CyberSim User Manual:

Installation guide

First of all, make sure you have the minimum requirements installed.

For example, on Ubuntu:

pip3 install -r requirements.txt

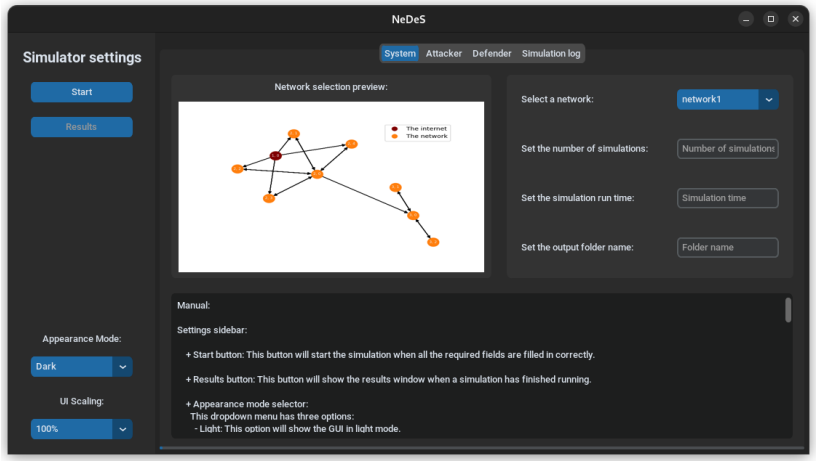
After running this command all the requirements are installed and you can immediately use the CyberSim simulator.

Starting the simulator

To start the simulator, you can use the following command:

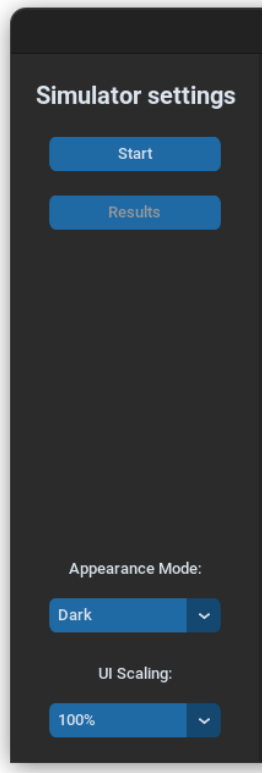
python3 simulator.py

After this command is done the simulator will start and the following graphical user interface will appear:



Explaining the simulator:

Settings sidebar:



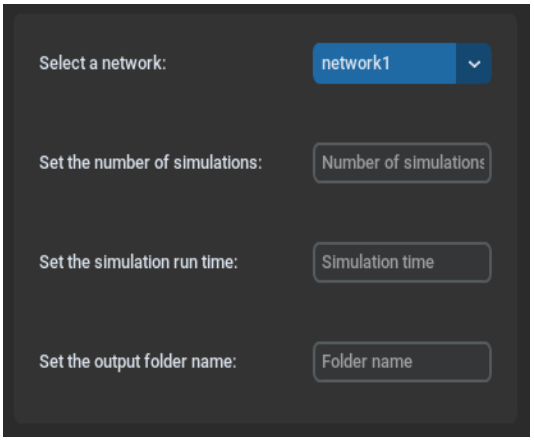
Start button: This button will start the simulation when all the required fields are filled in correctly.

Results button: This button will show the results window when a simulation has finished running.

Appearance mode selector:
This dropdown menu has three options:

- **Light:** This option will show the GUI in light mode.
- **Dark:** This option will show the GUI in dark mode.
- **System:** This option will show the GUI in the mode your computer system is set on.

UI scaling selector: This dropdown menu has multiple options for scaling the simulator. These are 80%, 90%, 100%, 110%, and 120%.



