COGOPORT

OUR FUTURE WITH NETWORK SECURITY

Presented by Sachin Chopra

Mentored by Sanat Talwar

COVERED TODAY

A BRIEF OUTLINE OF INTERNSHIP WORK

Introduction to Security

Types of Security

Work done during Internship (The WHAT)

Implementation and Documentation (The HOW)

Live Demo

To the Future

THE STATE OF SECURITY

WHERE WE ARE TODAY

Network security is protection of the access to files and directories in a computer network against hacking, misuse and unauthorized changes to the system or Denial of Service provided by company. Cogoport has not taken explicit measures to prevent it’s network and services from such attacks and immediate action is required.

POPULAR ATTACK STYLES

SQL INJECTION

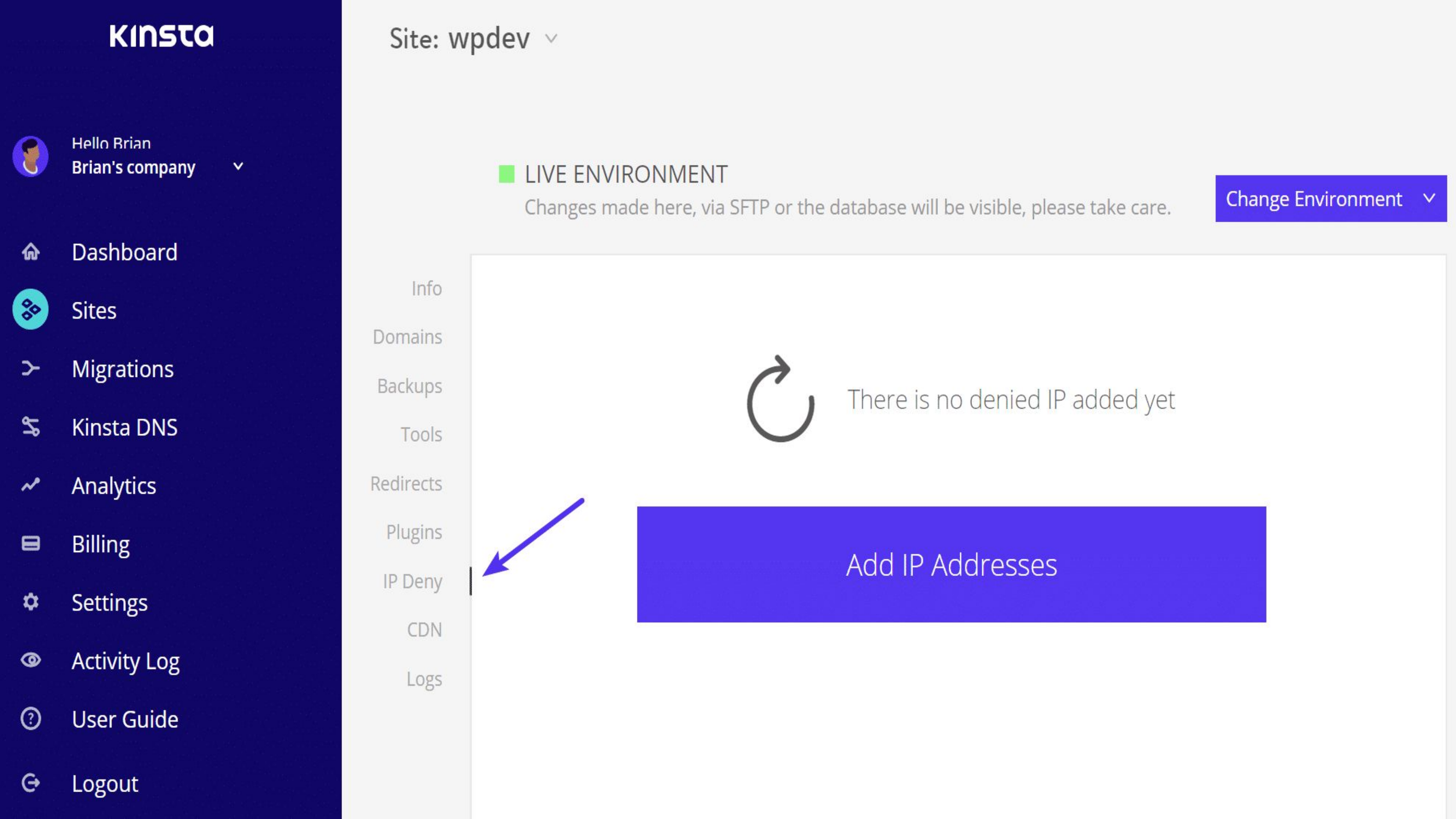
(HAAN KOI BAAT NAHI SAMBHAL LENGE)

DENIAL OF SERVICE (DOS)

(ISKO BLOCK MAAR RE)

DISTRIBUTED DENIAL OF SERVICE (DDOS)

(S#*T ,#**#)



🟩 LIVE ENVIRONMENT

Changes made here, via SFTP or the database will be visible, please take care.

There is no denied IP added yet

TYPES OF SECURITY

- Cyber Security
- Network Security
- Information Security
- Cloud Security

Types of Security

INFORMATION SECURITY

Ensures that both physical and digital data is protected from unauthorized access, use, disruption, modification, inspection, recording or destruction.

