Analyzation of CIC-IDS2017

Key Contributors: Garrett Stokes, Marcus Harmon, Briah Graves

UNIVERSITY OF THE INCARNATE WORD ®

12-1-2022

Table of Contents

Executive Summary

The CICIDS2017 Dataset is a dataset offered by the Canadian Institute for Cybersecurity, which presents benign and the most up-to-date common attacks, which resembles the true real-world data (PCAPs). The pcap files we used were already ingested through an open-source network traffic flow generator application, CICFLOWMETER, which generates bidirectional flows of the data, as well as 84 network traffic features concerning both the forward and backward directions of the data. This means the files all contained 84 headers, each pertaining to different data of the pcap file. The first step was configuring a total of 84 mappings, a total of 4 fields, IP, longs and doubles, and keywords, in an index template using Elastic Cloud. With this process finished, the uploading of the files using Elastic's was able to commence, and the file was successfully read by Elastic using the Index template, and an index for each upload on the specific days was created and the data was ready for analysis. We examined two different days, both the morning hours and afternoon hours of each day, a total of 4 file uploads, and a total of 4 examined attacks. The attacks on the network were a botnet, brute force, port scan, and a ddos. Each of these attacks presented specific anomaly indicators indicating what exactly was happening on the network during the given attack, and was able to be seen using visualizations using elastic clouds visualization feature. Thursday morning was the first analysis, examining a brute force attack. Digging into the data, we found the average initial window bytes, both forwards and backwards, to be radically different, as well as flag counts, in the attacking activity. On Friday morning, a botnet attack was examined. Digging into the morning data, we found the a new IP, identified to be the attacker, and interestingly a median port of 8080 being a constant in all of the bots activity in the network. Friday afternoon, two attacks, a ddos and a port scan, were examined. With the ddos, the average packet size and the average backward packet length standard deviation were key indicators of the ddos attack. In the port scan, the average of backward packets and push flags showed anomalous behavior related to the attacker's port scan. In retrospect, the manual process of going through network data and finding anomalous behavior of certain fields of the network data was interesting, and a great hands-on experience. Regarding intrusion detection systems, it is excellent practice to know exactly what the intrusion detection and prevention systems are looking at and for, and that is something we gained and can take with us through this process.

Project Milestones

1. **<u>Set up Elastic Cloud and configure mappings for dataset</u>**- Utilizing the elastic cloud is the main source of how we got our information for our report. The mappings of our template allowed us to see the information in a way for us to tell what our information means in the first place.

2. **<u>Upload dataset and analyze information</u>**- Once we had our mappings complete the next thing for us to do was to upload the files onto elastic. The information that we uploaded comes from the behavior of 25 users based on the HTTP, HTTPS, FTP, SSH, and email protocols on July 6th and July 7th of 2017, a Thursday morning hours and a Friday's morning and afternoon hours.

3. **<u>Breaking down findings</u>**- The dataset showed that there was 1 attack on Thursday morning being a Brute Force attack.. Friday morning a Botnet ARES attack occurred, and on Friday afternoon both a port scan attack and a ddos attack took place. We will break down these specific findings these findings later in the report
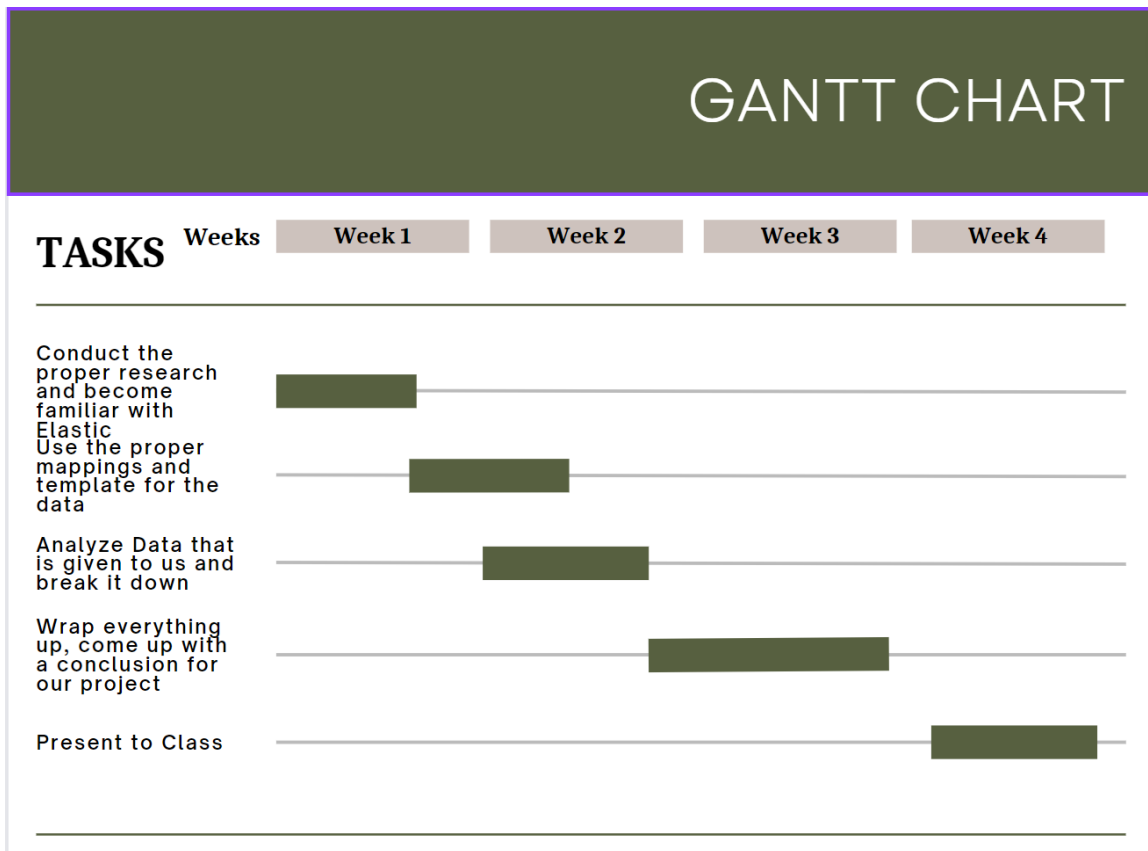
Deliverables

1. Powerpoint Presentation
2. Report
3. Findings and explanation

Materials List

1. Elastic Cloud
2. CICIDS-2017 Dataset

Project Schedule Management

Project Management Board Link (QR Code Only).
https://trello.com/b/RReQZQt0/f22-gs-mh-bg-ids-project

Create a Github Project Repository and add the user "cyberknowledge" as a contributor.
https://github.com/stokesgarrett/IDSPROJECT

Introduction

The CICIDS 2017 dataset contains real world pcap files, as well as generated label flows of these pcap files, including added header features and the retaining of the most important data points for analysis. In our analysis, we examined the generated label flows files, meaning not the raw pcap file, but the CICFLOWMETER generated file, which added 84 network labels to the file, all of which pertain to forward and backward packet data, as well as IP information and labeling of the data.

