IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 13, May 2023

Backdoor Entry to a Windows Computer

B. Kavya Reddy[1], B. Sai Nikhil[2], V. Vamshi Krishna[3], Dr. Preethi Jeevan[4]
Students, Department of Computer Science and Engineering[1,2,3]
Associate Professor, Department of Computer Science and Engineering[4]
Sreenidhi Institute of Science and Technology, Telangana, India

Abstract: *There are two access points on every machine that can be utilised for remote access. The secondary access point is also referred to as a backdoor access point, while the first requires user credentials to connect. Users can log in without going through security checks. Installed on the target computer, the backdoor is a straightforward programme that may be used to obtain a reverse shell if necessary. Making a backdoor into a computer can be done in a number of ways. An intelligent attacker can simply build a unique backdoor. The Windows security system can quickly identify the majority of these customised backdoors as malicious files. We have created a sophisticated backdoor that functions like a regular file but is actually a backdoor in order to address this issue.*

Keywords: Privileges, Access, Intruder, Remote Code Execution, Susceptability

I. INTRODUCTION

Anyone (hackers, governments, computer scientists, etc.) can use a backdoor. - Allow unauthorised remote access to your device without your knowledge or consent. By deploying malware, abusing flaws in your software, or even by inserting backdoors directly into your device's hardware or firmware, hackers can add backdoors to your system. After breaking into your computer without your knowledge, a hacker may utilise a backdoor for a number of purposes, including:

- Surveillance
- Data theft
- Cryptojacking
- Sabotage
- Malware attack.

Backdoor hackers always develop new techniques and malicious files to access people, so nobody is safe from them.

II. HOW DOES A BACKDOOR WORKS?

Every computer system has a recognised way for users to access it. This frequently involves a system of authentication that asks users for a password or other form of identification before granting access. If a user successfully authenticates, they are granted access to the system, but their access is restricted to the permissions associated with their account. This login technique may offer security, System administrators may require remote access to systems that do not permit it.

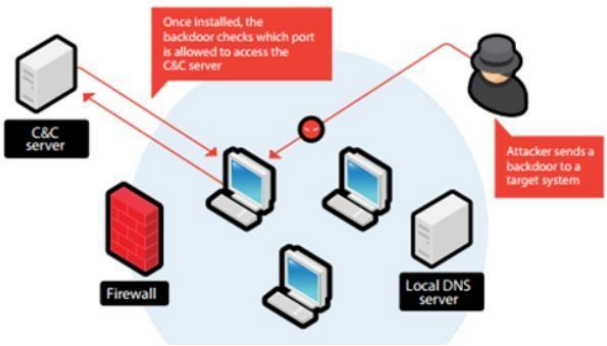

Fig-1: System Architecture

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 13, May 2023

Even if he lacks the appropriate credentials, an attacker can still wish to access a company's database server. To make installation, testing, and deploying system upgrades easier, system builders can include a default account. A system administrator might set up a web shell on a server, for instance. When users need to access a server, they go to the relevant website, where they may send instructions directly to the server without having to authenticate or set up the company's security procedures to support SSH.

III. TYPES OF BACKDOOR

There are several types of backdoors. Among the more typical types are:

- **Trojans**: The majority of backdoor software is built to go past an organization's defences, giving attackers access to corporates.
- **Built-in backdoors**: Backdoors may be incorporated into devices by manufacturers as undocumented remote access methods, default accounts, and other features. Although the manufacturer is typically the only one with access to these systems, they are typically built in such a way that they cannot be turned off and there is no backdoor to keep them a secret indefinitely, making these security gaps accessible to attackers.
- **Supply Chain Exploits:** Third-party libraries and code are frequently used in web applications and other types of software. In order to gain backdoor access to the computer executing the programme, an attacker could insert backdoor code into a library in the hopes that it will be utilised in a business application.