CYBER SECURITY

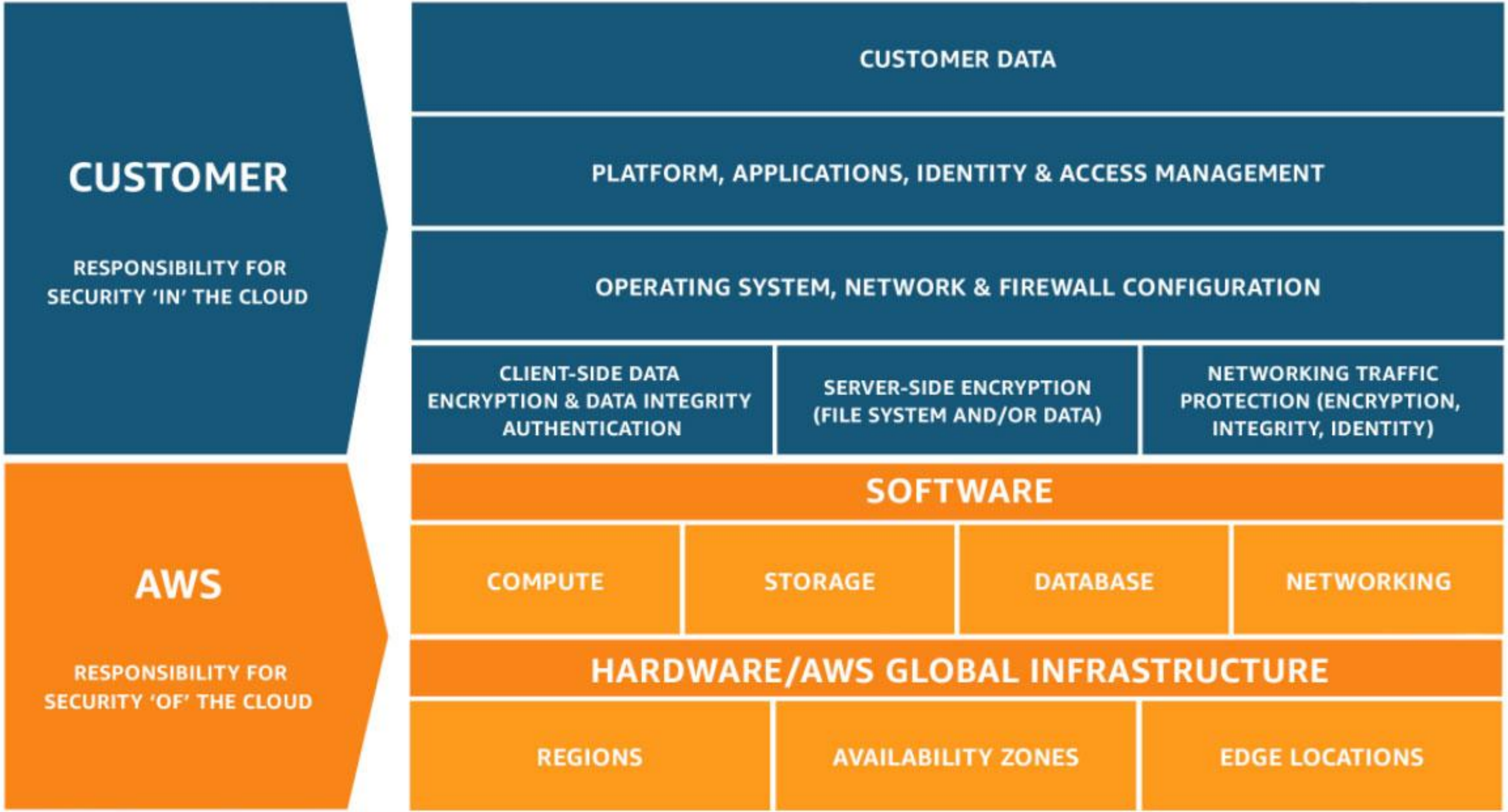
Practice of defending networks, computers and data from unauthorized digital access, attack or damage.

NETWORK SECURITY

Network security, aims to protect any data that is being sent through devices in your network to ensure that the information is not changed or intercepted.

CLOUD SECURITY

Protection of data, applications, and infrastructures involved in cloud computing. Shared Security model of AWS.



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION	SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)	NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE	STORAGE	DATABASE	NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS	AVAILABILITY ZONES	EDGE LOCATIONS

NETWORK SECURITY

FIREWALL AND ANTI-VIRUS

Monitors incoming and outgoing network traffic based on predetermined port rules

IDS/IPS

Identifies any suspicious pattern that may indicate an attack the system and acts as a security check on all transactions

VPN

Acts like a tunnel so you can exchange data securely and anonymously across the internet

cogoport

ANALOGY

WALLS OUTSIDE HOUSE

It's called Firewall in Network Security

MOTION SENSOR ALARMS

Intrusion Detection system (IDS) like Snort.

CALLING POLICE AUTOMATICALLY

Intrusion Prevention System

SUPERMAN

Super Next Generation firewall

FIREWALL

Building a firewall by rule management on port level for tcp/udp network packets.

SNORT

Open source tool for network packet dsniffing and rule matching to detect malicious traffic.

WIRESHARK

Network troubleshooting, analysis, software and communications protocol development

TOOLS AT DISPOSAL

SWATCHER

Used for reading log files in sys.log and sending mails.

KIBANA/LOGSTASH

Attractive interface for monitoring traffic to keep a check for activities not seen on network before.

