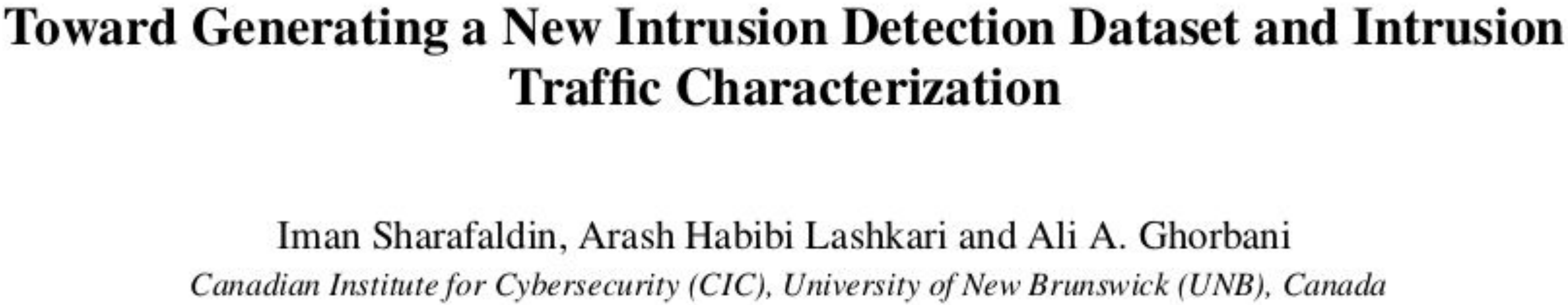


Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization

Iman Sharafaldin, Arash Habibi Lashkari and Ali A. Ghorbani
Canadian Institute for Cybersecurity (CIC), University of New Brunswick (UNB), Canada

CSE-CIC-IDS2018 - University of New Brunswick Canada

Nicolas Ricardo Enciso

UNSECURELAB

Available datasets

1. DARPA(1998): Not real world attacks, absence of false positives, outdated.
2. KDD99(1999): Redundant records, outdated, studded.
3. DEFCON(2000): Not real world traffic, outdated.
4. CAIDA(2002): Very specific to some attacks, anonymized payload.
5. LBNL(2004): No payload, anonymized, outdated.
6. CDX(2009): Lack of traffic diversity and volume, from competition.

Available datasets

1. Kyoto(2009): No labelling, only honeypot traffic.
2. Twente(2009): Unknow and uncorrelated alerts traffic, lack of diversity.
3. UMASS(2011): Lack of variety of traffic and attacks.
4. ISCX(2012): Distribution of attacks is not based in real world statistics.
5. ADFA(2013): Lack of attack diversity, not well separated behaviour.

Process overview

1. Configuration
2. Simulation
3. Capture
4. Traffic features extracted via CICFlowMeter software
5. Analysis to select the best features
6. Evaluation with 7 ML algorithms

Network profiles

B-profiles

1. Behaviour of benign users
2. Uses ML (K-mean, RandForest, SVM, J48).
3. Distributed packets are recreated from ML outputs, to simulate normal users.
4. Protocols: HTTPS, HTTP, SMTP, POP3, IMAP, SSH, FTP.
5. Majority from observations of users, HTTP - HTTPS.

Network profiles

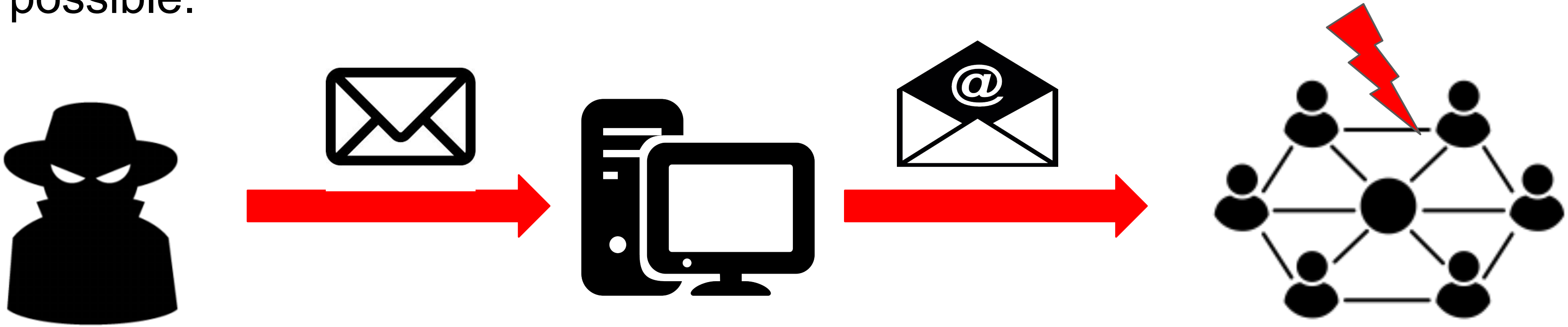
M-profiles

1. Behaviour of attack scenarios
2. Humans can interpret these profiles.
3. Can be executed in certain cases to generate attack traffic.
4. Protocols: HTTPS, HTTP, SMTP, POP3, IMAP, SSH, FTP.
5. Majority from observations of users, HTTP - HTTPS.

Attack scenarios

1. Infiltration of the network from inside

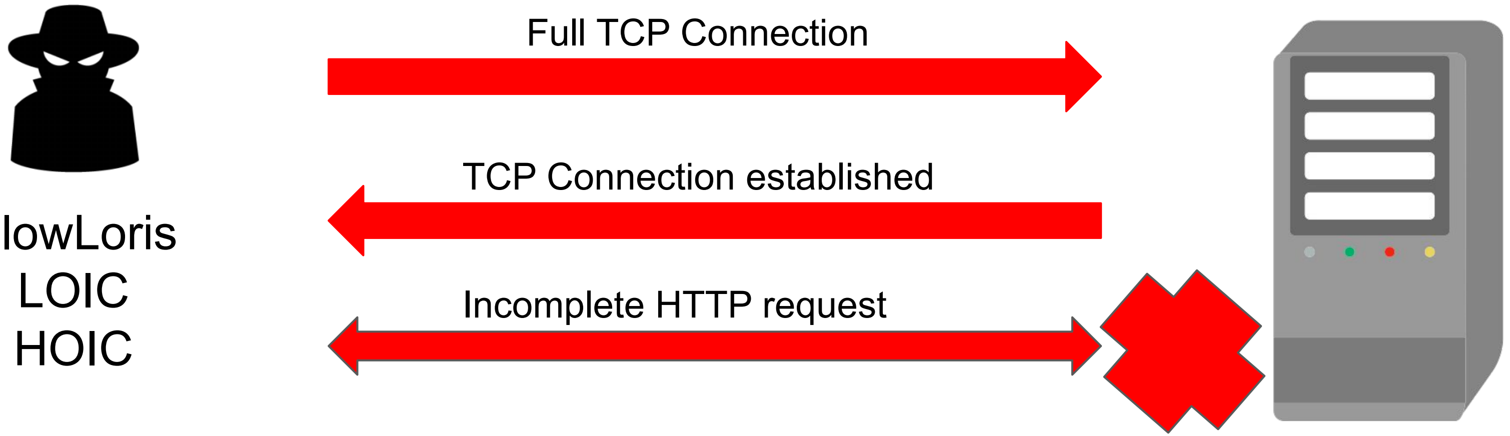
It was send a malicious file via an email to exploit an application vulnerability. A backdoor was executed on the victim, to scan the internal network for other vulnerable boxes and exploit them if possible.



Attack scenarios

2. HTTP denial of service

Make web servers completely inaccessible, sending incomplete but valid HTTP requests at intervals, until the server ended up with no sockets, and the service falls.



SlowLoris
LOIC
HOIC

Full TCP Connection

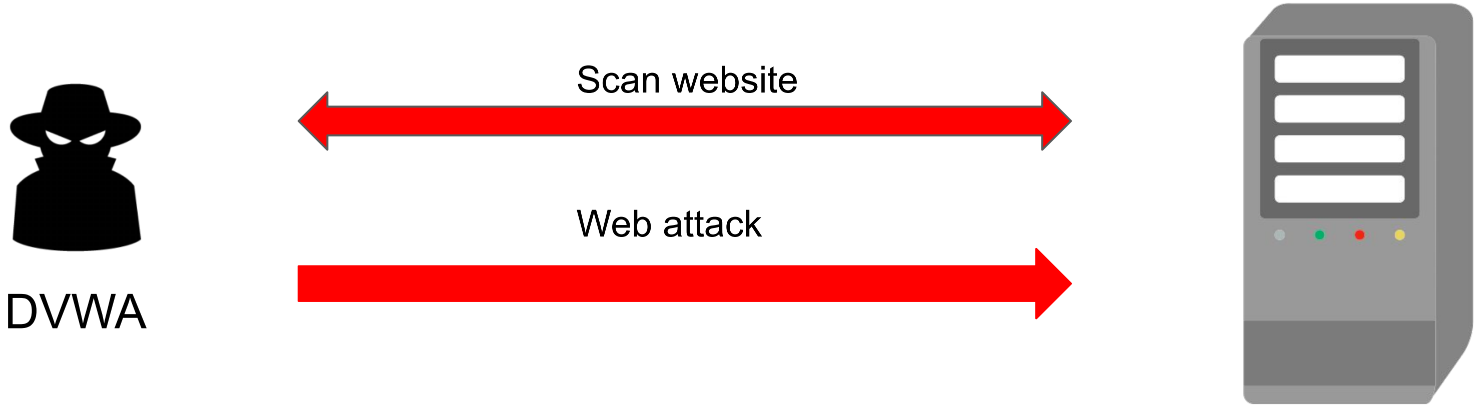
TCP Connection established

Incomplete HTTP request

Attack scenarios

3. Collection of web app attacks

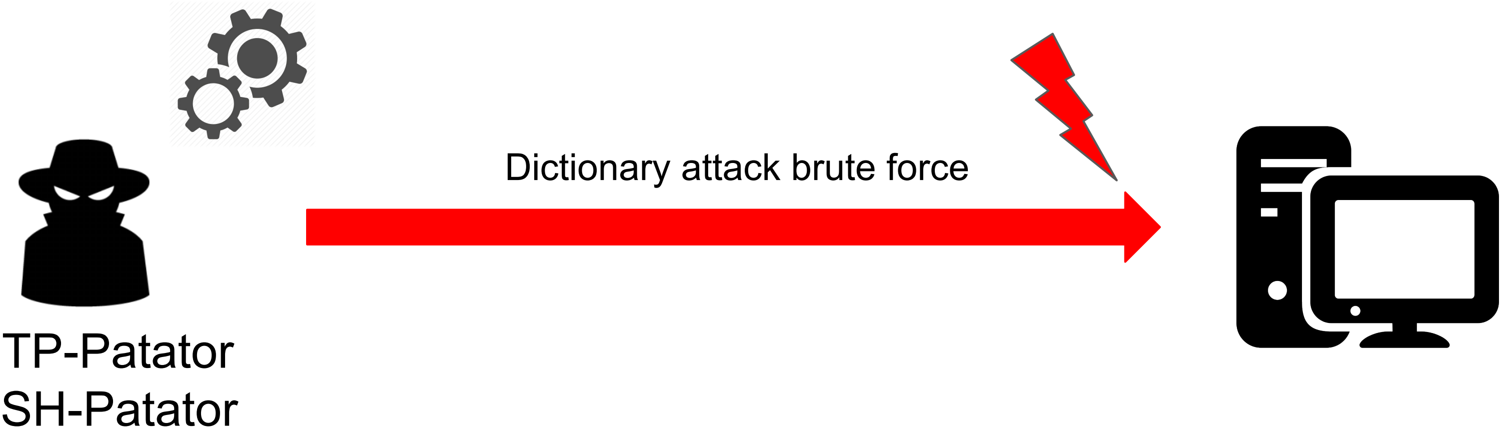
Damn Vulnerable Web App (DVWA) is used. It scan the website searching for vulnerabilities, and then conduct attacks such as SQL injection, command injection and unrestricted file upload.



