Critical Infrastructure
Attack Tree-Analysis Tool User Manual

Table of Contents

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 specific syntax formats to generate attack trees. One of the formats uses DSL syntax shown in Figure 1.1 and Figure 1.2.

Figure 1.1 shows an example of the basic DSL syntax format. 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, the node type, and the different metrics, if provided.

```
❶ Open Safe;OR
     →    Pick Lock;o=0.6;a=0.2;t=1;d=1
❷    →    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=0.2
❸    →        →        →    Eavesdrop;AND
     →        →        →        →    Listen to conversation;o=0.6;a=0.4;t=0.6;d=0.8
❹    →        →        →        →    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 1.1 – DSL Basic Tree Syntax

Figure 1.2 represents another DSL format option where the ‘O’ metric is calculated based on the weighted ‘A’, ‘T’, and ‘D’ metrics given. In the first line, the weights(❺) of the ‘A’, ‘T’, and ‘D’ metrics are listed, respectively. The three weights should add up to approximately 1, with the tool allowing a 0.03 margin for rounding. After the first line, each line represents a node on the tree. Semi-colons are used to delimitate between values.

```
❺ 0.33;0.33;0.33
❶ Open Safe;OR
     →    Pick Lock;a=0.2;t=1;d=1
❷    →    Learn Combo;OR
     →        →    Find Combo;a=0.2;t=1;d=1
     →        →    Acquire Combo;OR
     →        →        →    Threaten;a=0.4;t=0.2;d=0.2
❸    →        →        →    Eavesdrop;AND
     →        →        →        →    Listen to conversation;a=0.4;t=0.6;d=0.8
❹    →        →        →        →    Get target to say combination;a=0.4;t=0.6;d=0.8
     →    Cut Open Safe;a=1;t=0.4;d=1
```

Figure 1.2 - DSL Weighted Tree Syntax

The tool can also use CSV syntax to generate attack trees (see Figure 1.3 and Figure 1.4).

Figure 1.3 shows an example of the basic CSV syntax format. Each line represents a node on the tree. The first column represents the type of the node, ‘O’ for OR decision gates, ‘A’ for AND decision gates, and ‘T’ for terminal leaves. Commas are used to delimitate between the node type, the node ID, the node name, and the different metrics, if provided.

```
❶ O,1,Open Safe
  T,1.1,Pick Lock,0.6,0.2,1,1
❷ O,1.2,Learn Combo
  T,1.2.1,Find Combo,0.2,0.2,1,1
  O,1.2.2,Acquire Combo
  T,1.2.2.1,Threaten,0.2,0.4,0.2,0.2
❸ A,1.2.2.2,Eavesdrop
  T,1.2.2.2.1,Listen to conversation,0.6,0.4,0.6,0.8
❹ T,1.2.2.2.2,Get target to say combination,0.6,0.4,0.6,0.8
  T,1.3,Cut Open Safe,0.2,1,0.4,1
```

Figure 1.3 - CSV Basic Tree Syntax

Figure 1.4 represents another CSV format option where the 'O' metric is calculated based on the weighted 'A', 'T', and 'D' metrics given. In the first line, the weights(❺) of the 'A', 'T', and 'D' metrics are listed, respectively. The three weights should add up to approximately 1, with the tool allowing a 0.03 margin for rounding. After the first line, each line represents a node on the tree. Commas are used to delimitate between values.

```
❺ 0.33,0.33,0.33
❶ O,1,Open Safe
  T,1.1,Pick Lock,0.2,1,1
❷ O,1.2,Learn Combo
  T,1.2.1,Find Combo,0.2,1,1
  O,1.2.2,Acquire Combo
  T,1.2.2.1,Threaten,0.4,0.2,0.2
❸ A,1.2.2.2,Eavesdrop
  T,1.2.2.2.1,Listen to conversation,0.4,0.6,0.8
❹ T,1.2.2.2.2,Get target to say combination,0.4,0.6,0.8
  T,1.3,Cut Open Safe,1,0.4,1
```

Figure 1.4 - CSV Weighted 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 (❶). Both examples "Open Safe" uses disjunction, meaning at least one child must be executed (❷). "Eavesdrop" uses conjunction, requiring all its children to be executed (❸).

In the DSL tree syntax, parent-child relationships are represented with tab indentation (❷, ❸, ❹). In the CSV tree syntax, parent-child relationships are represented in the second column in the IDs of the nodes (❶, ❷, ❸, ❹).

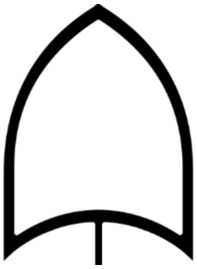


Figure 2 - OR Decision Gate

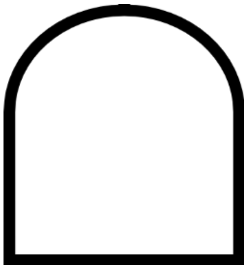


Figure 3 - AND Decision Gate

Terminal Nodes

In the DSL tree syntax, terminal leaf nodes follow the format `<node name>; o=#.# | a=#.# | t=#.# | d=#.# | none` (❹). In the CSV tree syntax, terminal leaf nodes follow the format `T, <node ID>, <node name>, <o> | <a> | <t> | <d> | none` (❹). The node name text is mandatory in both DSL and CSV formats and will appear inside a terminal node box (Figure 4). In the CSV format, the node type 'T' and the node ID are also mandatory. 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.

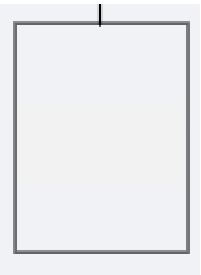


Figure 4 - Terminal Node

In the DSL format, indentation represents the tree levels, while in the CSV format, the decimal points in the ID number represents the tree levels. "Pick Lock," "Learn Combo," and "Cut Open Safe" are children of "Open Safe." "Learn Combo" uses OR, so either "Find Combo" or "Acquire Combo" suffices. "Eavesdrop" uses AND, requiring both "Listen to conversation" and "Get target to say combination." For the root goal, either "Pick Lock," "Learn Combo," or "Cut Open Safe" 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:

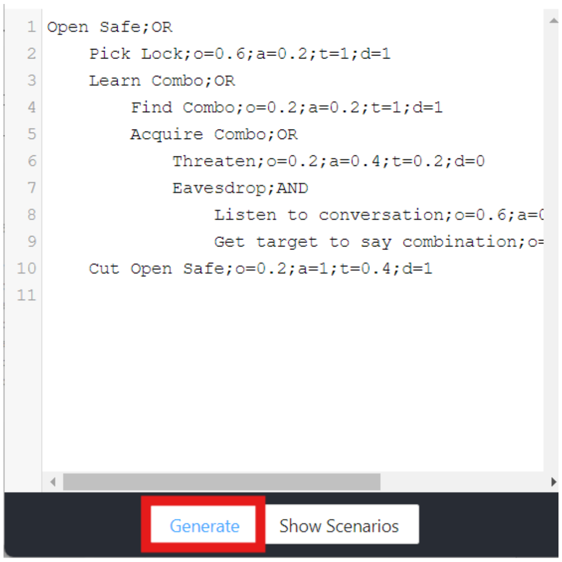
1. Enter text in the DSL format in the text area, such as:

```
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
```

Text can also be entered in one of the CSV formats in the text area, such as:

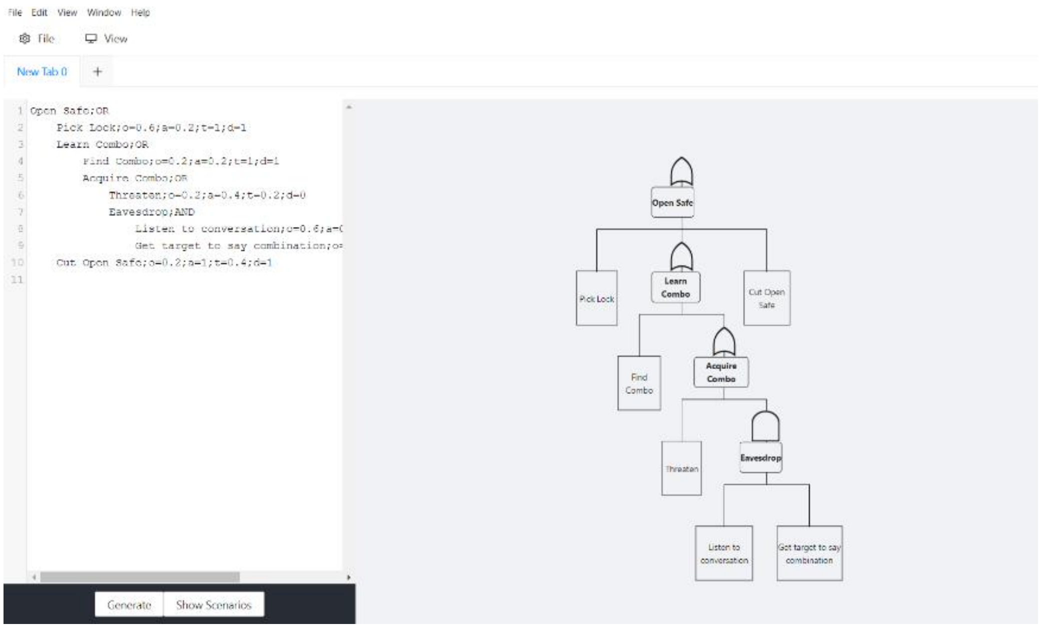
```
O,1,Open Safe
T,1.1,Pick Lock,0.6,0.2,1,1
O,1.2,Learn Combo
T,1.2.1,Find Combo,0.2,0.2,1,1
```

2. Click “Generate”



