SCE Tech Fest 25
Innovation Sustainability Community

SE – A – 14

Software Engineering

Students: Shay Hahiashvili | Maxim Subotin
Advisor: Ms. Alona Kutsyy

SCE
SHAMOON COLLEGE OF ENGINEERING

Anomaly Based Detection

We developed two SVM models designed to classify network cyberattacks in real time. The first model targets the detection of Port Scanning and DoS attacks, while the second identifies DNS Tunneling. In our approach we applied a unique traffic segmentation method and robust feature selection, along with K-Fold cross-validation to ensure model reliability and generalization. This enabled both models to achieve real-time detection capabilities with a remarkable 100% accuracy.

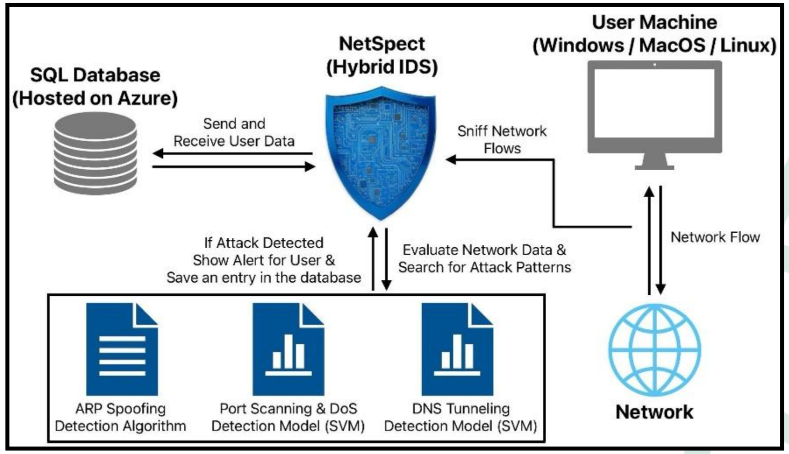
Signature Based Detection

We developed a unique algorithm capable of detecting ARP Spoofing attacks in real time across multiple subnets. The algorithm incorporates an authentication mechanism for each IP-MAC address pair within every subnet, enabling accurate identification of both IP-to-MAC and MAC-to-IP anomalies. Furthermore, it intelligently adapts to legitimate network changes, such as DHCP lease renewals for dynamic IP addresses. As a result, our algorithm delivers real-time detection with high accuracy and is resistant to false positives.

GitHub

NetSpect

Hybrid Intrusion Detection System



Collection Methods

- ❖ Collected network traffic from home networks and the SCE campus.
- ❖ Simulated DNS traffic using custom scripts.
- ❖ Generated attack datasets from small samples via feature correlation and randomization.
- ❖ Applied Round-Robin segmentation to organize packets into flows.
- ❖ Flows: (src_ip, src_mac, dst_ip, dst_mac, protocol)

Main Features

Real Time Detection, Data Collection, Download Reports, Filter Previous Alerts by Year, Visual Analytics, Tray Icon Notifications, Light/Dark Modes, Integrated Logger, etc.

Datasets

UDP & TCP 393,000 → Featuring: number of ports, SYN flag count, packets per second, IATs, etc.

DNS 360,000 → Featuring: TXT record count, number of unique sub domains, DF flag count, etc.

