**“XKEYSCORE”**

**A Minor Project**

**Submitted in partial fulfillment of the requirement for the award of Degree of Bachelor of Engineering in Computer Science and Engineering**

**Submitted to**



**RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL (M.P.)**

**Submitted by:**

* **SAURAV PAUL (0192CS141083)**
* **VIKASH KUMAR (0192CS141104)**
* **DINESH KUMAR DAS(0192CS141032)**

**Under The Supervision Of:**

**Prof. Balwant Singh Raghuvanshi.**

**Description: C:\Users\anirudh\Desktop\Untitled456.png**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**TECHNOCRATS INSITUTE OF TECHNOLOGY AND SCIENCE**

**BHOPAL**

**SESSION: 2016– 2017**

**TECHNOCRATS INSITUTE OF TECHNOLGY AND SCIENCE, BHOPAL**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**Description: C:\Users\anirudh\Desktop\Untitled456.png**

**CERTIFICATE**

This is to certify that the work embodies in this Minor Project entitled **“XKEYSCORE”** being submitted by **Saurav Paul, Vikash kumar and Dinesh kumar Das** in partial fulfillment of the requirement for the award of degree of **Bachelor of Engineering in Computer Science and Engineering** to **Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal** during the academic year 2016-17 is a record of bonafide piece of work, carried out by him under my supervision and guidance in the **Department of Computer Science and Engineering, Technocrats Institute of Technology and Science, Bhopal**.

**SUPERVISED / APPROVED BY**

**Supervisor Name**

**Prof. Balwant Singh Raghuvanshi**

**(Dept. of CSE)**

**FORWARDED BY**

**Dr. Neetesh Kumar Gupta**

**Associate Professor & Head**

**(Dept of CSE)**

**ACKNOWLEDGEMENT**

With due respect, we express our deep sense of gratitude to our respected guide **Prof. Balwant Singh Raghuvanshi**, Department of Computer Science and Engineering, TIT & Science , Bhopal, for the valuable help and guidance. We are thankful to the people who encouraged us through it all completing this project. We are also grateful to Dr. Neetesh Kumar Gupta , Head of Department, Computer Science and Engg, TIT & Science , Bhopal and to our respected **Sashi Jain**, Director, TIT & Science, Bhopal for providing us with all the necessary facilities. We are also thankful to all the other staff members of our department for their kind co-operations and suggestions for the improvements in the project. We would like to express our deep appreciation to our classmates for providing us with much needed suggestions and cordial atmosphere. Last, but not the least, we would like to thank our family members and mostly God, for their support and encouragement without which this project would not have been completed.

Saurav Paul (0192CS141083)

Vikash Kumar (0192CS141104)

Dinesh Kumar Das (0192CS141032)

**CONTENTS**

* Introduction-
* Objectives of the project.
* Scope of the project.
* Requirement Specifications-

* Hardware Requirements.
* Software Requirements.
* Components-

* System Design.
* Technology used.
* Test Documentation-
* System Testing and Screenshots.
* Conclusions-

* Summary.
* Glossary.
* References.

**OBJECTIVES**

* It finds out the IP address of the user computer along with open ports.
* It also finds out the IP address of a target machine, whether it is a Website or a system.
* It lets us chat through Linux Terminals or Windows Command Prompt and save the messages into a File.
* It also lets us transfer any file through Linux Terminals or Windows Command Prompt.
* It allows us create a Backdoor to take control over a compromised system.
* It allows execution of any files on any compromised systems remotely.

**SCOPE**

The software, in the near future, can be efficient as it comes with embedded features such as chatting through terminals, file transfer and also Backdoor can be created. It automatically finds the IP address of the compromised system along with the open port nos.

* Future Scope –
* An advanced hacking tool.
* Unethical tool to shutdown any website on earth.
* A tool to gain access over many machines.
* A chat application to chat via terminal.
* A program to share data over a network.
* A tool to find any IP address on earth anonymously.

**INTRODUCTION**

The Hacking world is getting much interesting in this Cyber era. Whether to hack into someone’s system, or to get access into an Organization’s website remotely, or whatever, the art of getting the unauthorized entries into any system is new trends.