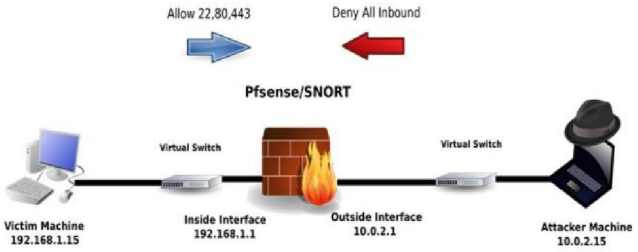

Fig-2

VI. SCOPE AND OVERVIEW

The project intends to produce finished apps that may be applied in a business setting. A non-technical person should be able to configure the programme, thus it should be as straightforward as feasible. In this project, we programme in Python and develop the application using the Socket, OS, and subprocess modules. It's simple to comprehend.

A backdoor is any method through which a system can be accessed by anyone by evading standard security precautions. Backdoors are frequently incorporated into the coding of some pieces of software, allowing engineers and developers to get beyond their own safeguards and fix user issues. Cybercriminals use these access points in backdoor attacks to obtain unauthorised access to data and systems. Because hackers can often access networks without being detected, these incidents frequently go unreported—at least at first. Criminals have the ability to monitor user activities, implant malware, and steal data once they have remote access to a network or device.

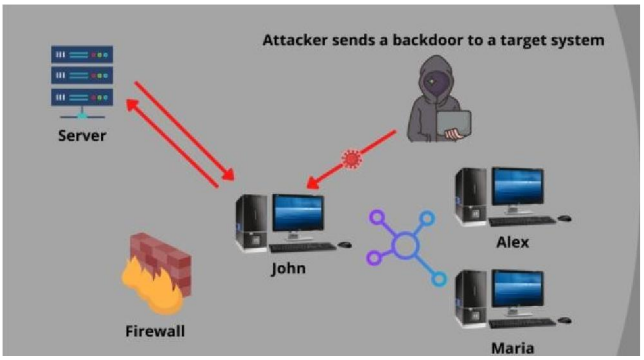

Figure 3

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 13, May 2023

V. PROPOSED SYSTEM

To solve the holes in the current system, we have used modules like os, subprocess, socket, etc. in the suggested system. The contents of the file can now be changed under the proposed system, and the user/hacker information is also made public. It is challenging to identify the hacker. The suggested system now supports network commands like ipconfig and netsh.

VI. EXISTING SYSTEM

Backdoor access is nothing more than having access to the target system and being able to run any command through the user command prompt. However, in the current system, we are unable to access network commands like ipconfig, netsh, etc., and we can only view/read certain files' contents through the backdoor, not modify them. Systems currently in use do not fully satisfy administrator and hacker needs.

REVERSE TCP CONNECTION

TCP reverse connection The primary language used on the Internet is TCP/IP, or Transmission Control Protocol/Internet Protocol. TCP/IP is used on the Internet to enable computer-to-computer communication by putting together packets of data and transmitting them to the right place. To prevent inbound connections, a simple firewall is utilised. In reverse_tcp, the attacker coerces the target into creating a connection with them. This is the reverse_tcp's fundamental concept.

TCP

TCP/IP has two layers; the first layer, TCP, is in charge of collecting the large amounts of data into network packets and transmitting them. The second layer, TCP, is in charge of receiving the packets and decoding them into useable bits of information

IP

The network packets are put together, and IP, or Internet Protocol, directs them to where they are supposed to go. Like GPS for packets, the IP layer is.

THIS ATTACK USES 2 BASIC CONCEPTS

- BINDSHELL: In this shell, the victim machine's communication port or listener is opened by the target machine, which then watches for incoming connections. After establishing a connection, the attacker issues the commands to the listener on the victim machine.
- REVERSE SHELL: This is a shell in which the target machine initiates a connection to the attacking machine. The attacking machine has a listening port that accepts connections, the use of which can lead to the execution of code or command.

VII. REQUIREMENTS

7.1 Functional Requirements

Windows systems must be capable of transmitting CONNECT signals to connect to distant computers through the Internet. Linux systems need to be able to recognise CONNECT signals from distant machines and create safe connections.

