Critical Infrastructure

Attack Tree-Analysis Tool User Manual

Table of Contents

[Acknowledgement 2](#_Toc173773294)

[Tree Syntax 3](#_Toc173773295)

[Decision Gate Nodes 3](#_Toc173773296)

[Terminal Nodes 3](#_Toc173773297)

[Start in Developer Mode 5](#_Toc173773298)

[Install 5](#_Toc173773299)

[Generate Tree 6](#_Toc173773300)

[Importing a Tree 7](#_Toc173773301)

[View Attack Scenarios 9](#_Toc173773302)

[Export Tree 11](#_Toc173773303)

[View Recommendations 12](#_Toc173773304)

[Export Report 13](#_Toc173773305)

## Acknowledgement

We would like to acknowledge the work of Anandarajah Yathuvaran, Anil Menon, Dylan Leveille, Eric Leung, and Dr. Jason Jaskolka, their supervisor, of Carleton University who created the Attack Tree – Analysis Tool (AT-AT) which was the foundation for this project. This manual is a modified version of the manual they created for their AT-AT, which can be found at <https://github.com/yathuvaran/AT-AT/blob/main/Documentation/User%20Manual.pdf>.

## Tree Syntax

The Critical Infrastructure Attack Tree-Analysis Tool uses a specific syntax (see Figure 1) to generate attack trees.

Each line represents a node on the tree. Nodes can be either decision gates(❶) or terminal leaves(❹). Semi-colons are used to delimitate between the name of the node to be displayed in the tree, and the type of node

|  |  |
| --- | --- |
| A group of arrows pointing to the right  Description automatically generated❶  ❷  ❸  ❹ | Open Safe;OR  Pick Lock;o=0.6;a=0.2;t=1;d=1  Learn Combo;OR  Find Combo;o=0.2;a=0.2;t=1;d=1  Acquire Combo;OR  Threaten;o=0.2;a=0.4;t=0.2;d=0  Eavesdrop;AND  Listen to conversation;o=0.6;a=0.4;t=0.6;d=0.8  Get target to say combination;o=0.6;a=0.4;t=0.6;d=0.8  Cut Open Safe;o=0.2;a=1;t=0.4;d=1 |

Figure 1-Tree Syntax

### Decision Gate Nodes

Decision-gate nodes require a logical operator (OR, Figure 2 or AND, Figure 3) and can be chained to create complex logical relationships (❷). Both examples "Open Safe" uses disjunction, meaning at least one child must be executed. "Eavesdrop" uses conjunction, requiring all its children to be executed(❸).

Parent-child relationships are represented with tab indentation (❷, ❸, ❹).

A black background with a black square

Description automatically generated with medium confidence

Figure 2 OR Decision Gate

A black background with a black square

Description automatically generated with medium confidence

Figure 3 - AND Decision Gate

### Terminal Nodes

Leaf nodes follow the format <node name>; o=#.# | a=#.# | t=#.# | d=#.# | none (❹). The node name text is mandatory and will appear inside a terminal node box (Figure 4). The optional metrics are o, a, t, and d, each on a decimal scale of 0.0 to 1.0. o is the Occurrence Score, a relative likelihood metric which is calculated separately. a is the Attack Cost, the perceived cost in terms of time and money to an attacker to accomplish the specific terminal node’s actions. t is the Technical Difficulty for the attacker to accomplish the terminal node. d is Discovery Difficulty, how difficult it is for defenders to discover an attacker success for the terminal node, during or after the attempt.

A screen shot of a phone

Description automatically generated

Figure 4 - Terminal Node

Indentation represents tree levels. "Pick Lock" and "Learn Combo" are children of "Open Safe." "Pick Lock" uses OR, so either "Pick With Bobby Pin" or "Break Lock" suffices. "Dynamite" uses AND, requiring both "Add Chemical" and "Add Heat." For the root goal, either "Pick Lock" or "Dynamite" must be achieved.

## Start in Developer Mode

Users can initiate a developer application of AT-AT using the node package manager command ‘npm run dev’. This will initiate a React web application that can be edited in real time.