After downloading the generated label flow files of the different days, the next step was uploading them to our Elastic Cloud deployment. We decided to do a file upload, which is not the most complicated process, nor the most optimal in a real world situation, but for the process of our project, we decided to focus on network data analyzation, rather than the deployment of an IDS, as that is a tedious process in of itself, and was not optimal as only one of us would have access to the system. With this, uploading a file was straightforward, and allowed us to get right into the data analysis.

Before uploading a specific day's network data, we were to create an index template, primarily focused on creating mappings for the specific data fields (headers) of the files. Thankfully, each day's file had the exact same 84 fields, so only one template was necessary. Interestingly enough, after the mappings were created and we attempted to upload a file, the file's headers were still not being read, and we were presented with labeling of generic columns, ie. "column 1", "column 2". This was an error on our part, as after examining the file analysis explanation offered by Elastic, it was detected there was a duplicate column in the first row of the file, so the header was not presumed to be an actual header.

After looking into the files with excel, we found that there actually was a duplicate column, the forward header length. We are not quite sure why this column was included twice in the files with the exact same data points, and if there was some sort of reason for this. To proceed, we had to delete the duplicate column in each of the files, which had no actual effect on the data, and forward header length was not particularly an important data point in our analysis in the first place.

After this duplicate column deletion, our files were now being read seemingly properly, and the mappings of each specific data point kicked in. After further analysis, seeing that there were 5 keyword values read, we quickly realized we were not out of the jungle yet. There were supposed to be only 2 keyword values, label and flow id, yet timestamp, flow bytes's, and flow packets's were also being read as keywords.

There had to be a reason for this, and after further examination we realized the culprit for flow packets's and flow bytes's being identified as keywords. Most of the data points of these columns were floating point numbers and integers, but some of them actually read "Infinity", which is the reason as to why this field was being grouped as a keyword. We replaced these data points with 0, which may or may not have been the best approach but

these fields were not particularly useful in our analysis, similar to the forward header length mentioned earlier.

	Type	Name ↑	Documents (%)	Distinct values	Distributions		
	#	Flow Duration	999 (100%)	753	min 0	median 796	max 119671512
	#	Flow IAT Max	999 (100%)	672	min 0	median 651	max 117000000
	#	Flow IAT Mean	999 (100%)	777	min 0	median 101	max 37200000
	#	Flow IAT Min	999 (100%)	208	min -1	median 3	max 4155641
	#	Flow IAT Std	999 (100%)	749	min 0	median 103.06	max 64400000
	#	Flow Packets/s	999 (100%)	790	min 0	median 12235.82	max 3000000
	#	Fwd Avg Bulk Rate	999 (100%)	1	min 0	median 0	max 0
	#	Fwd Avg Packets/Bulk	999 (100%)	1	min 0	median 0	max 0
	#	Fwd Header Length	999 (100%)	123	min 0	median 64	max 90920
	#	Fwd IAT Max	999 (100%)	295	min 0	median 4	max 112000000
	#	Fwd IAT Mean	999 (100%)	353	min 0	median 4	max 112000000
	#	Fwd IAT Min	999 (100%)	104	min 0	median 3	max 112000000
	#	Fwd IAT Std	999 (100%)	339	min 0	median 0	max 52200000

Finally, after some tweaks of the data, the headers of the files were being read properly. There was one field, Timestamp, that continued to give us issues that we will go into detail about later. This was a big upset for us, as this was what prevented us from doing machine learning anomaly detection jobs on this uploaded data. Besides this, after each day's file upload of network data, an index was added for each file, meaning we could now visualize and dig into the data of each day.

Before we go exactly into what we found in these attacks, we wanted to include a brief explanation of each attack, giving the reader insight as to what kind of attacks we are dealing with, as well as offering some advice in order to prevent these kind of attacks within their network. These will be helpful, as it will give some backstory and insight to the reader when examining our findings.

Attack Explanation 1: Botnet

A botnet attack is when a malicious hacker has internet connected devices that are infected by malware. it involves phishing, data theft, or even exposing sensitive information. To prevent a botnet attack make sure your systems are regularly updated, strong passwords and multi factor authentication help as well.
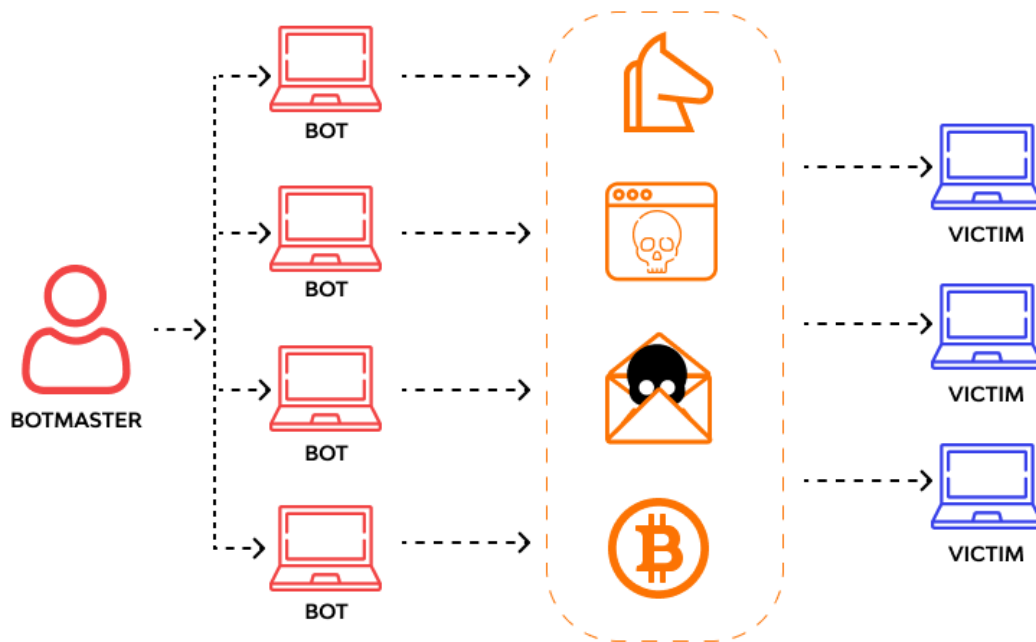
https://assets.website-files.com/5ff66329429d880392f6cba2/61bb4196035abe0abebabf87_Botnet%20example.png

