UNB

Intrusion Detection System for DOS attack with focus on Slowloris attack type

Nasim Maleki

Network Security

Fall 2017

Canadian Institute for Cybersecurity (CIC)

DOS attack

Requests from one host to make the server/destination inaccessible!

- **UDP Flood**, sending requests to the ports not listening
- **ICMP Flood** (ping)
- **SYN Flood**, Sending TCP SYN Request with spoofed IP
- **Slowloris**, Sending requests to port 80(HTTP)
- **Ping of death**, Sending request with packet size >1500 byte and it has malformed fragmentations!

Solution to detect DOS!

- Features
  - Maximum number of connections **from the same source IP** address(source) in a fixed interval (in this experiment I used 10 seconds)
  - Maximum Number of connections **to the same service and protocol** in a fixed time interval from the **same IP address.(It may intend to break only one application)**
  - **Number of zero-sized packets\number of connections** in a fixed time interval

Related Jobs!

- **Activity Profiling,** packet rates of outbound or inbound flow and monitoring individual clustered flows and increasing activity among clusters means abnormality
- **Sequential change point detection,** first storing the raw flow as a time series and clusters are represented by time-domain and by calculating cusum(statistics methods) if any deviation happened to time series it detects it as an attack
- **Machine learning approaches,** In this technique it classified different type of DoS attack like(Smurf,Teardrop,…) and considered different features for each of them and trained the machine with different machine learning methods(BayesNet,Logistic,…)

Method

1. Packet sniffing , Virtual network made
2. Making a dataset based on the mentioned features (around 13000 records) and labeling them
3. For rule based we need threshold, so I used machine learning methods
4. Using ID3 classification to train the machine
5. Using the classifier in real time detection for incoming packets
6. Instead using classifier in step 3, we can extract the rules from ID tree visualized and used these rules to detect faster!
7. It can detect Slowloris attack in its first 10 – 20 seconds

Experiment

- A virtual network is made to run slowloris attack besides that the host is also connected to the internet to have incoming an outgoing legitimate packets
- It can detect the slowloris attack in its first 10 seconds!

Attachments

All data sets as a training set and the final tree which is visualized are attached to this file .

One hour output is also attached.

Questions?