THOR’S HAMMER

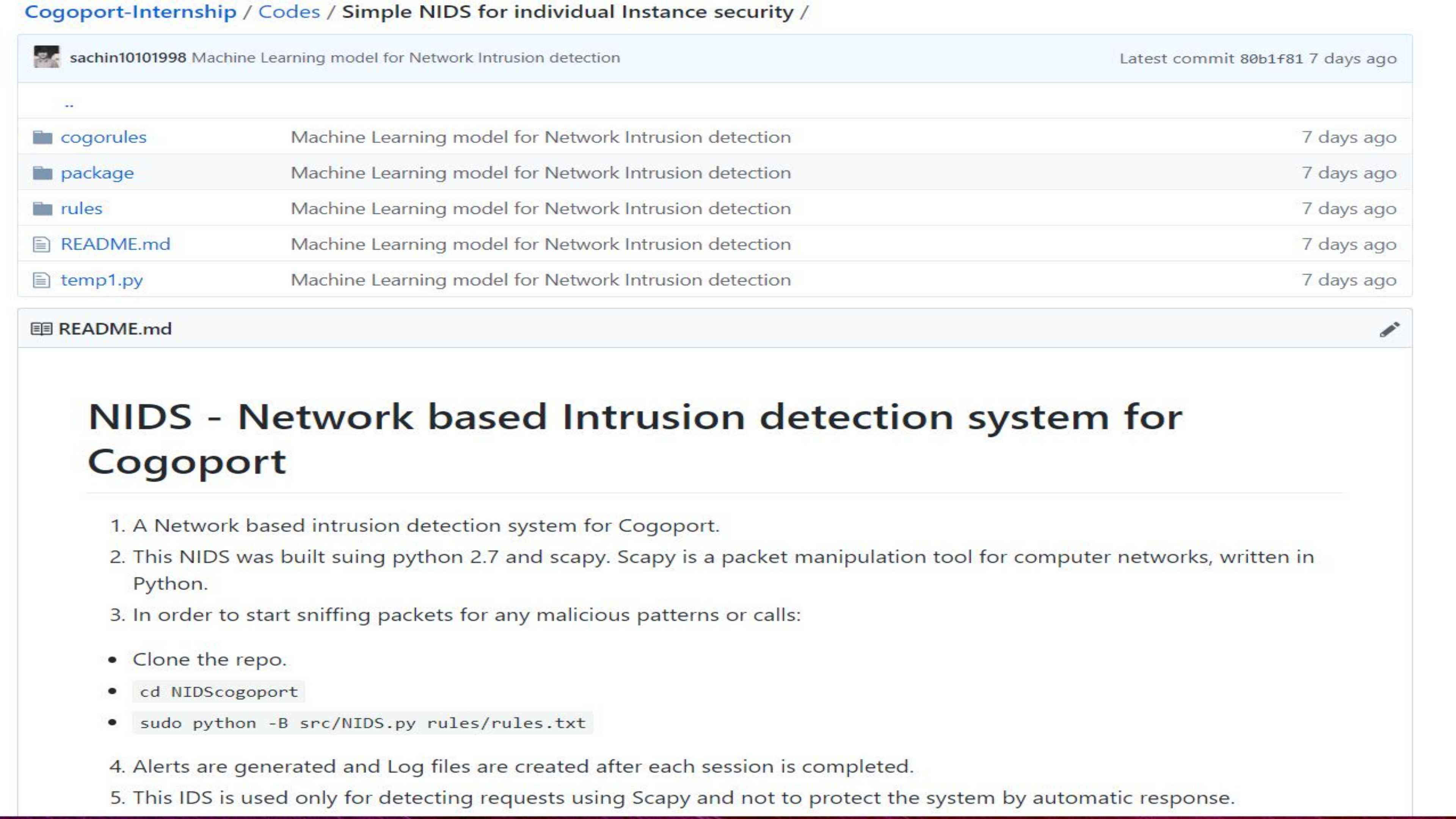
My pre-final year project for DoS attacks and DDos attacks (keeping in view the legal stuff).

TOOLS AT DISPOSAL

SCAPY

TECHNOLOGY
IN OUR DAILY LIVES

Scapy is a packet manipulation tool for computer networks, written in Python by Philippe Biondi. It can forge or decode packets, send them on the wire, capture them, and match requests and replies. It can also handle tasks like scanning, tracerouting, probing, unit tests, attacks, and network discovery



Cogoport-Internship / Codes / Simple NIDS for individual Instance security /

sachin10101998 Machine Learning model for Network Intrusion detection — Latest commit 80b1f81 7 days ago

..		
cogorules	Machine Learning model for Network Intrusion detection	7 days ago
package	Machine Learning model for Network Intrusion detection	7 days ago
rules	Machine Learning model for Network Intrusion detection	7 days ago
README.md	Machine Learning model for Network Intrusion detection	7 days ago
temp1.py	Machine Learning model for Network Intrusion detection	7 days ago