Attack scenarios

4. Brute force attacks

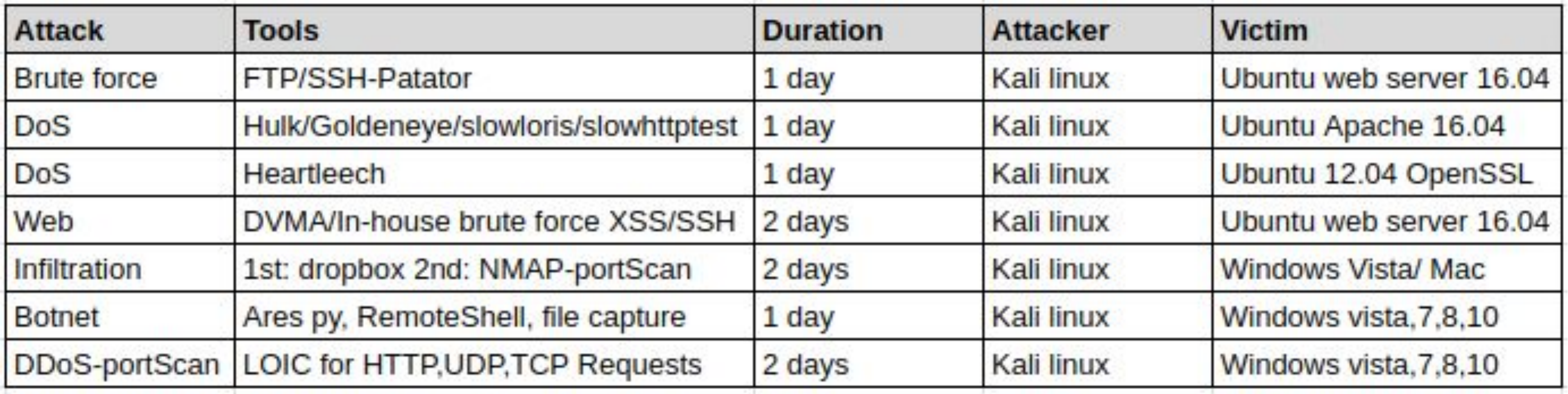
Breaking into username and passwords of SSH and MySQL accounts, using a dictionary. It includes FTP brute force attacks.



Dictionary attack brute force

FTP-Patator
SSH-Patator

Executed attacks



Attack	Tools	Duration	Attacker	Victim
Brute force	FTP/SSH-Patator	1 day	Kali linux	Ubuntu web server 16.04
DoS	Hulk/Goldeneye/slowloris/slowhttptest	1 day	Kali linux	Ubuntu Apache 16.04
DoS	Heartleech	1 day	Kali linux	Ubuntu 12.04 OpenSSL
Web	DVMA/In-house brute force XSS/SSH	2 days	Kali linux	Ubuntu web server 16.04
Infiltration	1st: dropbox 2nd: NMAP-portScan	2 days	Kali linux	Windows Vista/ Mac
Botnet	Ares py, RemoteShell, file capture	1 day	Kali linux	Windows vista,7,8,10
DDoS-portScan	LOIC for HTTP,UDP,TCP Requests	2 days	Kali linux	Windows vista,7,8,10

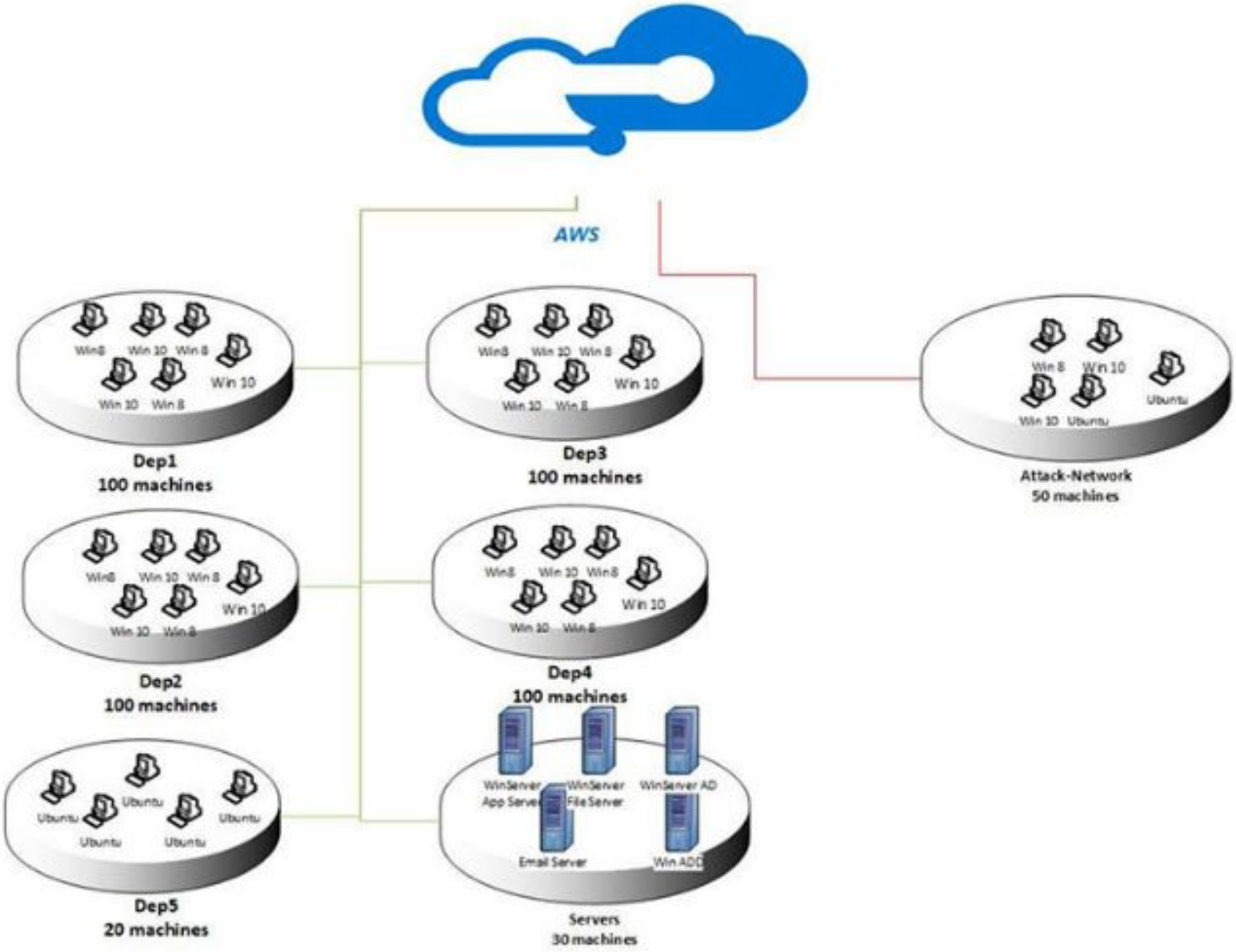
Architecture

B-Profile (Benign)

- 5 departments
- Dep1: 100 machines
- Dep2: 100 machines
- Dep3: 100 machines
- Dep4:100 machines
- Dep5: 20 machines
- Servers: 30 machines

M-Profile (Attack)

- Kali Linux, Windows 8.1.
- Attack-network: 50 machines


AWS
Win8
Win 10
Win 8
Win 10
Win 10
Win 8
Dep1
100 machines
Dep2
100 machines
Dep3
100 machines
Dep4
100 machines
Ubuntu
Dep5
20 machines
WinServer App Server
WinServer File Server
WinServer AD
Email Server
Win ADD
Servers
30 machines
Win 8
Win 10
Win 10
Ubuntu
Ubuntu
Attack-Network
50 machines

