MTDSim Documentation

# Setup

This was all run on Python 3.9.13 64 Bit. In the root directory in terminal, run the following commands in your virtual environment to setup the environment:

* Python setup.py install
* Python -r requirements.txt
* Python -m mtdnetwork.run -m IPShuffle -n 50 -e 10 -s 5 -l 3 results.json
  + The following is only an example of how the function can be made, reference the run.py file or use the –help command to understand the parameters.

# Architecture

The system uses the 3-layer HARM model to represent the network. This is a representation of the network, with the lowest levels on the bottom and the highest levels on the top:

|  |  |
| --- | --- |
| Layer | Description |
| Network | Made up of all the Hosts, connected in an Attack Graph, with exposed and un-exposed hosts that attackers will attempt to compromise |
| Host | Made up of several services (internal and external) in an Attack Graph. The host is compromised when an internal service is compromised |
| Services | An attack tree of vulnerabilities. A service is compromised when the sum of the vulnerabilities exploited impact is above 7 |
| Vulnerabilities | Generated with a set Attack Complexity and Impact |