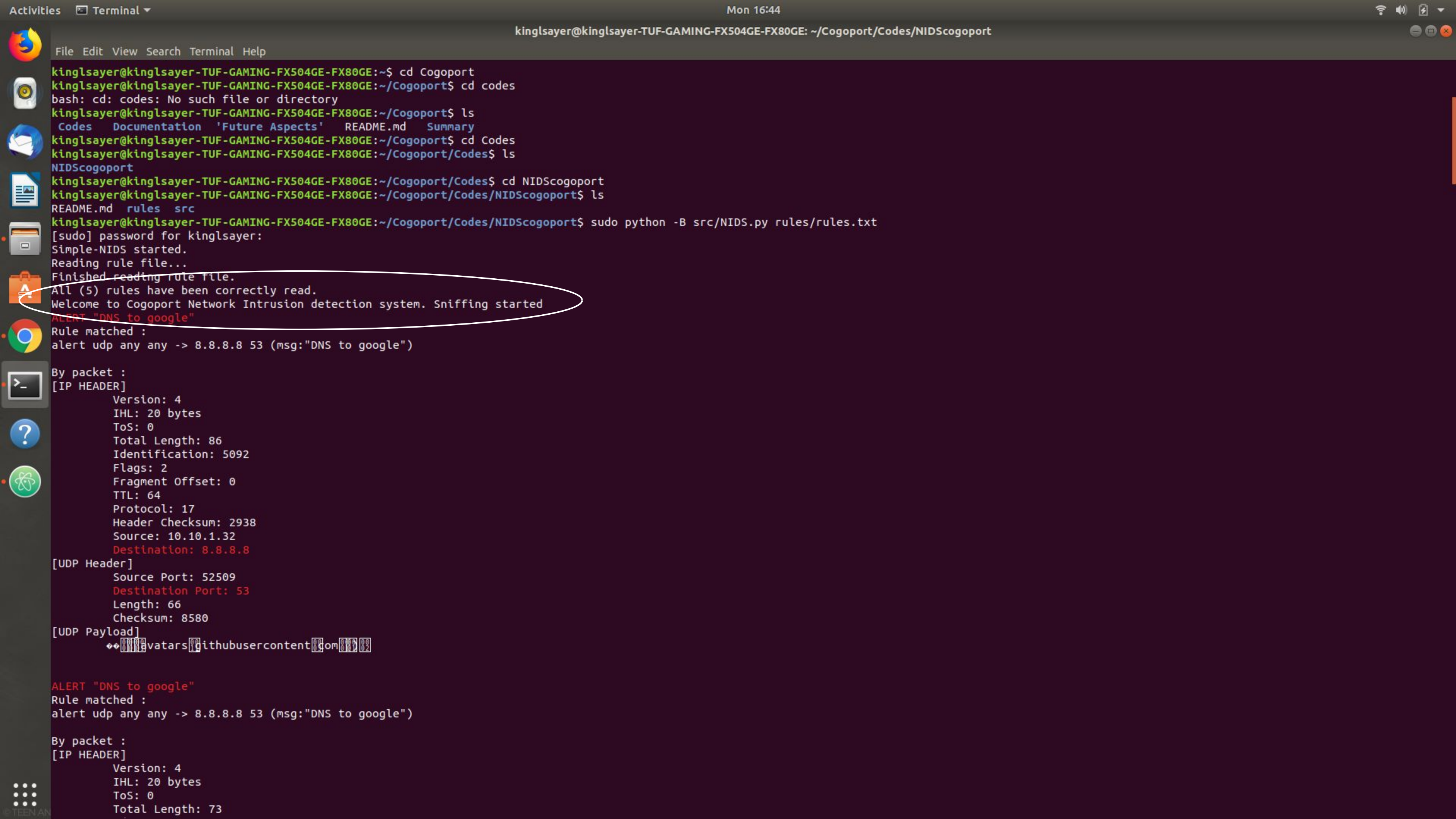
README.md

NIDS - Network based Intrusion detection system for Cogoport

1. A Network based intrusion detection system for Cogoport.
2. This NIDS was built suing python 2.7 and scapy. Scapy is a packet manipulation tool for computer networks, written in Python.
3. In order to start sniffing packets for any malicious patterns or calls:

- Clone the repo.
- `cd NIDScogoport`
- `sudo python -B src/NIDS.py rules/rules.txt`

4. Alerts are generated and Log files are created after each session is completed.
5. This IDS is used only for detecting requests using Scapy and not to protect the system by automatic response.


Activities
Terminal
Mon 16:44
kinglsayer@kinglsayer-TUF-GAMING-FX504GE-FX80GE: ~/Cogoport/Codes/NIDScogoport
File
Edit
View
Search
Terminal
Help

