TU-CANNON SERVER PROGRAM

Ram Charan Baishya , Nazrul Hoque and Dhruba Bhattacharyya

January 9, 2014

0.1 Server program

This program needs dotnet framework 3.5 to be installed in the computer.

Using this program we communicate with the machines which are configured as bots in the test-bed. This program is developed with a user interface through which one can easily specify and control different properties of the attack traffic. Such properties are the protocol type (TCP, UDP and ICMP), the attack pattern (constant rate attack, increasing rate attack and pulsing attack) and the type of source IP (actual IP of the machine or randomly generate valid but spoofed IP address), no of threads (where each thread executes one copy of the slave program inside a single bot machine) and range of ports of the victim to send the traffic. When the master starts, it waits for slaves to connect to it. Figure 1 is a snapshot of the GUI of the *server program.*

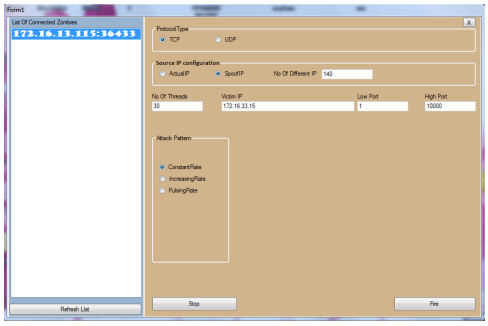

Figure 1: GUI of TUCANNON server program.

The following is a brief description of various components of the interface

List of Zombies: *When the attacker starts the server program, it waits for the client programs to connect to it. As soon as a client program connects to the server, the clients IP address is shown in the left side panel of the interface as shown in Figure 1.*
Protocol type: *To launch an attack , the attacker has to select the type of protocol by selecting any one of the corresponding radio button.*
Source IP configuration: *These options are used to specify whether the attack packet carries the actual source IP or a spoofed one. Also in case of spoof source IP, the attacker can specify the number of different unique spoofed IPs used in the attack. This option allows the attacker to spread the required attack traffic over a specified number of source IP.*
No of threads: *The number of machines in our test bed is very limited (around 50). Hence to increase the amount of traffic each client program sends traffic by using multiple threads. The number of threads used by each client can be specified by the attacker through this input.this feature is used by the attacker to control the traffic rate in the attack.*
Victim IP: *this input field is used by the attacker to specify the IP address of the victim machine.*
Low port and high port: *The attacker can specify the range of ports where to send the traffic via these input.*
Attack pattern: *As mentioned earlier there can be four different traffic pattern. The Attacker can select the pattern from this list.*
Fire: *when the attacker clicks on this button, attack command along with the specified input is sent to all clients currently connected to the server.*
Stop: *The attacker can stop the attack by clicking on this button*