Not just hacking anonymously, the cyber world is more of sharing information and data, including their security. Providing security to the data is the major problem in communication these days. Not only security, data been sent should be accurate and in time. Hence the software provides necessary facilities to send data and information or messages through command line interface using only IP address. The system acts as server and thus can take control over many compromised systems.

IP address has been the widely used information to gain access to many systems. Not only just IP address is to be known, but also the open port nos. to listen to any feedback or to get into any system remotely. This project is based on all these stuffs. It can let us chat through terminals, transfer files, hack into the systems, and etc. And hence this project comes with all these embedded features and user friendly usability.

**REQUIREMENT SPECIFICATIONS**

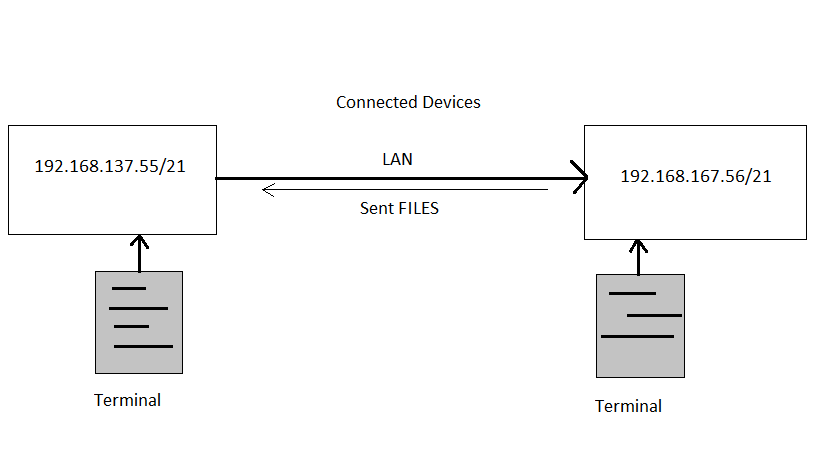
* Hardware Requirements:-
* Intel Core I3/I5 processor.
* RAM - 3GB.
* Hard Disk - 500GB.
* Software Requirements:-
* Operating System - Linux.
* Codeblocks.
* Gedit.
* Terminal.
* cmd.exe.
* Notepad.

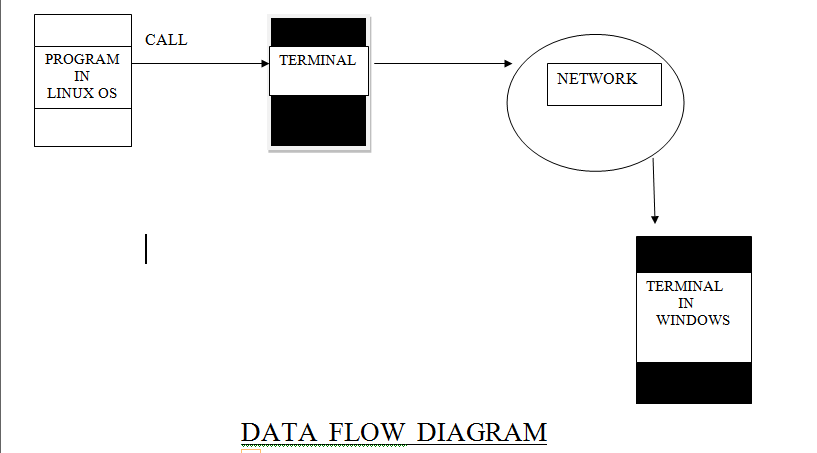
**SYSTEM DESIGN**

The basic programming languages, i.e. C, C++, Bash Scripting, etc. have being used in order to code the main source code, using the software Codeblocks. The inputs and some outputs are stored in files, i.e. Batch files, and are being invoked by system calls.

The IP addresses and the open port nos. are found out using netcat and nmap commands. Chatting and file transfer can be done using these commands in the terminal, so as to create a backdoor.

The commands call the other systems and get the responds in return, hence connections are made.





* In the data flow diagram, the terminal invokes the batch files which executes the commands. Then the packets are sent to the target and connection is made. Once connected, we can take control over the compromised system and play our tasks.