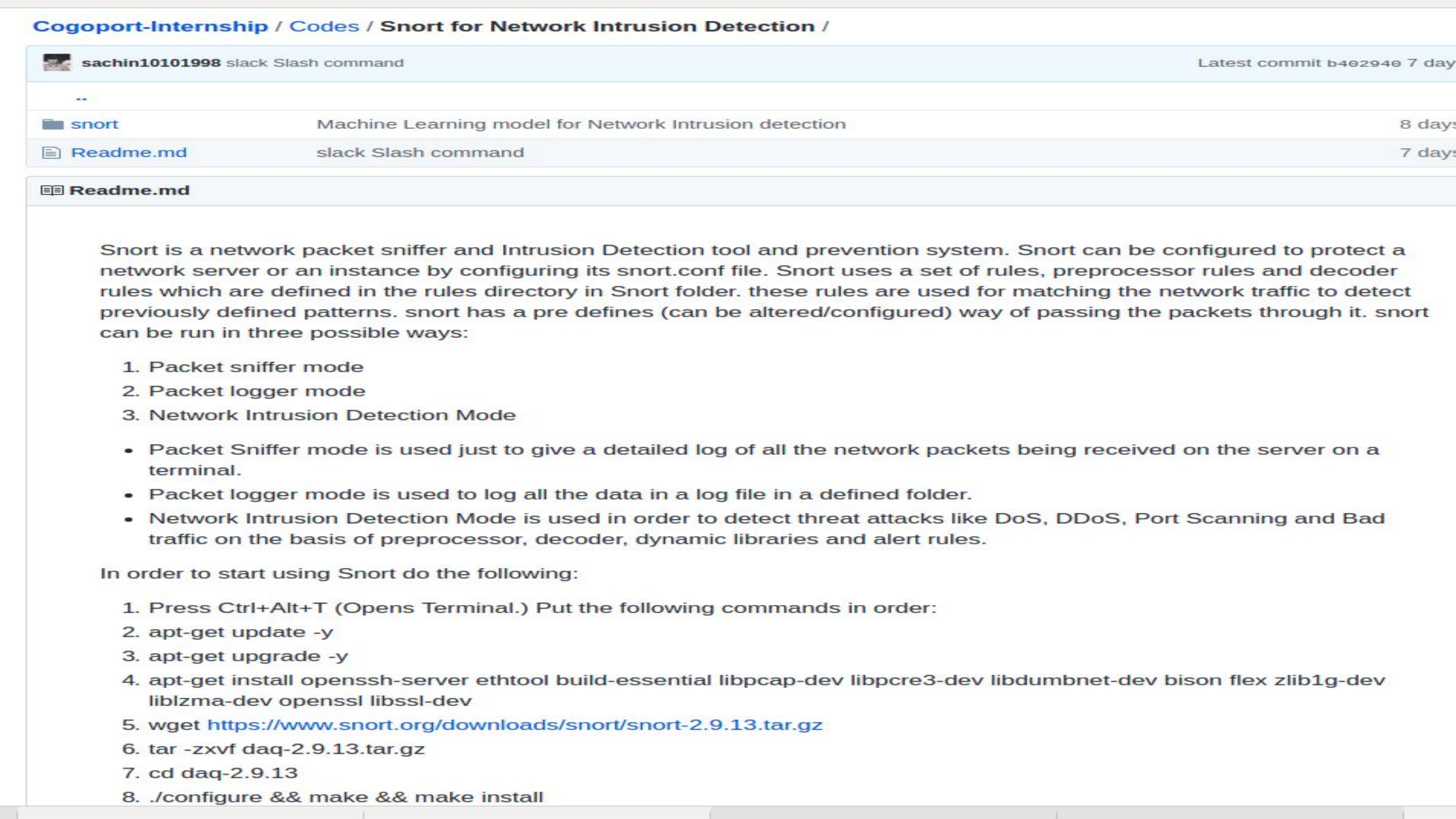
```
kinglsayer@kinglsayer-TUF-GAMING-FX504GE-FX80GE:~$ cd Cogoport
kinglsayer@kinglsayer-TUF-GAMING-FX504GE-FX80GE:~/Cogoport$ cd codes
bash: cd: codes: No such file or directory
kinglsayer@kinglsayer-TUF-GAMING-FX504GE-FX80GE:~/Cogoport$ ls
 Codes   Documentation  'Future Aspects'   README.md   Summary
kinglsayer@kinglsayer-TUF-GAMING-FX504GE-FX80GE:~/Cogoport$ cd Codes
kinglsayer@kinglsayer-TUF-GAMING-FX504GE-FX80GE:~/Cogoport/Codes$ ls
NIDScogoport
kinglsayer@kinglsayer-TUF-GAMING-FX504GE-FX80GE:~/Cogoport/Codes$ cd NIDScogoport
kinglsayer@kinglsayer-TUF-GAMING-FX504GE-FX80GE:~/Cogoport/Codes/NIDScogoport$ ls
README.md  rules  src
kinglsayer@kinglsayer-TUF-GAMING-FX504GE-FX80GE:~/Cogoport/Codes/NIDScogoport$ sudo python -B src/NIDS.py rules/rules.txt
[sudo] password for kinglsayer:
Simple-NIDS started.
Reading rule file...
Finished reading rule file.
All (5) rules have been correctly read.
Welcome to Cogoport Network Intrusion detection system. Sniffing started
ALERT "DNS to google"
Rule matched :
alert udp any any -> 8.8.8.8 53 (msg:"DNS to google")

By packet :
[IP HEADER]
         Version: 4
         IHL: 20 bytes
         ToS: 0
         Total Length: 86
         Identification: 5092
         Flags: 2
         Fragment Offset: 0
         TTL: 64
         Protocol: 17
         Header Checksum: 2938
         Source: 10.10.1.32
         Destination: 8.8.8.8
[UDP Header]
         Source Port: 52509
         Destination Port: 53
         Length: 66
         Checksum: 8580
[UDP Payload]
        ��□□□avatars□githubusercontent□com□□)□


ALERT "DNS to google"
Rule matched :
alert udp any any -> 8.8.8.8 53 (msg:"DNS to google")

By packet :
[IP HEADER]
         Version: 4
         IHL: 20 bytes
         ToS: 0
         Total Length: 73
```

SNORT

Network IDS, capable of performing real-time traffic analysis and packet logging on IP networks. Can perform protocol analysis, content searching, and can be used to detect a variety of attacks, such as buffer overflows, port scans, CGI attacks, SMB probes, OS fingerprinting attempts etc.

WIRESHARK

Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.



Cogoport-Internship / Codes / Snort for Network Intrusion Detection /

sachin10101998 slack Slash command — Latest commit b402940 7 day

..

snort	Machine Learning model for Network Intrusion detection	8 days
Readme.md	slack Slash command	7 days

Readme.md

Snort is a network packet sniffer and Intrusion Detection tool and prevention system. Snort can be configured to protect a network server or an instance by configuring its snort.conf file. Snort uses a set of rules, preprocessor rules and decoder rules which are defined in the rules directory in Snort folder. these rules are used for matching the network traffic to detect previously defined patterns. snort has a pre defines (can be altered/configured) way of passing the packets through it. snort can be run in three possible ways:

1. Packet sniffer mode
2. Packet logger mode
3. Network Intrusion Detection Mode

- Packet Sniffer mode is used just to give a detailed log of all the network packets being received on the server on a terminal.
- Packet logger mode is used to log all the data in a log file in a defined folder.
- Network Intrusion Detection Mode is used in order to detect threat attacks like DoS, DDoS, Port Scanning and Bad traffic on the basis of preprocessor, decoder, dynamic libraries and alert rules.