Attack Explanation 2: Brute Force

A brute force attack is when a user or a bot tries different variations of symbols and words until the password is correctly guessed. The best way for a user to prevent a brute force attack is to have a long and unique password, as well as having two factor authentication. The best way for a server to prevent these attacks is to have rate limiting which causes a delay if the password is wrong.

HOW A BASIC BRUTE FORCE ATTACK WORKS

Attacker

Guess List Of Username & Password Combination

Repeats Login Attempts Until One Is Successful

Username
****

Successful Credential Validation

https://www.ssl2buy.com/wiki/wp-content/uploads/2021/09/basic-brute-force-attack.jpg

Attack Explanation 3: Port Scan

A port scan attack is when port scans are used to find weak points in a network, it helps find open ports and lets the hacker know if they are receiving or sending data. Hackers send a message to the port and the response they get lets them know if that port is being used or not, it also lets hackers know if a firewall is being used. To prevent a port scan attack it is best if you have a strong firewall.

https://media.geeksforgeeks.org/wp-content/uploads/20220520112919/portscanning.jpg
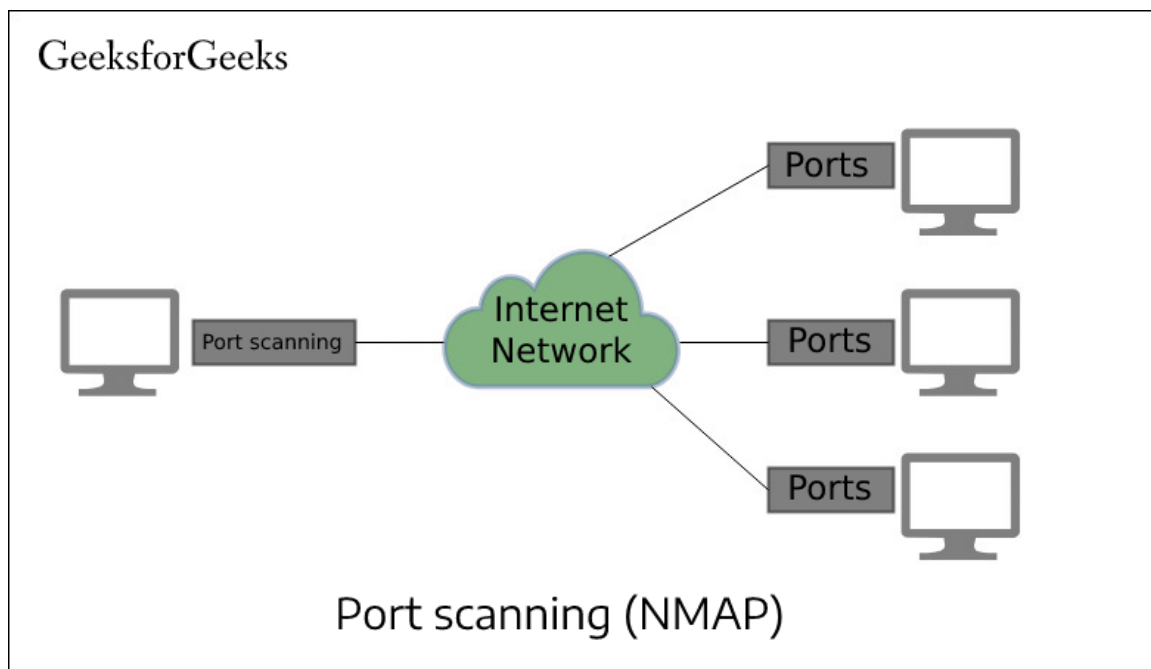
Attack Explanation 4 : DDOS

A DDOS attack is an attempt to affect the availability of a targeted system, typically a website to legitimate end users. The attackers will generate large packets or requests which will overwhelm the targeted system causing it to slow down or crash. The best method to protect your server or network from a DDOS attack is to have a firewall and reduce the attack surface area.
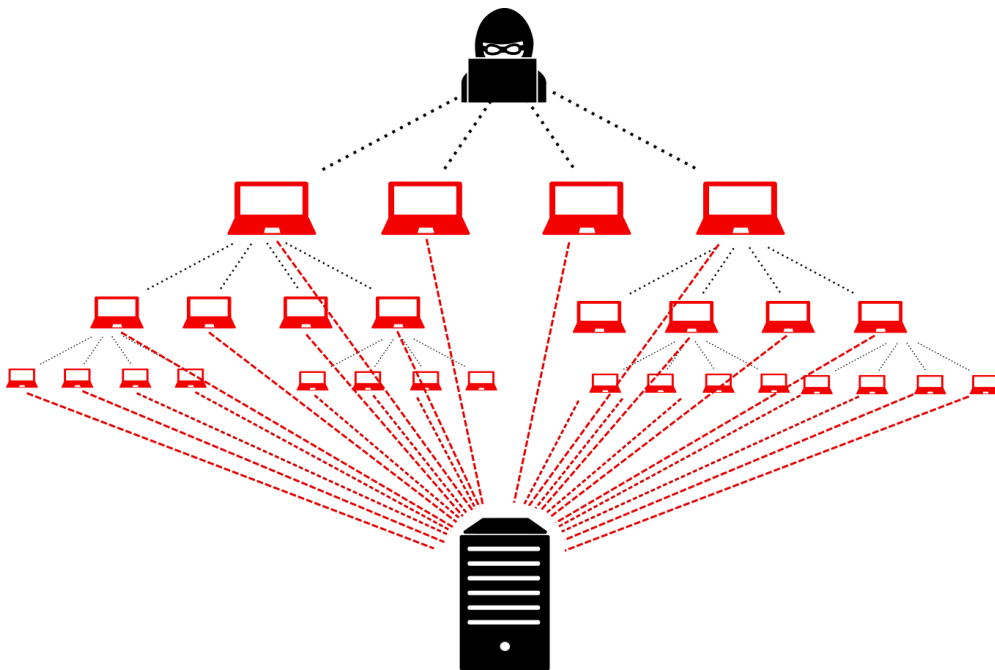
https://ruggedtooling.com/wp-content/uploads/2018/09/Botnet_Attack.png

Attack Analyzation 1: Botnet

These next 4 sections will consist of the data analysis process and the specific anomaly data points regarding each attack.