Data Flow :-

User 🡪 Program 🡪 Terminal 🡪 Network 🡪 Target

* Header Files 🡪
* #include<iostream>
* #include<stdlib.h>
* #include<stdio.h>
* #include<unistd.h>
* #include<string.h>
* Functions 🡪
* void show\_ip();
* void nslookup();
* int port();
* void chat (char\*);
* void transfer(char\*);
* void backdoor(char\*);

**TECHNOLOGY USED**

* Languages Used –
* C 🡪

A programming language developed by Dennis Ritchie in 1972 at T&T Bell Labs.

* C++ 🡪

C++ was developed by Bjarne Strousstrup at Bells Labs .

* Bash Scripting 🡪

A **Bash** shell **script** is a computer program written in the **Bash**programming language. Shell **scripting** is the art of creating and maintaining such**scripts**. Shell **scripts** can be called from the interactive command-line described above; or, they can be called from other parts of the system.

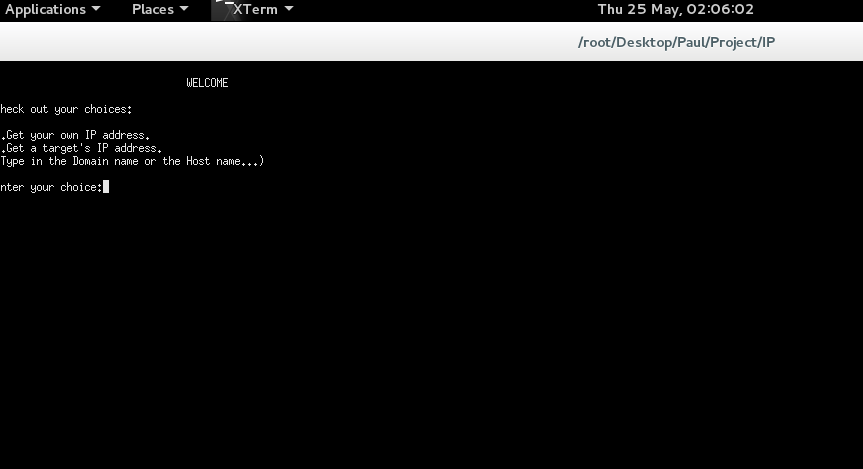
* Implementation Requirements –
* Codeblocks.
* NetCat.
* Nmap.
* Nslookup.
* LAN.
* Bash Shell.
* Connected Systems.