## Install

Users can compile a Windows executable version of AT-AT using the command ‘npm run make’. This will create a folder with a standalone executable with all necessary packages and libraries.

## Generate Tree

Users can manually input text to generate an attack tree. Follow these steps to generate a tree:

1. Enter text in the DSL format in the text area, such as:

Open Safe;OR

Pick Lock;o=0.6;a=0.2;t=1;d=1

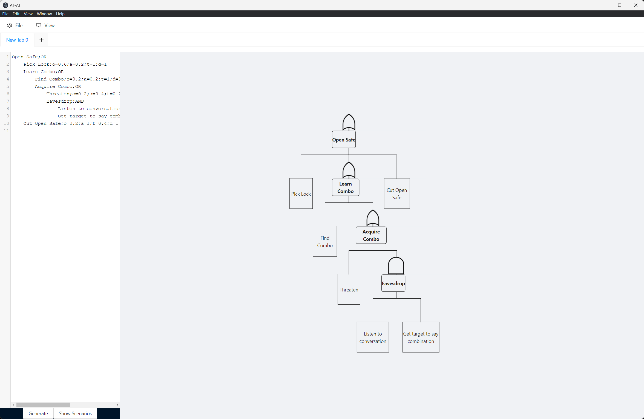
Learn Combo;OR

Find Combo;o=0.2;a=0.2;t=1;d=1

1. Click “Generate”

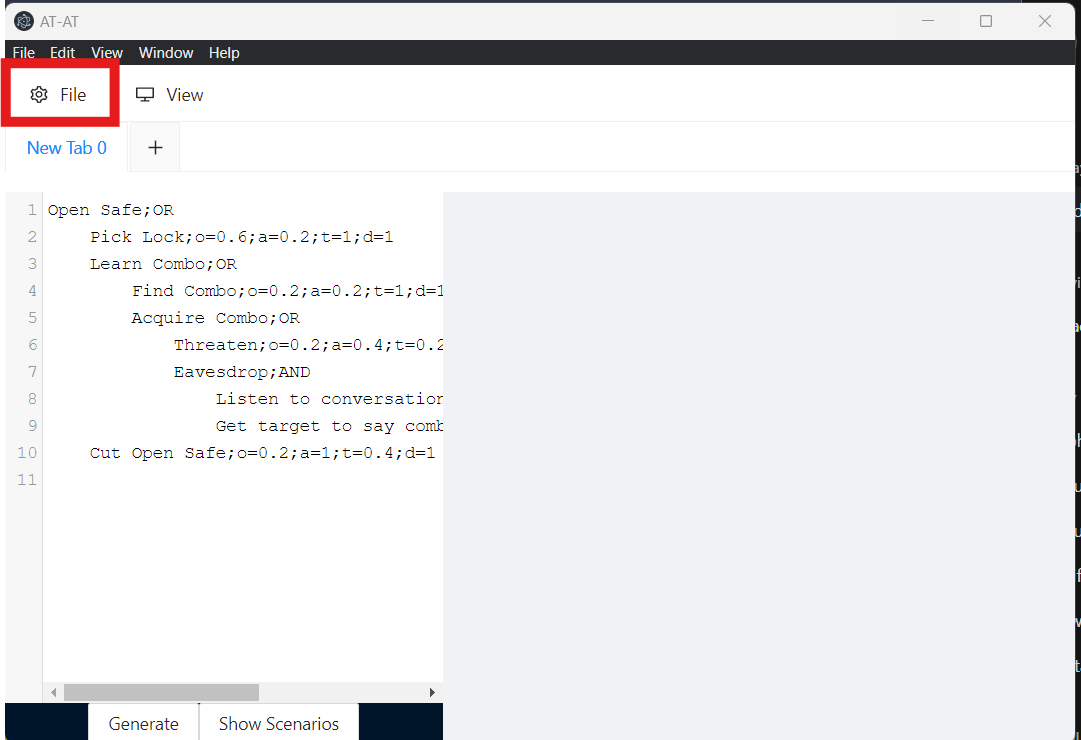
A screenshot of a computer program

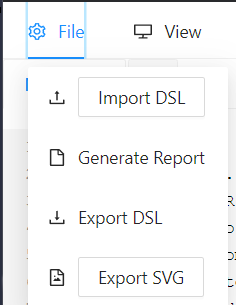
Description automatically generated

1. The tree should now be displayed.

## Importing a Tree

Users can automatically populate the DSL text box by importing any plain text (i.e. .txt) file with the properly formatted data. Follow these steps to import the data and generate a tree:

1. Click “File”
2. 
3. Select “Import DSL” (Figure 1: Import DSL)

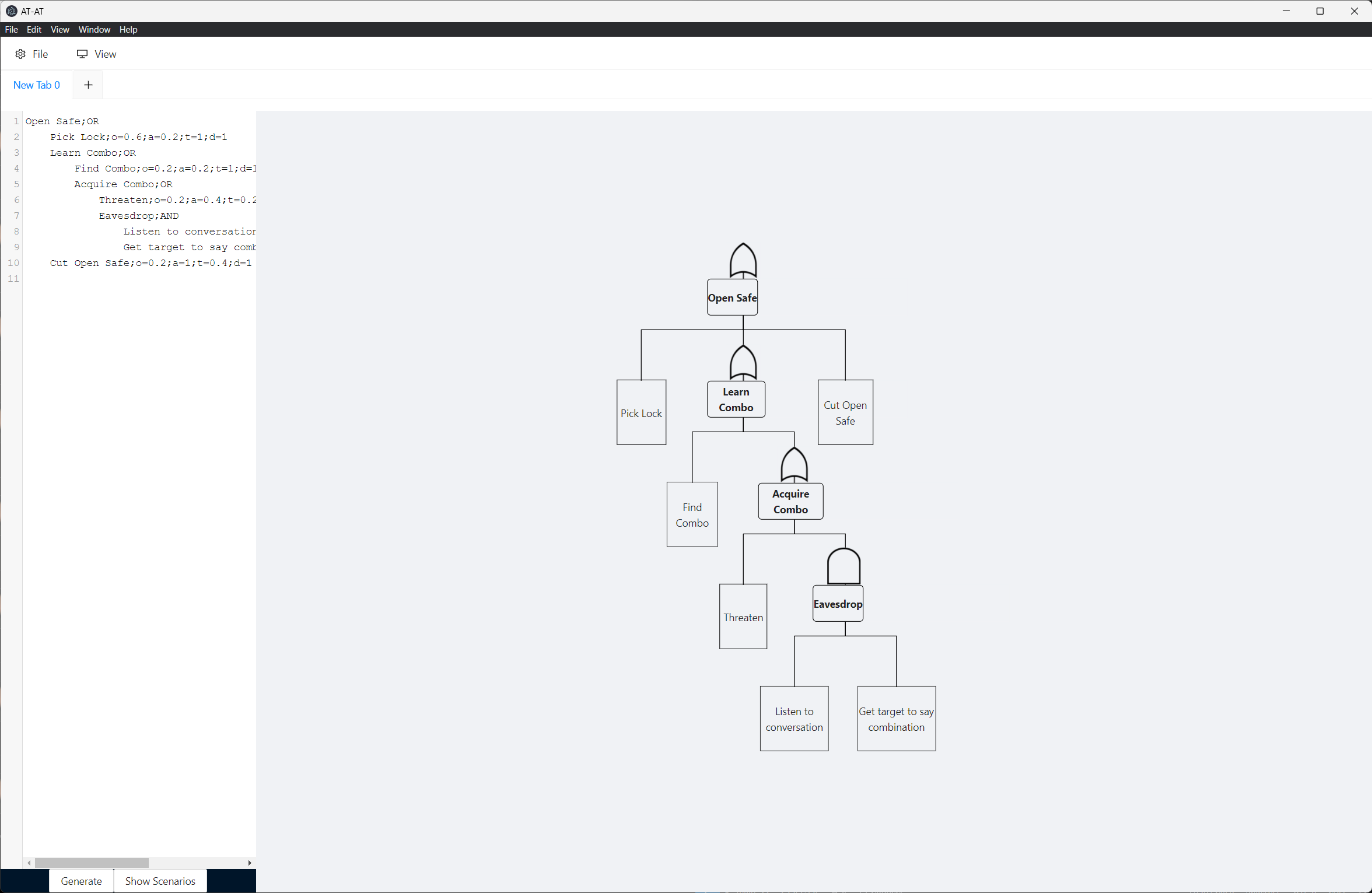


1. Choose your desired text file
2. Click “Generate”

A screenshot of a computer program

Description automatically generated

1. The tree should now be displayed.



