ICMP Flooding

Software Recommended: NetSim Standard v12.2

Follow the instructions specified in the following link to clone/download the project folder from GitHub using Visual Studio:
https://tetcos.freshdesk.com/support/solutions/articles/14000099351-how-to-clone-netsim-file-exchange-project-repositories-from-github-

Other tools such as GitHub Desktop, SVN Client, Sourcetree, Git from the command line, or any client you like to clone the Git repository.

Note: It is recommended not to download the project as an archive (compressed zip) to avoid incompatibility while importing workspaces into NetSim.

Secure URL for the GitHub repository:
https://github.com/NetSim-TETCOS/ICMP_Flooding_v12.2.git

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.

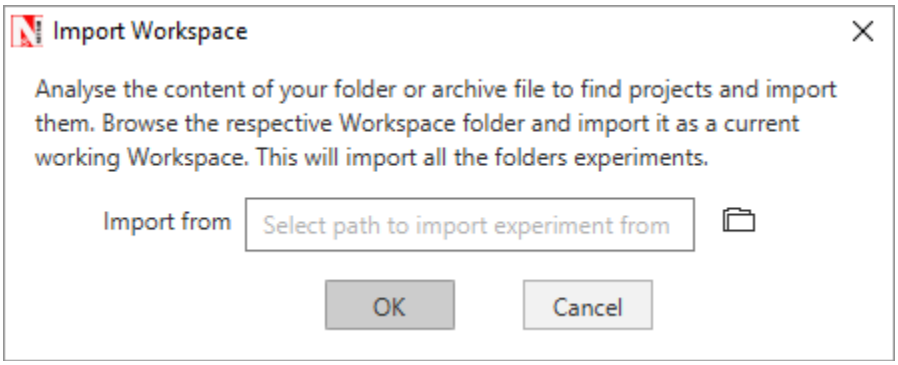
By flooding the target with request packets, the network is forced to respond with an equal number of reply packets. This causes the target to become inaccessible to normal traffic.

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

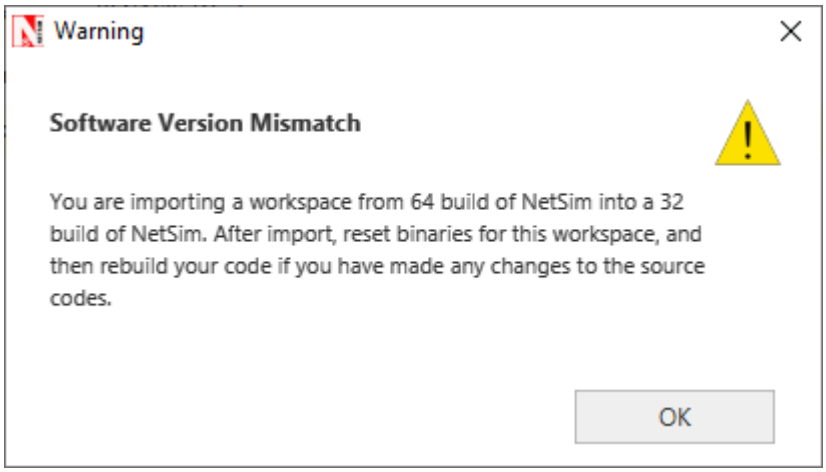
In Interactive simulation, NetSim allows users to interact with the simulation at runtime through a file.

Steps

- After cloning the project folder, Open NetSim Home Page click on Open Simulation->Workspace options->More Options and click on the Import button.



- Browse to the ICMP_Flooding_Workspace folder and click on select folder.
- After this click on OK button in the Import Workspace window. The Imported workspace will be set as the current workspace automatically.
- While importing the workspace, if the following warning message indicating Software Version Mismatch is displayed, you can ignore it and proceed.



- Go to NetSim home page, click on **Open Simulation**, Click on examples scenario.
- Choose 5G_ICMP_Flood scenario.

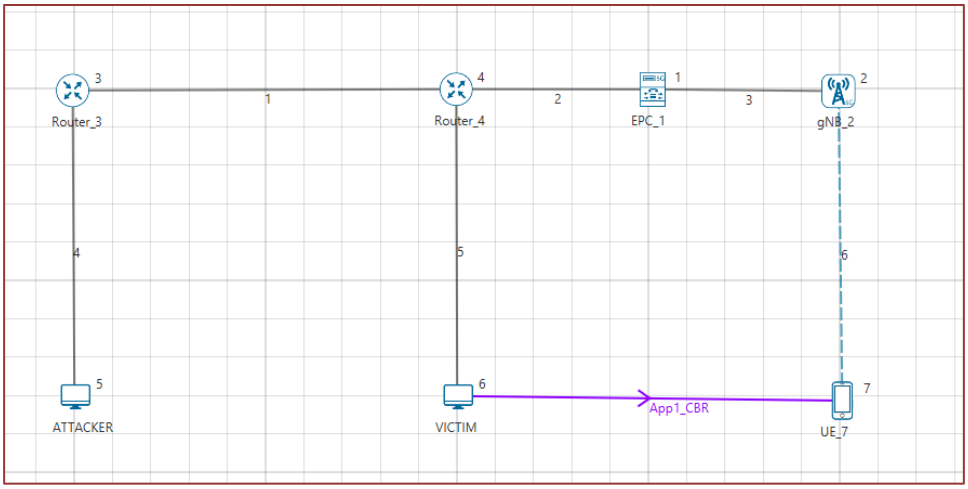


Figure 1 : Internetworks Example Scenario

- 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

- Since there is an RRC Connection establishment in 5G network, note that PING command should start from TIME=1s
- 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.

