Possible Viewpoints on Network Flow Data in CIC-IDS2018

Jonas Ferdigg

November 9, 2020

Contents

1 Attacks

Cyber attacks as listed on UNB CSE-CIC-IDS2018 [1]

- **Bruteforce attack**
  - FTP – Patator
  - SSH – Patator
- **DoS attack**
  - Hulk
  - GoldenEye
  - Slowloris
  - Slowhttptest
  - Heartleech
- **Web attack**
  - Damn Vulnerable Web App (DVWA)
  - In-house selenium framework (XSS and Brute-force)
- **Infiltration attack**
  - First level: Dropbox download in a windows machine
  - Second Level: Nmap and portscan
- **Botnet attack**
  - Ares (developed by Python)
    - remote shell
    - file upload/download
    - capturing
  - Screenshots and key logging
- **DDoS attack + PortScan**
  - Low Orbit Ion Canon (LOIC)
    - UDP
    - TCP
    - HTTP

2 Viewpoints

In this section I am discussing different viewpoints on the network flow and which advantages and disadvantages they might have when detecting different kinds of attacks. This includes looking at the features available from each viewpoint, which attacks are best visible from which viewpoint and how feasible are the methods in terms of resource utility when training the network and when applying it for IDS.

short	**Definition**
min	Smallest value that has been occurred
max	Biggest value that has been occurred
mean	Mean value over a specific range of values
stdev	Standard deviation
num	Aggregated number of occurrences
one	One-hot representation
var	Variance of the feature

Table 1: Definition of flow prefixes

2.1 SourceIP Aggregates

2.1.1 Available Features

- num_packetCount
- var_packetsPerChannel
- num_octetCount
- var_octetsPerChannel
- num_uniqueSourcePorts
- num_uniqueDestIpAddr
- num_uniqueDestPorts
- min_interPacketTime
- max_interPacketTime
- mean_interPacketTime
- stdev_interPacketTime
- num_tcpSyn
- num_tcpAck
- num_tcpFin

2.2 Channel Aggregates

2.2.1 Available Features

- num_packetCount
- var_packetsPerDestPort

- num_octetCount
- var_octetsPerDestPort
- num_uniqueSourcePorts
- num_uniqueDestPorts
- min_interPacketTime
- max_interPacketTime
- mean_interPacketTime
- stdev_interPacketTime
- num_tcpSyn
- num_tcpAck
- num_tcpFin