## View Attack Scenarios

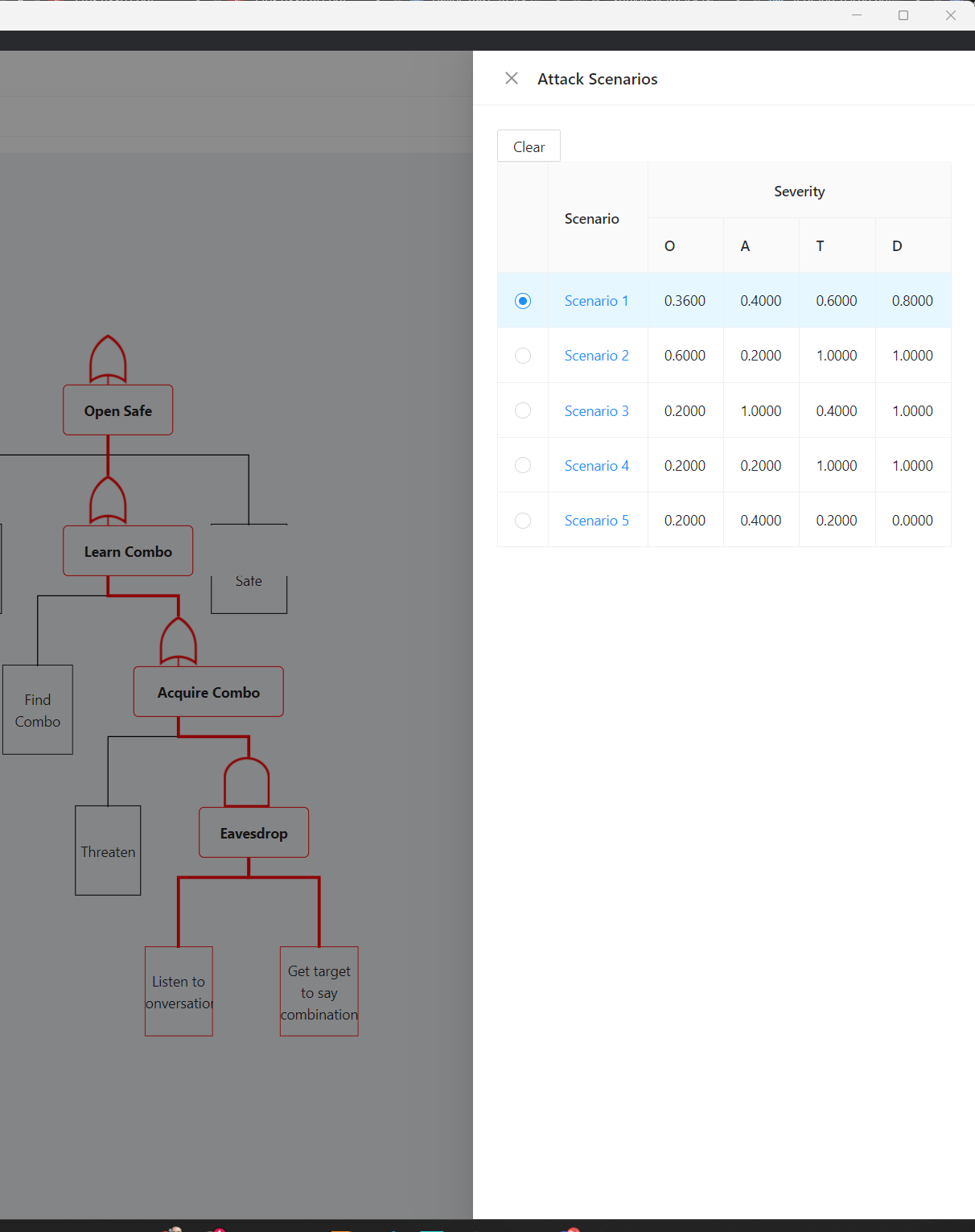
When an input attack tree is generated, the AT-AT tool also analyzes it to produce a list of all possible attack scenarios. This list can be accessed by clicking the “Show Scenarios” button:

1. **Display Scenarios**: Click “Show Scenarios”.

A screenshot of a computer

Description automatically generated

1. **Select Scenario**: Choose a specific scenario by clicking the radio button next to it.



The list can be closed by clicking outside the "drawer" component or by clicking the "X" button. This action will highlight the path of the selected scenario in red.

A screen shot of a computer

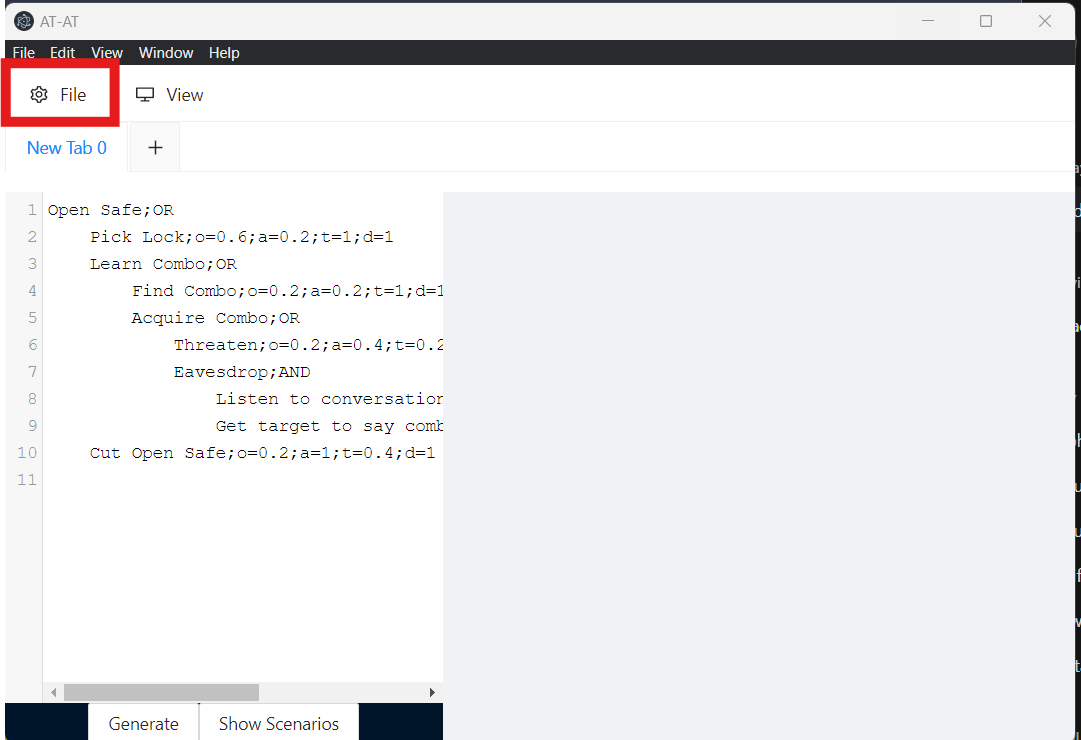
Description automatically generated

To display the attack scenarios list again, click “Show Scenarios.” To remove the highlighted scenario and return to the default view, click the “Clear” button. You can also select another scenario to be highlighted.

