2018

Covert Communication Application

FINAL PROJECT – USER MANUAL

DANNY LIEU

Table of Contents

Requirements

In order to run the Covert Communication Application, the machine need to meet these following requirements:

- Python 2.7.x installed (prefer 2.7.14)
- Pip installed
- Root privilege to run the script

All modules needed to run the application properly are included in the preparation script which are:

- Scapy
- Netifaces
- Setproctitle
- Pycryto
- Watchdog
- Pynput

The preparation script can be found in `../Listings/`. After that, make the script executable by entering the following command:

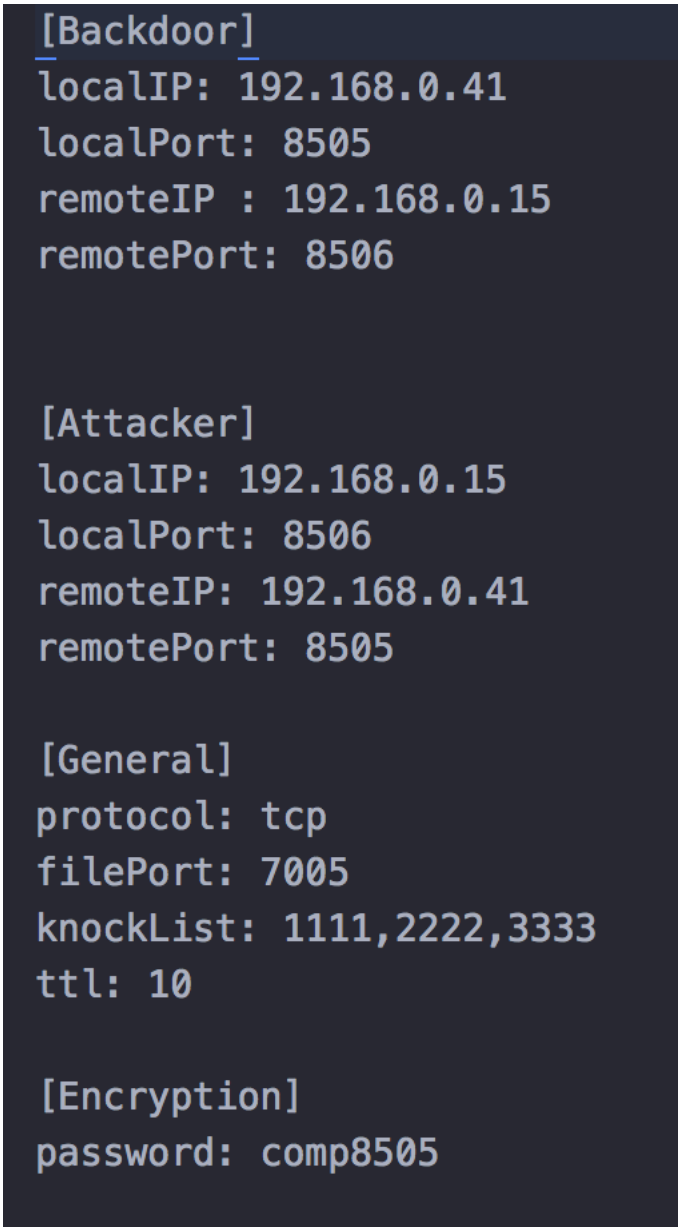
```
chmod +x preparation.sh
```

Finally, run the script to install all necessary module for the application:

```
./preparation.sh
```

Configuration

A sample of configuration as below:



The configuration file is divided into 4 sections:

1. Backdoor
    - localIP: the IP address of the machine that the backdoor was installed
    - localPort: the port that the backdoor will listen for commands
    - remoteIP: the IP address of the attacker machine
    - remotePort: the port that the backdoor will knock for file exfiltration

2. Attacker
    - localIP: the IP address of the attacker machine
    - localPort: the port that will listen for knocking from the backdoor
    - remoteIP: the IP address of the machine that the backdoor was installed
    - remotePort: the port that all commands will be sent to
3. General
    - Protocol: the protocol for sending and receive packets
    - filePort: the port that will handle the actually file transfer
    - knockList: the sequence of port for port knocking
    - ttl: the time for the firewall to remain opening for file transfer
4. Encryption
    - Password: the password to encrypt or decrypt the data

Usage

Attacker

To run the attacker script, run the following command:

```
python attackerMain.py
```

Once the script is running, the user can start entering the command for the backdoor to execute. The available commands are:

- GET: get the specified file from the victim machine and send to the attacker machine.
- KEYON: start the keylogger

- KEYOFF: stop the keylogger
- WATCH: add a watch for a file or directory
- RMWATCH: remove the watch for a file or directory
- CLOSE: send CLOSE command to the backdoor application and close itself
- Other shell commands: cd, ls, ps, pwd, ifconfig, etc.

Backdoor

To run the backdoor script, run the following command:

```
python backdoorMain.py
```

Once the script is running, the backdoor will start to listen for commands. The available commands for the backdoor are:

- GET: extract the name of the file and start sending to the attacker machine
- KEYON: start the keylogger
- KEYOFF: stop the keylogger
- WATCH: add a watch to a file or directory
- RMWATCH: remove the watch to a file or directory
- CLOSE: close the backdoor application
- Other shell commands: cd, ls, ps, pwd, ifconfig, etc.