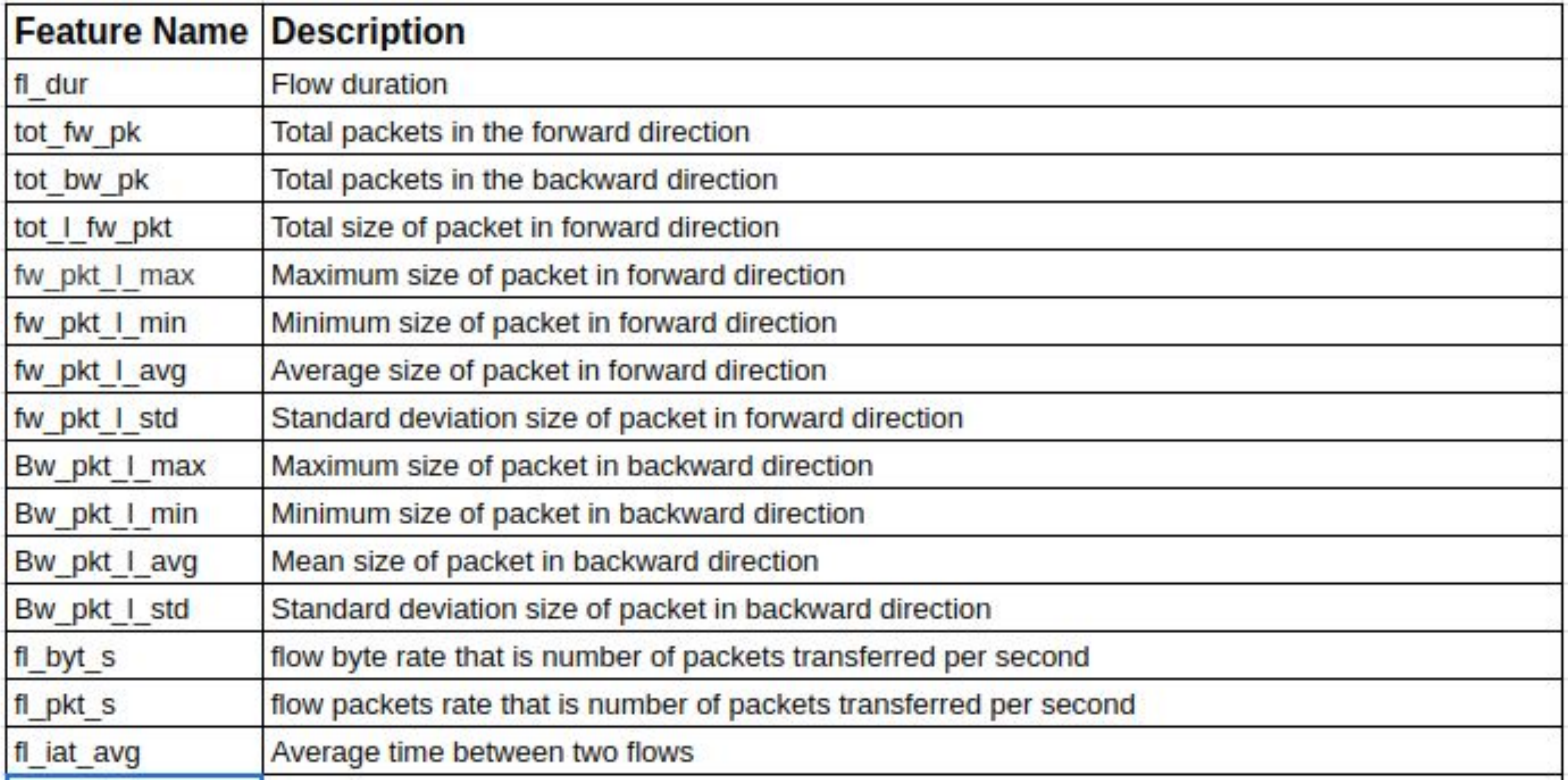
Dataset

1. 5 days of capture traffic, in intervals at the morning one type of attack, and at the afternoon another type of attack, first day to capture benign traffic.
2. Two versions of the dataset:

   2.1 Raw version of PCAP files for each day, allocated on AWS, total of 450GB of data.

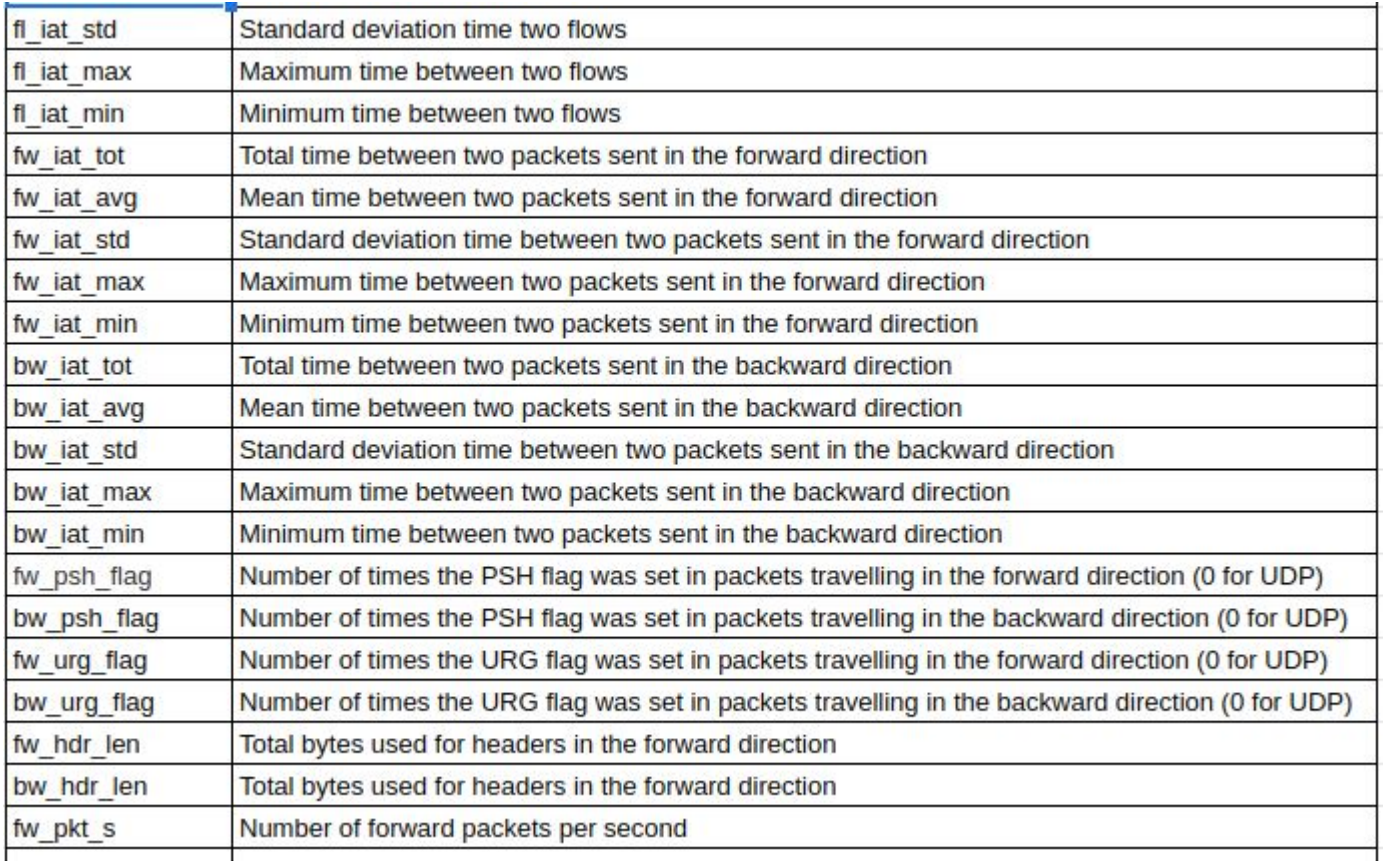
   2.2 Extracted features from CICFlowMeter, 80 features on 6 columns, 7GB of data on CSV.

Dataset extracted features



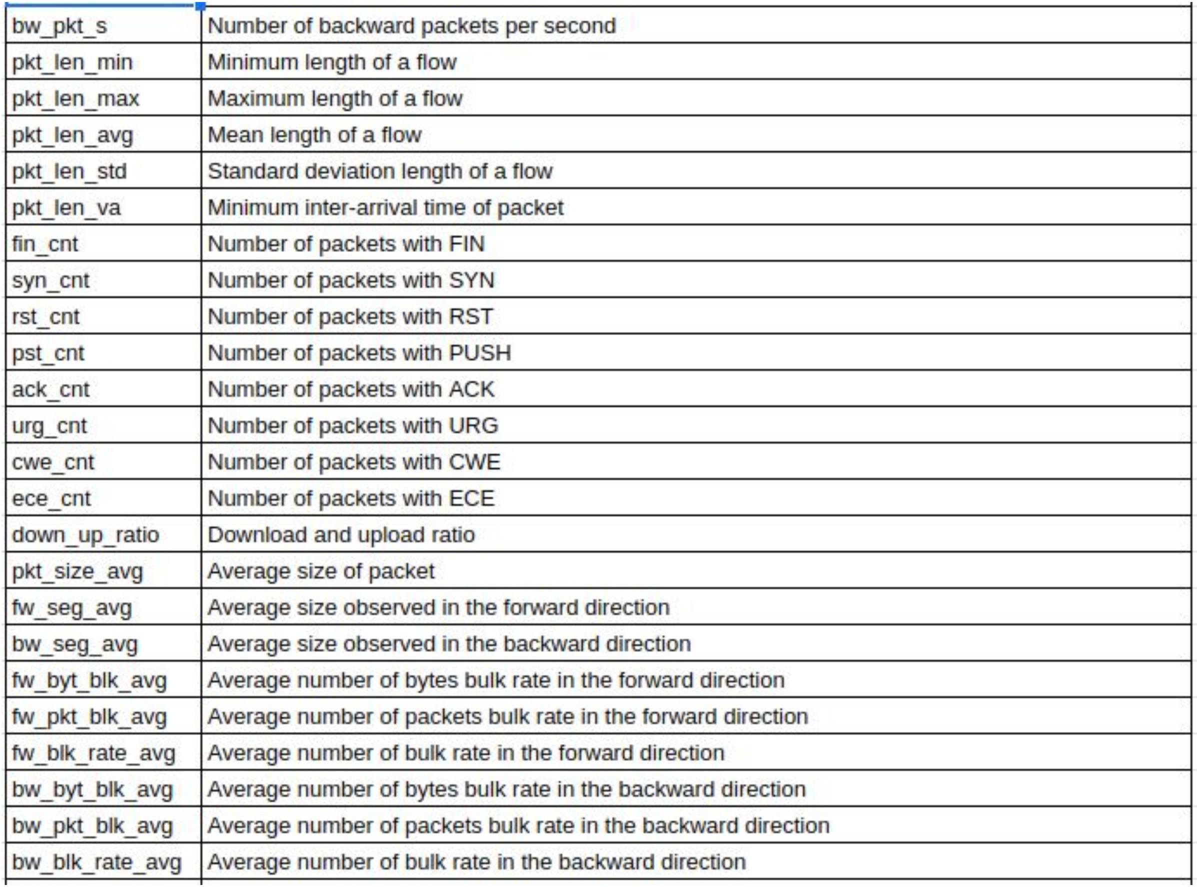
Feature Name	Description
fl_dur	Flow duration
tot_fw_pk	Total packets in the forward direction
tot_bw_pk	Total packets in the backward direction
tot_l_fw_pkt	Total size of packet in forward direction
fw_pkt_l_max	Maximum size of packet in forward direction
fw_pkt_l_min	Minimum size of packet in forward direction
fw_pkt_l_avg	Average size of packet in forward direction
fw_pkt_l_std	Standard deviation size of packet in forward direction
Bw_pkt_l_max	Maximum size of packet in backward direction
Bw_pkt_l_min	Minimum size of packet in backward direction
Bw_pkt_l_avg	Mean size of packet in backward direction
Bw_pkt_l_std	Standard deviation size of packet in backward direction
fl_byt_s	flow byte rate that is number of packets transferred per second
fl_pkt_s	flow packets rate that is number of packets transferred per second
fl_iat_avg	Average time between two flows

