-2018


Port in use: 22
Port in use: 23
Port not in use: 24
172.25.13.2 is reachable
Port not in use: 20
Port not in use: 21
Port in use: 22
Port in use: 23
Port not in use: 24
172.25.13.3 is reachable
Port not in use: 20
Port not in use: 21
Port in use: 22
Port in use: 23
Port not in use: 24
172.25.13.4 is reachable
Port not in use: 20
Port not in use: 21
Port in use: 22
Port in use: 23
Port not in use: 24
172.25.13.5 is reachable
Port not in use: 20
Port not in use: 21
Port in use: 22
Port in use: 23
Port not in use: 24
172.25.13.6 is reachable
Port not in use: 20
Port not in use: 21
Port in use: 22
Port in use: 23
Port not in use: 24
172.25.13.7 is reachable
Port not in use: 20
Port not in use: 21
Port in use: 22
Port in use: 23
PORT_SCANNER (run)
running...
158:21
INS
ENG
US
16:21
29-10-2018