The first attack we analyzed occurred during Thursday's morning hours. For the analyzation process, we used Elastic's visualization feature, and selected the proper index to analyze using multiple visualization features, tabular, and graphical. The attack that occurred that day was identified to be a botnet. First, we used a table visualization to see different data points, we included the fields label, source and destination IPs, timestamp, count of records, as well as median of source and destination ports.

friday morning botnet

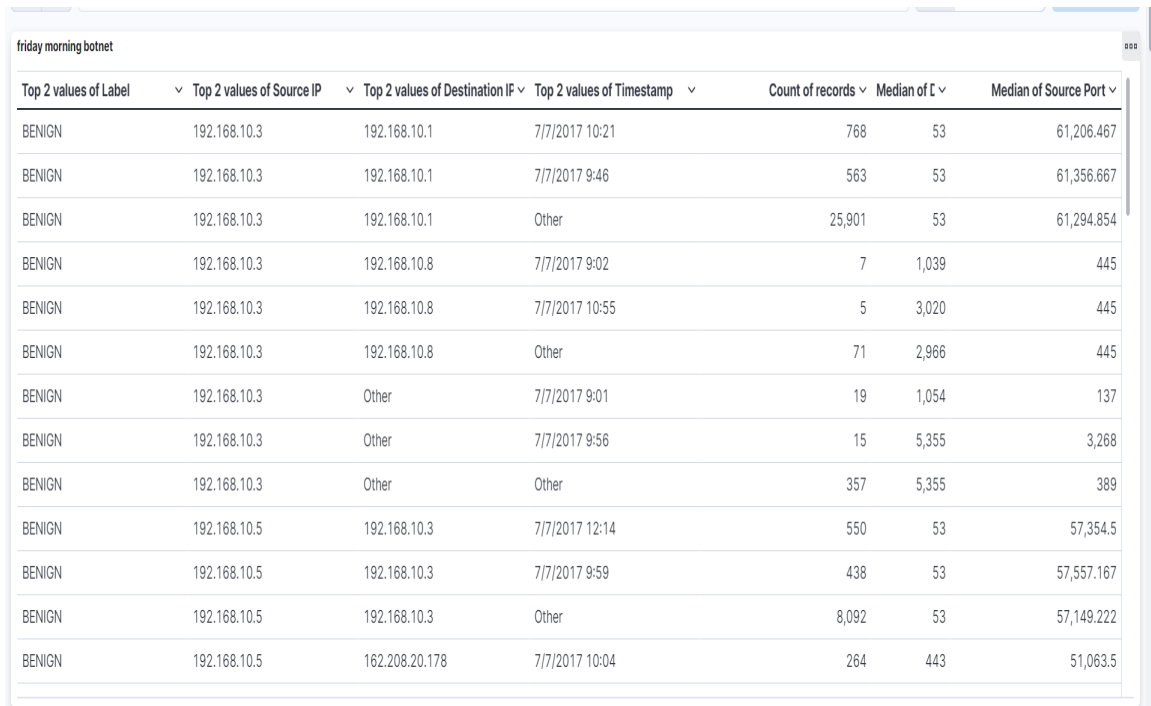| Top 2 values of Label	Top 2 values of Source IP	Top 2 values of Destination IP	Top 2 values of Timestamp	Count of records	Median of D	Median of Source Port
BENIGN	192.168.10.3	192.168.10.1	7/7/2017 10:21	768	53	61,206.467
BENIGN	192.168.10.3	192.168.10.1	7/7/2017 9:46	563	53	61,356.667
BENIGN	192.168.10.3	192.168.10.1	Other	25,901	53	61,294.854
BENIGN	192.168.10.3	192.168.10.8	7/7/2017 9:02	7	1,039	445
BENIGN	192.168.10.3	192.168.10.8	7/7/2017 10:55	5	3,020	445
BENIGN	192.168.10.3	192.168.10.8	Other	71	2,966	445
BENIGN	192.168.10.3	Other	7/7/2017 9:01	19	1,054	137
BENIGN	192.168.10.3	Other	7/7/2017 9:56	15	5,355	3,268
BENIGN	192.168.10.3	Other	Other	357	5,355	389
BENIGN	192.168.10.5	192.168.10.3	7/7/2017 12:14	550	53	57,354.5
BENIGN	192.168.10.5	192.168.10.3	7/7/2017 9:59	438	53	57,557.167
BENIGN	192.168.10.5	192.168.10.3	Other	8,092	53	57,149.222
BENIGN	192.168.10.5	162.208.20.178	7/7/2017 10:04	264	443	51,063.5

