PACKET-SNIFFING BACKDOOR

Design Work

Danny Lieu

A00831407 | MAY 22, 2018

Table of Contents

Preparation

Requirements

In order to run this application, the machine need to have the following requirements:

- Python 3.x.x (prefer Python 3.6.5)
- Pip3 installed
- Root privilege to run the script

Running preparation script

To install all necessary libraries for the application, find the preparation.sh in ../Listings/. After that, make the script executable by entering the following command:

```
root$ chmod +x preparation.h
```

finally, run the script to install all libraries:

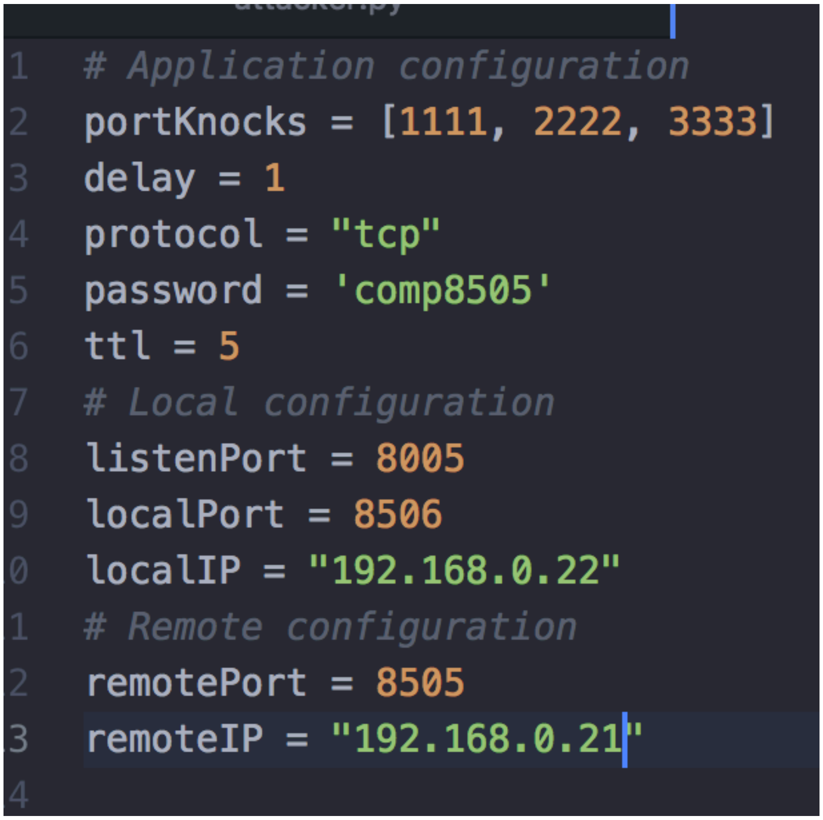
```
root$ ./preparation.sh
```

Script usage

Attacker

We need to change the configuration in the attackerConfig.py. The important fields are localIP, localPort, listenPort, remoteIP, remotePort.

A sample of the configure as below:



```
# Application configuration
portKnocks = [1111, 2222, 3333]
delay = 1
protocol = "tcp"
password = 'comp8505'
ttl = 5
# Local configuration
listenPort = 8005
localPort = 8506
localIP = "192.168.0.22"
# Remote configuration
remotePort = 8505
remoteIP = "192.168.0.21"
```

To run the attacker script, simply type as the following:

```
root$ Python3 attacker.py
```

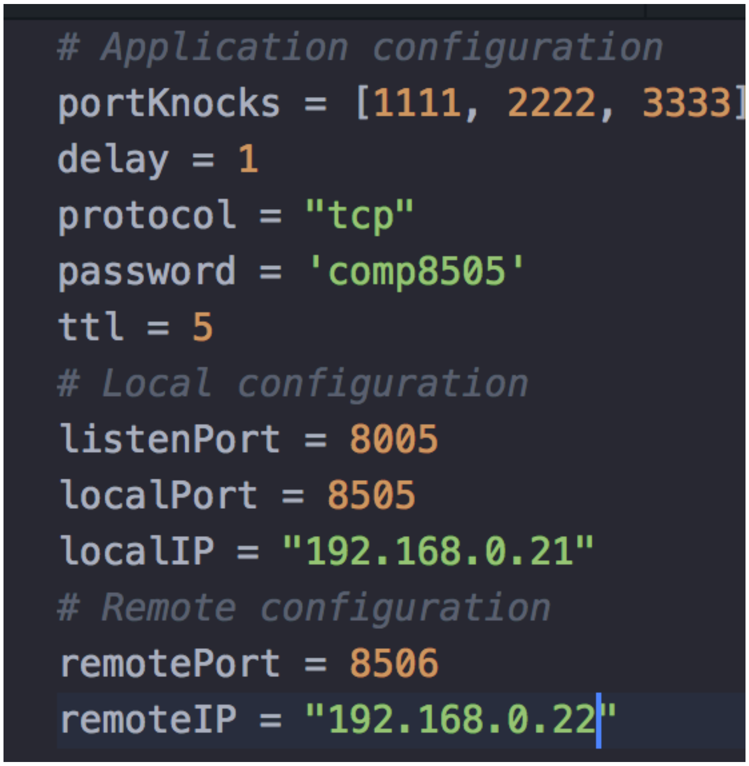
Possible commands that can be use:

- Cd: navigate around the remote machine
- Close: terminate the backdoor program.

Backdoor

The same thing is needed to be done in the backdoor side. We also need to change the backdoorConfig.py to fit the local machine and remote machine.

A sample of backdoorConfig.py as below:



```
# Application configuration
portKnocks = [1111, 2222, 3333]
delay = 1
protocol = "tcp"
password = 'comp8505'
ttl = 5
# Local configuration
listenPort = 8005
localPort = 8505
localIP = "192.168.0.21"
# Remote configuration
remotePort = 8506
remoteIP = "192.168.0.22"
```

To run the backdoor script, simply type as below:

```
root$ python3 backdoor.py
```