In order to start using Snort do the following:

1. Press Ctrl+Alt+T (Opens Terminal.) Put the following commands in order:
2. apt-get update -y
3. apt-get upgrade -y
4. apt-get install openssh-server ethtool build-essential libpcap-dev libpcre3-dev libdumbnet-dev bison flex zlib1g-dev liblzma-dev openssl libssl-dev
5. wget https://www.snort.org/downloads/snort/snort-2.9.13.tar.gz
6. tar -zxvf daq-2.9.13.tar.gz
7. cd daq-2.9.13
8. ./configure && make && make install

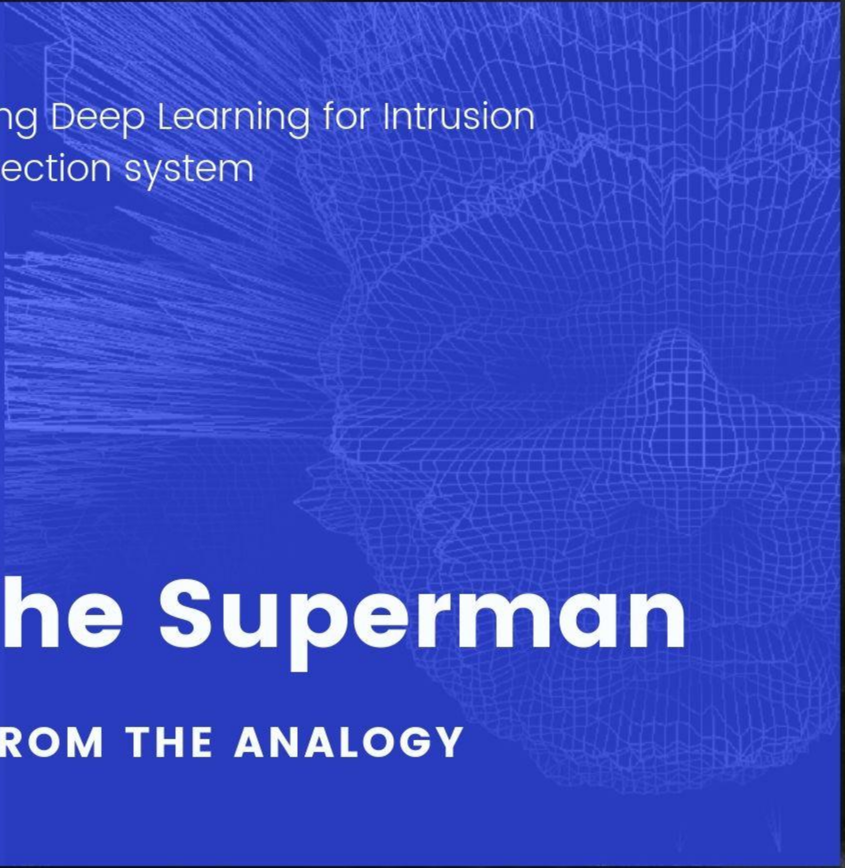
JUST ~~LISTEN~~

SEE!

INTERESTED

IN SEEING LIVE ATTACK DEMO?

Using Deep Learning for Intrusion Detection system



The Superman

FFROM THE ANALOGY

Cogoport

Cogoport

the Procedure

DATA COLLECTION

ISCX 2012 Dataset collected by the Canadian Institute for Cybersecurity

DATA VISUALISATION

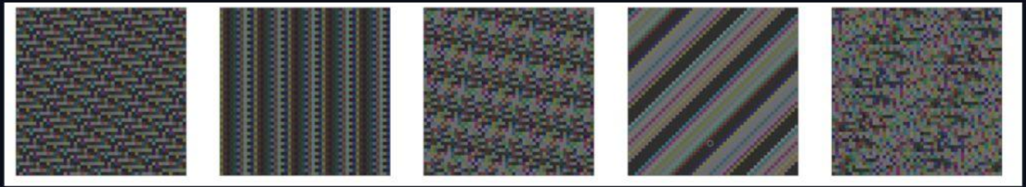
By using the Matplotlib library to check how much data for each class (Normal and Anomaly) is contained.

DATA PRE-PROCESSING

When downloaded, the ISCX data set is unreadable to the deep learning model when it is in its original .PCAP file format so to change this we use an open source software program known as ISCX Flowmeter .