## Export Tree

This tool allows users to export a DSL tree to a text file, which can then be imported later. Follow these steps to export the tree:

1. Click “File”



1. Select “Export DSL”

A screenshot of a computer

Description automatically generated

1. Choose a file name
2. Select a location
3. Click “Save”

The file should now be generated and saved to the chosen location.

## View Recommendations

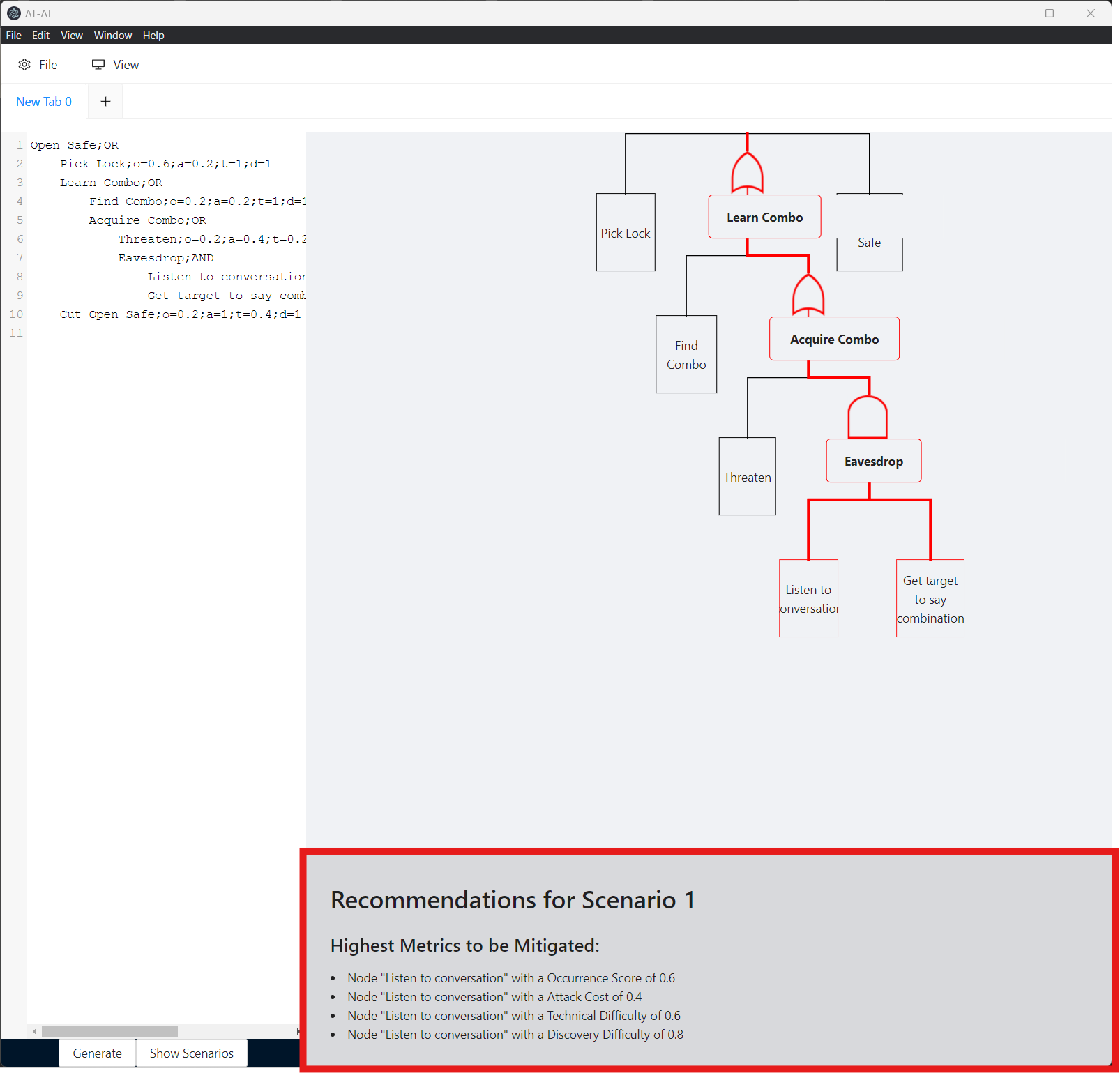
To view recommendations for an attack scenario, ensure the scenario is selected. Then, click the “View” button and choose “Enable Recommendations”:

1. **Enable Recommendations**: Click “View” and select “Enable Recommendations”.

