

## PYRAT

**Rishav Raj<sup>1</sup>, Akshay Bharti<sup>2</sup>, Saurabh Rastogi<sup>3</sup>**

<sup>1,2</sup>U.G Student, Dept. of Computer Science and Engineering, MAIT, Delhi. <sup>3</sup>Associate Professor, Dept.

of Computer Science and Engineering, MAIT, Delhi.

-----\*\*\*-----

### Abstract

Remote command shell enables a privileged user to open a virtual command line interface to the remote computer. The user can then type locally but have the commands executed on the remote computer. You can work from multiple shells. When we checked the other remote Access tools available in the market we found those were complex and confusing so we knew there's still a need for remote access tool that is easy to use and is less complex in order for less technically skilled people to be able to make use of it. Three different python modules were used for this application, ie., 'os'- used for system operations, 'socket'- for network, shutil- File handling. In conclusion we created an application that is platform independent, user friendly, light weight and secure Remote Access tool using Python which we named PYRAT.

### 1. Introduction

Many people today have multiple computer accounts on multiple computers. If you are a smart user, you will choose working remotely on most of them rather than visiting every system on its use. It is always easier to operate everything from a single place.

A RAT or remote administration tool, is software that gives a person full control a tech device, remotely. The RAT gives the user access to your system, just as if they had physical access to your device. With this access, the person can access your files.

pyRAT is a remote tool which can give you access of client system to do various kind of admin task as follows

- Access to the current working directory.
- Access to custom directory.
- Deletion of file from client system.

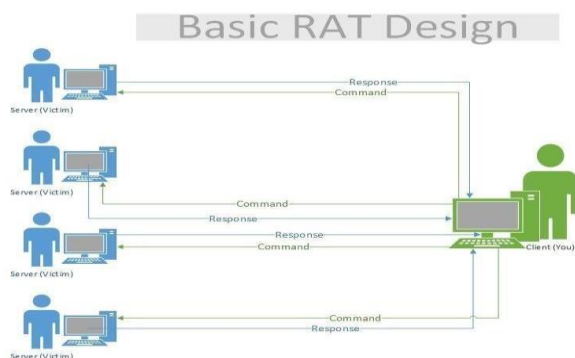
- Downloading of files from client system.

RAT is used to remotely connect and manage single or multiple computers. It provides server with nearly unlimited access to File management along with Screen Capture, shell control and device drivers control.

While multiple utilities like telnet and ssh already exist, **Py RAT** is completely different. "Py RAT " is a standalone program capable of sharing your terminal and all its features with authorization using shell key. In addition to this authentication before terminal and service sharing, the application is completely transparent.

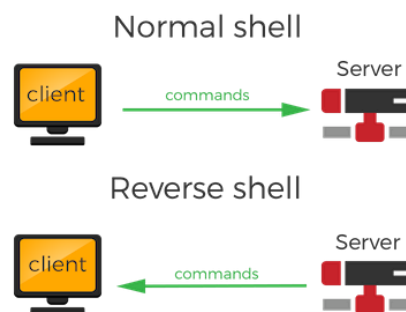
## 2. Methodology

Remote desktop sharing is accomplished through a common client/server model. The client, or VNC viewer, is installed on a local computer and then connects via a network to a server component, which is installed on the remote computer. In a typical VNC session, all keystrokes and mouse clicks are registered as if the client were actually performing tasks on the end-user machine.



## SYSTEM FLOW DIAGRAM

After discussing about the symbol we can easily understand the data flow diagram related to project modules we have system flow diagram of "PyRAT" of each module which we are going to discuss below



**BUILDING REMOTE ACCESS TOOL:** For us to Build a Remote access tool we need the following essentials:

1. A stable internet connection between the client and the host.
2. Installation of our Remote access tool on both the devices.
  - a. This includes the host which gives instructions to the remote desktop.
  - b. And also includes the client which operates wirelessly according to the instructions parsed by the host.

## FUNCTIONALITY

- Admin has access to the current working directory.
- Admin can use custom commands.