```
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=
                Get target to say combination;o=
    Cut Open Safe;o=0.2;a=1;t=0.4;d=1
```

3. The tree should now be displayed.



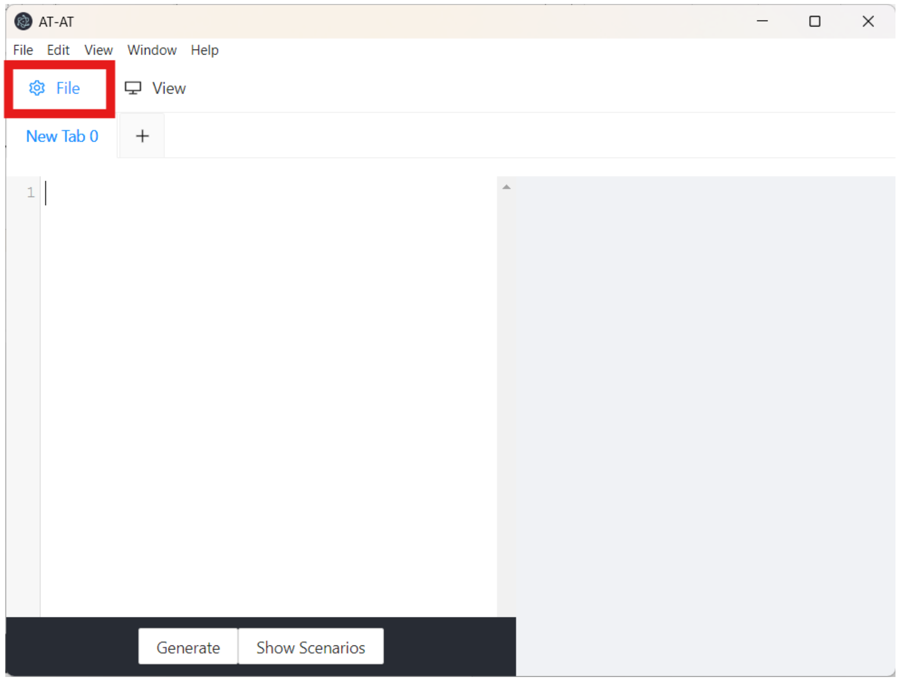
```
Open Safe;OR
    Pick Lock;o=0.6;a=0.2;t=1;d=1
    Learn Combo;OR
        Find Combo;o=0.2;a=0.2;t=1;d=1
        Acquire Combo;OR
            Threaten;o=0.2;a=0.4;t=0.2;d=0
            Eavesdrop;AND
                Listen to conversation;o=0.6;a=0
                Get target to say combination;o=
    Cut Open Safe;o=0.2;a=1;t=0.4;d=1
```

Importing a Tree

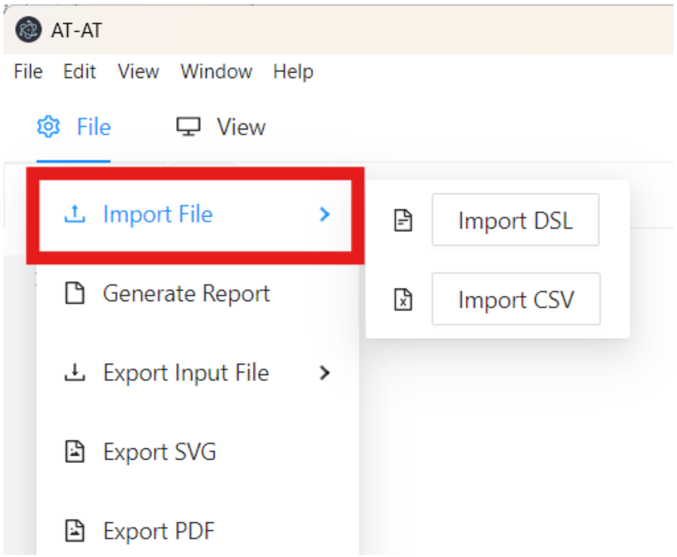
Users can automatically populate the text area by importing a file with the formatted DSL or CSV data.

To import a DSL, users can upload any plain text (i.e. .txt) file with the properly formatted data. Follow these steps to import the data and generate a tree from a DSL:

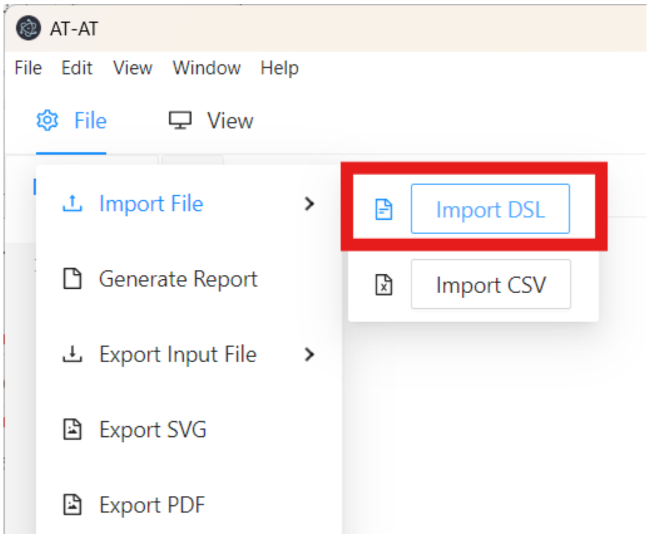
1. Click "File"



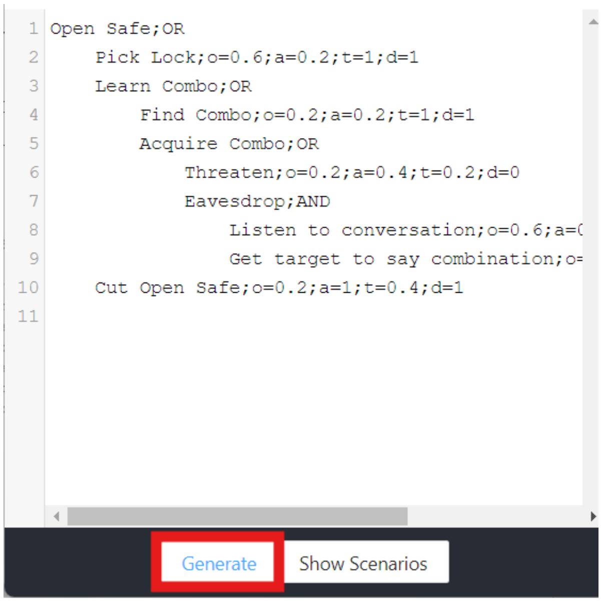
2. Click "Import File"



3. Select “Import DSL” (Figure 1.1 & Figure 1.2: Import DSL)

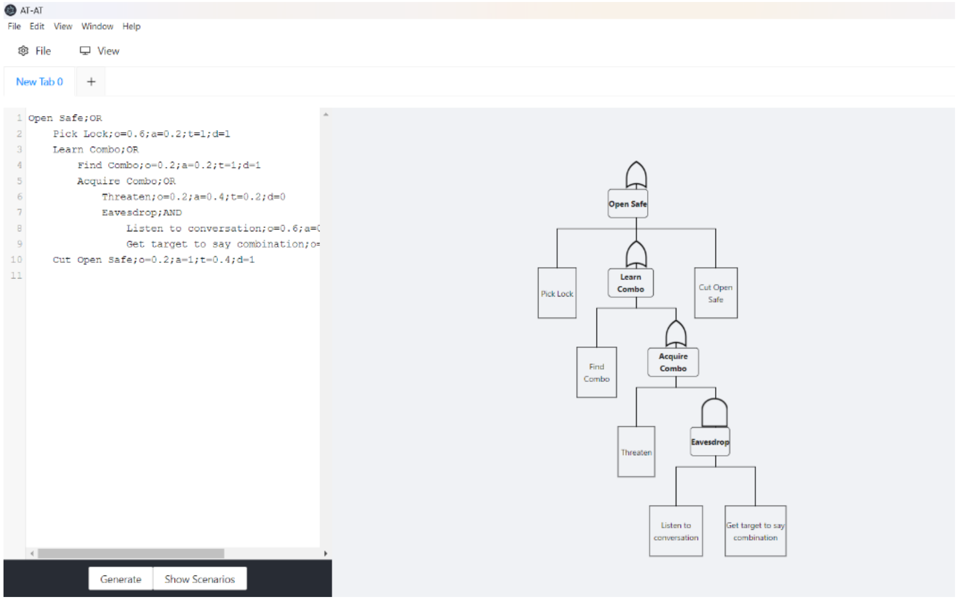


4. Choose your desired text file
5. Click “Generate”