A screenshot of a computer

Description automatically generated

1. This action will display a box showing the recommendations for the selected scenario. An example is shown below.



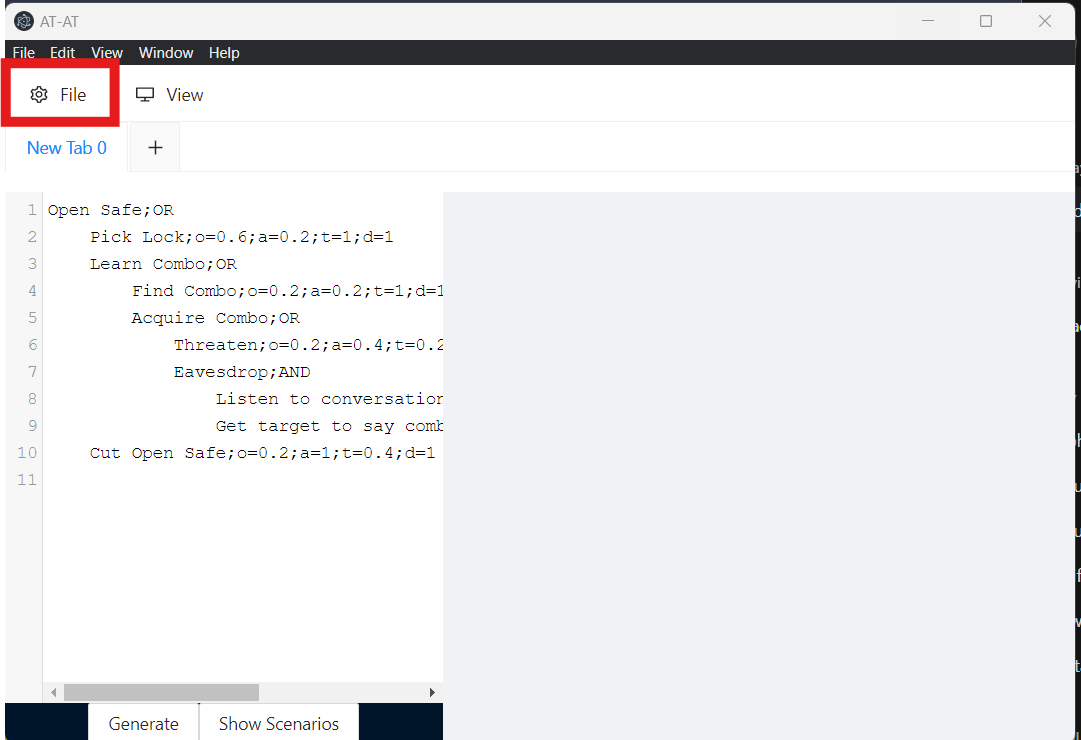
The recommendations box provides information on the highest values of each metric in the attack scenario. It also suggests specific mitigations for common attacks identified within the scenario by analyzing the text in the nodes for common attack keywords. For example, if the term "phishing" is detected, recommendations for mitigating phishing attacks will be provided.

To remove the recommendations box, click the “View” button again and select “Disable Recommendations.” The box will disappear.

## Export Report

Users can export their generated tree and all its scenarios into an HTML file, making it convenient to save and access the attack tree and its analysis anytime. Here are the steps to export a report:

1. Ensure you have either entered some text or imported text that conforms to syntax so that a tree is generated.
2. Click “File”



1. Select “Generate Report”

A screenshot of a computer

Description automatically generated

1. Click “Save Report”
2. Choose a destination folder
3. Ensure the filename ends with .html
4. Click “Save”

The report will be saved as an HTML file which can be opened by any web browser.