**TEST DOCUMENTATIONS**

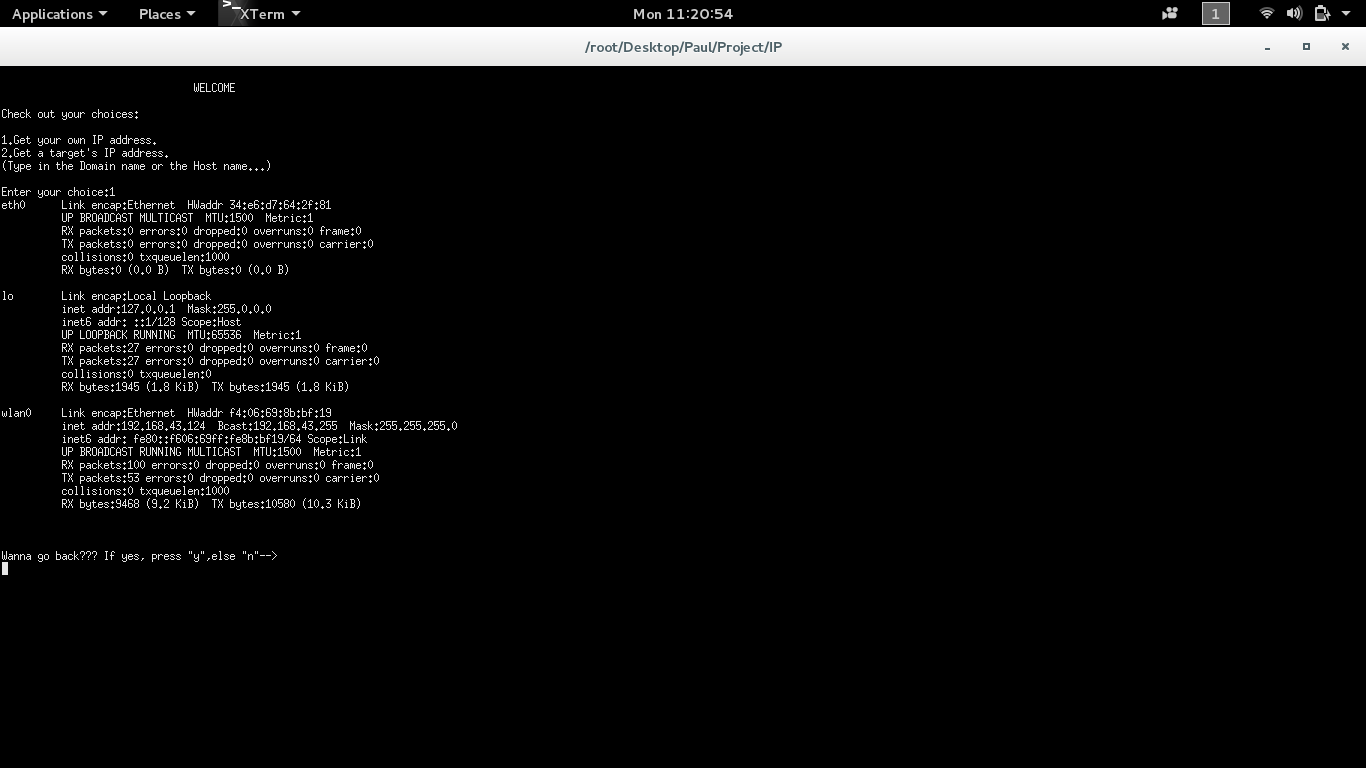
* System Testing –

The Software has been tested on Linux Platform and can be connected to any system (Linux or Windows). It acts as a server, hence the server should be only on Linux machine but the compromised machine (client) can be of both Linux and Windows.

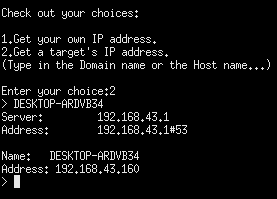
* Output Screenshots –
* Start screen



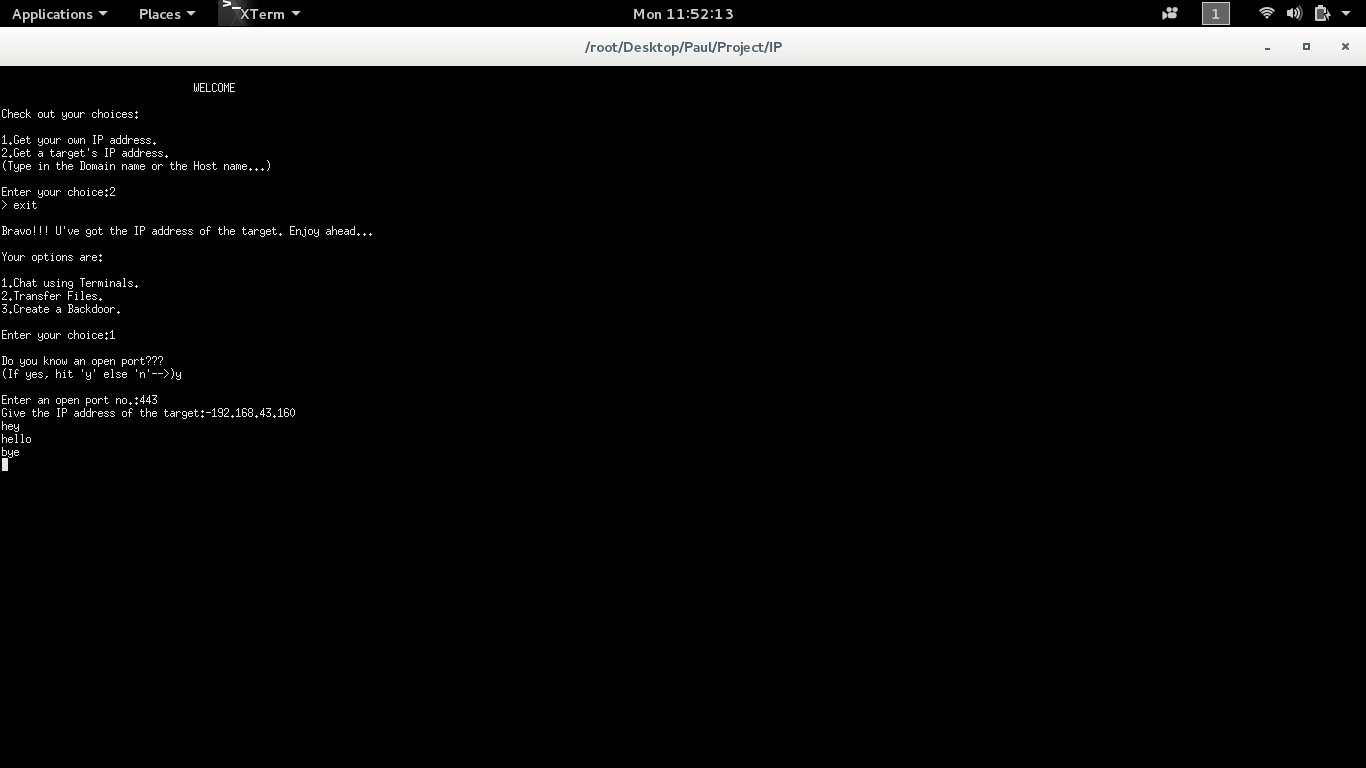
* Finds the IP address of the user system and also the targeted system.