```
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=
                Get target to say combination;o=
    Cut Open Safe;o=0.2;a=1;t=0.4;d=1
```

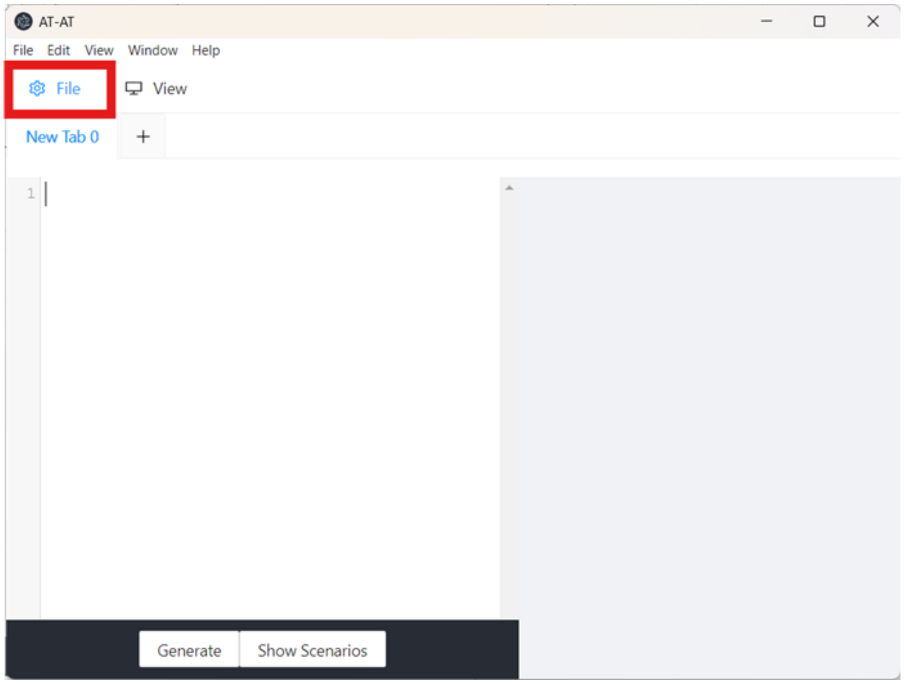
6. The tree should now be displayed.



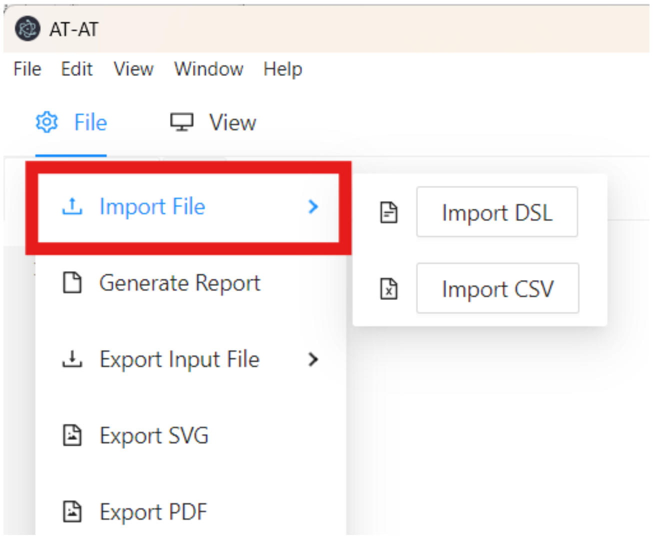
```
Open Safe;OR
    Pick Lock;o=0.6;a=0.2;t=1;d=1
    Learn Combo;OR
        Find Combo;o=0.2;a=0.2;t=1;d=1
        Acquire Combo;OR
            Threaten;o=0.2;a=0.4;t=0.2;d=0
            Eavesdrop;AND
                Listen to conversation;o=0.6;a=(
                Get target to say combination;o=
    Cut Open Safe;o=0.2;a=1;t=0.4;d=1
```

To import a CSV, users can upload any comma-separated values (i.e. .csv) file with the properly formatted data. Follow these steps to import the data and generate a tree from a CSV:

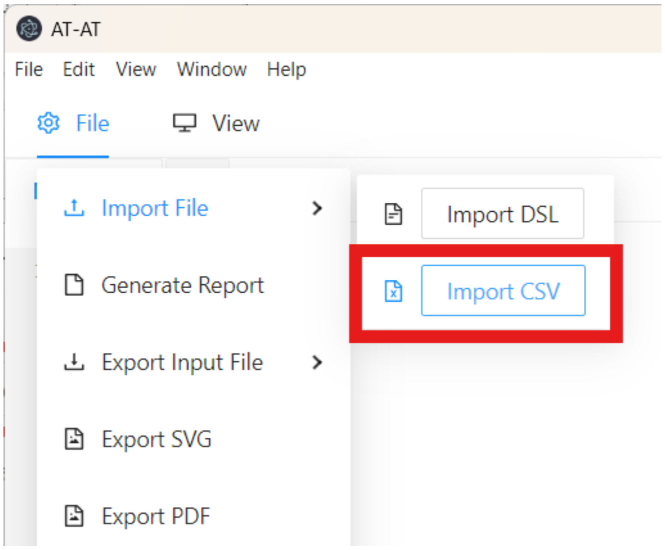
1. Click “File”



2. Click “Import File”

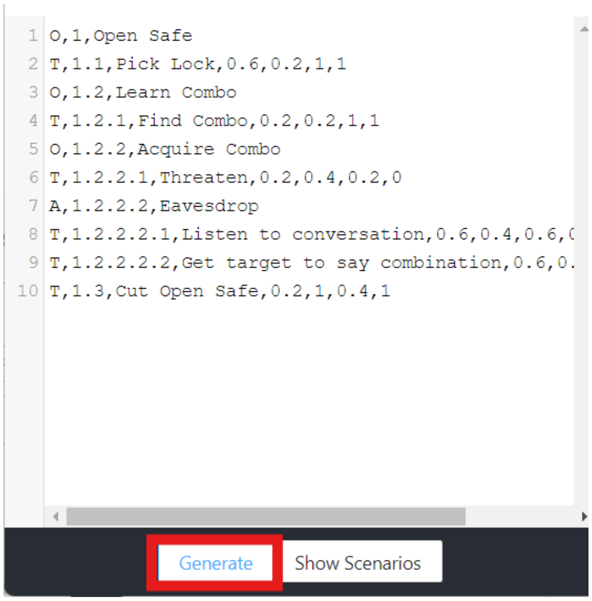


3. Select “Import CSV” (Figure 1.3 & Figure 1.4: Import CSV)



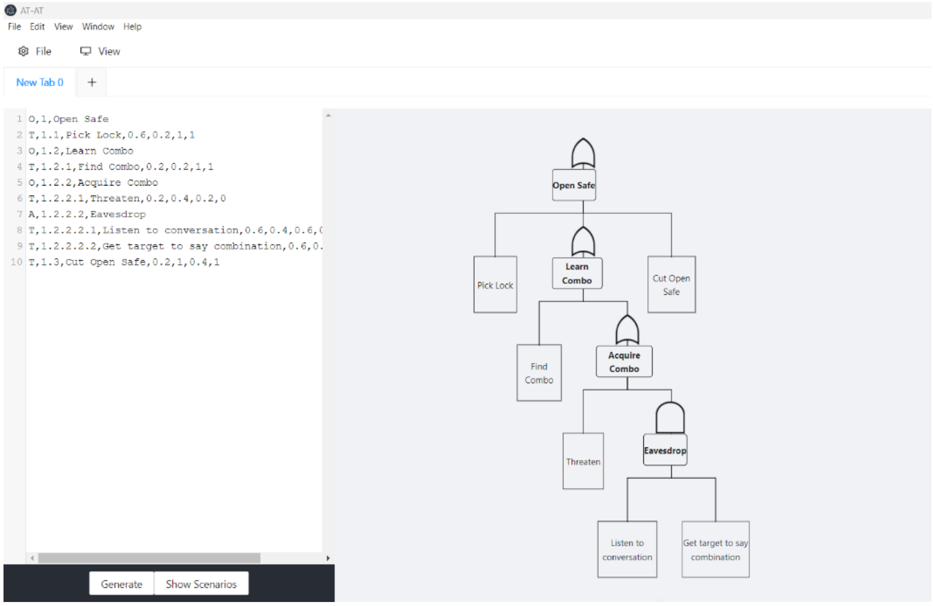
4. Choose your desired text file

5. Click “Generate”