Dataset extracted features



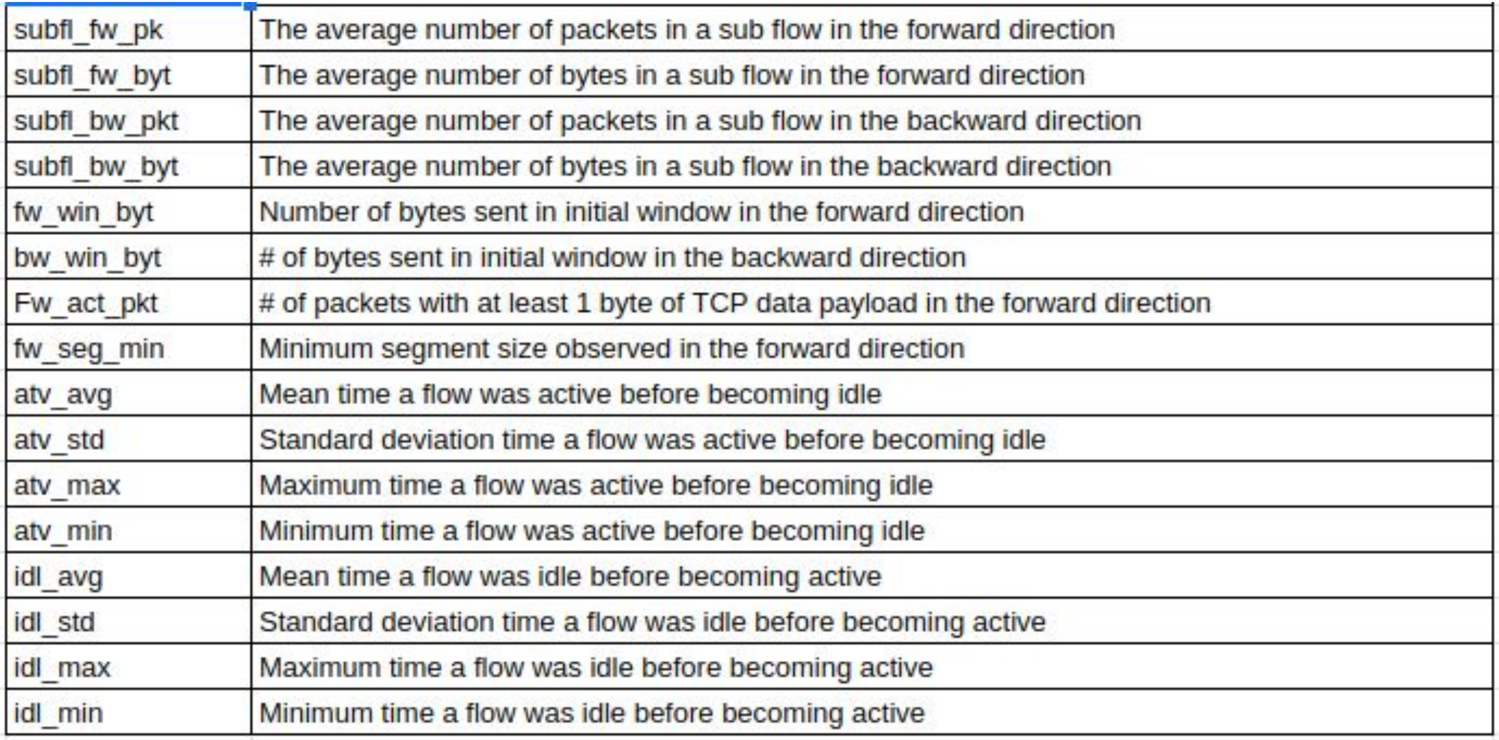
fl_iat_std	Standard deviation time two flows
fl_iat_max	Maximum time between two flows
fl_iat_min	Minimum time between two flows
fw_iat_tot	Total time between two packets sent in the forward direction
fw_iat_avg	Mean time between two packets sent in the forward direction
fw_iat_std	Standard deviation time between two packets sent in the forward direction
fw_iat_max	Maximum time between two packets sent in the forward direction
fw_iat_min	Minimum time between two packets sent in the forward direction
bw_iat_tot	Total time between two packets sent in the backward direction
bw_iat_avg	Mean time between two packets sent in the backward direction
bw_iat_std	Standard deviation time between two packets sent in the backward direction
bw_iat_max	Maximum time between two packets sent in the backward direction
bw_iat_min	Minimum time between two packets sent in the backward direction
fw_psh_flag	Number of times the PSH flag was set in packets travelling in the forward direction (0 for UDP)
bw_psh_flag	Number of times the PSH flag was set in packets travelling in the backward direction (0 for UDP)
fw_urg_flag	Number of times the URG flag was set in packets travelling in the forward direction (0 for UDP)
bw_urg_flag	Number of times the URG flag was set in packets travelling in the backward direction (0 for UDP)
fw_hdr_len	Total bytes used for headers in the forward direction
bw_hdr_len	Total bytes used for headers in the forward direction
fw_pkt_s	Number of forward packets per second

Dataset extracted features

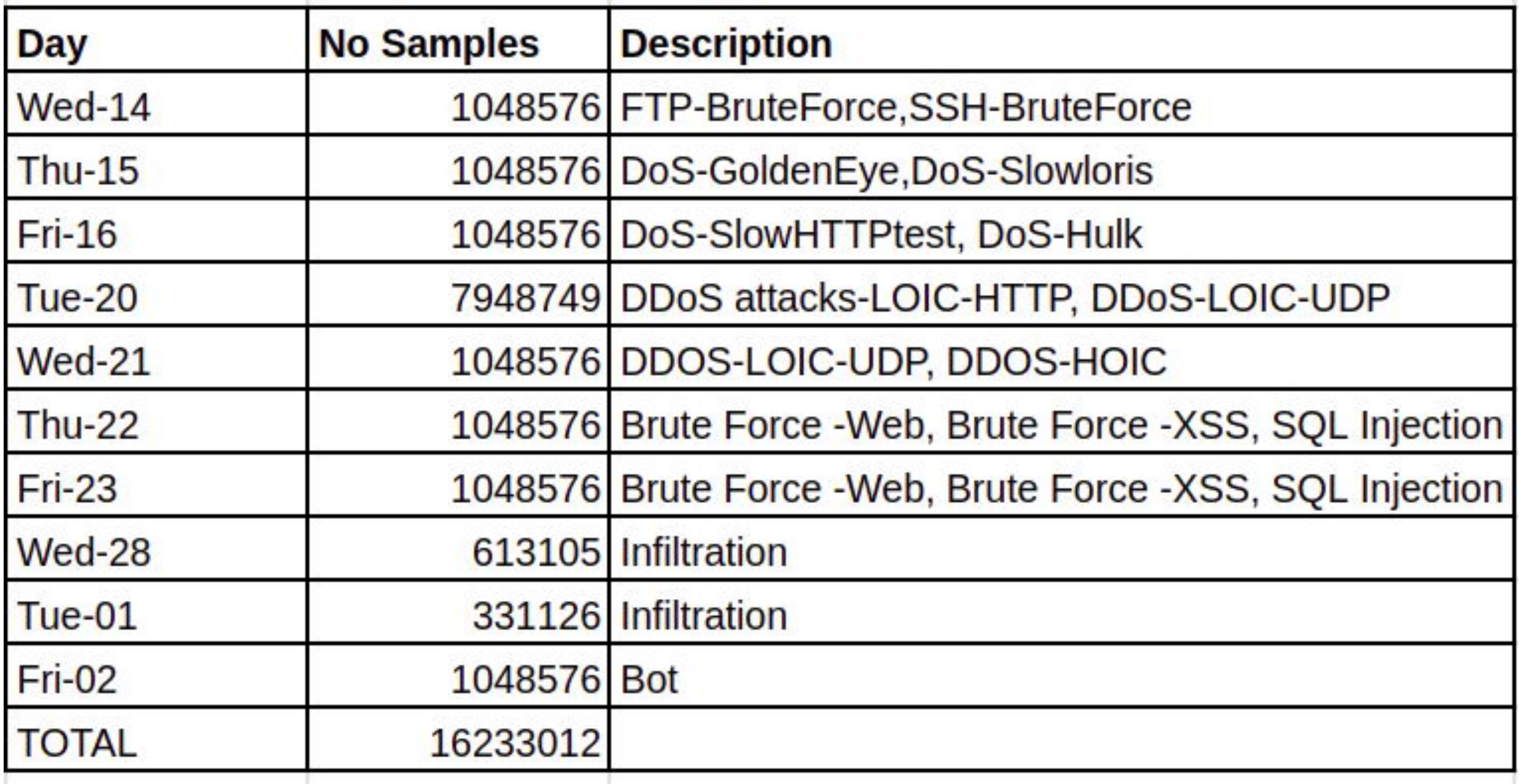


bw_pkt_s	Number of backward packets per second
pkt_len_min	Minimum length of a flow
pkt_len_max	Maximum length of a flow
pkt_len_avg	Mean length of a flow
pkt_len_std	Standard deviation length of a flow
pkt_len_va	Minimum inter-arrival time of packet
fin_cnt	Number of packets with FIN
syn_cnt	Number of packets with SYN
rst_cnt	Number of packets with RST
pst_cnt	Number of packets with PUSH
ack_cnt	Number of packets with ACK
urg_cnt	Number of packets with URG
cwe_cnt	Number of packets with CWE
ece_cnt	Number of packets with ECE
down_up_ratio	Download and upload ratio
pkt_size_avg	Average size of packet
fw_seg_avg	Average size observed in the forward direction
bw_seg_avg	Average size observed in the backward direction
fw_byt_blk_avg	Average number of bytes bulk rate in the forward direction
fw_pkt_blk_avg	Average number of packets bulk rate in the forward direction
fw_blk_rate_avg	Average number of bulk rate in the forward direction
bw_byt_blk_avg	Average number of bytes bulk rate in the backward direction
bw_pkt_blk_avg	Average number of packets bulk rate in the backward direction
bw_blk_rate_avg	Average number of bulk rate in the backward direction