In this tabular visualization, which we used for each attack, we get a nice layout of different data points of the various fields previously mentioned. As seen in the label field, we are seeing what benign (normal) activity on the network looks like here, specifically zoning in on the source and destination ports, as well as the IP addresses of the computers involved in this network activity. We are also presented with the timestamp, which is not necessarily formatted correctly, but still serves a role of telling us the time even though it is labeled as a keyword. An important point here is that looking at the port data, we can see the median of the ports that are being used for normal activity
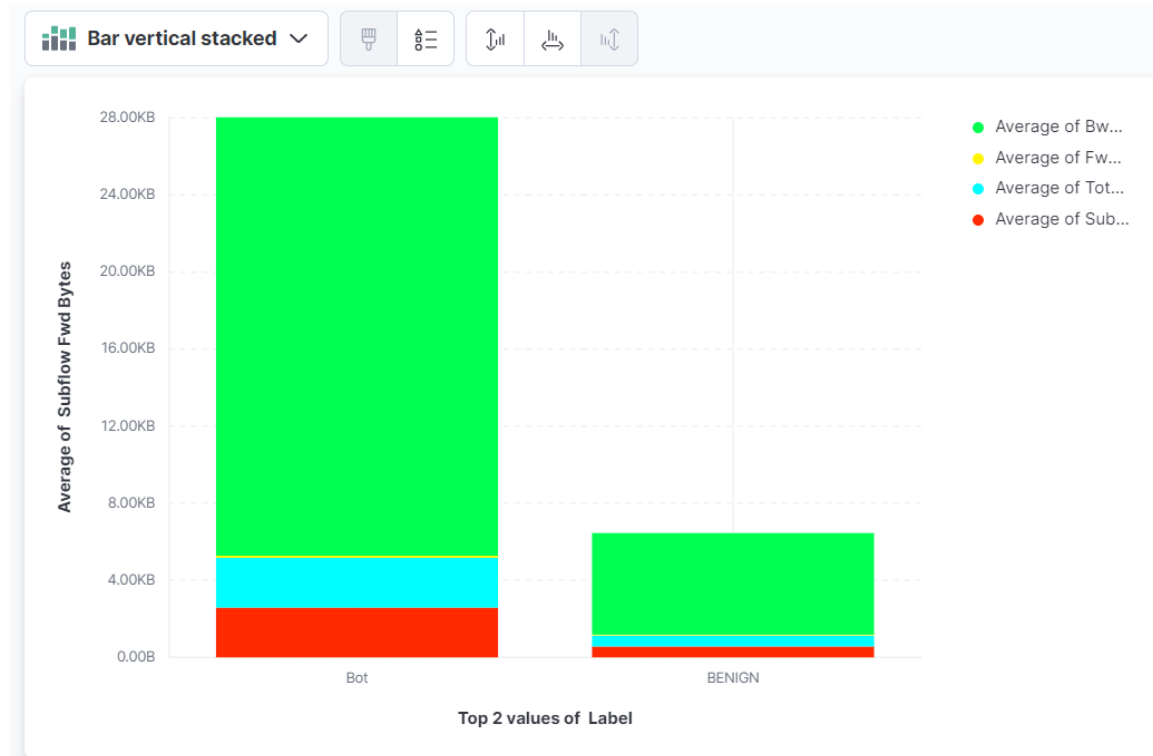
friday morning botnet

Top 2 values of Label	Top 2 values of Source IP	Top 2 values of Destination IP	Top 2 values of Timestamp	Count of records	Median of D	Median of Source Port
BENIGN	Other	Other	Other	77,347	443	6,684.747
Bot	205.174.165.73	192.168.10.15	7/7/2017 10:45	10	52,916.5	8,080
Bot	205.174.165.73	192.168.10.15	7/7/2017 10:46	10	52,928.5	8,080
Bot	205.174.165.73	192.168.10.15	Other	189	52,343	8,080
Bot	205.174.165.73	192.168.10.9	7/7/2017 10:44	8	4,087.5	8,080
Bot	205.174.165.73	192.168.10.9	7/7/2017 10:36	7	3,649	8,080
Bot	205.174.165.73	192.168.10.9	Other	131	3,643	8,080
Bot	205.174.165.73	Other	7/7/2017 10:38	23	51,706	8,080
Bot	205.174.165.73	Other	7/7/2017 10:45	20	51,749.5	8,080
Bot	205.174.165.73	Other	Other	307	51,702	8,080
Bot	192.168.10.15	205.174.165.73	7/7/2017 10:45	14	8,080	52,913.5
Bot	192.168.10.15	205.174.165.73	7/7/2017 10:43	10	8,080	52,857.5
Bot	192.168.10.15	205.174.165.73	Other	347	8,080	52,940

Upon further examination, we begin to see some bot activity. A new IP address is associated with each bot labeled activity, which is the attacker's IP address, 205.174.185.73. Another key data point anomaly here is that we see port 8080 is associated with all bot entries, which means the attacker was using port 8080 as a port of attack.

Bar vertical stacked

Average of Bw...		
Average of Fw...		
Average of Tot...		
Average of Sub...		

Top 2 values of Label

BENIGN

Average of Bwd Packets/s	5.27KB
Average of Fwd Packet Length Mean	51.31B
Average of Total Length of Fwd Packets	579.80B
Average of Subflow Fwd Bytes	579.80B

Bot

Average of Bwd Packets/s	22.76KB
Average of Fwd Packet Length Mean	113.28B
Average of Total Length of Fwd Packets	2.58KB
Average of Subflow Fwd Bytes	2.58KB

Looking further into the data using graphical visualizations, and taking into account the entire file's contents (records), we included some more fields to be analyzed, average of backward packets, the average of forward packet length mean, average of total length of forward packets, and average of subflow forward bytes, all features identified to be anomalous in this dataset. As seen above, there is a massive difference in each of the fields. All of the field's values are massively bigger in botnet activity.

Attack Analyzation 2: Brute Force

Our second analysis took place on Friday morning, and was revolved around a brute force attack attempt by the attacker. The fields we analyzed here were label, source and destination IPs, timestamp, average initial window bytes forward and backward, and the sum of ACK, PSH, and SYN flags. As mentioned in the introduction, this data had been labeled through the open source application CICFLOWMETER, whom gives us information on what exactly some of these labels are referring to.

cicids-thursmorn-bruteforce

Top 2 values of La ⌄	Top value of Sour⌄	Top value of Desti⌄	Top 2 values of Ti ⌄	Count of records ⌄	Average of Init_W ⌄	Average of Init_W ⌄	Sum of ACK Flag (⌄	Sum of PSH Flag (⌄	Sum of SYN Flag (⌄
BENIGN	192.168.10.3	192.168.10.1	6/7/2017 9:39	451	-1	-1	-	-	-
BENIGN	192.168.10.3	192.168.10.1	6/7/2017 9:29	442	-1	-1	-	-	-
BENIGN	192.168.10.3	192.168.10.1	Other	23,197	-1	-1	-	-	-
BENIGN	192.168.10.3	Other	6/7/2017 9:01	47	1,839.298	150.213	46	-	-
BENIGN	192.168.10.3	Other	6/7/2017 9:05	15	9,823.667	4,336.4	14	-	-
BENIGN	192.168.10.3	Other	Other	398	4,180.201	1,788.374	217	58	21
BENIGN	Other	192.168.10.3	6/7/2017 9:39	1,092	-1	-1	-	-	-
BENIGN	Other	192.168.10.3	6/7/2017 11:46	981	32.407	7.364	-	4	-
BENIGN	Other	192.168.10.3	Other	52,452	310.037	33.212	518	629	125
BENIGN	Other	Other	6/7/2017 9:39	1,497	8,388.576	3,977.134	677	789	109
BENIGN	Other	Other	6/7/2017 11:46	1,296	11,607.287	4,769.913	554	724	105
BENIGN	Other	Other	Other	85,879	10,897.269	3,998.474	43,835	36,254	7,034
Web Attack � Bru...	172.16.0.1	192.168.10.50	6/7/2017 9:40	42	26,499.095	23,578.143	4	38	-
Web Attack � Bru...	172.16.0.1	192.168.10.50	6/7/2017 9:46	41	26,433.22	23,446.878	4	37	-
Web Attack � Bru...	172.16.0.1	192.168.10.50	Other	1,424	26,510.178	23,440.39	135	1,289	-