```
O,1,Open Safe
T,1.1,Pick Lock,0.6,0.2,1,1
O,1.2,Learn Combo
T,1.2.1,Find Combo,0.2,0.2,1,1
O,1.2.2,Acquire Combo
T,1.2.2.1,Threaten,0.2,0.4,0.2,0
A,1.2.2.2,Eavesdrop
T,1.2.2.2.1,Listen to conversation,0.6,0.4,0.6,(
T,1.2.2.2.2,Get target to say combination,0.6,0.
T,1.3,Cut Open Safe,0.2,1,0.4,1
```

6. The tree should now be displayed.

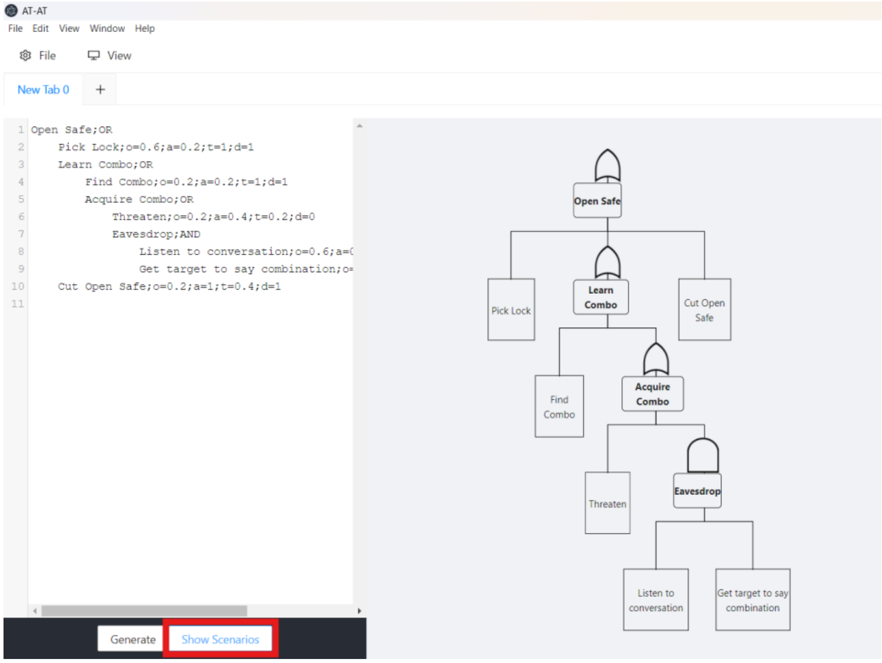


```
O,1,Open Safe
T,1.1,Pick Lock,0.6,0.2,1,1
O,1.2,Learn Combo
T,1.2.1,Find Combo,0.2,0.2,1,1
O,1.2.2,Acquire Combo
T,1.2.2.1,Threaten,0.2,0.4,0.2,0
A,1.2.2.2,Eavesdrop
T,1.2.2.2.1,Listen to conversation,0.6,0.4,0.6,(
T,1.2.2.2.2,Get target to say combination,0.6,0.
T,1.3,Cut Open Safe,0.2,1,0.4,1
```

View Attack Scenarios

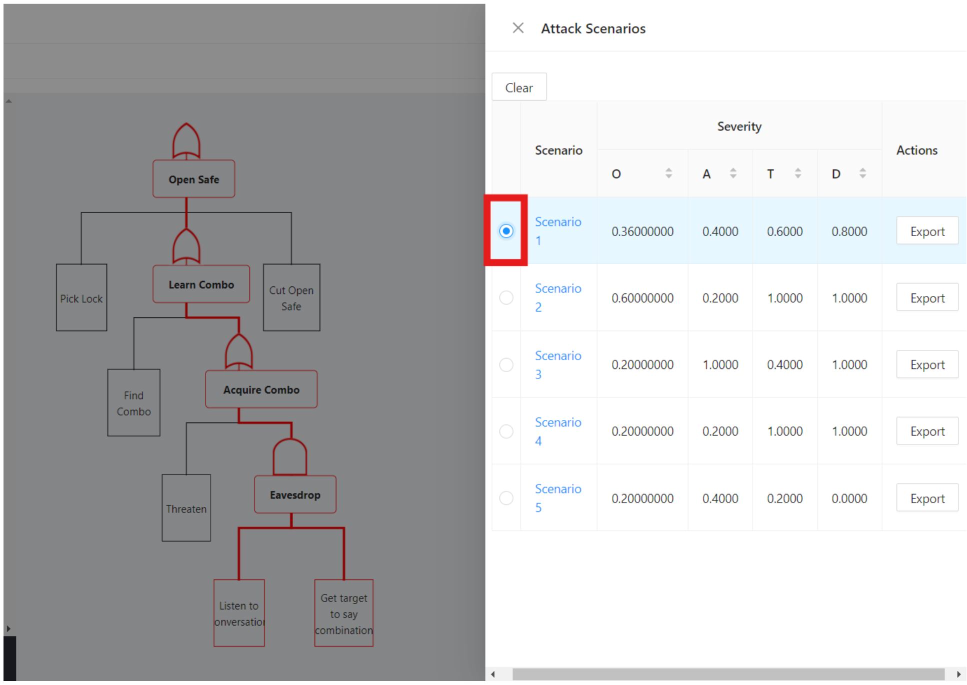
When an input attack tree is generated, the AT-AT tool also analyzes it to produce a list of all possible attack scenarios. This list can be accessed by clicking the “Show Scenarios” button:

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



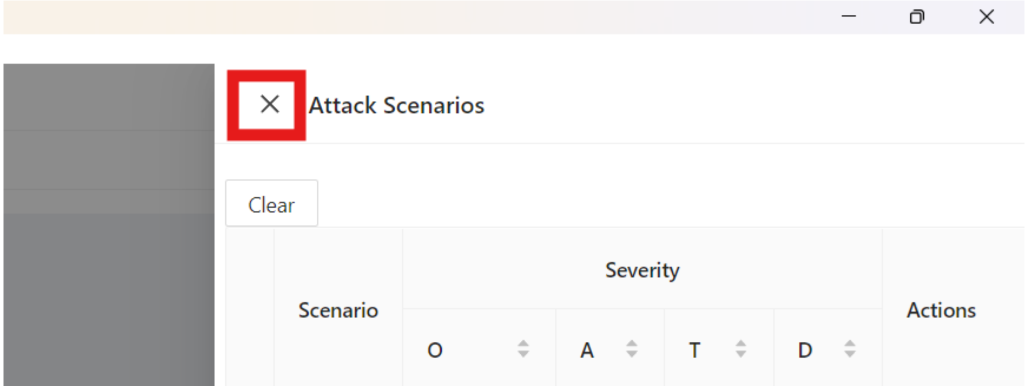
```
Open Safe;OR
    Pick Lock;o=0.6;a=0.2;t=1;d=1
    Learn Combo;OR
        Find Combo;o=0.2;a=0.2;t=1;d=1
        Acquire Combo;OR
            Threaten;o=0.2;a=0.4;t=0.2;d=0
            Eavesdrop;AND
                Listen to conversation;o=0.6;a=
                Get target to say combination;o=
    Cut Open Safe;o=0.2;a=1;t=0.4;d=1
```

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



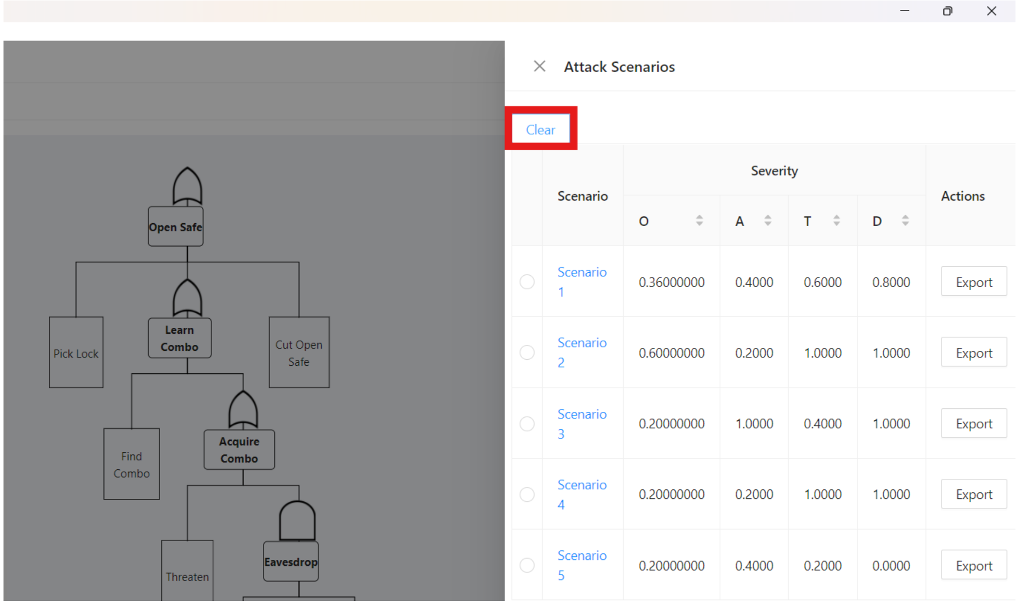
	Scenario	Severity				Actions
		O	A	T	D	
●	Scenario 1	0.36000000	0.4000	0.6000	0.8000	Export
○	Scenario 2	0.60000000	0.2000	1.0000	1.0000	Export
○	Scenario 3	0.20000000	1.0000	0.4000	1.0000	Export
○	Scenario 4	0.20000000	0.2000	1.0000	1.0000	Export
○	Scenario 5	0.20000000	0.4000	0.2000	0.0000	Export

3. 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.



	Scenario	Severity				Actions
		O	A	T	D	

4. To display the attack scenarios list again, click “Show Scenarios.”
5. To remove the highlighted scenario and return to the default view, click the “Clear” button.



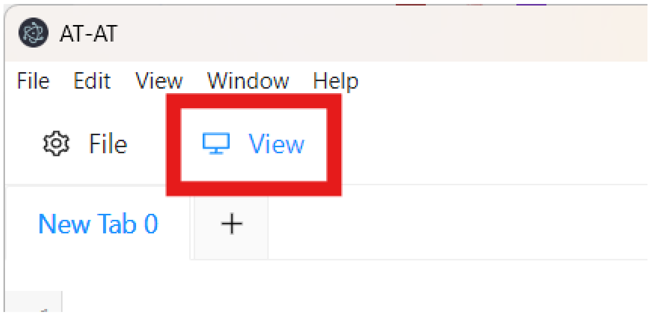
	Scenario	Severity				Actions
		O	A	T	D	
○	Scenario 1	0.36000000	0.4000	0.6000	0.8000	Export
○	Scenario 2	0.60000000	0.2000	1.0000	1.0000	Export
○	Scenario 3	0.20000000	1.0000	0.4000	1.0000	Export
○	Scenario 4	0.20000000	0.2000	1.0000	1.0000	Export
○	Scenario 5	0.20000000	0.4000	0.2000	0.0000	Export

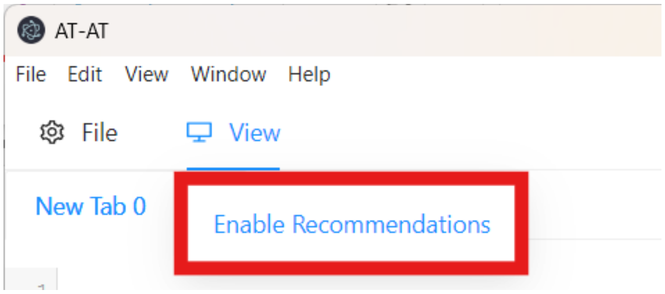
6. You can also select another scenario to be highlighted.

View Recommendations

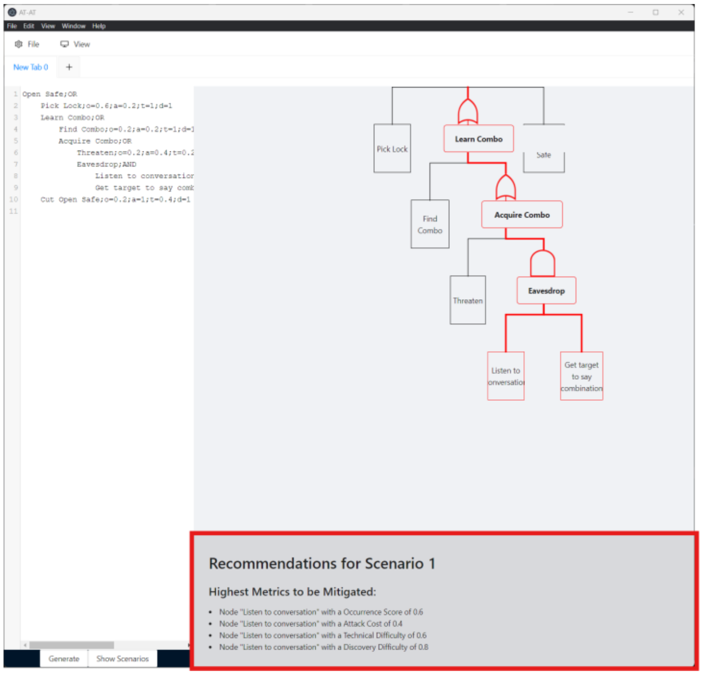
To view recommendations for an attack scenario, first ensure the scenario is selected. Then, you can follow the steps below to view the recommendations:

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





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



