Intrusion Detection System Using Deep Learning

Keerthi, Mandeep, Sandip

IDS

Mandatory line of defense to protect critical networks against the ever-increasing issues of intrusive activities.

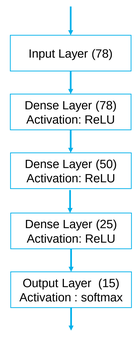
USP

- Real world DL based problem modelling
- Potential to evaluate existing signature based methods for efficiency and performance.
- Potential to become foundation for more advanced game theoretic approach based IDS

Model

DNN

- Input Layer : 78 inputs
- 3 Hidden Layers : 78, 50 and 25 neurons
- Output Layer : 15 neurons
- 11,777 trainable parameters
- Activation function
- Hideen Layers: RELU
- Output layer: Softmax
- Loss Function: Categorical cross- entropy



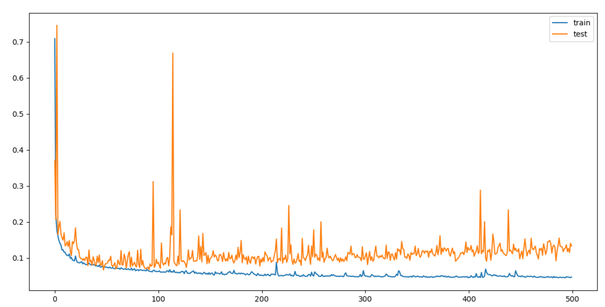
Data Set

- CICIDS2017 - https://www.unb.ca/cic/datasets/ids-2017.html
- Latest available data set – addresses short coming of currently available other IDS data sets like KDD Cup 1999 and NSL KDD 2009
- The generated attack diversity includes the most common attacks based on the 2016 McAfee report
- Around 80 network flow features
- In this project we are using 78 flow features

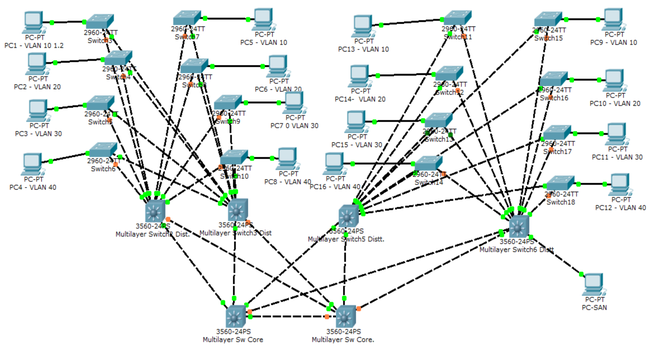
Train and Test data

Category	Training samples	Test Samples
BENIGN	528911	22501
FTP-Patator	6938	1000
SSH-Patator	4897	1000
DoS slowloris	4796	1000
DoS Slowhttptest	230073	1000
DoS GoldenEye	4499	1000
DoS Hulk	9293	1000
Heartbleed	6	5
Web Attack XSS	352	300
Web Attack Sql Injection	11	10
Web Attack Brute Force	1007	500
Infiltration	21	15
Bot	966	1000
PortScan	127027	1000
DDoS	157930	1000
Total	1076727	32331

Loss vs Epoch



Live Topology



Results

Category	Precision	Recall	F1 Score	Support
BENIGN	0.98	1.00	0.99	22501
FTP-Patator	1.00	0.99	1.00	1000
SSH-Patator	0.96	1.00	0.98	1000
DoS slowloris	0.93	0.99	0.96	1000
DoS Slowhttptest	1.00	0.93	0.96	1000
DoS GoldenEye	0.98	0.94	0.96	1000
DoS Hulk	1.00	1.00	1.00	1000
Heartbleed	1.00	0.80	0.89	5
Web Attack XSS	0.70	0.05	0.10	300
Web Attack Sql Injection	0.00	0.00	0.00	10
Web Attack Brute Force	0.57	0.98	0.72	500
Infiltration	1.00	0.07	0.12	15
Bot	1.00	0.67	0.80	1000
PortScan	0.99	0.91	0.95	1000
DDoS	0.99	0.98	0.99	1000

Binary Classification

	Precision	Recall	F1-Score
BENIGN	0.98	1.00	0.99
Attack	1.00	0.96	0.98

Future Extension

- **CNN**
- **RNN**
- **SMOTE**
- **LIVE data generation with attacks**

References

- Iman Sharafaldin, Arash Habibi Lashkari, and Ali A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization”, 4th International Conference on Information Systems Security and Privacy (ICISSP), Portugal, January 2018
- N. Shone, T. N. Ngoc, V. D. Phai and Q. Shi, ”A Deep Learning Approach to Network Intrusion Detection,” in IEEE Transactionson Emerging Topics in Computational Intelligence, vol.2, no.1, pp.41-50, Feb.2018.
- C. Yin, Y. Zhu, J. Fei and X. He, ”A Deep Learning Approach for Intrusion Detection Using RecurrentNeural Networks”, in IEEE Access, vol. 5, pp. 21954-21961, 2017
- https://www.unb.ca/cic/datasets/ids-2017.html