SCE Tech Fest 25
Innovation Sustainability Community

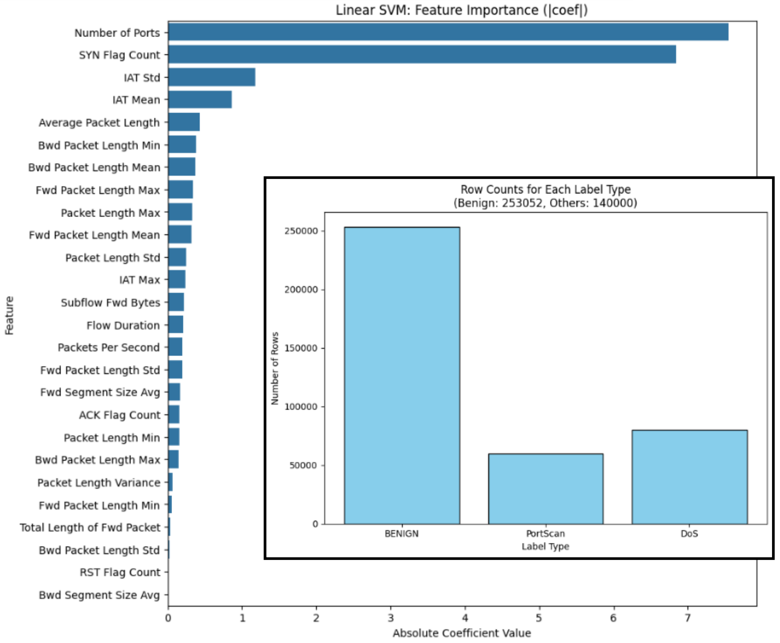
SE – A – 14

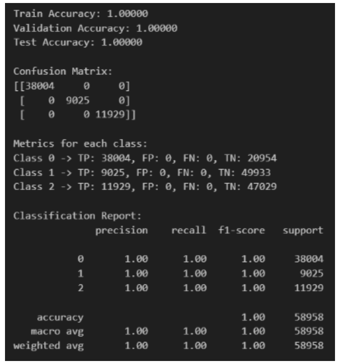
Software Engineering

Students: Shay Hahiashvili | Maxim Subotin
Advisor: Ms. Alona Kutsyy

SCE
SHAMOON COLLEGE OF ENGINEERING

Port Scan & DoS Results



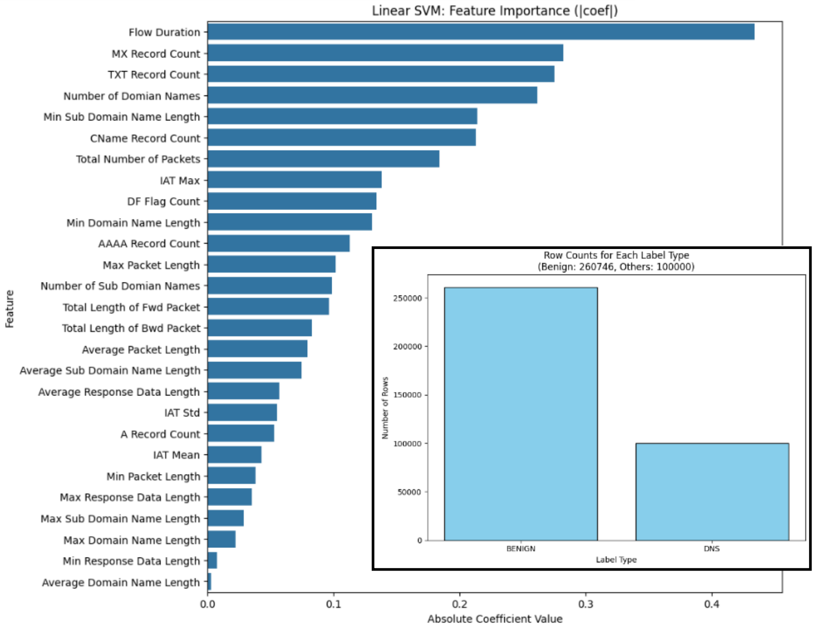


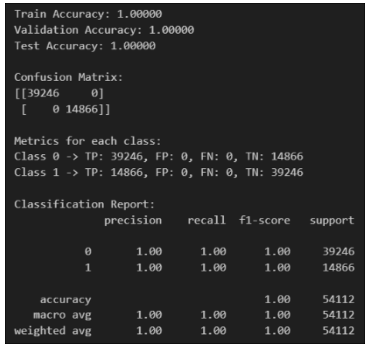
```
Train Accuracy: 1.00000
Validation Accuracy: 1.00000
Test Accuracy: 1.00000

Confusion Matrix:
[[38004     0     0]
 [    0  9025     0]
 [    0     0 11929]]

Metrics for each class:
Class 0 -> TP: 38004, FP: 0, FN: 0, TN: 20954
Class 1 -> TP: 9025, FP: 0, FN: 0, TN: 49933
Class 2 -> TP: 11929, FP: 0, FN: 0, TN: 47029

Classification Report:
              precision    recall  f1-score   support

           0       1.00      1.00      1.00     38004
           1       1.00      1.00      1.00      9025
           2       1.00      1.00      1.00     11929

    accuracy                           1.00     58958
   macro avg       1.00      1.00      1.00     58958
weighted avg       1.00      1.00      1.00     58958
```

Port Scanning - DoS SVM Model K-Fold Cross Validation :

Fold	Train Accuracy	Validation Accuracy	Precision	Recall	F1-Score	Samples
1	1.0000	1.0000	1.00	1.00	1.00	25,436
2	1.0000	1.0000	1.00	1.00	1.00	25,436
3	1.0000	1.0000	1.00	1.00	1.00	25,436
4	1.0000	1.0000	1.00	1.00	1.00	25,436
5	1.0000	1.0000	1.00	1.00	1.00	25,436
6	1.0000	1.0000	1.00	1.00	1.00	25,436
7	1.0000	1.0000	1.00	1.00	1.00	25,435
8	1.0000	1.0000	1.00	1.00	1.00	25,435
9	1.0000	1.0000	1.00	1.00	1.00	25,435
10	1.0000	1.0000	1.00	1.00	1.00	25,435

DNS Tunneling Results





```
Train Accuracy: 1.00000
Validation Accuracy: 1.00000
Test Accuracy: 1.00000

Confusion Matrix:
[[39246     0]
 [    0 14866]]

Metrics for each class:
Class 0 -> TP: 39246, FP: 0, FN: 0, TN: 14866
Class 1 -> TP: 14866, FP: 0, FN: 0, TN: 39246

Classification Report:
              precision    recall  f1-score   support

           0       1.00      1.00      1.00     39246
           1       1.00      1.00      1.00     14866

    accuracy                           1.00     54112
   macro avg       1.00      1.00      1.00     54112
weighted avg       1.00      1.00      1.00     54112
```

DNS SVM Model K-Fold Cross Validation :

Fold	Train Accuracy	Validation Accuracy	Precision	Recall	F1-Score	Samples
1	1.0000	1.0000	1.00	1.00	1.00	25,253
2	1.0000	1.0000	1.00	1.00	1.00	25,253
3	1.0000	1.0000	1.00	1.00	1.00	25,252
4	1.0000	1.0000	1.00	1.00	1.00	25,252
5	1.0000	1.0000	1.00	1.00	1.00	25,252
6	1.0000	1.0000	1.00	1.00	1.00	25,252
7	1.0000	1.0000	1.00	1.00	1.00	25,252
8	1.0000	1.0000	1.00	1.00	1.00	25,252
9	1.0000	1.0000	1.00	1.00	1.00	25,252
10	1.0000	1.0000	1.00	1.00	1.00	25,252

Conclusions

In conclusion, our project successfully delivered a **real-time IDS** capable of accurately identifying **four critical types of network cyber attacks**: Port Scanning, DoS, ARP Spoofing, and DNS Tunneling through an optimized, multi-threaded solution integrating detection algorithms and machine learning models. By addressing the **limitations of existing datasets** through manual data collection, the system achieves **high accuracy with minimal false positives**, offering a reliable and user-friendly solution for modern network security challenges.