Average Init_Win_Bytes_Fwd, and average Init_Win_Bytes_Bwd, and sum of Push flag count are some major anomaly data points in this brute force attack we can see at first glance in the table.The average Init bytes in both directions are much higher in brute force attacks network activity, as well as push flags being absurdly high in the records of brute force activity.
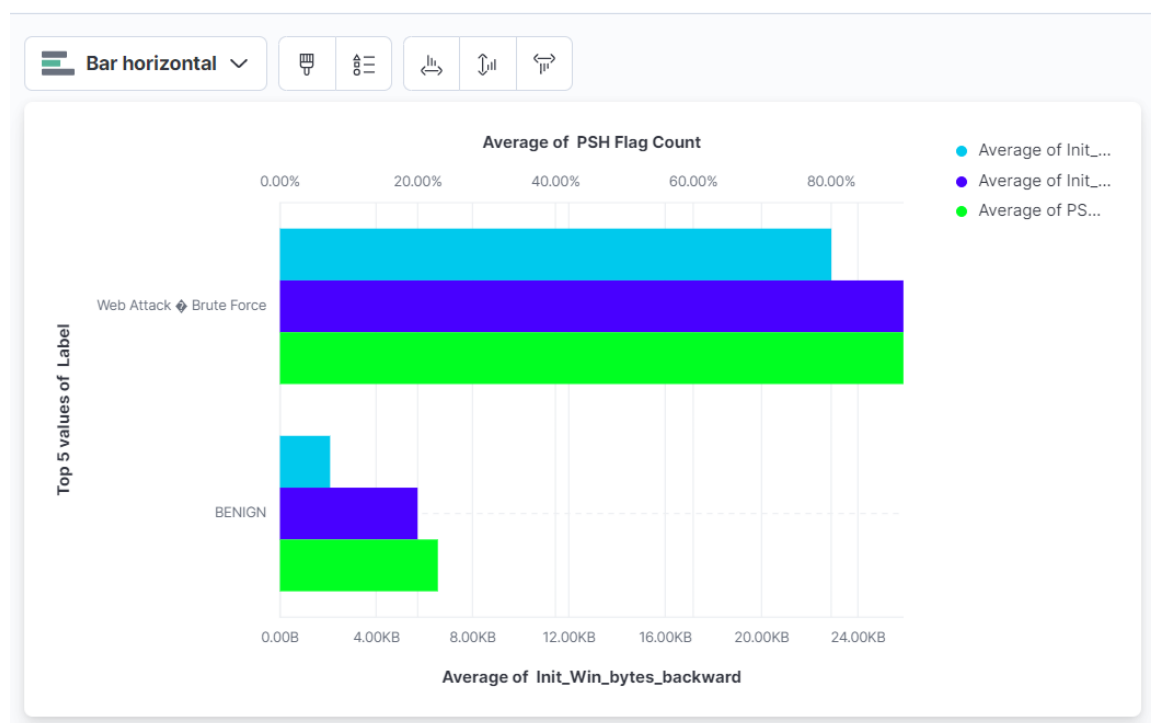
With further analysis, zoning in on those previous suspicious fields, Init_Win_Bytes_Fwd, and average Init_Win_Bytes_Bwd, and sum of Push flag count, the creation of this Horizontal bar graph visualization offered by Elastic, shows us just how anomalous these data points are. We see that the average of initial window bytes both forwards and backwards are extremely higher in brute force records than in benign records, with the average initial window bytes backward in activity being 2.08KB and average initial window bytes forward being 5.71KB, while in brute force activity the average initial window bytes backwards being raised substantially, being 22.89KB, as well as the average initial window bytes forward being 25.89KB, With all records factored in (a lot of records). Another interesting number, percent actually, is the average PSH flag count, being about 67% higher in brute force labeled network data points than it is in benign labeled network data points.

Attack Analyzation 3: Port Scan

The third attack analysis took place on Friday afternoon, and this attack was identified to be a port scan. The first thing that was apparent in this case was that the port scan consisted of more than 50% of activity on the network. This is expected, as in a port scan attack, an attacker is sending packets to all kinds of ports to scope out the network environment, and to find vulnerabilities within the network.

cicids-frimorn-portscan

Top 2 values of Label ⌄	Count of records ⌄
PortScan	158,930
BENIGN	127,498

The key anomaly features we found within the port scan analyzation were the average of bwd packets being significantly higher in port scan activity, and the high percentage use of PSH flags by the attacker.

cicids-frimorn-portscan (copy)

Top 2 values of Label ⌄	Top 2 values of Source IP ⌄	Top 2 values of Destination ⌄	Top 10 values of Timestamp ⌄	Count of records ⌄	Average of Bwd Packets/s ⌄	Sum of PSH Flag Count ⌄
PortScan	172.16.0.1	192.168.10.50	7/7/2017 2:55	44,410	31,497.764	44,410
PortScan	172.16.0.1	192.168.10.50	7/7/2017 2:52	43,603	31,750.11	43,603
PortScan	172.16.0.1	192.168.10.50	7/7/2017 2:54	34,620	30,709.87	34,620
PortScan	172.16.0.1	192.168.10.50	7/7/2017 2:51	10,916	31,088.691	10,914
PortScan	172.16.0.1	192.168.10.50	7/7/2017 3:22	5,014	30,209.598	5,006
PortScan	172.16.0.1	192.168.10.50	7/7/2017 3:08	5,002	32,713.222	4,993
PortScan	172.16.0.1	192.168.10.50	7/7/2017 3:09	4,025	31,520.03	4,016
PortScan	172.16.0.1	192.168.10.50	7/7/2017 3:23	4,010	29,828.581	4,000
PortScan	172.16.0.1	192.168.10.50	7/7/2017 2:53	3,957	33,326.207	3,957
PortScan	172.16.0.1	192.168.10.50	7/7/2017 3:10	2,009	31,544.195	2,005
PortScan	172.16.0.1	192.168.10.50	Other	1,364	24,984.118	1,338
BENIGN	192.168.10.3	192.168.10.1	7/7/2017 1:34	572	52.304	-
BENIGN	192.168.10.3	192.168.10.1	7/7/2017 1:36	344	179.338	-
BENIGN	192.168.10.3	192.168.10.1	7/7/2017 3:10	343	66.958	-
BENIGN	192.168.10.3	192.168.10.1	7/7/2017 2:13	310	116.065	-
BENIGN	192.168.10.3	192.168.10.1	7/7/2017 3:22	306	169.039	-