```
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
            Eavesdrop;AND
                Listen to conversatior
                Get target to say comk
    Cut Open Safe;o=0.2;a=1;t=0.4;d=1
```

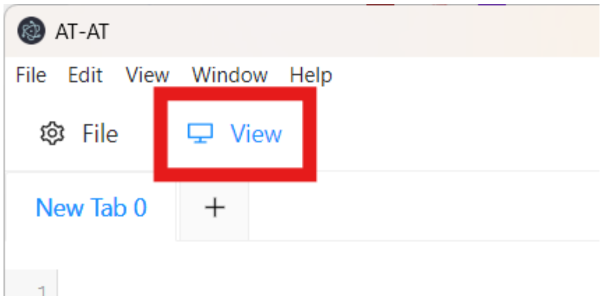
Recommendations for Scenario 1

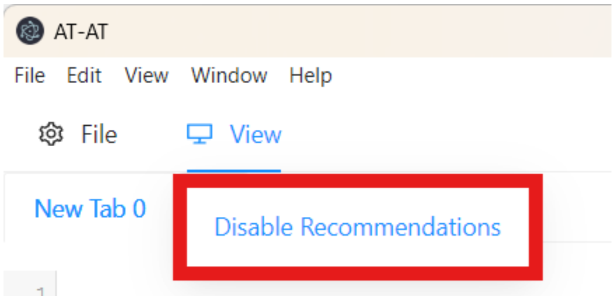
Highest Metrics to be Mitigated:

- Node "Listen to conversation" with a Occurrence Score of 0.6
- Node "Listen to conversation" with a Attack Cost of 0.4
- Node "Listen to conversation" with a Technical Difficulty of 0.6
- Node "Listen to conversation" with a Discovery Difficulty of 0.8

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.

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

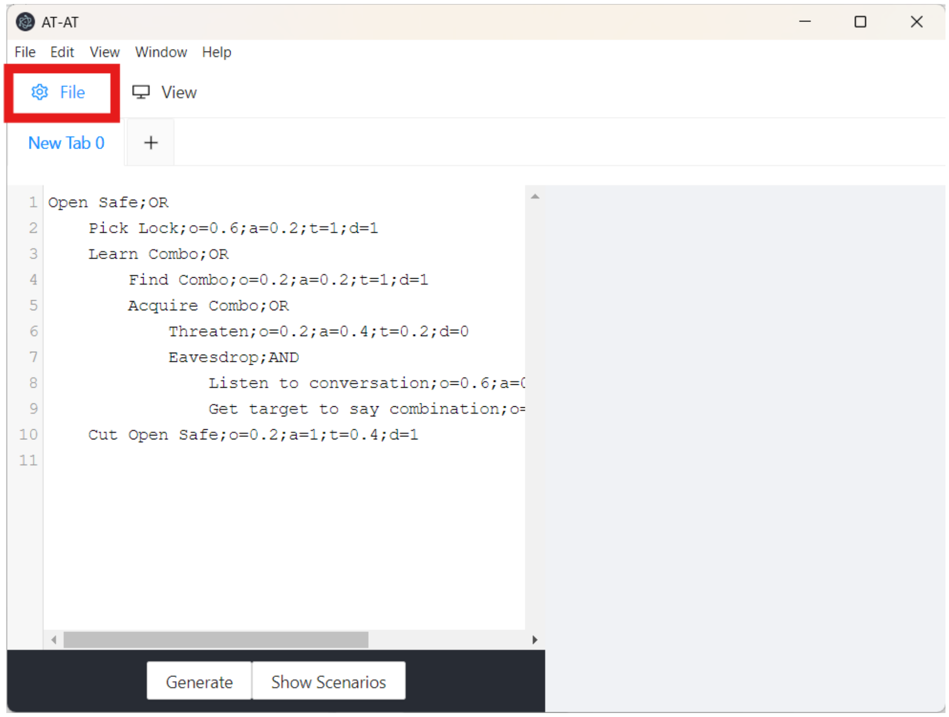




Export Report

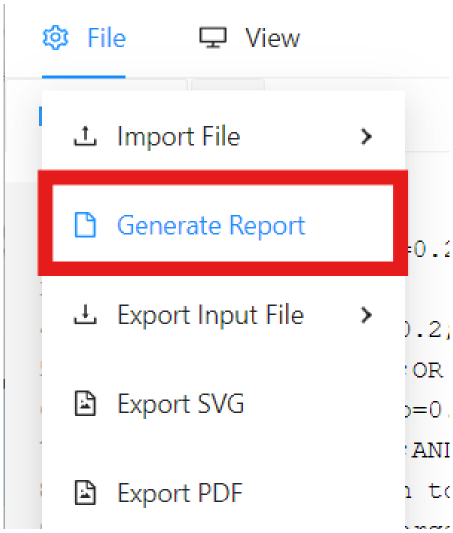
Users can export their generated tree and all its scenarios into an HTML file, making it convenient to save and access the attack tree and its analysis anytime. Here are the steps to export a report:

1. Click “File”

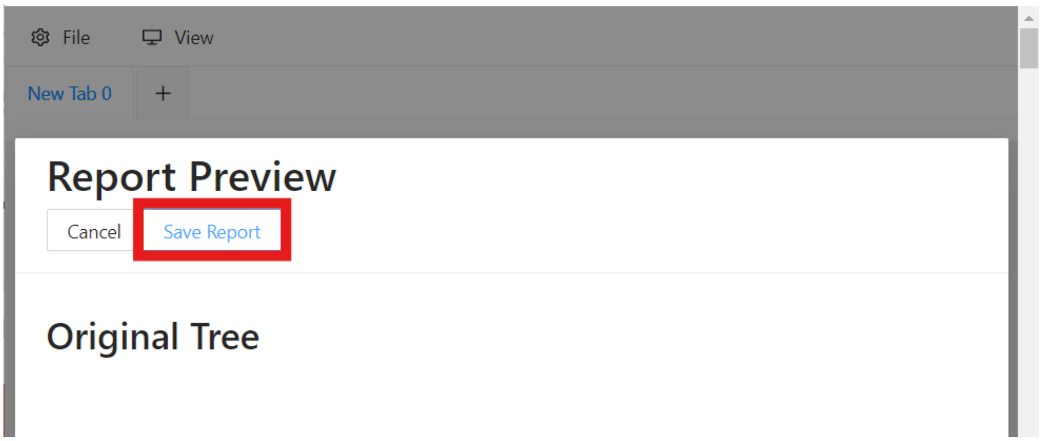


