The project represents URMA- the Utility Risk Mapping and Analysis tool designed for utilities. The tool determines the active state of the network corresponding to scanning information, security vulnerabilities currently present on the system and build up analytics on top of that to determine the threat landscape of the network. It also enumerates the criticality of the potential attack paths could be exploited by the attacker which can be effective for remediation prioritization.

Platform requirement-

-Linux

-Mac OS

Required tool and Library-

- MulVAL (http://people.cs.ksu.edu/~xou/argus/software/mulval/readme.html)

- Graph-tool (<https://graph-tool.skewed.de/>)

To run:

- Open a console

- cd [file path]

- ./urma.sh

- Insert numeric value depending on your choice. Any of the options generate attack paths, perform analytics on the paths and measure exploitability of each path as well as exploitability of each state.

put vertices file

- only supports .CSV format. Example file given 'VERTICES.CSV'. This file represents the nodes of the graph.

put arcs file

- only supports .CSV format. Example file given 'ARCS.CSV'. This file represents the edges of the graph.

Insert target state-

- put state from dict\_keys. Make sure it is not the starting node. Example target state '1'

Insert IP address of assumed attacker location-

- If you like to analyze with the attack paths from a specific physical machine. Make sure it's not the target machine. Example IP- 192.168.1.25

Insert state address of assumed attacker location-

- put state from dict\_keys. Make sure it does not match with target state. Example state '13'

The tool enables generating attack paths and compute the criticality of paths to any target state from any source IP address and state.

Each path criticality is shown with a numerical score in 'path\_exploit'.