7.2 Performance Requirements:

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

7.3 Software Requirements

- Windows7
- Python3
- LinuxOS

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 13, May 2023

- Netcattool

7.4 Hardware Requirements

- 2 computers with i5 processors
- 8gb RAM
- 10GB freespace

VIII. FEASIBILITY STUDY

8.1 Operational Feasibility

The benefit of the suggested system is that it may be transformed into an information system that can analyse flows to satisfy the operational requirements of the organisation. The file is delivered to the destination securely, and the server receives a confirmation. There is no traffic while sending large amounts of data

8.2 Technical Feasibility

Technical viability focuses on the amount to which the proposed addition can be supported by the current computer systems (hardware, software, etc.). For instance, if the computer is now operating at 80% of its potential. This will accelerate the process by requiring more hardware (RAM and six more CPUs). On the software end, PYTHON, an open-source language, is utilised. The Linux operating system is an additional option. The system is more practical on these standards because the technical prerequisite for this project is the Python Socket module. Software and standard hardware settings are sufficient.

8.3 Economic Feasibility

The most popular technique for determining whether a system is effective is to consider its economic viability. The method, which is frequently referred to as a cost/benefit analysis, entails figuring out the candidate's anticipated savings and advantages and contrasting them with the costs. if the advantages outweigh the drawbacks. Afterward, decide to develop and put the system in place. Otherwise, shut down the programme. The system's implementation makes it practical for traffic analysis. Therefore, no additional tools or materials are needed for its implementation. Its use is therefore commercially viable.

IX. MODULES AND SYSTEM DESIGN

.

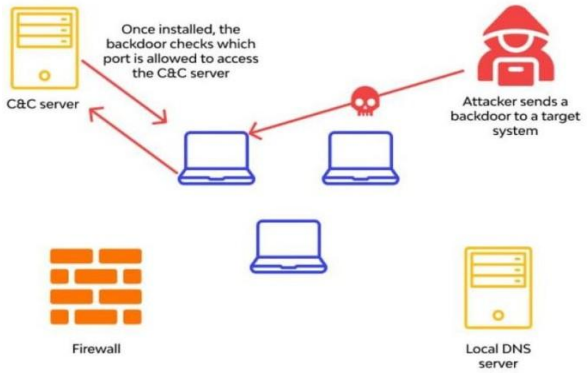

Fig-4

Socket Module

Using socket programming, two nodes on a network can connect and communicate with one another. While one socket makes connections with other sockets, another socket listens on a particular IP port. A listening socket is created by the server when a client connects to it.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 13, May 2023

They really form the basis of web browsing. There is a server and a client, to put it simply. Importing the socket library is the first step in socket programming

Sockets=socket.socket(socket.AF_INET,socket.SOCK_STREA M)

Here, two parameters are passed to a socket instance that is created. AF_INET is the first parameter, while SOCK_STREAM is the second. The ipv4 address family is referred to as AF_INET. A TCP protocol with a connection-oriented identifier is SOCK_STREAM. Now, we may connect to the server using this socket.

Threading

The "thread" module, which should be utilised, offers basic functionality and a higher-level interface into the threading module. Importing Thread is the first thing you must accomplish by typing: import Thread from threading As previously indicated, the threading module includes a Thread class to implement threads and a preset method for multithreaded programming. As follows:

run():as thread input
start():used to start a thread by calling run()
isAlive():used to check if there is output
getName():used for return a thread name
setName():used to set the thread name OS MODULE:

The Python OS module streamlines user-operating system communication during system development. It offers a variety of practical operating system features that can be used to carry out operations that are operating system-specific and gather pertinent data about the operating system. The standard utility modules for Python include an operating system. This module offers a portable way to use functions that depend on the operating system.The name of the OS system module it imports is given by the os.name () function.

os.mkdir()–used to create a new directory
os.getcwd()–returns the current working directory
os.chdir()-changes the current working directory
os.rmdir()-removes the specified directory an absolute or relative path
os.popen()-opens a file or specified from the command it returns an object of return file connected to the pipe.
os.close()-closes the file associated with the description.