```
Open Safe;OR
    Pick Lock;o=0.6;a=0.2;t=1;d=1
    Learn Combo;OR
        Find Combo;o=0.2;a=0.2;t=1;d=1
        Acquire Combo;OR
            Threaten;o=0.2;a=0.4;t=0.2;d=0
            Eavesdrop;AND
                Listen to conversation;o=0.6;a=(
                Get target to say combination;o=
    Cut Open Safe;o=0.2;a=1;t=0.4;d=1
```

2. Select “Generate Report”



3. Click “Save Report”



Report Preview

Original Tree

4. Choose a destination folder
5. Ensure the filename ends with .html
6. Click “Save”

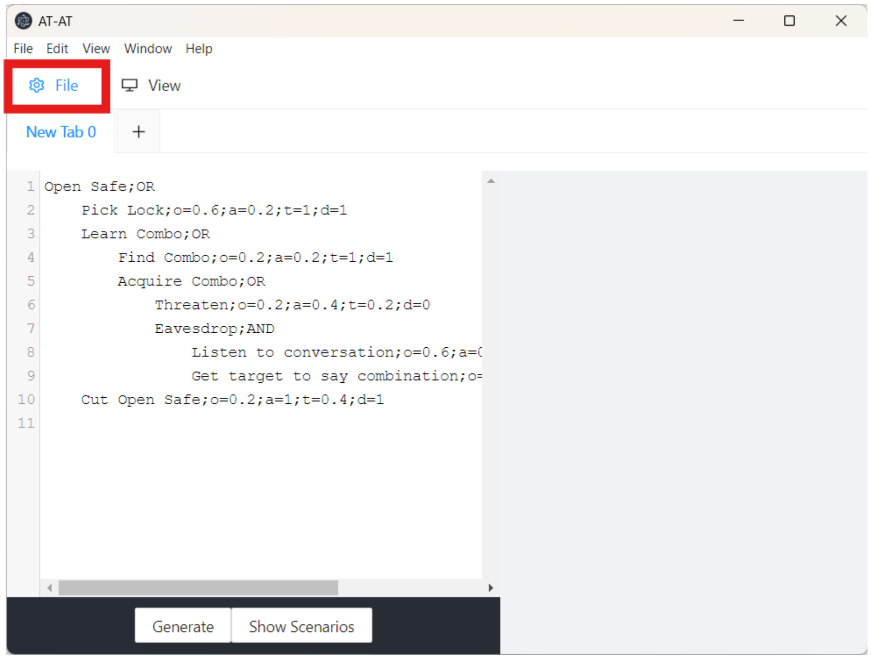
The report will be saved as an HTML file which can be opened by any web browser.

Export Input File

This tool allows users to export a tree to a DSL text file or a CSV file, which can then be imported later. A tree can be exported to either a DSL or CSV file regardless of whether the original text entered was in DSL or CSV format.

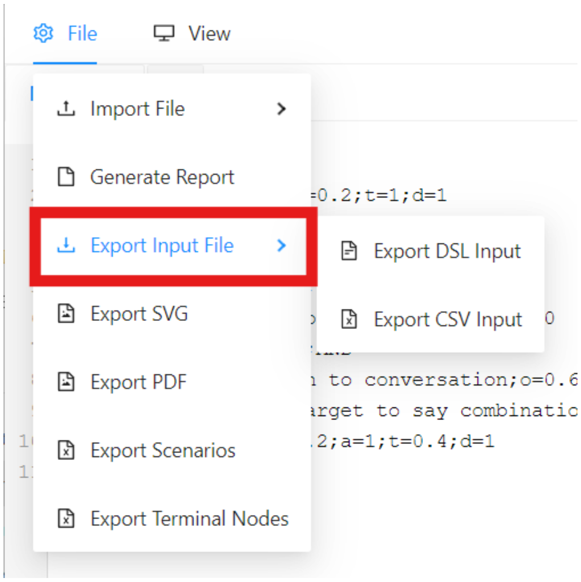
Follow these steps to export the tree to a DSL text file:

1. Click “File”

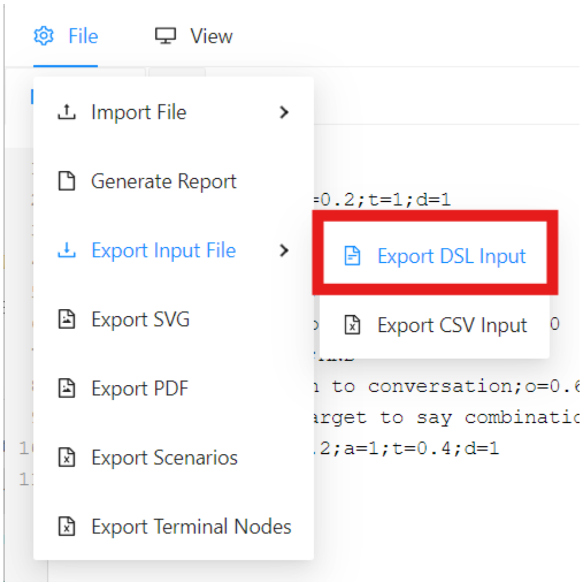