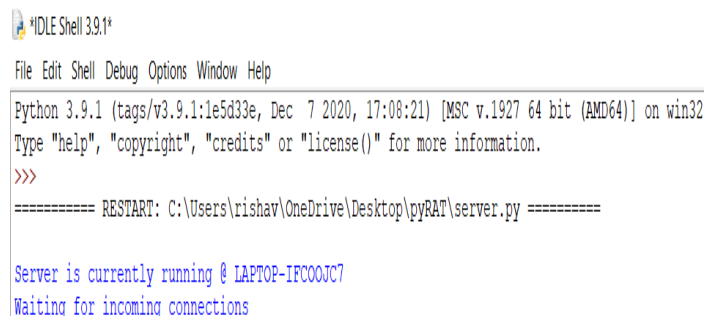
- Admin can view custom directory
- Admin can download files on the client's device.
- Admin can delete files on the client's device.
- Admin can create files on the client's device.

### 3.Implementation

- The connection between the client and server is made through SOCKS5, which makes it very secure and reduces the lag.
- Client.py is run on the client side while server.py is used on the server side application of the program.
- After connection is established, you get greeted with a set of options of commands/request(s) that can be made. These include :
  - View CWD
  - View custom directory
  - Download files
  - Delete files
- All these commands process in real-time and do not require an internet connection because they operate on a LAN-based network system.
- All the previous logs are stored logfile.txt

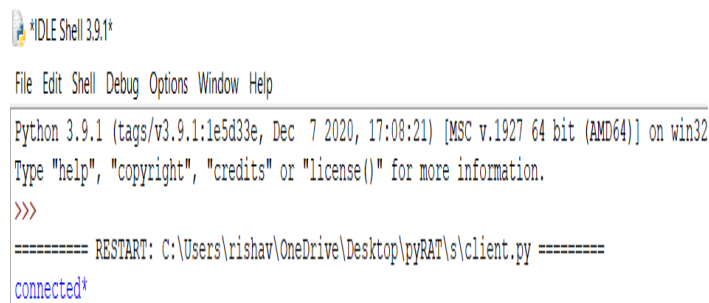
## 4.Result

### FIRST VIEWS OF SERVER SIDE



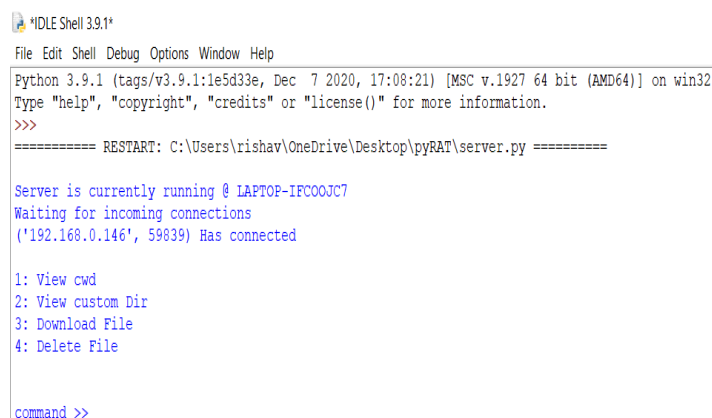
```
File Edit Shell Debug Options Window Help
Python 3.9.1 (tags/v3.9.1:1e5d33e, Dec 7 2020, 17:08:21) [MSC v.1927 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: C:\Users\rishav\OneDrive\Desktop\pyRAT\server.py =====
Server is currently running @ LAPTOP-IFCOOJC7
Waiting for incoming connections
```

### FIRST VIEW OF CLIENT SIDE



```
File Edit Shell Debug Options Window Help
Python 3.9.1 (tags/v3.9.1:1e5d33e, Dec 7 2020, 17:08:21) [MSC v.1927 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: C:\Users\rishav\OneDrive\Desktop\pyRAT\s\client.py =====
connected*
```

### AFTER CONNECTION IS ESTABLISHED



```
File Edit Shell Debug Options Window Help
Python 3.9.1 (tags/v3.9.1:1e5d33e, Dec 7 2020, 17:08:21) [MSC v.1927 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: C:\Users\rishav\OneDrive\Desktop\pyRAT\server.py =====
Server is currently running @ LAPTOP-IFCOOJC7
Waiting for incoming connections
('192.168.0.146', 59839) Has connected

1: View cwd
2: View custom Dir
3: Download File
4: Delete File

command >>
```