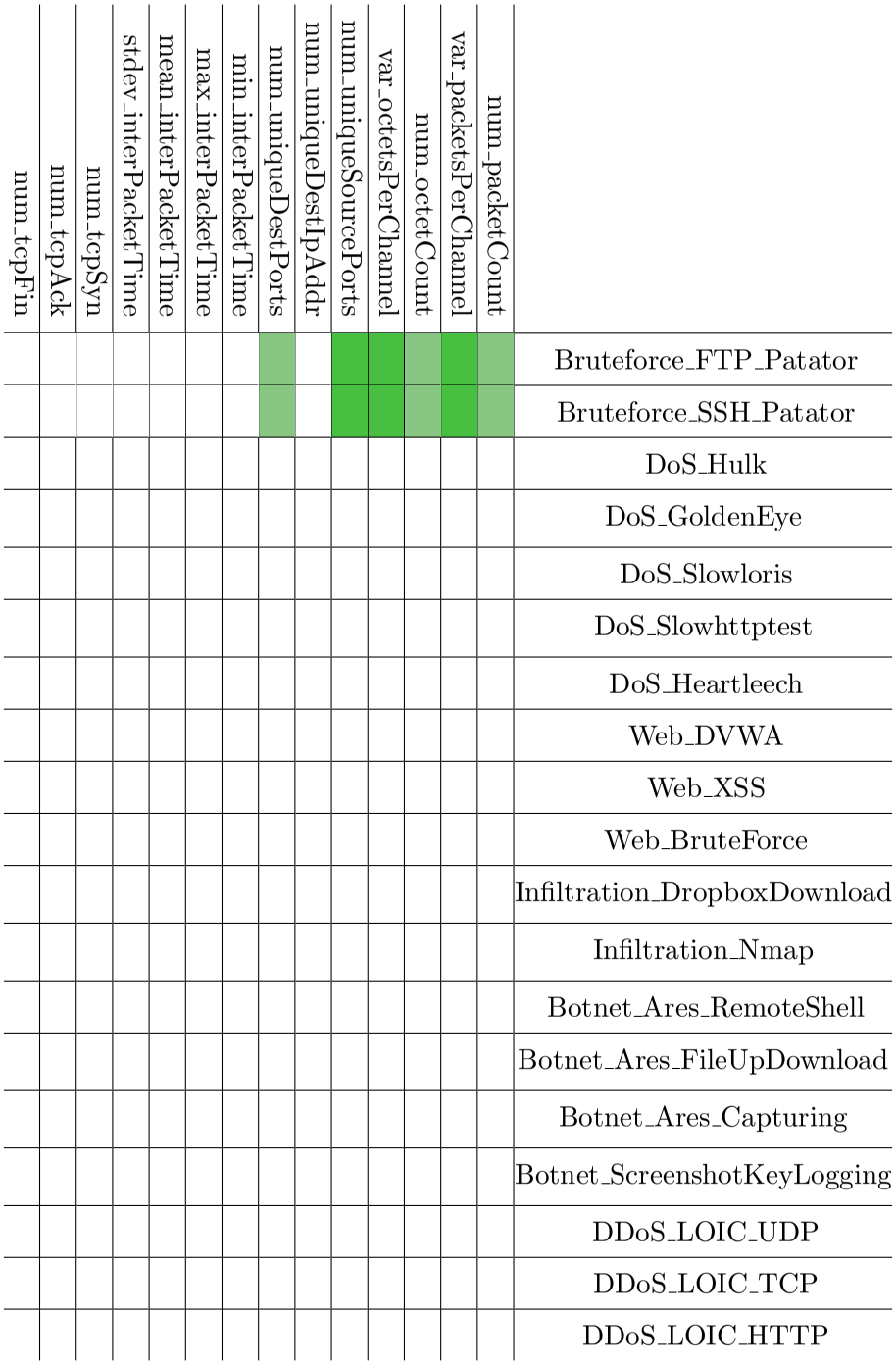
2.3 Socket Aggregates

2.3.1 Available Features

- num_packetCount
- num_octetCount
- min_interPacketTime
- max_interPacketTime
- mean_interPacketTime
- stdev_interPacketTime
- num_tcpSyn
- num_tcpAck
- num_tcpFin

3 Feature-Attack Correlation

3.1 SourceIP Aggregate Features


num_tcpFin
num_tcpAck
num_tcpSyn
stdev_interPacketTime
mean_interPacketTime
max_interPacketTime
min_interPacketTime
num_uniqueDestPorts
num_uniqueDestIpAddr
num_uniqueSourcePorts
var_octetsPerChannel
num_octetCount
var_packetsPerChannel
num_packetCount
Bruteforce_FTP_Patator
Bruteforce_SSH_Patator
DoS_Hulk
DoS_GoldenEye
DoS_Slowloris
DoS_Slowhttptest
DoS_Heartleech
Web_DVWA
Web_XSS
Web_BruteForce
Infiltration_DropboxDownload
Infiltration_Nmap
Botnet_Ares_RemoteShell
Botnet_Ares_FileUpDownload
Botnet_Ares_Capturing
Botnet_ScreenshotKeyLogging
DDoS_LOIC_UDP
DDoS_LOIC_TCP
DDoS_LOIC_HTTP

References

[1] "IDS 2018 | Datasets | Research | Canadian Institute for Cybersecurity | UNB."