Attack Scenarios Tested

1. Data Manipulation (DM) in `stNum` & `sqNum`

Overview:

This test case involved injecting GOOSE messages with abnormally high values for the state number (stNum) and sequence number (sqNum). The purpose was to evaluate the IDS's ability to detect anomalous increments that deviate significantly from the normal progression.

Execution:

The script modified the GOOSE messages by setting stNum and sqNum to high values far beyond typical operational ranges.

2. Data Manipulation (DM) in `stNum`, `sqNum`, and `bool`

Overview:

This test case involved direct manipulation of the stNum, sqNum, and boolean data within the GOOSE messages. The aim was to see how well the IDS could detect a combination of multiple manipulated fields.

Execution:

The script simultaneously modified stNum, sqNum, and boolean data in the GOOSE messages.

3. Data Manipulation in `stNum`, `sqNum`, and `GOOSE Length`

Overview:

This test case focused on manipulating stNum, sqNum, and the length of the GOOSE message. The objective was to test the IDS's ability to detect

inconsistencies in multiple parameters, including the overall message length.

Execution:

The script adjusted stNum, sqNum, and modified the length of the GOOSE message to create an anomalous packet.

4. Data Manipulation in `GOOSE Length`

Overview:

This test case isolated the manipulation to the length of the GOOSE message. The purpose was to see if the IDS could detect anomalies based solely on the length of the messages.

Execution:

The script modified the length field of the GOOSE messages without altering any other parameters.

5. Data Manipulation in `sqNum` , `stNum` , `bool` & `Goose Length`

Overview:

In this test case, the focus was on manipulating all the important parameters of Goose message. The goal was to evaluate the IDS's sensitivity to changes in these sequence-related parameters.

Execution:

The attack script modified sqNum , stNum, boolean and goose length values in the GOOSE messages.

Impact

In all test cases mentioned above, the IDS has successfully detected the manipulations.

Conclusion

The IDS algorithm demonstrated robust detection capabilities across a variety of test cases, successfully identifying all simulated attacks. The comprehensive testing, including manipulation of individual and multiple fields, confirmed the IDS's effectiveness in safeguarding the real-time system against various types of GOOSE message anomalies.