ICMP Flooding

Software: NetSim Standard/Pro v13.0

Project Download Link:

https://github.com/NetSim-
TETCOS/ICMP_FLOODING_Workspace_v13.0/archive/refs/heads/main.zip

Follow the instructions specified in the following link to download and setup the Project in NetSim:

https://support.tetcos.com/en/support/solutions/articles/14000128666-downloading-and-setting-up-
netsim-file-exchange-projects

ICMP Flooding: An Internet Control Message Protocol (ICMP) flood is also known as a Ping flood attack is a common Denial-of-Service (DoS) attack in which an attacker attempts to overwhelm a targeted device with ICMP echo-requests (pings). Normally, ICMP echo-request and echo-reply messages are used to ping a network device to check whether devices are connected to the Network.

By flooding the target with request packets, the network is forced to respond with an equal number of reply packets. This causes the target to become inaccessible to normal traffic.

In NetSim to generate ICMP packets from the attacker node to the victim node, Interactive Simulation feature can be used.

In Interactive simulation, NetSim allows users to interact with the simulation at runtime through a file.

Steps to simulate

- Go to NetSim home page, click on your work, Click on examples scenario from the list of experiments.
- Choose any scenario for e.g., choose Intern No ICMP and open.
- An example Scenario as shown below with applications modeled can be seen.
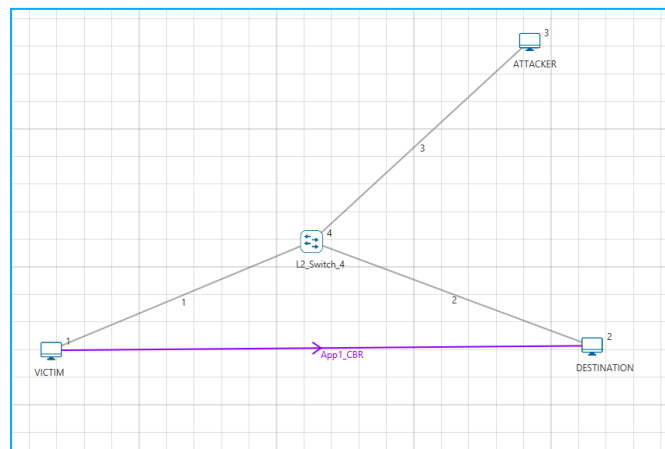

Figure 1 : Internetworks Example Scenario

- Enable ICMP in all nodes. (Currently 5G UE does not support ICMP Protocol)

- Right click on devices->Properties→Network Layer->**ICMP →TRUE**
- Write/generate a text file for interactive simulation as explained in the format provided below throughout the simulation time set.

Format of Input File to Interactive Simulations in NetSim

TIME=<SIMULATION TIME IN SECONDS>

DEVICE=<DEVICE_NAME>

<COMMAND TO BE EXECUTED>

TIME=<SIMULATION TIME IN SECONDS>

DEVICE=<DEVICE_NAME>

<COMMAND TO BE EXECUTED>

Example File format

TIME=1.0001

DEVICE=ATTACKER

Ping VICTIM

TIME=1.0002

DEVICE=ATTACKER

ping VICTIM

TIME=1.0003

DEVICE=ATTACKER

Ping VICTIM

- In run simulation enable the Interactive simulation by clicking on Run time Interaction and select TRUE using File from the drop down.
- Browse and select the interactive simulation input file (input.txt) provided as part of this project and click on Accept.
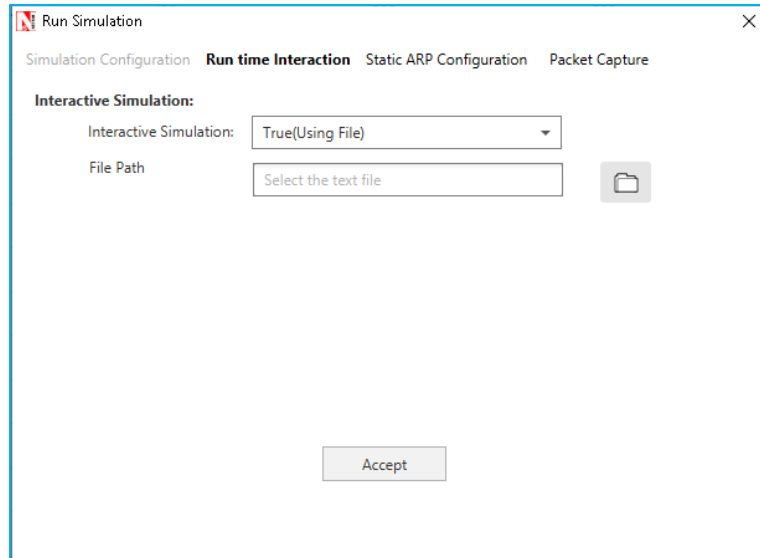
Figure 2: Enabling Interactive simulation in Run simulation Window.

- Run the simulation for 10 secs and check the impact on results before the attack and after the attack, that is by providing Interactive file as Input and without providing Interactive file as input.

Note: To check the impact of ICMP on the network performance you could vary the frequency of ICMP requests, the number of attackers, and by setting processing delay in the network layer of the attacked node.

Wire shark Capture of ICMP request and reply Packets

Wire Shark capture of ICMP packets can be observed parallelly along with simulation by setting Wire Shark Capture to Online in ATTACKER Devices by right clicking on device properties→**General Properties,** in respective Networks.

Figure 3: Wire shark Capture of ICMP Packets.

NetSim packet trace log file also contains the entries of all the ICMP requests and responses exchanged between the attacker and the victim node.