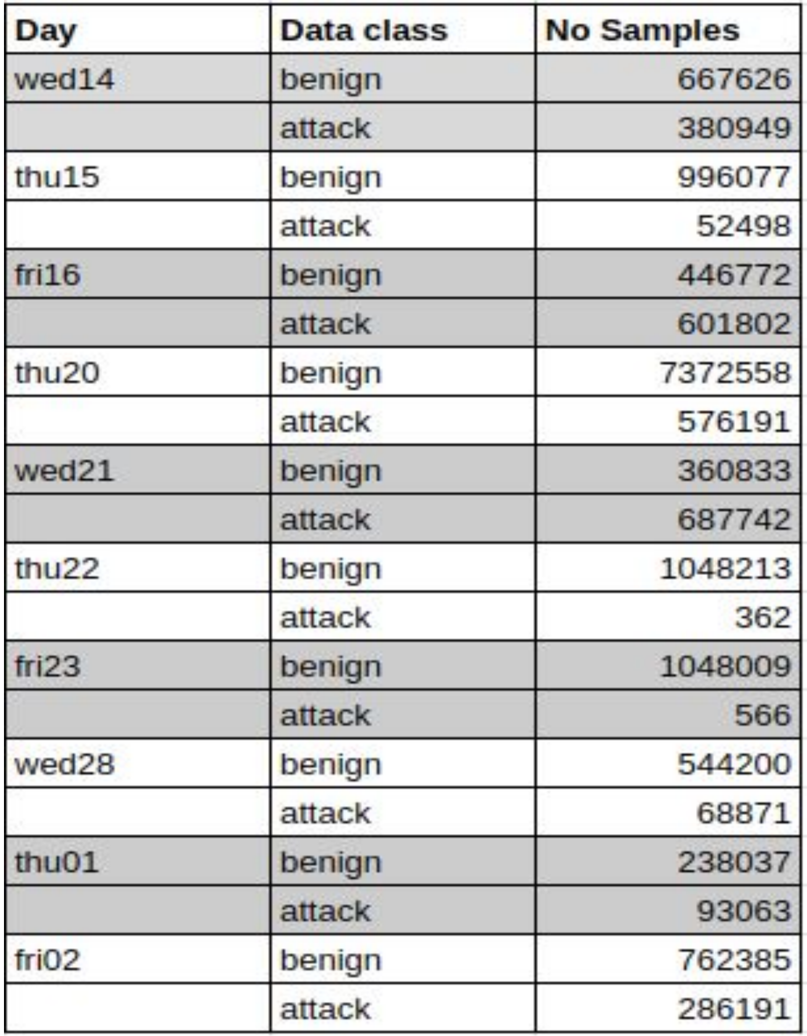
Dataset extracted features



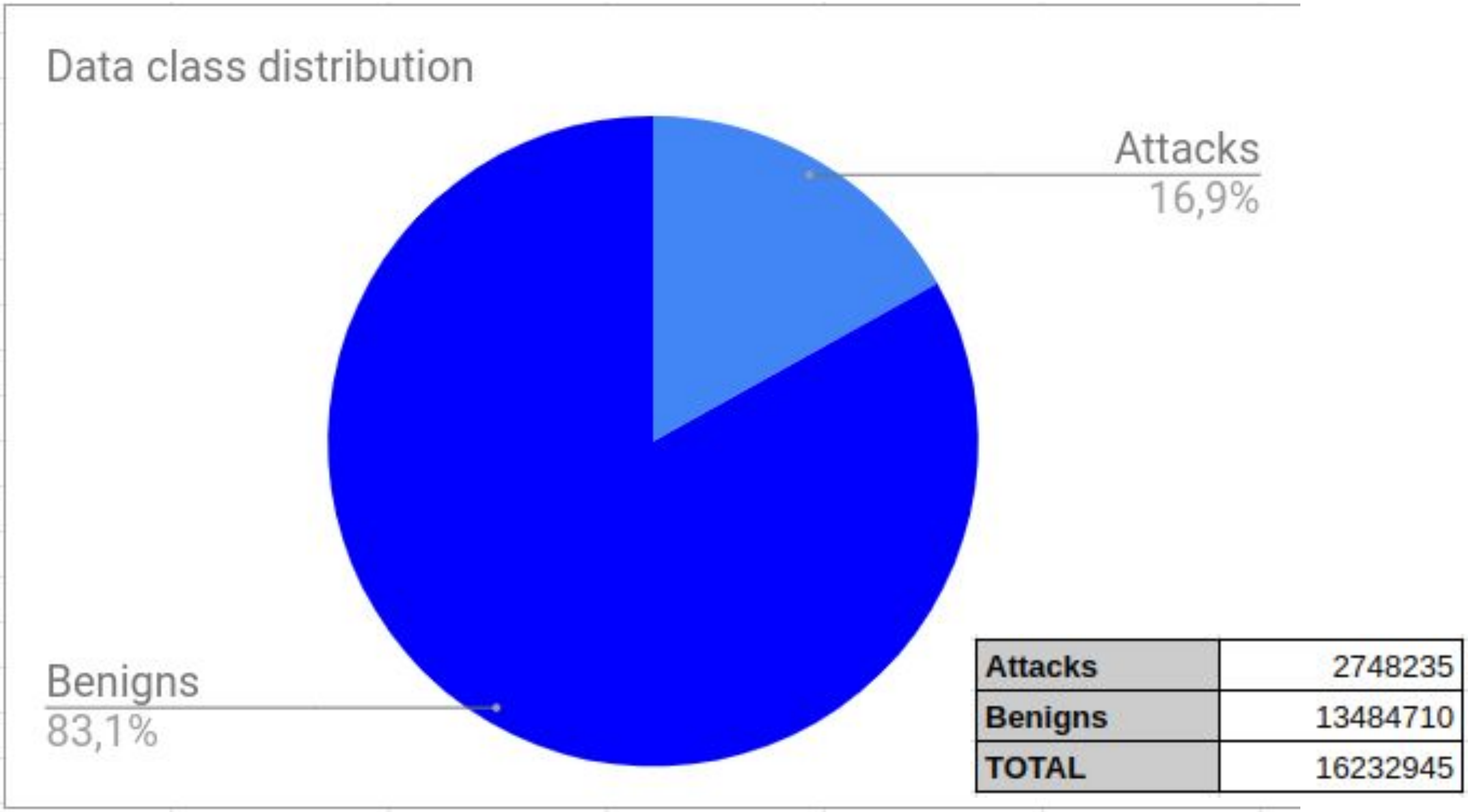
subfl_fw_pk	The average number of packets in a sub flow in the forward direction
subfl_fw_byt	The average number of bytes in a sub flow in the forward direction
subfl_bw_pkt	The average number of packets in a sub flow in the backward direction
subfl_bw_byt	The average number of bytes in a sub flow in the backward direction
fw_win_byt	Number of bytes sent in initial window in the forward direction
bw_win_byt	# of bytes sent in initial window in the backward direction
Fw_act_pkt	# of packets with at least 1 byte of TCP data payload in the forward direction
fw_seg_min	Minimum segment size observed in the forward direction
atv_avg	Mean time a flow was active before becoming idle
atv_std	Standard deviation time a flow was active before becoming idle
atv_max	Maximum time a flow was active before becoming idle
atv_min	Minimum time a flow was active before becoming idle
idl_avg	Mean time a flow was idle before becoming active
idl_std	Standard deviation time a flow was idle before becoming active
idl_max	Maximum time a flow was idle before becoming active
idl_min	Minimum time a flow was idle before becoming active



Day	No Samples	Description
Wed-14	1048576	FTP-BruteForce,SSH-BruteForce
Thu-15	1048576	DoS-GoldenEye,DoS-Slowloris
Fri-16	1048576	DoS-SlowHTTPtest, DoS-Hulk
Tue-20	7948749	DDoS attacks-LOIC-HTTP, DDoS-LOIC-UDP
Wed-21	1048576	DDOS-LOIC-UDP, DDOS-HOIC
Thu-22	1048576	Brute Force -Web, Brute Force -XSS, SQL Injection
Fri-23	1048576	Brute Force -Web, Brute Force -XSS, SQL Injection
Wed-28	613105	Infiltration
Tue-01	331126	Infiltration
Fri-02	1048576	Bot
TOTAL	16233012	

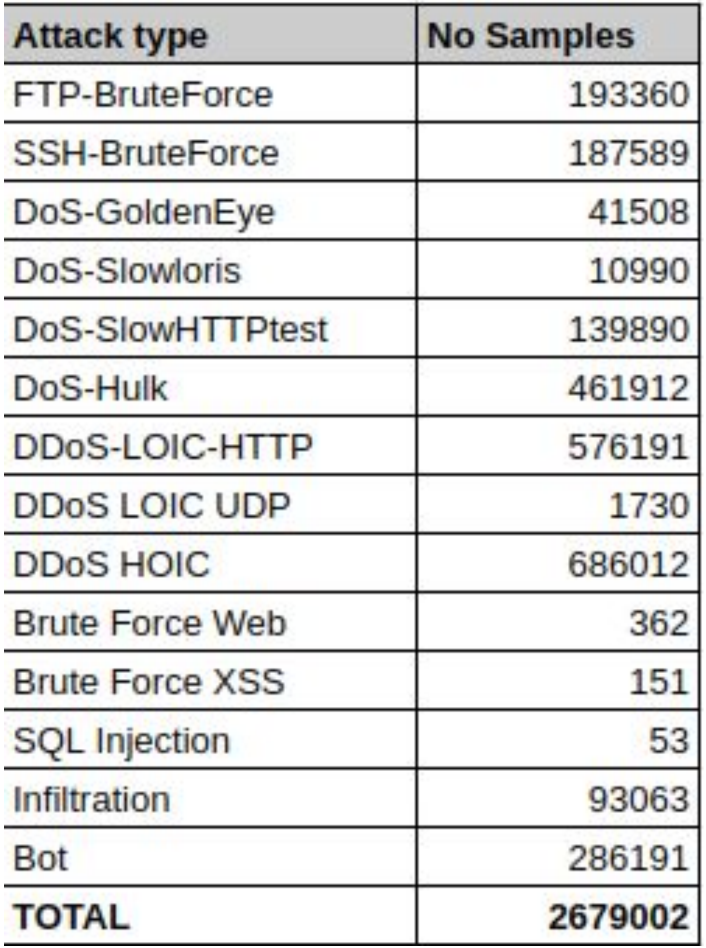


Day	Data class	No Samples
wed14	benign	667626
	attack	380949
thu15	benign	996077
	attack	52498
fri16	benign	446772
	attack	601802
thu20	benign	7372558
	attack	576191
wed21	benign	360833
	attack	687742
thu22	benign	1048213
	attack	362
fri23	benign	1048009
	attack	566
wed28	benign	544200
	attack	68871
thu01	benign	238037
	attack	93063
fri02	benign	762385
	attack	286191

