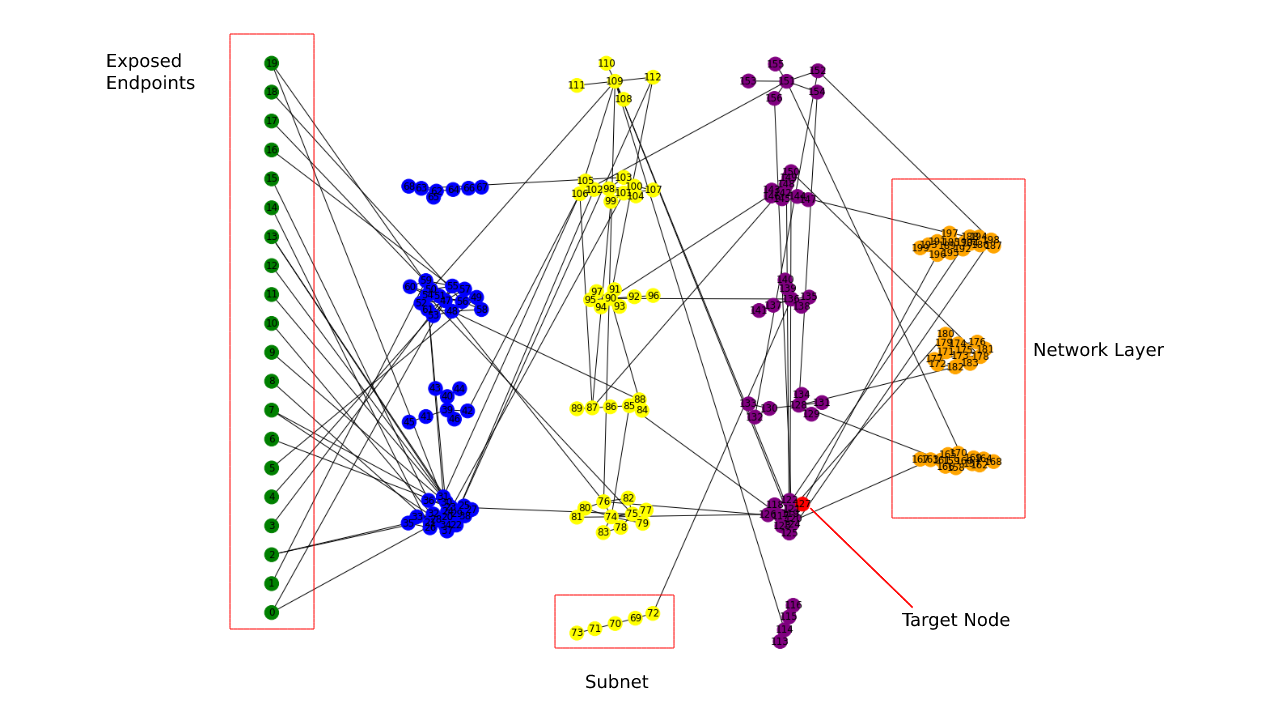
# MTD Sim Parameters

## Network Parameters

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| Total Nodes | Number of nodes that will be generated for the network |
| Total Endpoints | The number of nodes that are generated as exposed (i.e. attacker will always find these nodes without compromising any nodes and the connection point will remain static [IP and ports remain static]) |
| Total Subnets | Number of subnets found in network (randomly spread between layers) |
| Total Layers | Number of layers found in network |
| Target Layer | Layer number the target node will be on (if targeted attack) |

## Network Example



## Host Parameters

NOTE: Every network node has ONE host instance

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| Operating System | One of the operating systems (selected from constants.py) |
| OS Version | Version number of the operating system (selected from constants.py) |
| Host ID | The Node ID of the host on the network graph |
| Host IP | IP Address of the Host |
| Users List | List of users assigned to Host (Picked randomly from users setup from data/first-name.txt) |
| Service Generator | Instance of the ServiceGenerator Class (found in services.py) |
| Action Manager | Action Manager that Queues actions and questions |
| K Nearest Neighbour | Used to generate internal network for services (using Watts Strogatz) |
| Probability Strogatz Rewire | Used to generate internal network for services (using Watts Strogatz) |

## Service Generator Parameters

(Generates all the service objects for the Host)

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| Services per OS | Number of services generated per OS (determined in constants.py) |
| Percent cross platform | Percent the service generated is compatible with all platforms (determined in constants.py) |
| Max Vulnerability Probability | Maximum probability for older version of services having a vulnerability (determined in constants.py) |
| Vulnerability Patch Mean | The average number of version numbers required for a vulnerability to be patched (determined in constants.py) |
| Vulnerability Patch Range | Max version range the vulnerability will be patched in (determined in constants.py) |
| Vulnerability Initial Chance | Chance there will be a vulnerability in the first version of a service (determined in constants.py) |

## Service Parameters

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| Service Name | Name of the service (decided from service generator) |
| Service Version | Version of the service (decided from service generator) |
| Vulnerabilities | The vulnerabilities that are found on the service (decided from service gen) |

## Vulnerability Parameters

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| Have OS Dependency | Can only be exploited if found on Host that is OS in on self.vuln\_os\_list |
| OS List | List of OS that vulnerability can be found on |
| Complexity | How hard it is to compromise vulnerability (randomly determined with a baseline limit set in constants.py) |
| Impact | The amount the attacker will gain from compromising vulnerability (randomly generated) |

## Attacker/Hacker Parameters

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| Attacker Threshold | The number of attacks an attacker will attempt on a single host until giving up |