Filename: _6_best_model_prediction.ipynb
Title: XG Boost - Testing the best model with user input
Author: Raghava | GitHub: @raghavtwenty
Date Created: June 10, 2023 | Last Updated: May 13, 2024
Language: Python | Version: 3.10.14, 64-bit

XG Boost Chosen over other models.
It has the highest accuracy & performance metrics.
XG Boost is more robust to over fitting,
Highly scalable and suitable for large datasets
compared to Random forest.

Importing required libraries

In [2]:

```python
import xgboost as xgb
import numpy as np
from joblib import load
from _2_scale_transform import transform_new_input
```

Load the XGBoost model

In [3]:

```python
model = xgb.Booster()
model.load_model("../models/m3_xg_boost.model")
```

User input prediction

In [4]:

```python
def user_input_predict(user_input):

    user_input_result = model.predict(user_input)
    user_input_result = np.argmax(user_input_result)

    result_msg = ""
    result_msg_info = ""

    if user_input_result == 0:
        result_msg = "NORMAL, No possibility of attack."
        result_msg_info = "You are safe!"

    elif user_input_result == 1:
        result_msg = "Higher Possibility of BLACKHOLE attack."
        result_msg_info = "Information : BLACKHOLE attacks occur when a rout

    elif user_input_result == 2:
        result_msg = "Higher Possibility of TCP-SYN attack."
        result_msg_info = "Information : A SYN flood (half-open attack) is a

    elif user_input_result == 3:
        result_msg = "Higher Possibility of PORTSCAN attack."
        result_msg_info = "Information : A port scan is an attack that sends
    elif user_input_result == 4:
        result_msg = "Higher Possibility of DIVERSION attack."
        result_msg_info = "Information : Diversion/Social engineering is an
    else:
        result_msg = "Try Again"
        result_msg_info = "Choose different values."

    return result_msg, result_msg_info
```

Test user input

In [20]:

```
user_input = [[2, 1733, 37865130, 38063670, 3187, 2152, 0, 556, 5, 3, 0, 4,
```

Preprocessing input

In [21]:

```
user_input = np.array(user_input)
user_input = transform_new_input(user_input)
user_input = xgb.DMatrix(user_input)
```

Prediction

In [22]:

```
res_msg, res_info = user_input_predict(user_input)
print(res_msg)
print(res_info)
```

```
Higher Possibility of DIVERSION attack.
Information : Diversion/Social engineering is an attack vector that relies h
eavily on human interaction and often involves manipulating people into brea
king normal security procedures and best practices to gain unauthorized acce
ss to systems, networks or physical locations or for financial gain. Spoofin
g, Phishing falls into this category.
```