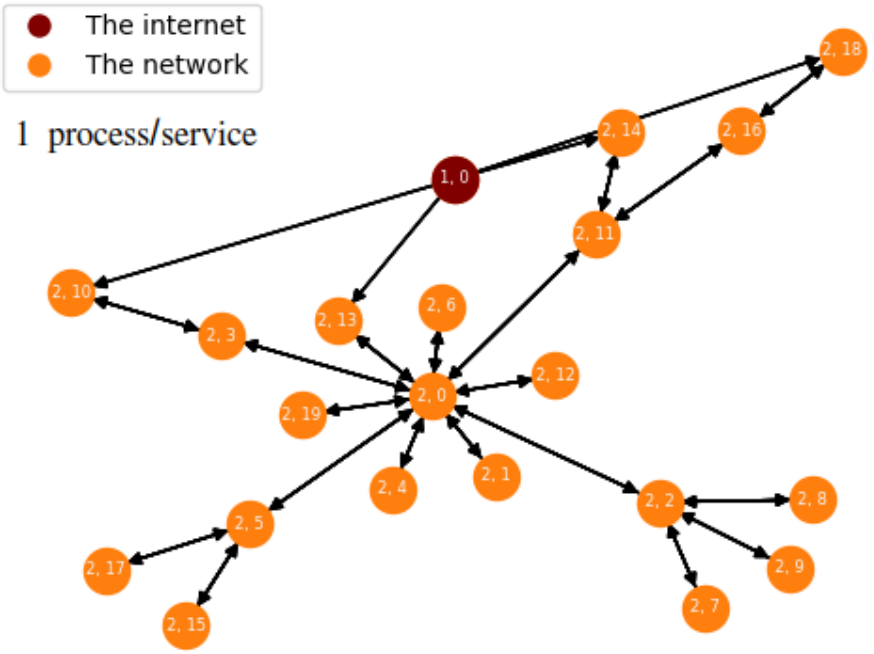
Systems tab:

Network selector: This dropdown menu will show the available networks to run the simulation on. When selecting a network the network preview will change with it.
The user can not create his own network and can only choose from the 5 options.

The number of simulations entry field: This entry field will decide how many times the simulation will be run. Must be an integer.

Simulation run time entry field: This entry field will decide how long the simulated time will be in seconds. Must be an integer. 500 is a good starting point for experiments on network 2, 3, 4, and 5. On network 1, a run time of 200 is enough.

Output folder name entry field: This entry field will decide the name of the output folder, which contains all the results. This folder will be saved in the same directory the simulator is located in.



Preview of network 2

Network selection preview:

All the networks have a preview that shows the topology of the network. The preview of network 2 is shown above. The orange dots are the hosts of the network, while the dark red dot is the internet. The arrows are the edges between the hosts. Each host also has an address. The addresses are the numbers in the dots. The addresses can be used in combination with the log to check what happened during a run. The preview also shows how many processes each host has and how many services each edge allows. This is the “1 process/service” in the top left corner. Network 2 thus has 1 process per host and 1 service per edge. The number of processes and services are not mentioned for network 1, because it differs per host or edge. Some hosts have 2 processes, while others have 1. The same goes for the edges.

Attacker tab:

On the attacker tab, we create the number of attackers we want for a simulation and then decide which strategy and which actions they should use.

To create attackers, fill in an integer in the attacker entry field and follow that by pressing the **create attackers** button. The graphical user interface will now generate that amount of attackers in the scrollable frame.

Each attacker has its own id. Each attacker can also be set with an attacker strategy by selecting it in the dropdown menu.
The options are

Random Strategy:

The random strategy is based on random probabilities just as its name implies

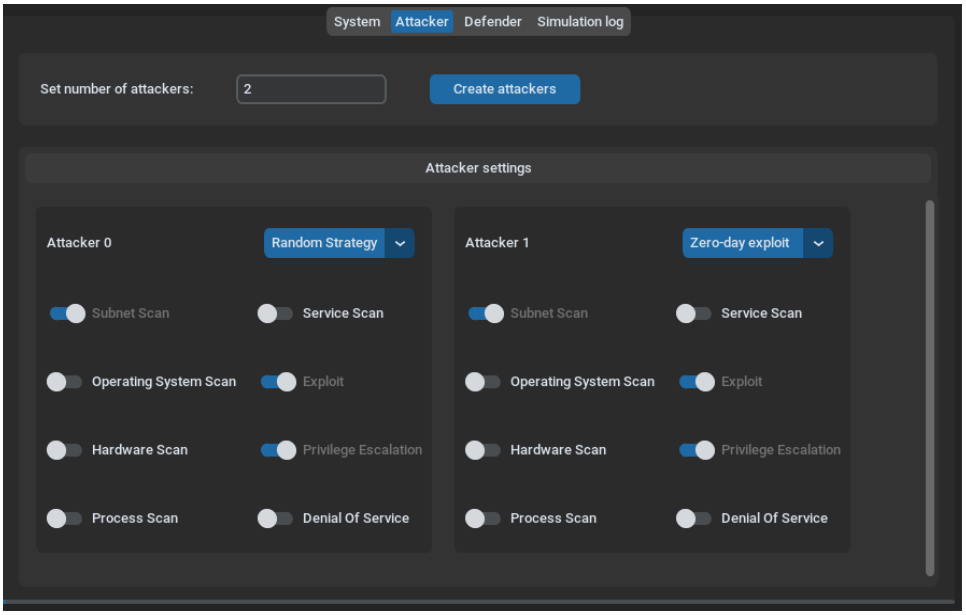
Zero-day exploit:

A zero-day exploit is a software vulnerability that has not been disclosed to the public and which is also unknown to the software vendor. The difference in knowledge gives cyber attackers the advantage so that they can attack targets, while the vulnerabilities remain undetected.

Advanced Persistent Threats:

The term Advanced Persistent Threats a.k.a. APTs. First, Advanced represents the sophisticated form of the attacker as it is not the same as simple scans and probes. The Persistent means that the attackers select their target and when necessary repeatedly attack that target over a long period of time. Finally, Threat means that the actor behind the attack is relevant and wants something from the target.

You will notice that each strategy has actions which are blocked, these can not be unselected and will remain selected, the other actions however can be selected or unselected.



Defender tab:

There is only one defender in the simulator therefore all the options for the defender are shown in this tab. First, the defender can choose its strategy by selecting one from the dropdown menu. These are the five strategies of the defender:

The first strategy is **random**. This means that the defender randomly picks a host or edge and hardens that host or edge as much as possible. The probability of hardening a host or edge are equal.

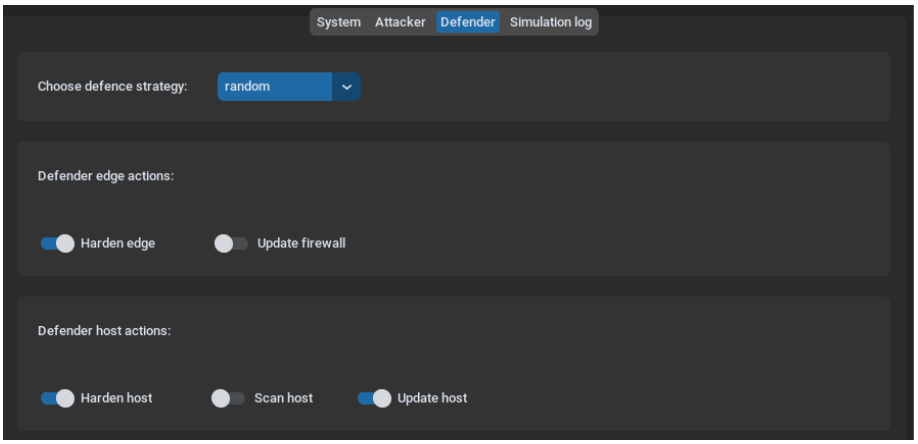
The second strategy is **last layer defense**. This strategy prevents the attackers from getting the score of the most important hosts. The first step is to use host hardening on these hosts to prevent privilege escalation. The second step is to fully harden all the edges that go towards the sensitive hosts. The order in which the sensitive hosts are hardened is based on score. The host with the highest score is hardened first. The edges of the host with the highest score are hardened first as well. The random strategy is used after hardening all the sensitive hosts and their incoming edges.