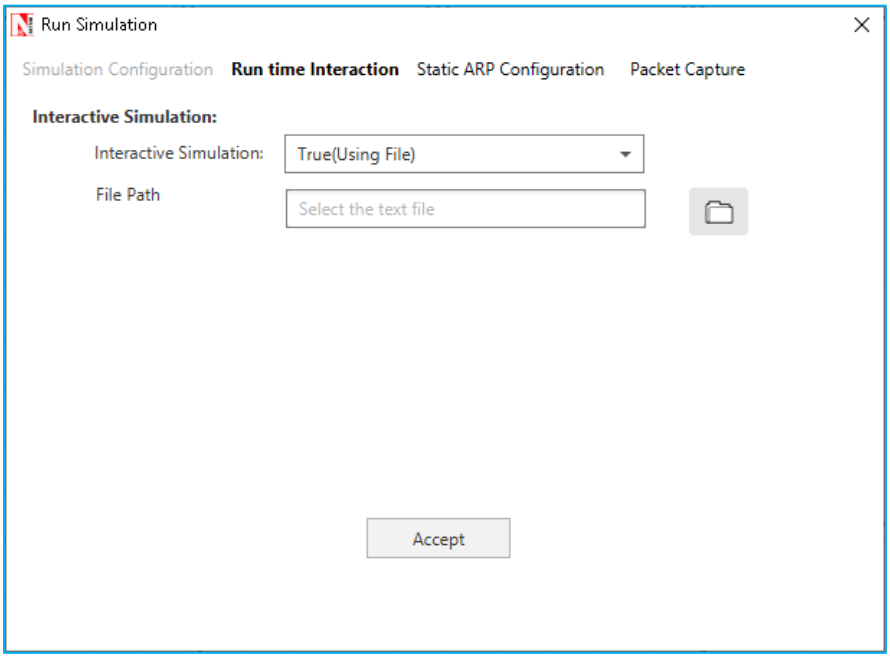


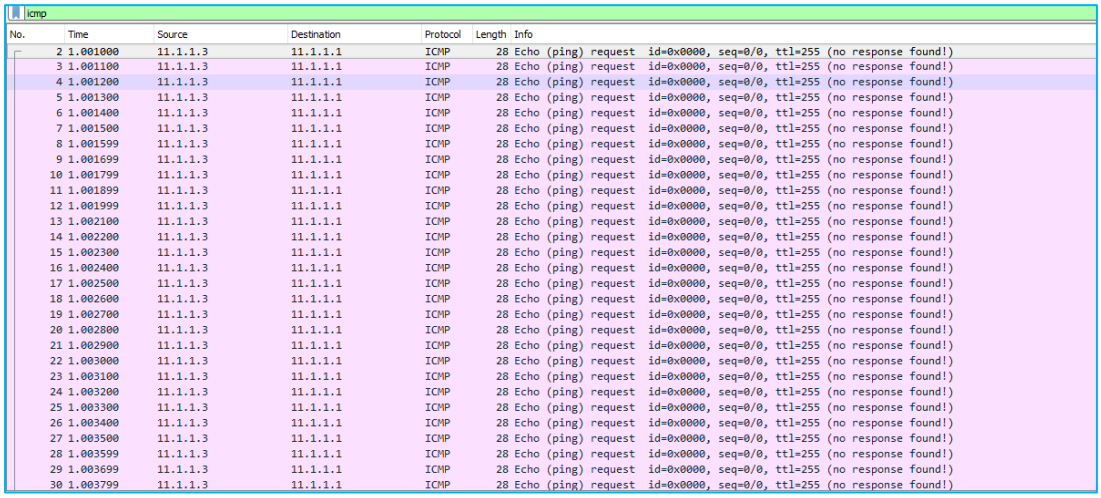
Figure 2: Enabling Interactive simulation in Run simulation Window.

- 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.



icmp

No.	Time	Source	Destination	Protocol	Length	Info
2	1.001000	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
3	1.001100	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
4	1.001200	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
5	1.001300	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
6	1.001400	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
7	1.001500	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
8	1.001599	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
9	1.001699	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
10	1.001799	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
11	1.001899	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
12	1.001999	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
13	1.002100	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
14	1.002200	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
15	1.002300	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
16	1.002400	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
17	1.002500	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
18	1.002600	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
19	1.002700	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
20	1.002800	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
21	1.002900	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
22	1.003000	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
23	1.003100	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
24	1.003200	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
25	1.003300	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
26	1.003400	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
27	1.003500	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
28	1.003599	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
29	1.003699	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)
30	1.003799	11.1.1.3	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (no response found!)

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.