```
Open Safe;OR
    Pick Lock;o=0.6;a=0.2;t=1;d=1
    Learn Combo;OR
        Find Combo;o=0.2;a=0.2;t=1;d=1
        Acquire Combo;OR
            Threaten;o=0.2;a=0.4;t=0.2;d=0
            Eavesdrop;AND
                Listen to conversation;o=0.6;a=(
                Get target to say combination;o=
    Cut Open Safe;o=0.2;a=1;t=0.4;d=1
```

2. Click “Export Input File”



3. Select “Export DSL Input”

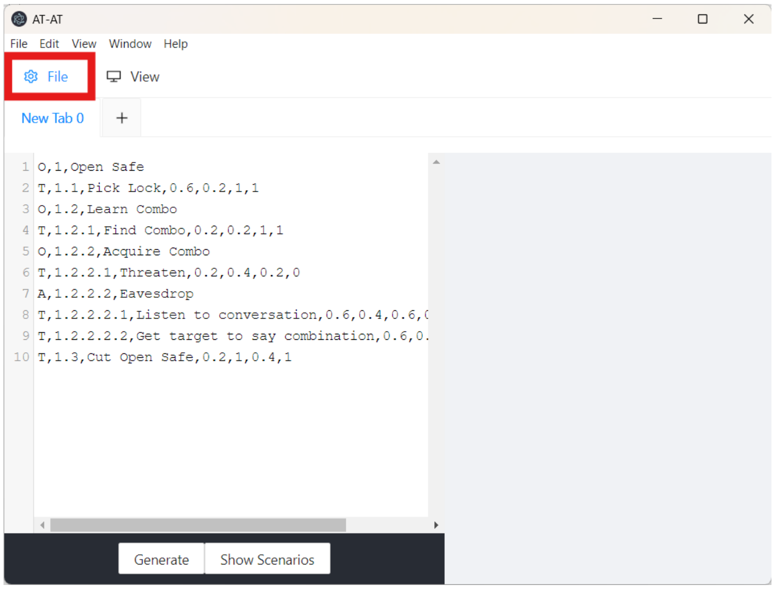


4. Choose a file name
5. Select a location
6. Click “Save”

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

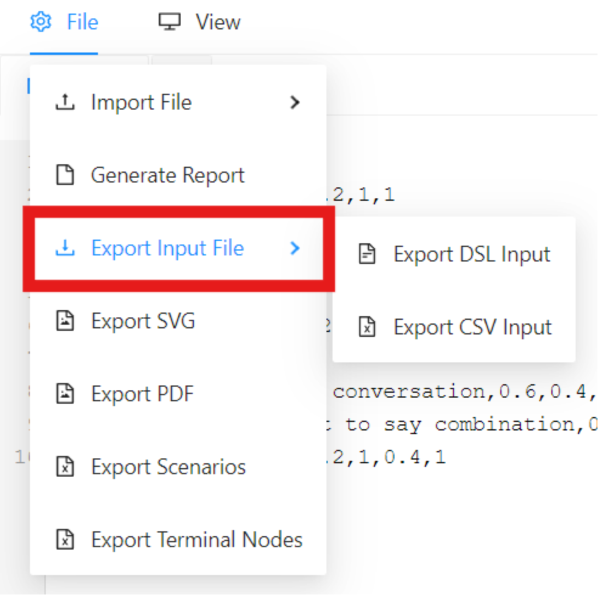
Follow these steps to export the tree to a CSV file:

1. Click “File”

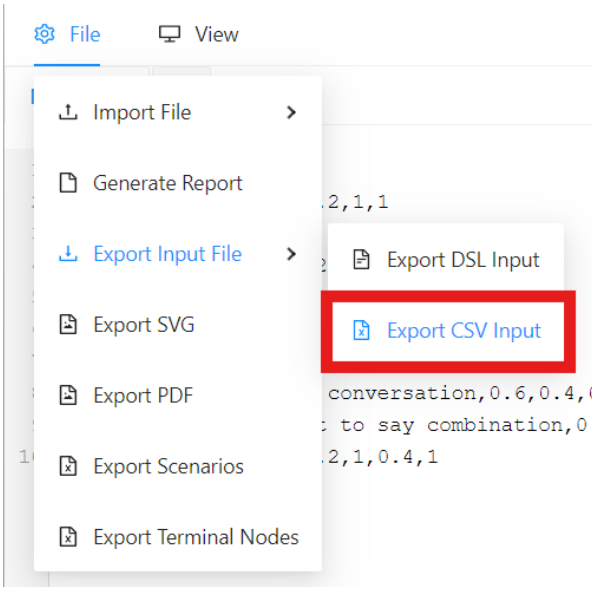


```
O,1,Open Safe
T,1.1,Pick Lock,0.6,0.2,1,1
O,1.2,Learn Combo
T,1.2.1,Find Combo,0.2,0.2,1,1
O,1.2.2,Acquire Combo
T,1.2.2.1,Threaten,0.2,0.4,0.2,0
A,1.2.2.2,Eavesdrop
T,1.2.2.2.1,Listen to conversation,0.6,0.4,0.6,
T,1.2.2.2.2,Get target to say combination,0.6,0.
T,1.3,Cut Open Safe,0.2,1,0.4,1
```

2. Click “Export Input File”



3. Select “Export CSV Input”



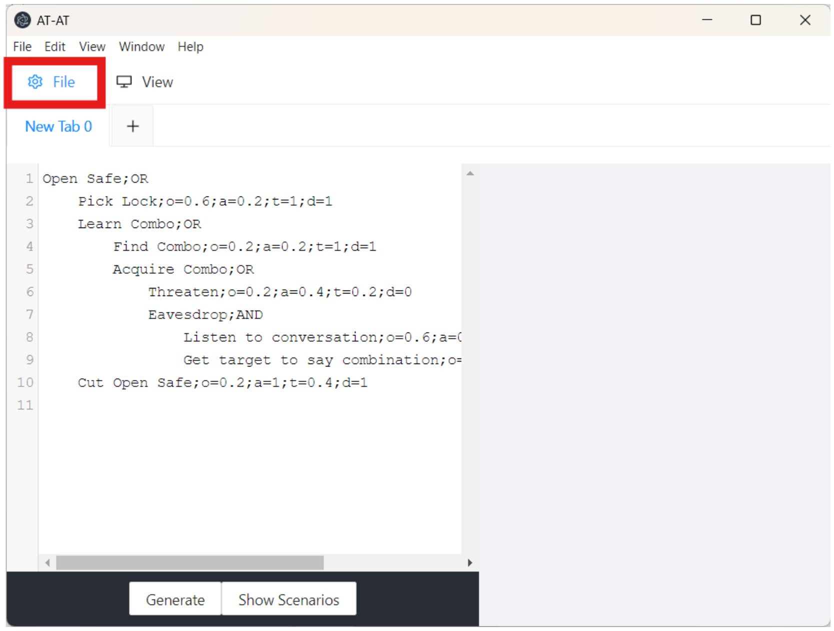
4. Choose a file name
5. Select a location
6. Click “Save”

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

Export Tree as SVG

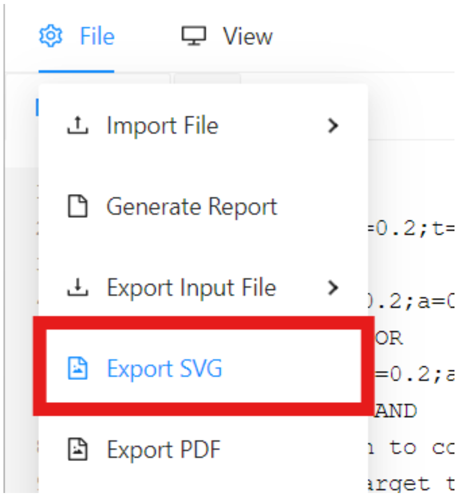
Users can export the visual representation of a generated tree as a SVG file, making it easy to save and access the attack tree. Here are the steps to export the tree as an SVG:

1. Click “File”



```
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=
                Get target to say combination;o=
    Cut Open Safe;o=0.2;a=1;t=0.4;d=1
```

2. Select “Export SVG”



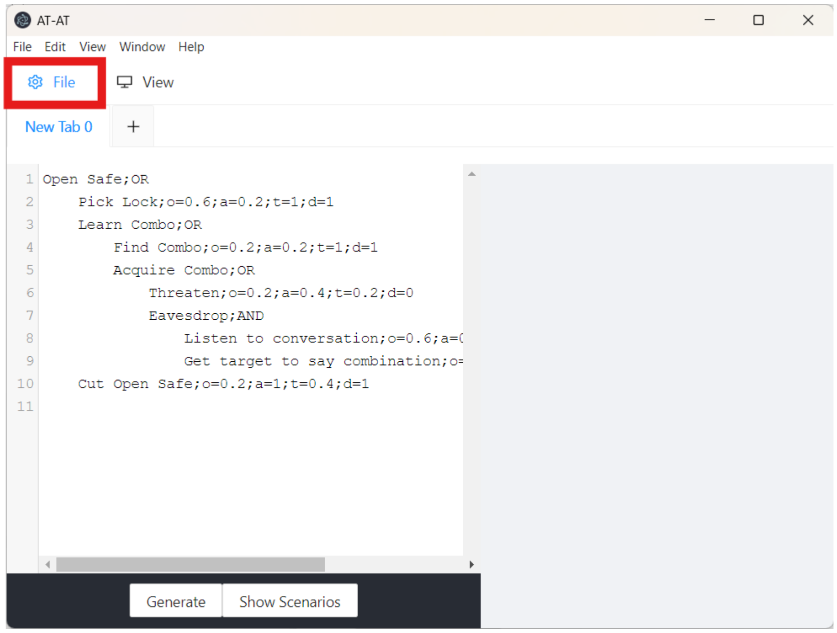
3. Choose a file name
4. Select a location
5. Click “Save”

The SVG file of the attack tree should now be generated and saved to the chosen location.

Export Tree as PDF

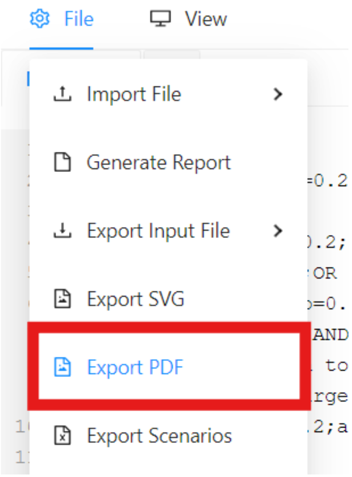
Users can export the visual representation of a generated tree as a PDF file. Here are the steps to export the tree as PDF:

1. Click “File”