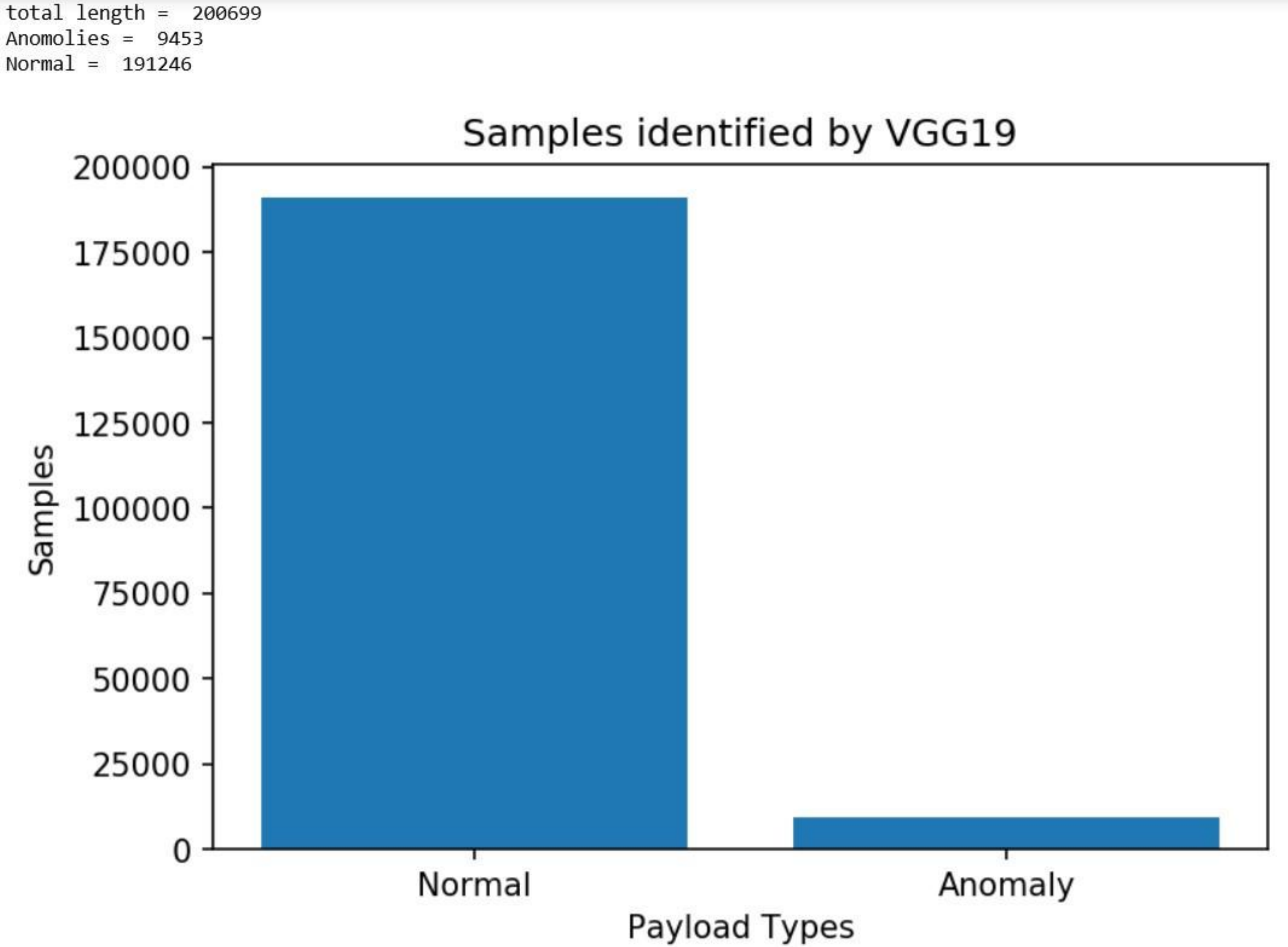
EXTRACTING USEFUL DATA

So after running the Flowmeter on the data set we get multiple XML files that we extract the two main data values from each tree per file. Then we concatenated the payload data so that its length was of 7500 and once completed we then re-shaped it into a NumPy array of 50x50x3 dimensions.