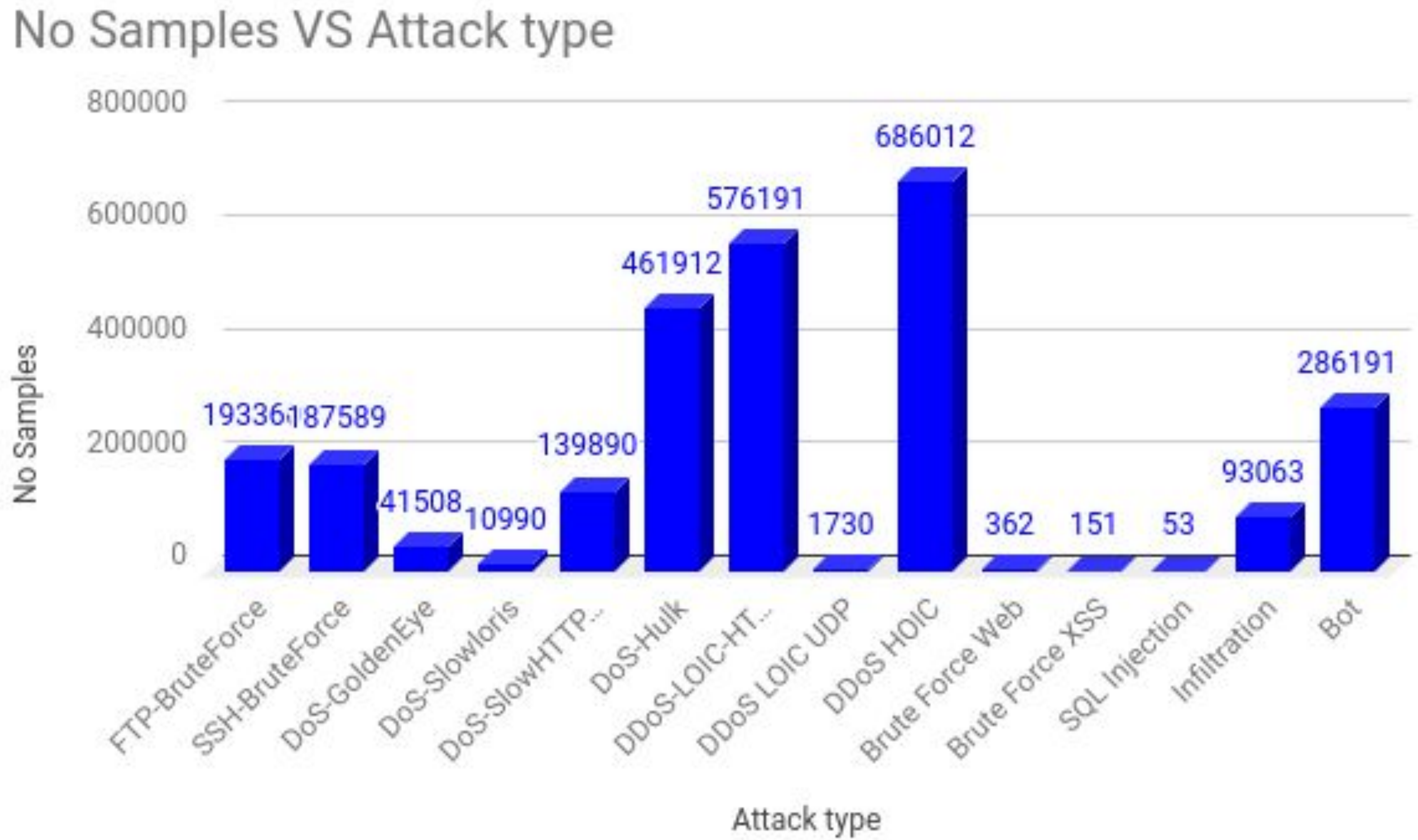


Data class distribution

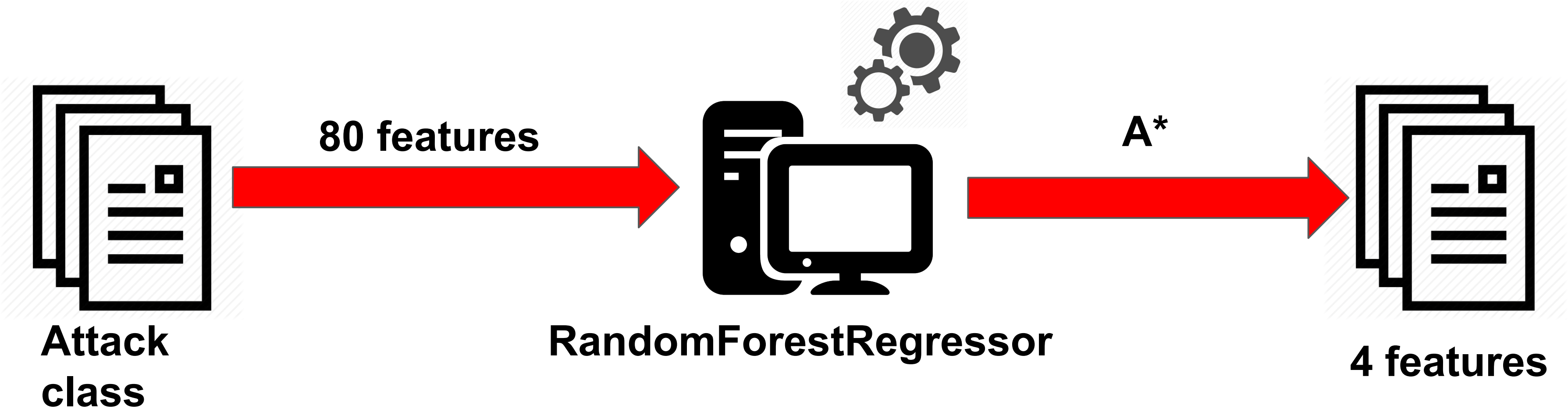
Attacks	2748235
Benigns	13484710
TOTAL	16232945



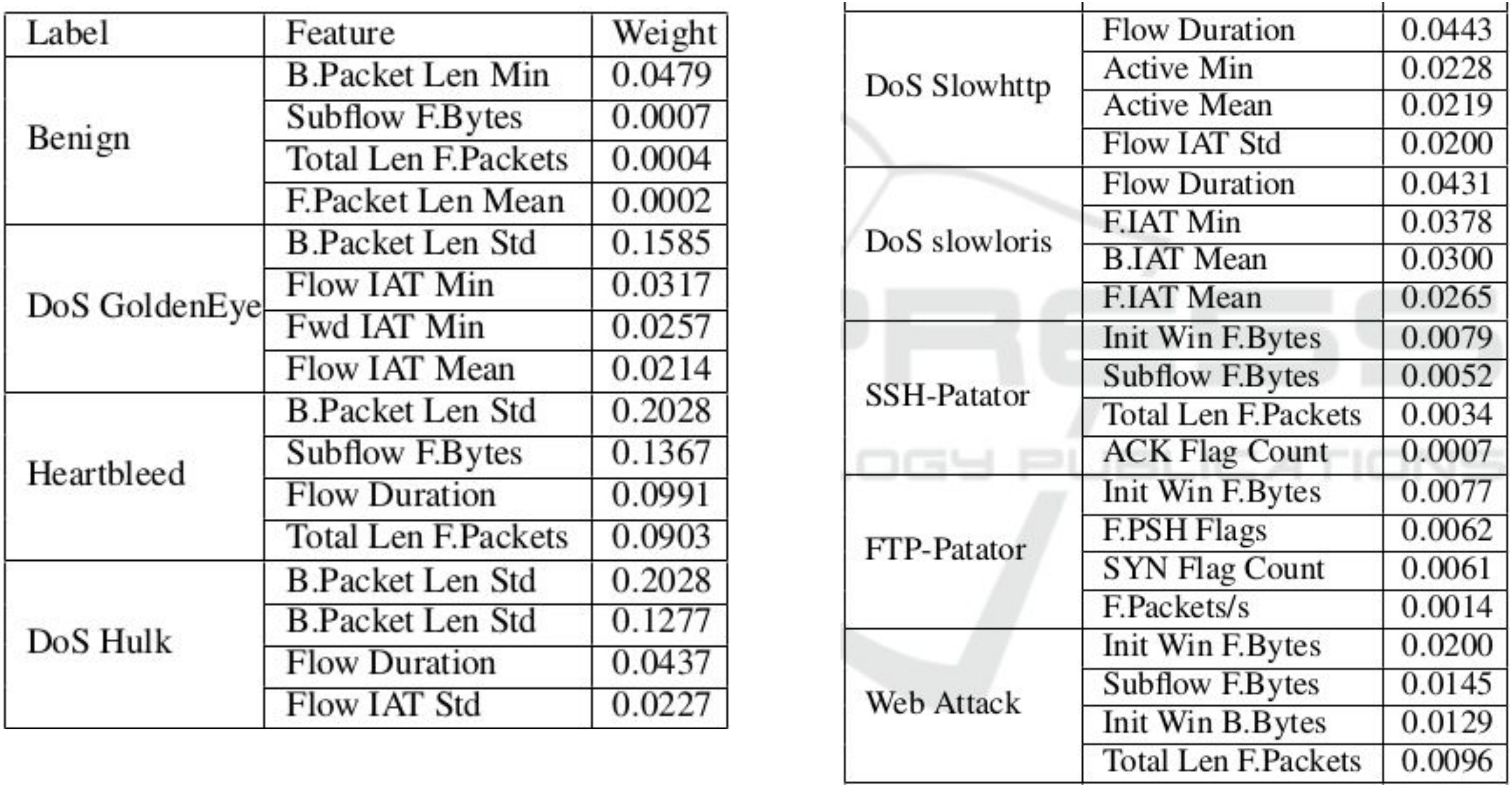
Attack type	No Samples
FTP-BruteForce	193360
SSH-BruteForce	187589
DoS-GoldenEye	41508
DoS-Slowloris	10990
DoS-SlowHTTPtest	139890
DoS-Hulk	461912
DDoS-LOIC-HTTP	576191
DDoS LOIC UDP	1730
DDoS HOIC	686012
Brute Force Web	362
Brute Force XSS	151
SQL Injection	53
Infiltration	93063
Bot	286191
TOTAL	**2679002**


No Samples VS Attack type
800000
600000
400000
200000
0
No Samples
19336
187589
41508
10990
139890
461912
576191
1730
686012
362
151
53
93063
286191
FTP-BruteForce
SSH-BruteForce
DoS-GoldenEye
DoS-Slowloris
DoS-SlowHTTP...
DoS-Hulk
DDoS-LOIC-HT...
DDoS LOIC UDP
DDoS HOIC
Brute Force Web
Brute Force XSS
SQL Injection
Infiltration
Bot
Attack type

Data analysis



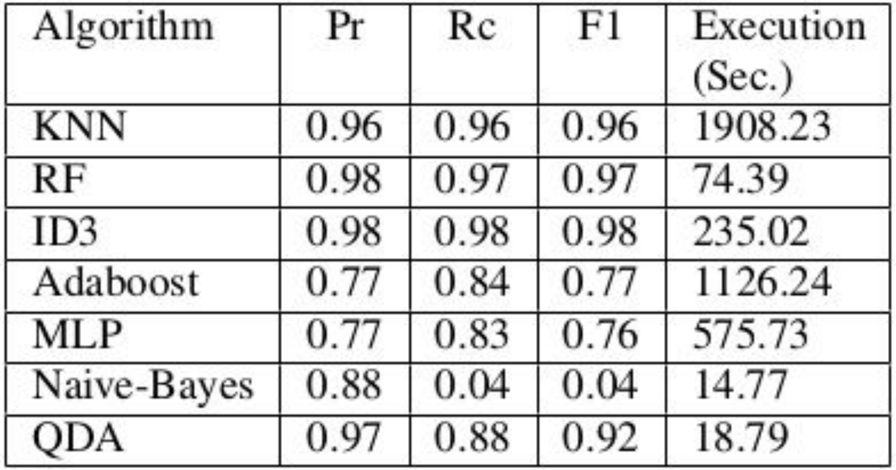
A*: Calculated importance of each feature in the whole dataset, then achieve the final result by multiplying the average standardized mean value of each feature split on each class, with the corresponding feature importance's value.