```
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=
                Get target to say combination;o=
    Cut Open Safe;o=0.2;a=1;t=0.4;d=1
```

2. Select “Export PDF”



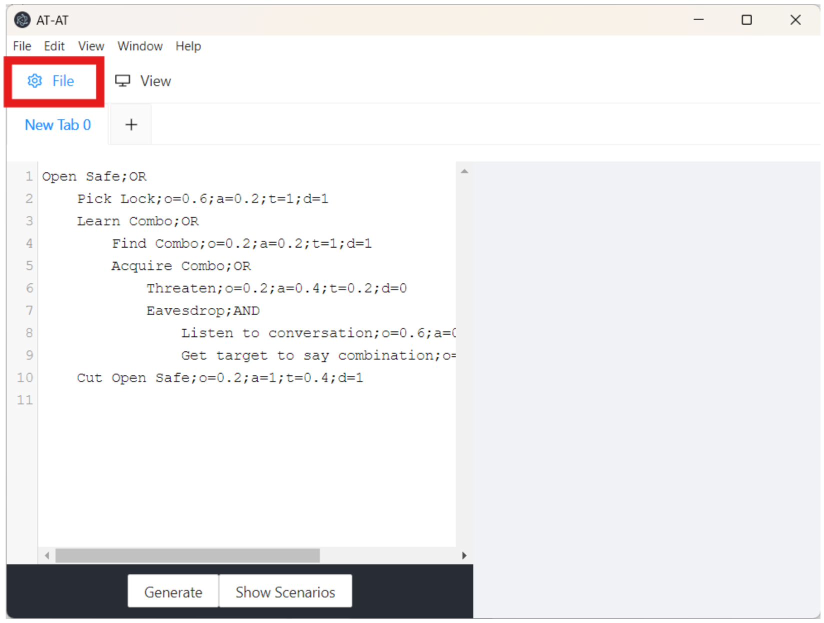
3. Choose a file name
4. Select a location
5. Click “Save”

The PDF file of the attack tree should now be generated and saved to the chosen location.

Export Scenarios

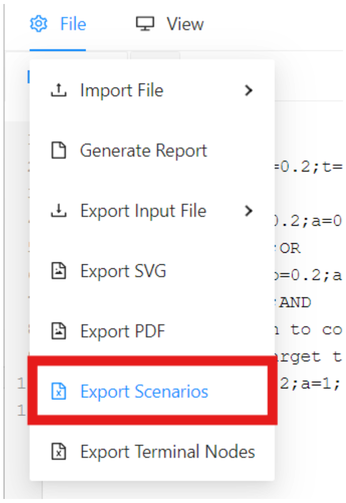
Users can export the list of scenarios, including their metrics and terminal nodes, to analyze the scenarios of a tree. Here are the steps to export a file with a list of the scenarios:

1. Click “File”



```
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=(
                Get target to say combination;o=
    Cut Open Safe;o=0.2;a=1;t=0.4;d=1
```

2. Select “Export Scenarios”



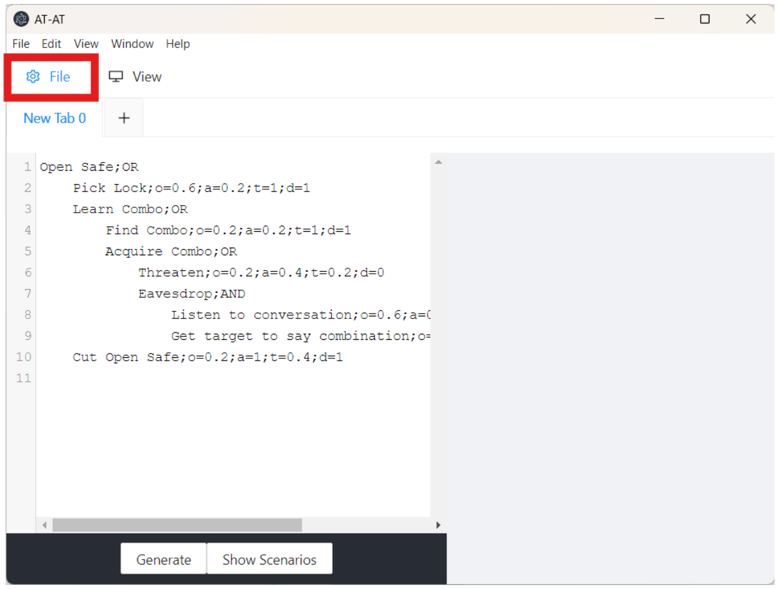
3. Choose a file name
4. Select a location
5. Click “Save”

The CSV file with the list of scenarios should be generated and saved to the chosen location.

Export Terminal Nodes

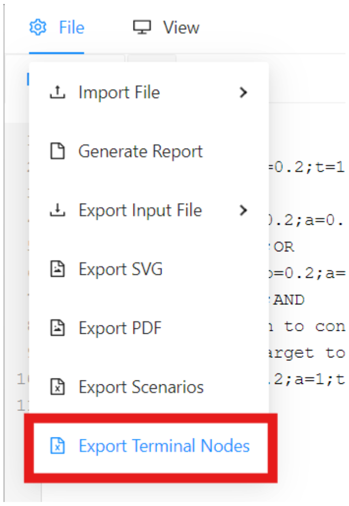
Users can export the list of terminal nodes of a tree to review the nodes and their metrics. Here are the steps to export a file listing the terminal nodes of a tree:

1. Click “File”



```
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=(
                Get target to say combination;o=
    Cut Open Safe;o=0.2;a=1;t=0.4;d=1
```

2. Select “Export Terminal Nodes”



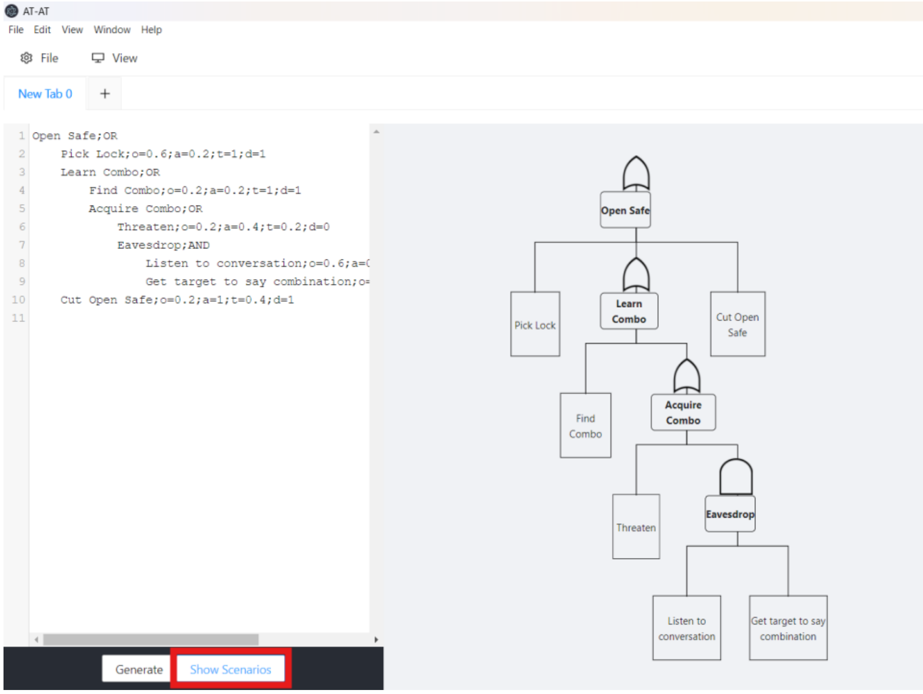
3. Choose a file name
4. Select a location
5. Click “Save”

The CSV file with the list of terminal nodes should be generated and saved to the chosen location.

Export Scenario Report

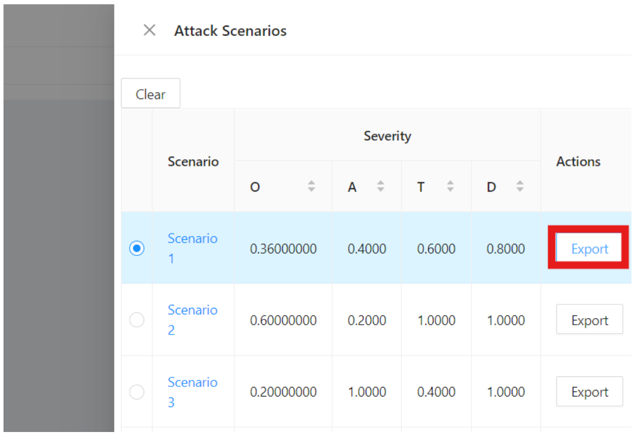
Users can export a scenario report to view the visual representation of the scenario and the list of the terminal nodes in the scenario. Here are the steps to export a report of a scenario:

1. Click "Show Scenarios"



```
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=
                Get target to say combination;o=
    Cut Open Safe;o=0.2;a=1;t=0.4;d=1
```

2. Select the "Export" button in the Actions column of the scenario you want the report of



	Scenario	Severity				Actions
		O	A	T	D	
●	Scenario 1	0.36000000	0.4000	0.6000	0.8000	Export
○	Scenario 2	0.60000000	0.2000	1.0000	1.0000	Export
○	Scenario 3	0.20000000	1.0000	0.4000	1.0000	Export

3. Choose a file name
4. Select a location
5. Click "Save"

The PDF report of the scenario should now be generated and saved to the chosen location.