Firstly, taking a look at our tabular visualization, we can see the average of backward packets being super high, and push flags being utilized in all port scan network entries. No PSH flags are existent in the small amount of records being shown here in the benign activity in the table.
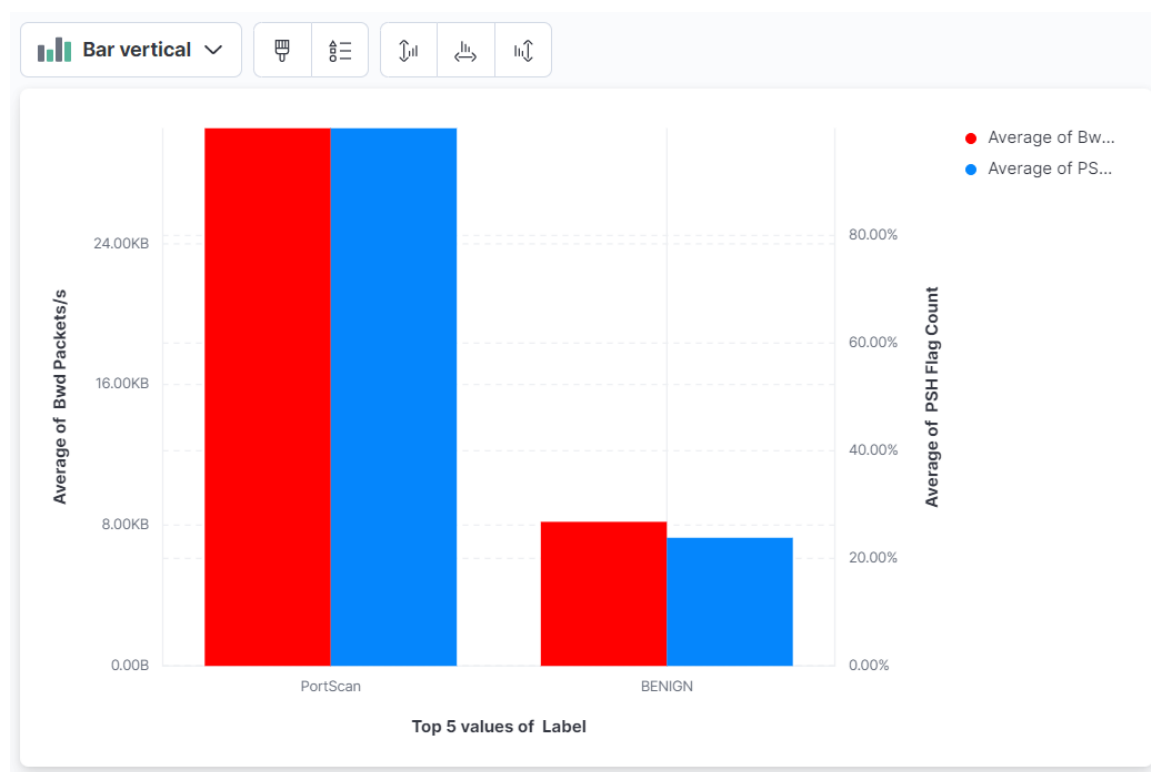
Taking all network entries into account on this Friday afternoon with a graphic visualization, we can see the average backward packet of all port scan activity being 31,313 KB, as well as a whopping 99.96% entries having a PSH flag attached. In benign activity, a measly average backward packets of 8.20KB and only 23.83% entries having a PSH flag attached, we can clearly see the anomaly here, showing us that something very fishy is going on in the network with backward packets and PSH flags, identified as a port scan attack.

We found the PSH flag data here to be very interesting, as a PSH flag instructs the operating system to send and receive data immediately, and in the case of a port scan attack this makes perfect sense. The attacker would want to initially scan the network obviously, but they would also want to get the feedback of what is going on with the destination as fast as possible. In the case if they were scanning, perhaps their malicious activity would be detected very fast, so they would want to get results immediately, and a PSH flag is a very flag to help them in this, as they could receive the data of their target quickly and retain it, before their port scan attack could be stifled.