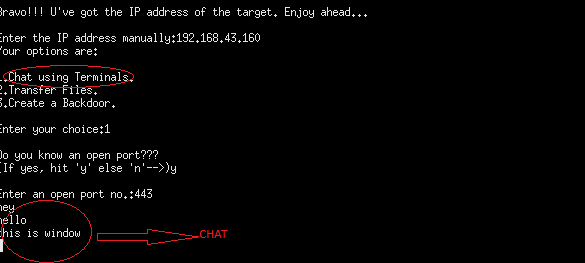


* Finds the IP address of another System.

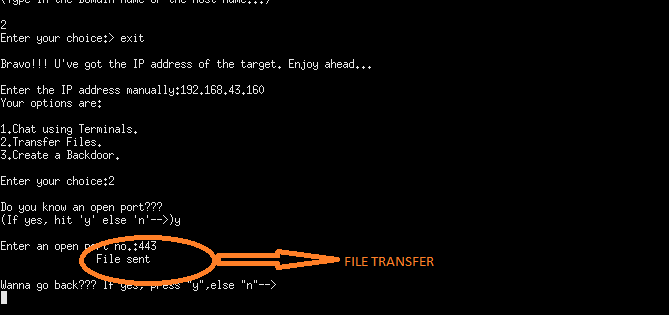


* Chatting and sending of files can be done through this project.