Label	Feature	Weight
Benign	B.Packet Len Min	0.0479
	Subflow F.Bytes	0.0007
	Total Len F.Packets	0.0004
	F.Packet Len Mean	0.0002
DoS GoldenEye	B.Packet Len Std	0.1585
	Flow IAT Min	0.0317
	Fwd IAT Min	0.0257
	Flow IAT Mean	0.0214
Heartbleed	B.Packet Len Std	0.2028
	Subflow F.Bytes	0.1367
	Flow Duration	0.0991
	Total Len F.Packets	0.0903
DoS Hulk	B.Packet Len Std	0.2028
	B.Packet Len Std	0.1277
	Flow Duration	0.0437
	Flow IAT Std	0.0227
DoS Slowhttp	Flow Duration	0.0443
	Active Min	0.0228
	Active Mean	0.0219
	Flow IAT Std	0.0200
DoS slowloris	Flow Duration	0.0431
	F.IAT Min	0.0378
	B.IAT Mean	0.0300
	F.IAT Mean	0.0265
SSH-Patator	Init Win F.Bytes	0.0079
	Subflow F.Bytes	0.0052
	Total Len F.Packets	0.0034
	ACK Flag Count	0.0007
FTP-Patator	Init Win F.Bytes	0.0077
	F.PSH Flags	0.0062
	SYN Flag Count	0.0061
	F.Packets/s	0.0014
Web Attack	Init Win F.Bytes	0.0200
	Subflow F.Bytes	0.0145
	Init Win B.Bytes	0.0129
	Total Len F.Packets	0.0096

Infiltration	Subflow F.Bytes	4.3012
	Total Len F.Packets	2.8427
	Flow Duration	0.0657
	Active Mean	0.0227
Bot	Subflow F.Bytes	0.0239
	Total Len F.Packets	0.0158
	F.Packet Len Mean	0.0025
	B.Packets/s	0.0021
PortScan	Init Win F.Bytes	0.0083
	B.Packets/s	0.0032
	PSH Flag Count	0.0009
DDoS	B.Packet Len Std	0.1728
	Avg Packet Size	0.0162
	Flow Duration	0.0137
	Flow IAT Std	0.0086

ML classification results



Algorithm	Pr	Rc	F1	Execution (Sec.)
KNN	0.96	0.96	0.96	1908.23
RF	0.98	0.97	0.97	74.39
ID3	0.98	0.98	0.98	235.02
Adaboost	0.77	0.84	0.77	1126.24
MLP	0.77	0.83	0.76	575.73
Naive-Bayes	0.88	0.04	0.04	14.77
QDA	0.97	0.88	0.92	18.79

