

Exercise

You are tasked to create a program using Python programming language. The program is a simulation of the interaction between two machines, which consists of two of the following modes:

1. Command Mode

The command mode is a simulation of Reverse Shell where the attacker can attack the victim machine if the victim connects to it. The attacker will listen to a port and wait for the victim to connect to it. The attack is done by sending a Windows command to be executed by the victim.

2. Chat Mode

The chat mode is just simply a chatting simulation, where both attacker and victim can send and receive messages.

The program will run based on the arguments given when it is started. Note that the attacker and the victim script must be included as one file.

Attacker Argument List

| Short Option | Long Option | Description & Requirements |
|--------------|-------------|---|
| -p | --port | <ul style="list-style-type: none">• The port that the attacker is listening at.• Required.• Must be numeric.• Must be between 2000 – 2500. |
| -l | --listen | <ul style="list-style-type: none">• Specifies that the program runs as the attacker.• If the argument is used, the program will run as the attacker. Otherwise, the program will run as the victim. |
| -c | --command | <ul style="list-style-type: none">• Specifies that the program mode will be in command mode.• If the argument is used, the program will run in command mode. Otherwise, the program will run in chat mode. |
| -h | --help | <ul style="list-style-type: none">• If the argument is used, the program will show the help menu and exit. |

Victim Argument List

| Short Option | Long Option | Description & Requirements |
|--------------|-------------|---|
| -p | --port | <ul style="list-style-type: none">• The port that the victim wants to connect to.• Required.• Must be numeric.• Must be between 2000 – 2500. |
| -i | --ip | <ul style="list-style-type: none">• The IP address that the victim wants to connect to.• Must be a valid IP address (“localhost” is not allowed) |

| | | |
|----|-----------|--|
| -c | --command | <ul style="list-style-type: none"> • Specifies that the program mode will be in command mode. • If the argument is used, the program will run in command mode. Otherwise, the program will run in chat mode. |
| -h | --help | <ul style="list-style-type: none"> • If the argument is used, the program will show the help menu and exit. |

Help Menu

- The help menu will be shown if the argument is used, or if the program is run using invalid/incomplete arguments.

Command Mode

As attacker

- The attacker will be waiting for a new connection.
- If a victim connects to the attacker, the attacker can send any Windows Command to the victim.
- The result of the Windows command will be displayed in the program.
- If the Windows command has no output, the command will still be executed.
- If the command sent is “exit”, the connection will be closed, and the program will be quitted.

As victim

- The victim needs to connect to the attacker.
- If the connection is successful, the victim will execute each Windows Command that was sent by the attacker and send the output back to the attacker (if any).
- If the command sent by the attacker is “exit”, the connection will be closed, and the program will be quit.

Chatting Mode

- In chatting mode, the attacker will be waiting for a new connection.
- The chatting mode can only start when the victim has successfully connected to the attacker.
- Both attacker and victim can only handle one connection.
- Both attacker and victim can send and receive messages to each other simultaneously.
- Both attacker and victim can quit the program by sending “exit”.