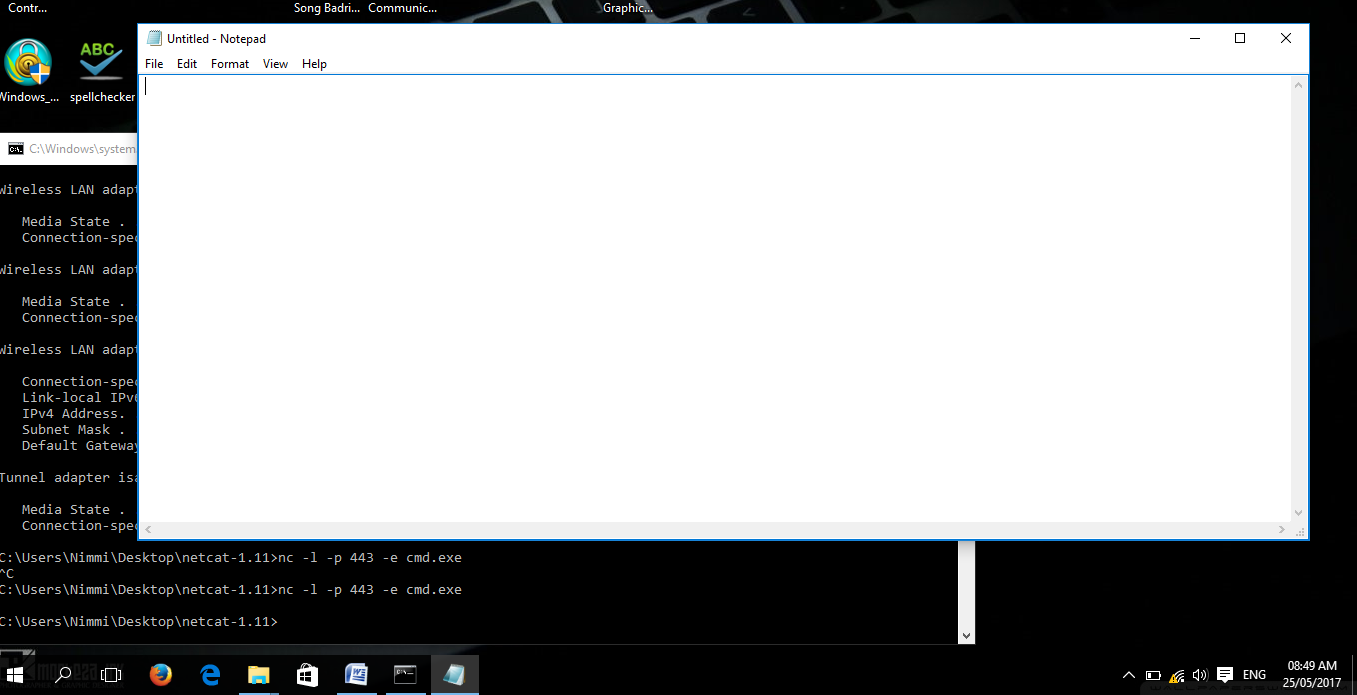




* It can be used to send Files over a network.



* It also can create backdoor on other systems.



* Backdoor created in windows 10( Notepad opened )

**CONCLUSION**

* Summary –

To conclude, this project has been accomplished keeping in mind the features of the software and its advantage and security.

Since this project is embedded with extra features like chatting, transferring files, etc., it thus can be used in near future taking the advantages of the project. This is a shortcut way to find IP addresses and accomplish the stuffs that can be carried out using the IP addresses. Thus this software is an efficient hacking tool to be used all over the world.

* Glossary –
* IP addresss –

An IP address (abbreviation of Internet Protocol address) is an identifier assigned to each computer and other device (e.g., printer, router, mobile device, etc.) connected to a TCP/IP network that is used to locate and identify the node in communications with other nodes on the network. IP addresses are usually written and displayed in human-readable notations, such as 172.16.254.1 in IPv4, and 2001:db8:0:1234:0:567:8:1 in IPv6.

* Port no. –

A port number is a way to identify a specific process to which an Internet or other network message is to be forwarded when it arrives at a server. For the Transmission Control Protocol and the User Datagram Protocol, a port number is a 16-bit integer that is put in the header appended to a message unit. This port number is passed logically between client and server transport layers and physically between the transport layer and the Internet Protocol layer and forwarded on.

* Nmap –

Nmap ("Network Mapper") is a free and open source (license) utility for network discovery 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.

* Netcat –

Netcat (often abbreviated to nc) is a computer networking utility for reading from and writing to network connections using TCP or UDP. Netcat is designed to be a dependable back-end that can be used directly or easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and investigation tool , since it can produce almost any kind of connection its user could need and has a number of built-in capabilities.

* Nslookup -

Nslookup is a network administration command- line tool available for many computer operating systems for querying the Domain Name System(DNS) to obtain domain name or IP address mapping or for any other specific DNS record.

* Bash –

Bash is Unix shell and command language .It is a default login shell for Linux distributions and Apple’s mac os.

**REFERENCES**

* [www.google.com](http://www.google.com)
* [www.wikipedia.com](http://www.wikipedia.com)
* [www.searchnetworking.techtarget.com](http://www.searchnetworking.techtarget.com)
* [www.nmap.org](http://www.nmap.org)
* [www.youtube.com](http://www.youtube.com)
* The Basic Of Hacking and Penetration
* The C programming Language