The third strategy is **minimum defense**. This defense only takes action when an attack fails. An attack can fail if the probability of the attack is not one. An attack can also fail if the targeted host or edge was hardened during the attack. When a failed attack is noticed, the defender fully hardens the host or edge that was the target of the failed attack. It then waits until another attack fails. The probability of succeeding is set to 1 for all attacks. This cannot be changed as a user. Minimum defense means in this case that no actions are taken by the defender.

The fourth strategy is **reactive and random** and is a combination of the first and third strategies. It does random hardenings until a failed attack is noticed. It then fully hardens the target of the attack. It goes back to random hardening afterwards. This is for a user the same as the random strategy, since no attack fails.

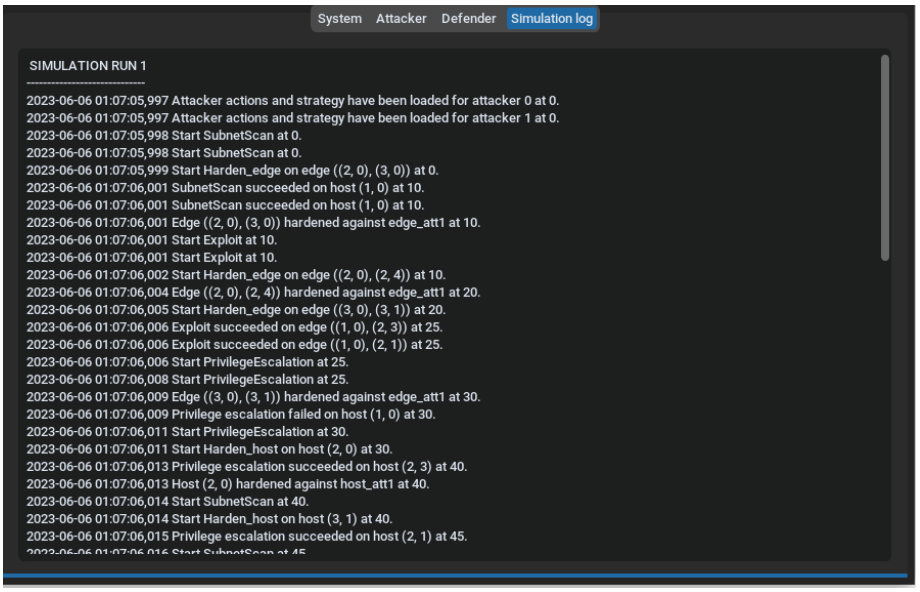
The last strategy is **highest degree neighbour**. This strategy first picks a random host in the network. It then takes the neighbour of this random host that has the highest degree. The degree is calculated by adding the number of incoming and outgoing edges together. An edge between host A and B that goes both ways is thus counted twice. The same process is then repeated on the neighbour with the highest degree. The degrees of all its neighbours are calculated and the best is chosen. There are now two best hosts as a result from the two rounds. Either one of the two hosts will be fully hardened or an edge between the two hosts will be fully hardened. A completely random host or edge is fully hardened if the target chosen by this method is already fully hardened.

The actions of the defender are split into two sections. One section contains the actions that affect edges. The other section contains actions that affect hosts. Actions that are selected can be used by the defender. At least one hardening must be selected, thus harden edge or harden host. The update firewall, scan host, and update host actions can be selected, but are not used in any of the provided strategies. Selecting or not selecting them will not change the actions of the defender.



Log tab:

The log tab displays the log for the latest simulation which has been finished running.



Results window

The results window will show a quick summary of the results of the simulation.

In the top left, we have the network topography after the simulation is finished. This topography will show which hosts have been compromised and which have not.

Underneath that, we have the plot of the scores of the attacker(s) and defender over time.

On the right side, there is a summary with all the valuable results from the simulation, which is divided into three parts: network, defender, and attacker. The total score of the defender is really the total score, the costs of the actions are already subtracted. The costs of the actions still need to be subtracted from the scores of the attackers.

When the simulation is run multiple times, then the results will be shown in an average over all the simulations.