Attack Analyzation 4: DDOS

The fourth and final attack we analyzed was a DDOS attack that took place Friday afternoon, similar to the port scan attack. Some key features we found to be anomalous with the DDOS attack was backward packet length standard deviation, average packet size, total length of backward packets, and backward packet length max.
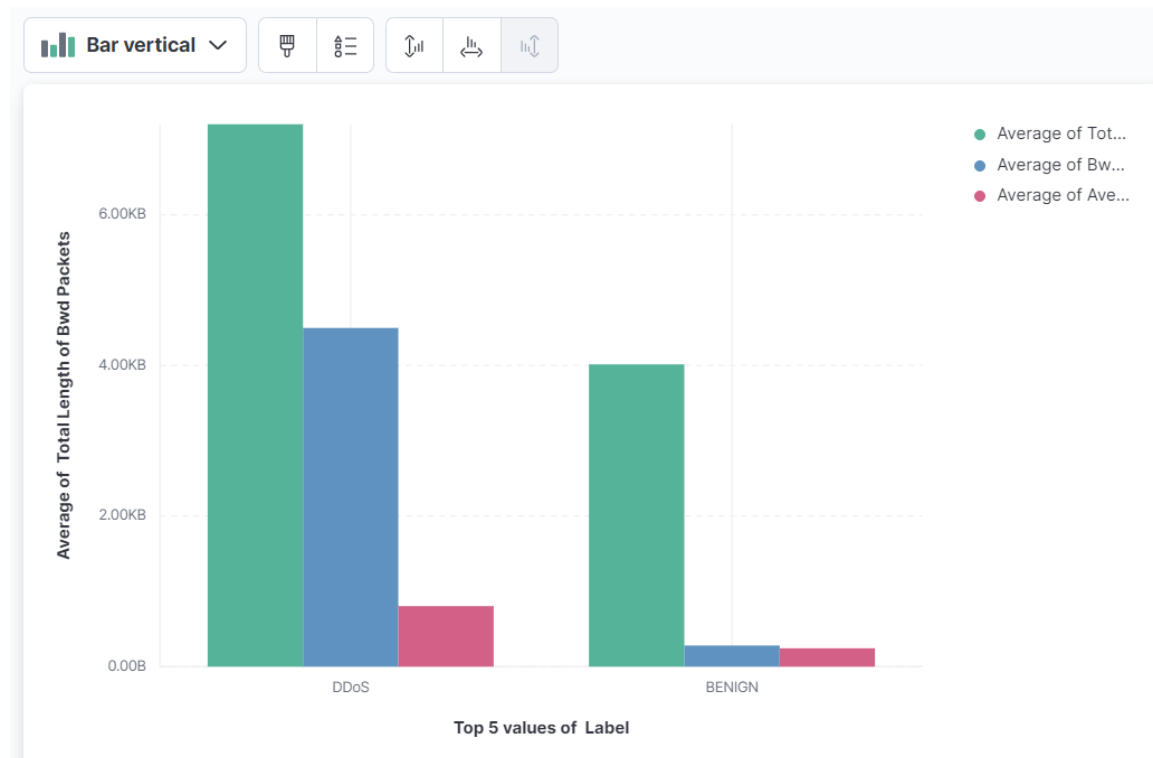
In normal activity, the average total length of Bwd packets were 4KB, while the average backward packet length max is 287B, and average packet size is 249B. In the DDOS activity, the average total length of backward packets is 7.20KB, and the average

backward packet length max is 4.5KB, while the average packet size is 822 bytes. We can see a drastic difference in these values, indicating anomalous behavior which is certified by the DDOS labeled activity.

With further visualization, we get another scope of the drastic anomalous network activity, this time taking into account the backward packet length standard deviation, as backward packets are the main feature which is affected by the ddos attack. Here we have the average of the average packet size, showing benign activity to have an average of 249B, and ddos activity having an average of 822B. The average of backward packet length standard deviation in normal activity is only 87 bytes, while the ddos activity is shown to have an average backward packet length of 2KB.

Professional Accomplishments

Elastic will be a key component in our work field if we need to break down and analyze packets. This also allows us to look at traffic that is being sent and received through a network. The information that elastic gives us, based on the mappings that we have configured will give us a visualization of what we choose. In our case we now know how to tell if a network is going through a DDOS attack, Botnet attack, Port scan attack, or a Brute force attack.

With the help of this project, we were able to sharpen our skills using elastic, as well as learning more about pcap files and some of their key features. We were able to see some of the fields of the file that were most important when related to botnet, brute force, port scan, and ddos attacks. Though the pcap file was not raw and was already processed using CICFLOWMETER, it was extremely good practice to manually dig into this data using elastic, as well as becoming more familiar with elastic along the way.

This kind of practice and knowledge we got through this project is paramount, and since it was manual without the use of an IDS, we in a way served as the IDS. Because of this, we can now have more understanding of exactly how an IDS works, as well as be familiar with anomalous data they detect.

Difficulties And Problems

The main problem that we encountered was trying to get the timestamps to properly display on to our file that we uploaded into elastic from our dataset. There was a problem with excel that kept messing up the format of the timestamps whenever we tried to change the format of the time that we wanted. Without the timestamps it made it hard to make the visualization part of our project the way that we wanted it.

Aside from the timestamp problem on the excel spreadsheet one of the other difficulties was finding the right PCAPS and files that we wanted to break down and analyze. We also had to make sure that these files weren't too big because if the file was too big then we couldn't put it into elasic. The two specifc CICIDS2017 packets that we used were the network traffic from a Thursday morning and a Friday morning afternoon. We originally wanted to use Wednesday morning traffic as well but that file was too big for elastic. That was the main problem that we had with the files.

Conclusion

This project has helped with our understanding of being able to see what is being sent through networks and with the help of Elastic we can break down the information and see what is actually happening in the network. In the cyber workforce we will know how to read these packets which will make our future careers easier.

After hours spent configuring mappings to read these data files, and analyzing these data files through elastic via upload, we have gained quite a bit of insight into certain attacks happening within a network, and have learned how an IDS would detect these attacks and relay the detection to us. There were many fields in these files that had anomalous behavior related to the specific attack, and we were able to visualize and see the various anomalous data points within the botnet, brute force, port scan, and ddos attacks.

Each of these 4 attacks have their own giveaways and keys that we can read that will tell us what attack is happening on the network. For instance, when you see a high "average of BWD packets" and some type of "PSH Flag Count" that lets us know that a Port Scan attack is taking place. Looking at these clues and knowing exactly what we're looking for will always keep us ready and know how to exactly defend our networks and systems in the predicament of us being under some type of attack. Just remember to always keep your passwords long and unique, update your systems regularly, have two factor authentication, reduce your surface area, and have strong firewalls. Having these simple precaution measures and limiting your user mistakes will keep your networks and systems in a safe state.

References

Anderson, P. (1982). Shield. Amazon. Retrieved November 29, 2022, from https://aws.amazon.com/shield/ddos-attack-protection/

Search UNB. University of New Brunswick est.1785. (n.d.). Retrieved November 28, 2022, from https://www.unb.ca/cic/datasets/ids-2017.html

Sharafaldin, I. (2018). *Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization*. ScitePress. Retrieved November 28, 2022, from https://www.scitepress.org/papers/2018/66398/66398.pdf

What is a botnet attack? 5 ways to prevent it. SecurityScorecard. (n.d.). Retrieved November 29, 2022, from https://securityscorecard.com/blog/what-is-a-botnet-attack#:~:text=A%20botnet%20attack%20is%20a,or%20launching%20vicious%20DDoS%20attacks.

What is a brute force attack & how to prevent it? | Cybernews. (n.d.). Retrieved November 29, 2022, from https://cybernews.com/security/what-is-a-brute-force-attack/

What is a port scan? how to prevent port scan attacks? Fortinet. (n.d.). Retrieved November 29, 2022, from https://www.fortinet.com/resources/cyberglossary/what-is-port-scan