Pr: Precision or Positive predictive value

Rc: Recall or sensitivity

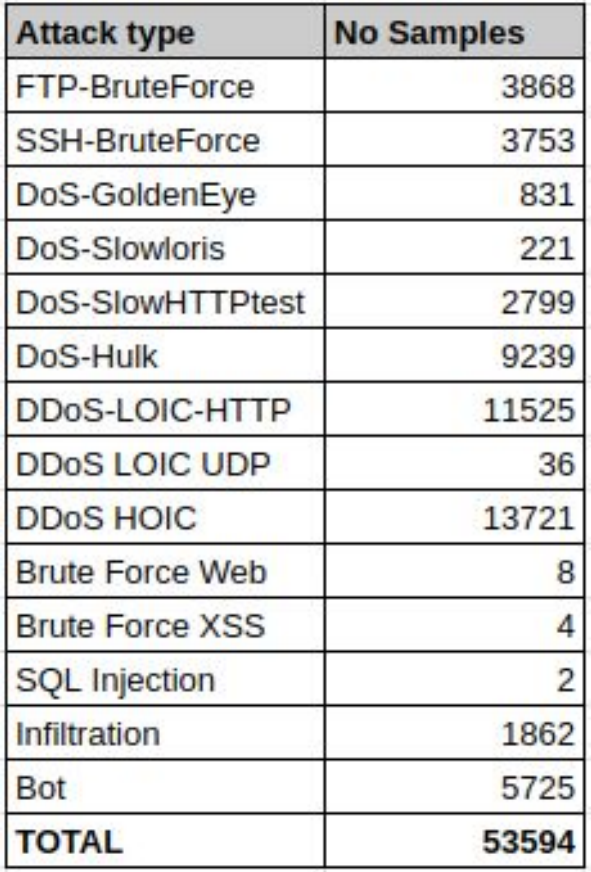
F1: F-measure

MLP: Multilayer perceptron

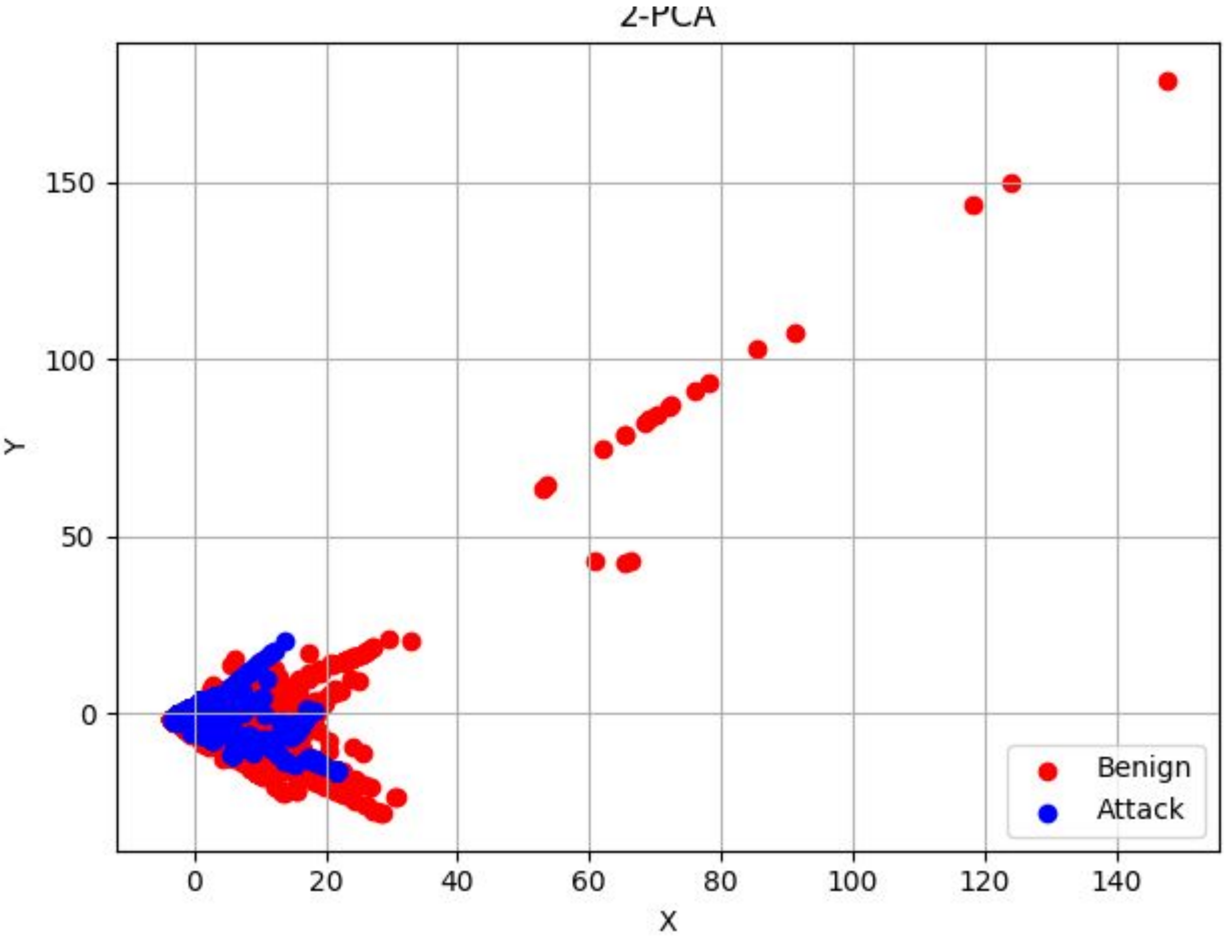
QDA: Quadratic Discriminant Analysis

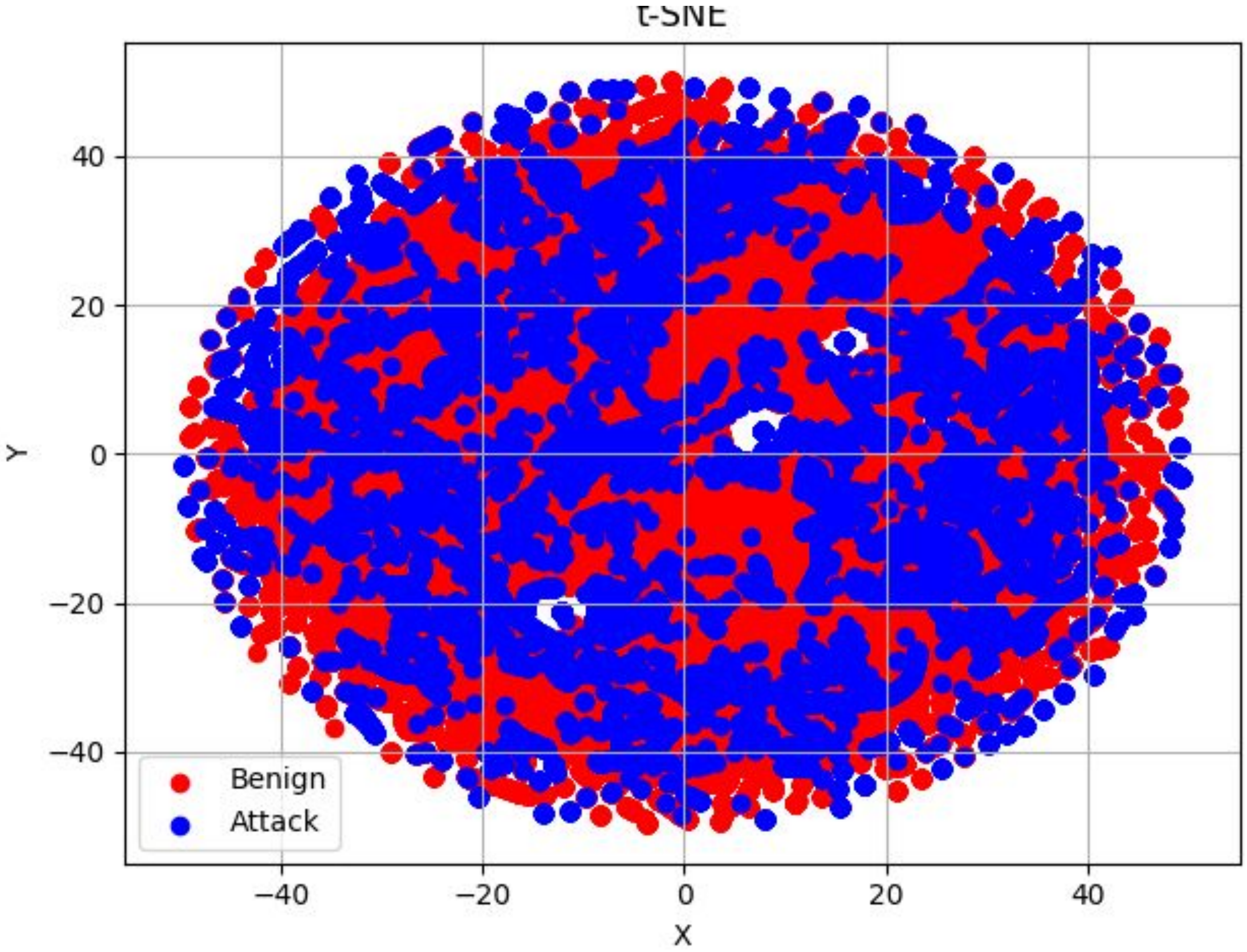
Own classification

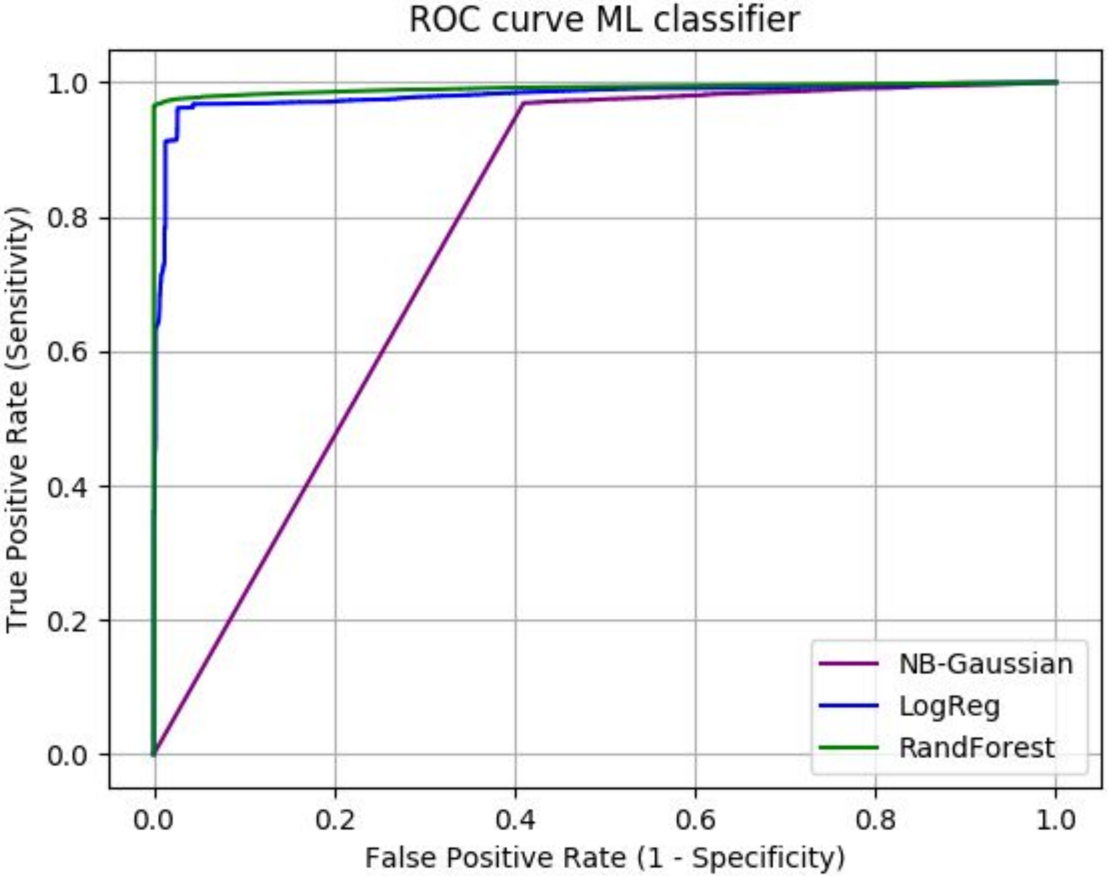
1. 2% of the overall dataset: 29% attacks (53594) and 71% benigns (131187), for a total of 184781 and a ratio benign/attack of 2.44.
2. The final 2% of data was taken from each attack, and their corresponding 2%.
3. 2 visualizations-dimensional reduction (PCA, TSNE).
4. 4 ML classifiers (Bayes, SVM, RandForest, LogicticReg).



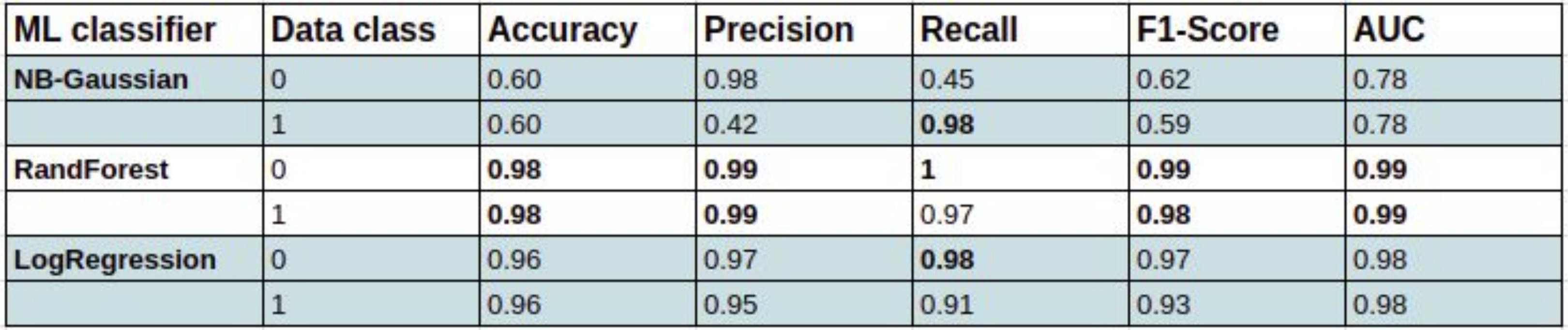
Attack type	No Samples
FTP-BruteForce	3868
SSH-BruteForce	3753
DoS-GoldenEye	831
DoS-Slowloris	221
DoS-SlowHTTPtest	2799
DoS-Hulk	9239
DDoS-LOIC-HTTP	11525
DDoS LOIC UDP	36
DDoS HOIC	13721
Brute Force Web	8
Brute Force XSS	4
SQL Injection	2
Infiltration	1862
Bot	5725
TOTAL	**53594**


2-PCA
Y
150
100
50
0
X
0
20
40
60
80
100
120
140
Benign
Attack


t-SNE
Y
X
40
20
0
−20
−40
−40
−20
0
20
40
Benign
Attack

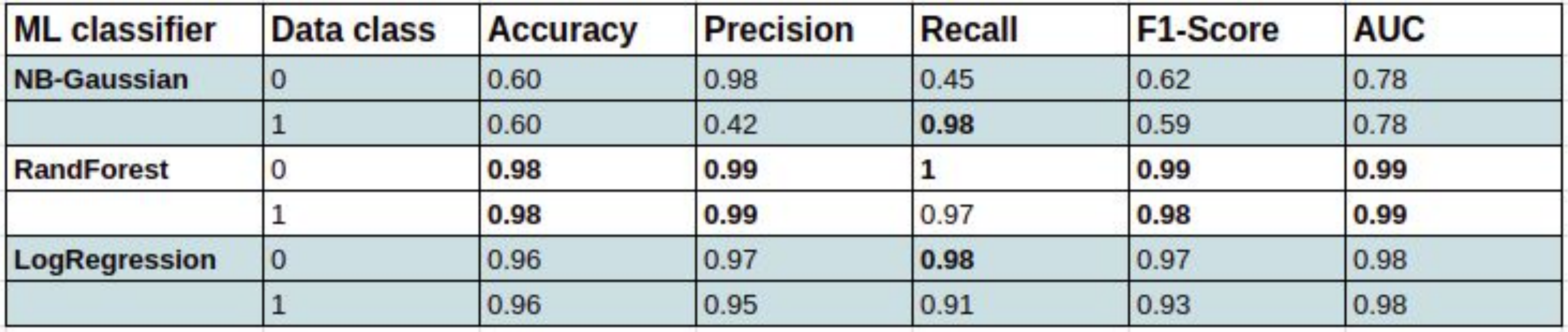

ROC curve ML classifier
True Positive Rate (Sensitivity)
False Positive Rate (1 - Specificity)
0.0
0.2
0.4
0.6
0.8
1.0
0.0
0.2
0.4
0.6
0.8
1.0
NB-Gaussian
LogReg
RandForest

ML results

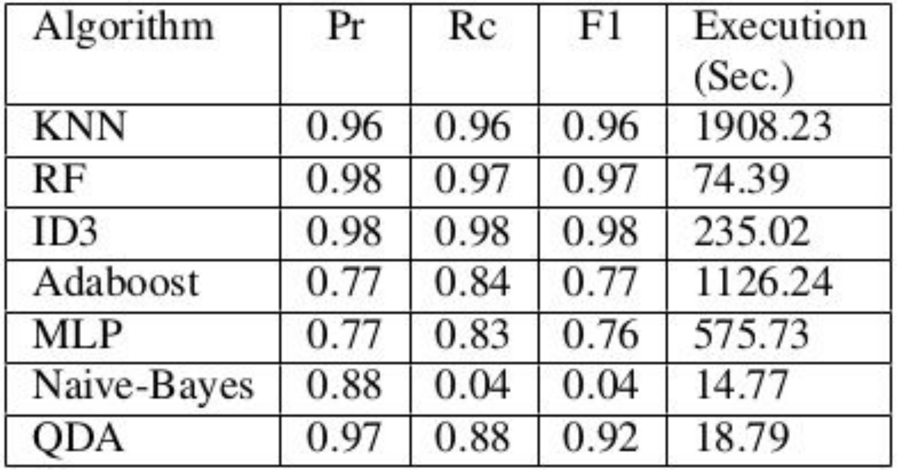


ML classifier	Data class	Accuracy	Precision	Recall	F1-Score	AUC
NB-Gaussian	0	0.60	0.98	0.45	0.62	0.78
	1	0.60	0.42	**0.98**	0.59	0.78
RandForest	0	**0.98**	**0.99**	**1**	**0.99**	**0.99**
	1	**0.98**	**0.99**	0.97	**0.98**	**0.99**
LogRegression	0	0.96	0.97	**0.98**	0.97	0.98
	1	0.96	0.95	0.91	0.93	0.98

ML comparison



ML classifier	Data class	Accuracy	Precision	Recall	F1-Score	AUC
NB-Gaussian	0	0.60	0.98	0.45	0.62	0.78
	1	0.60	0.42	**0.98**	0.59	0.78
RandForest	0	**0.98**	**0.99**	**1**	**0.99**	**0.99**
	1	**0.98**	**0.99**	0.97	**0.98**	**0.99**
LogRegression	0	0.96	0.97	**0.98**	0.97	0.98
	1	0.96	0.95	0.91	0.93	0.98



Algorithm	Pr	Rc	F1	Execution (Sec.)
KNN	0.96	0.96	0.96	1908.23
RF	0.98	0.97	0.97	74.39
ID3	0.98	0.98	0.98	235.02
Adaboost	0.77	0.84	0.77	1126.24
MLP	0.77	0.83	0.76	575.73
Naive-Bayes	0.88	0.04	0.04	14.77
QDA	0.97	0.88	0.92	18.79

Reference

- 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