Sub Process Module:

By establishing new processes, the subprocess module included in Python (2.x and 3.x) is used to run new applications or programmes through Python code. Obtaining exit codes and entry/exit/error channels from various commands is also helpful. In Python, you must use the Popen function to begin a new process, or to put it another way, a new sub-process. call. It is possible to pass two parameters when calling a function. The programme you want to launch comes first, followed by the file parameter. You will use the Unix cat command in the example below with example.py as two arguments. In Linux and Unix programming, the word "concatenate" is abbreviated to "cat" by the cat command. similar to "cat example.py" Unless you didn't make the programme, you can start any programme.

X. ALGORITHMS USED

Reverse TCP Attack:

We refer to a connection that a host starts as a forwarded connection. Otherwise, however, a connection is started between the server and host by the server, known as a reverse connection (rare). Every incoming connection is blocked by a firewall. The firewall subsequently blocks all incoming connections (also known as reverse connections). A host-initiated forward connection is permitted, and a host-initiated return connection is permitted if the host initiates the connection.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 13, May 2023

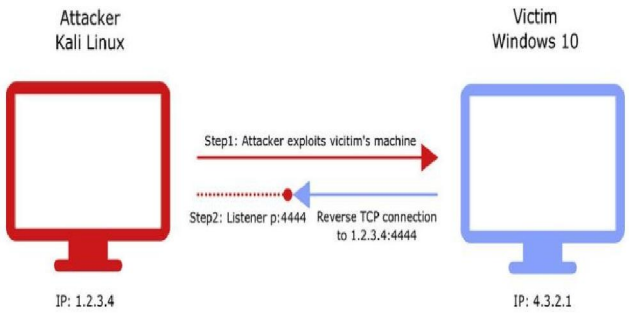

Fig-5: Reverse TCP

In essence, a firewall would enable a connection to the attacker even though it was initiated by a device rather than the attacker, who would naturally be prohibited by the firewall. after which the attacker seizes control of the machine and starts working. This kind of shell is backward.

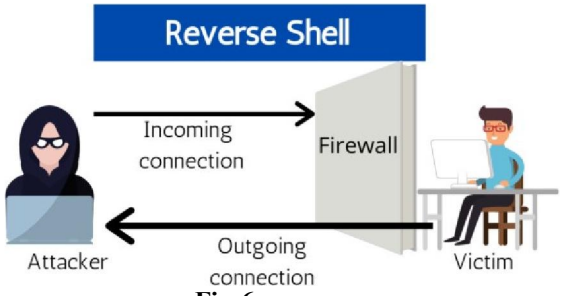

Fig-6

For this project to be set up, two Windows workstations and a Linux machine are required. The python file will be run in the background after creating a new one with the above script in it and saving it with the.pyw extension. As of right now, the system is delivering connection packets via the aforementioned port number to the aforementioned IP address. Run the following command on the Linux computer right now.

nc-nlvp4444

This command utilises the netcat programme to monitor port 4444 for any connections. The Linux machine will quickly accept a connection request from either system and connect the two devices together. The Linux machine with user rights displays the Windows system command prompt when the reverse TCP connection is created successfully.

XI. CONCLUSION

Backdoors' technical benefit is their capacity to keep an eye on distant systems. Most likely, software companies will use it to monitor employee computers and increase output. With the use of this backdoor software, parental supervision is also possible. Windows systems protected by firewalls are very vulnerable to backdoors that can be readily exploited to get remote access since firewalls cannot identify backdoors as malware. This backdoor can be used in both good and bad ways. One undesirable application of a backdoor is to connect to a machine to which we do not have access. The backdoors we built are exclusively intended for educational use; they cannot be put to any illicit use.

REFERENCES

[1] K. B, BSD Rlogin, SRI International, Menlo Park, CA,: Network Information Center, 1991.
[2] Mansfield R.,"Hacker Attack", Published Sybex Inc, USA, 2000.