Backdoor Entry to Windows Computer

By: 19311A0521
19311A0522
19311A0535

Team: A6
Guide: Dr.Preethi Jeevan

Contents

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 executable file that is installed on the target computer to gain a reverse shell whenever necessary. 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.

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 or 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.

Every computer system has an official means by which users are supposed to access it.

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.

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.

Types of Backdoor:

1.Trojans

2.Built-in Backdoors

3.Supply Chain Exploits

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.

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.

Requirements

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

SOFTWARE REQUIREMENTS

Windows7+, Python 3 and above

Linux OS

Netcat tool

HARDWARE REQUIREMENTS

2 computers with i5 processors

8gb RAM

10 GB free space

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.

References

•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


thank you