## VIEW CWD OPTION

```
*IDLE Shell 3.9.1*
File Edit Shell Debug Options Window Help
Python 3.9.1 (tags/v3.9.1:1e5d33e, Dec 7 2020, 17:08:21) [MSC v.1927 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: C:\Users\rishav\OneDrive\Desktop\pyRAT\server.py =====
Server is currently running @ LAPTOP-IFCO0JC7
Waiting for incoming connections
('192.168.0.146', 59839) Has connected

1: View cwd
2: View custom Dir
3: Download File
4: Delete File

command >> 1
Command output: C:\Users\rishav\OneDrive\Desktop\pyRAT\s
```

## VIEW CUSTOM DIR COMMAND

```
*IDLE Shell 3.9.1*
File Edit Shell Debug Options Window Help
Python 3.9.1 (tags/v3.9.1:1e5d33e, Dec 7 2020, 17:08:21) [MSC v.1927 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: C:\Users\rishav\OneDrive\Desktop\pyRAT\server.py =====
Server is currently running @ LAPTOP-IFCO0JC7
Waiting for incoming connections
('192.168.0.146', 59839) Has connected

1: View cwd
2: View custom Dir
3: Download File
4: Delete File

command >> 2
Custom Dir: F:
Custom dir: [\"D:\\307.D\\\", \"D\\307.D\\\", \"certificates\", \"downloads\", \"experiments\", \"file_list.json\", \"files.docx\", \"for the Registration Form.pdf\", \"intro.docx\", \"multimedia\", \"photo\", \"screenshot\", \"software\", \"system volume information\", \"video\"]

1: View cwd
2: View custom Dir
3: Download File
4: Delete File

command >> 3
```

## DOWNLOAD FILE COMMAND

```
*IDLE Shell 3.9.1*
File Edit Shell Debug Options Window Help
Python 3.9.1 (tags/v3.9.1:1e5d33e, Dec 7 2020, 17:08:21) [MSC v.1927 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: C:\Users\rishav\OneDrive\Desktop\pyRAT\server.py =====
Server is currently running @ LAPTOP-IFCO0JC7
Waiting for incoming connections
('192.168.0.146', 59898) Has connected

1: View cwd
2: View custom Dir
3: Download File
4: Delete File

command >> 3
please enter the files path: F:\intro.docx
please enter name of file with extension: abc.docx
Downloaded and saved
```

## DELETE FILE COMMAND

```
*IDLE Shell 3.9.1*
File Edit Shell Debug Options Window Help
Python 3.9.1 (tags/v3.9.1:1e5d33e, Dec 7 2020, 17:08:21) [MSC v.1927 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: C:\Users\rishav\OneDrive\Desktop\pyRAT\server.py =====
Server is currently running @ LAPTOP-IFCO0JC7
Waiting for incoming connections
('192.168.0.146', 59918) Has connected

1: View cwd
2: View custom Dir
3: Download File
4: Delete File

command >> 4
Enter path and name of file to delete: C:\Users\rishav\OneDrive\Desktop\pyRAT\abc.docx
removed
```

## 5.Future Scope

• Multiple User access: We plan on adding a multi user access to the software so that more than one client's system can be accessed by the server and more systems can be connected. An example is a Unix or Unix-like system where multiple remote users have access (such as via a serial port or Secure Shell) to the Unix shell prompt at the same time. Another example uses multiple X Window sessions spread across multiple terminals powered by a single machine - this is an example of the use of a thin client. Similar functions were also available on a variety of non-Unix-like operating systems, such as Multics, VM/CMS, OpenVMS and Multiuser DOS.

• Adding access filter for users: We plan on adding various filters to give specific amount of access to specific users according to their needs. • Camera access: adding the feature to open camera and take still pictures or view live footage from client's system to make the process of debugging easy

## 6. Conclusion

Py RAT, unlike the other remote shell protocols or programs, keeps the log for the time connection starts, date, commands, user and other stuff . In addition it also provides a realtime view of commands under execution by the remote client on the server. You are provided a simple and easiest way to start this remote shell application called Py RAT.

We can say that PyRat is a better option than the traditional telnet as it has various benefits over telnet such as commands run at faster time and administrative power over the clients system provides better access over the client's systems and a properly established connection.

## REFERENCES

- “Remote Desktop Software A Complete Guide” by Gerardus Blokdyk
- ”RDPwned” by Andy Milford, Ms Morna M Shah
- “Don't Panic! I'm A Professional Remote Desktop Engineer” by remote desktop publishing guru
- ”Remote Desktop Services A Complete Guide” by Gerardus blokdyk

- “Virtualizing Desktops and Apps with Windows Server 2012 R2 Inside Out”