Generate Artificial Traffic for the Online Covert Channel

This guide presents a small example of how to generate TCP and UDP packets with random content. The packets sent to the ccgen are crafted to inject the covert message using the online modus of the CCgen.v2.

With CCgen.v2 the setup of spammer machine and ccgen is automated. In the *CCgen.v2 Dashboard* one can start/install the virtual machine by clicking the *Start* button in the right bottom corner. The spammer virtual machine runs the spammer.py file as a service and tries to connect to the host. The spammer VM is connected to the host machine (ccgen) over a bridge adapter, so that they are both in the same network.

The listener script is running on the host machine and returns messages from spammer if CCgen.v2 is not running in online mode.

The spammer and the listener can be controlled separately by using the small buttons in right bottom corner. Important is, that listener script has to run before spammer script is started.

Listener

listener is a simple script that handles incoming TCP/UDP connections. Application data within the connections is dropped. This script does not reply in any way. TCP connections are torn gracefully.

Configuration

In CCgen.v2 the configuration for the listener is created automatically from the configuration of the spammer. If a TCP or UDP connection is configured in spammer.ini, the listener will listen to the method (TCP or UDP) and the defined destination port. For each connection a new line is used for listening. See the format (METHOD:DST_PORT) in the example below.

PROF

Example:

-------->8-------->8-------->8-------->8-------->8-------->8-------->8--------

[Stuff]

listen=TCP:1234

UDP:4321

-------->8-------->8-------->8-------->8-------->8-------->8-------->8--------

Spammer

spammer is a simple script for sending TCP/UDP data streams to a target. The streams are sent consecutively. Important is, to start the listener.py script before otherwise spammer cannot connect and create data streams.

Configuration

In CCgen.v2 the configuration is done from the configuration section of the *CCgen.v2 Dashboard* (right bottom corner). Generally, the config file is saved to spammer.ini file in the spammer folder and will be synchronised to the spammer virtual machine.
Target is the IP address of the target machine (online mode it is the ip address of the host computer), and send needs to be a list of instructions with one instruction per line. There are four types of instructions possible:

- **TCP** or **UDP**
  Sends tcp/udp packets to target and comes with following parameters:
  - src_host: ip address of the spammer machine [' '] or ['xxx.xxx.xxx.xxx']
  - src_port: source port [' '] or [Number]
  - dst_port: destination port [' '] or [Number]
  - packets: Number of packets to send [Number] or [Number-Number]
  - pattern: that will be sent per packet. It must be a hexadecimal number starting with 0x. [0xXX]
  - repeat: How often to repeat the pattern [Number] or [Number-Number]
- **wait**
  Waits for defined time between instructions and has one parameter:
  - duration: Number or Range defining duration of wait [Number] or [Number-Number]
- **restart**
  Restart the instructions from the beginning

Example:

[ClientA]

PROF

Target = 10.1.0.2

Send =

TCP:10.1.0.1::1234,0xAA,10-100,50-60

3-5

UDP:10.1.0.1:4321:1234,0xBB,30,10

2

restart