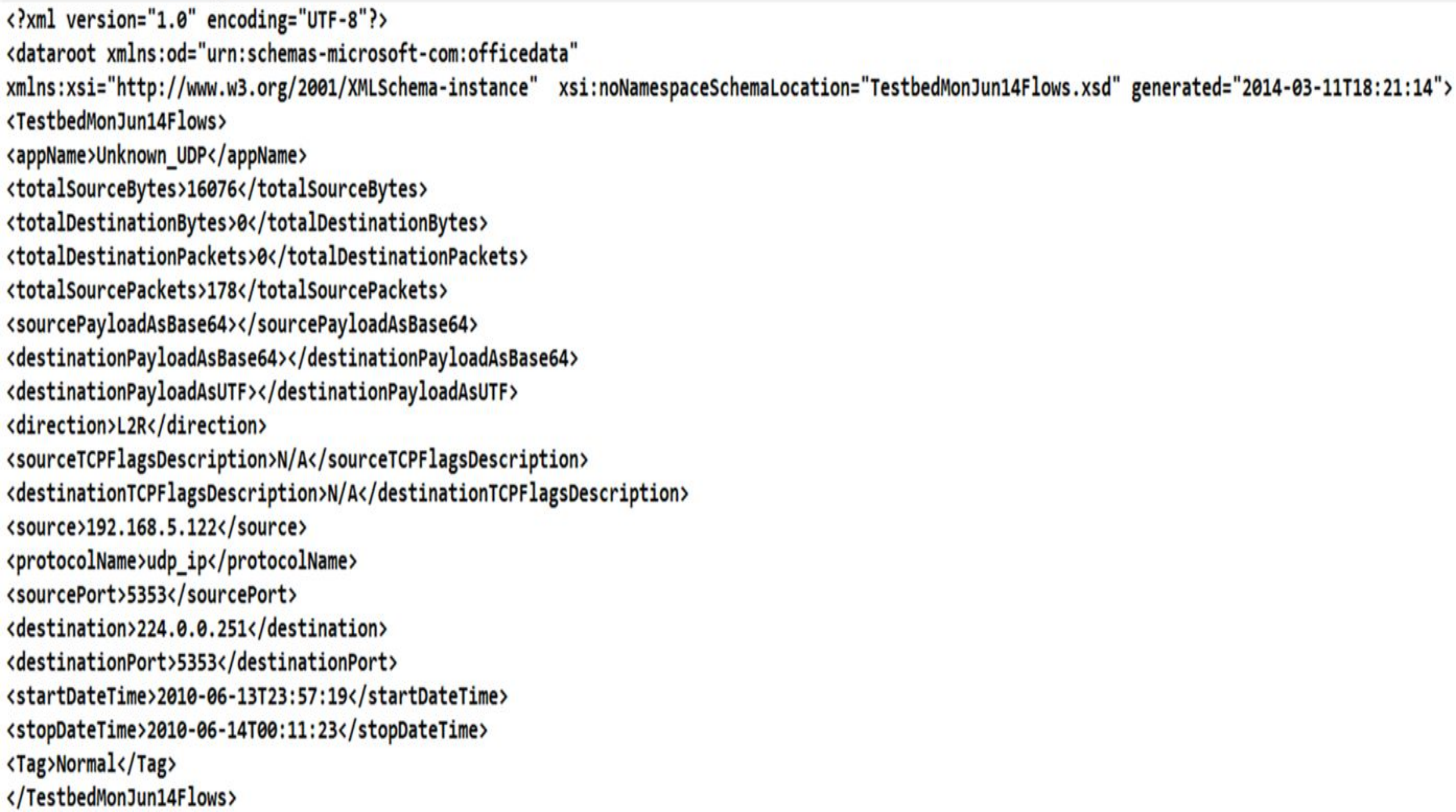


This is how the array looked like.

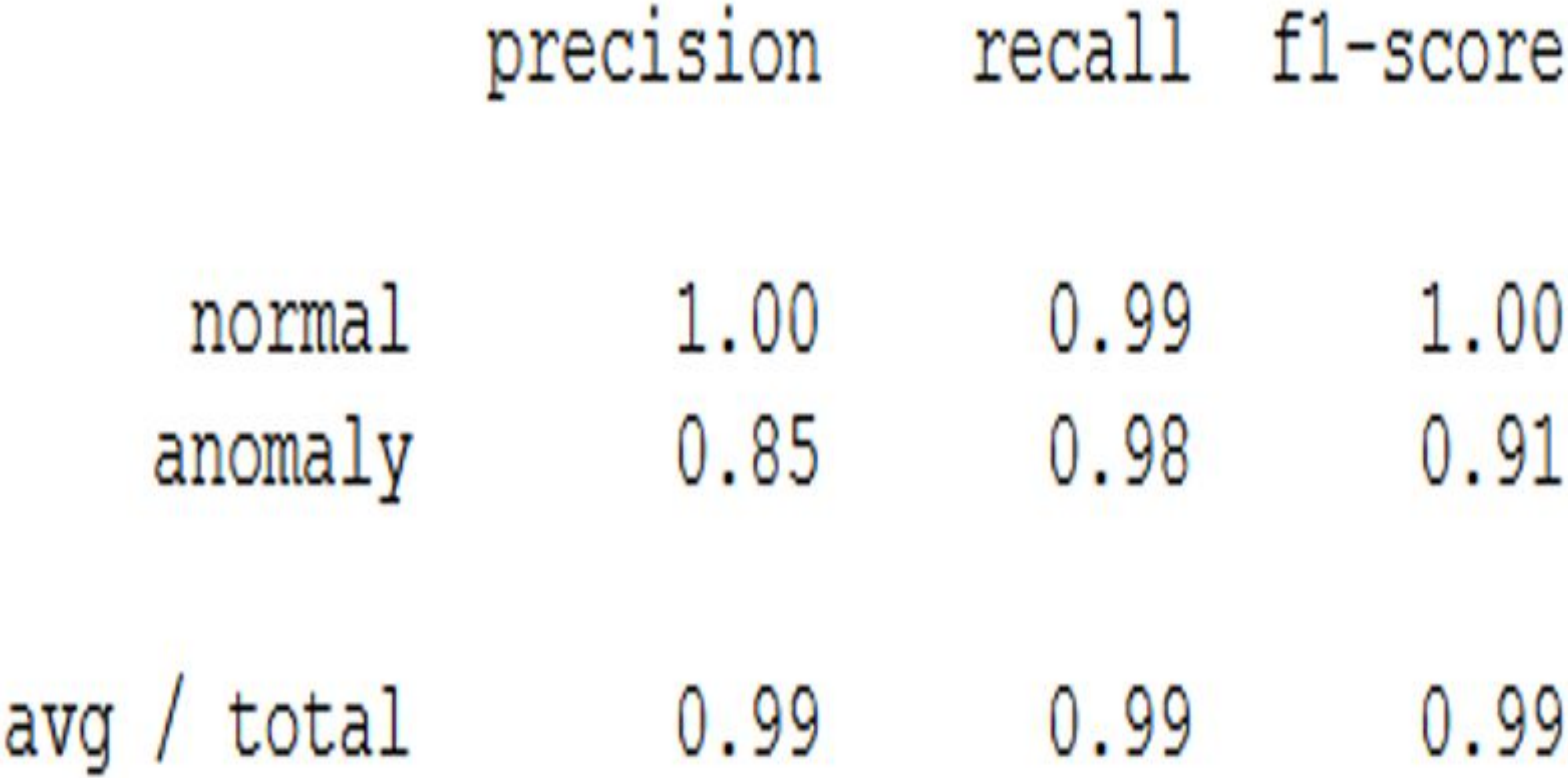
THE PROCEDURE



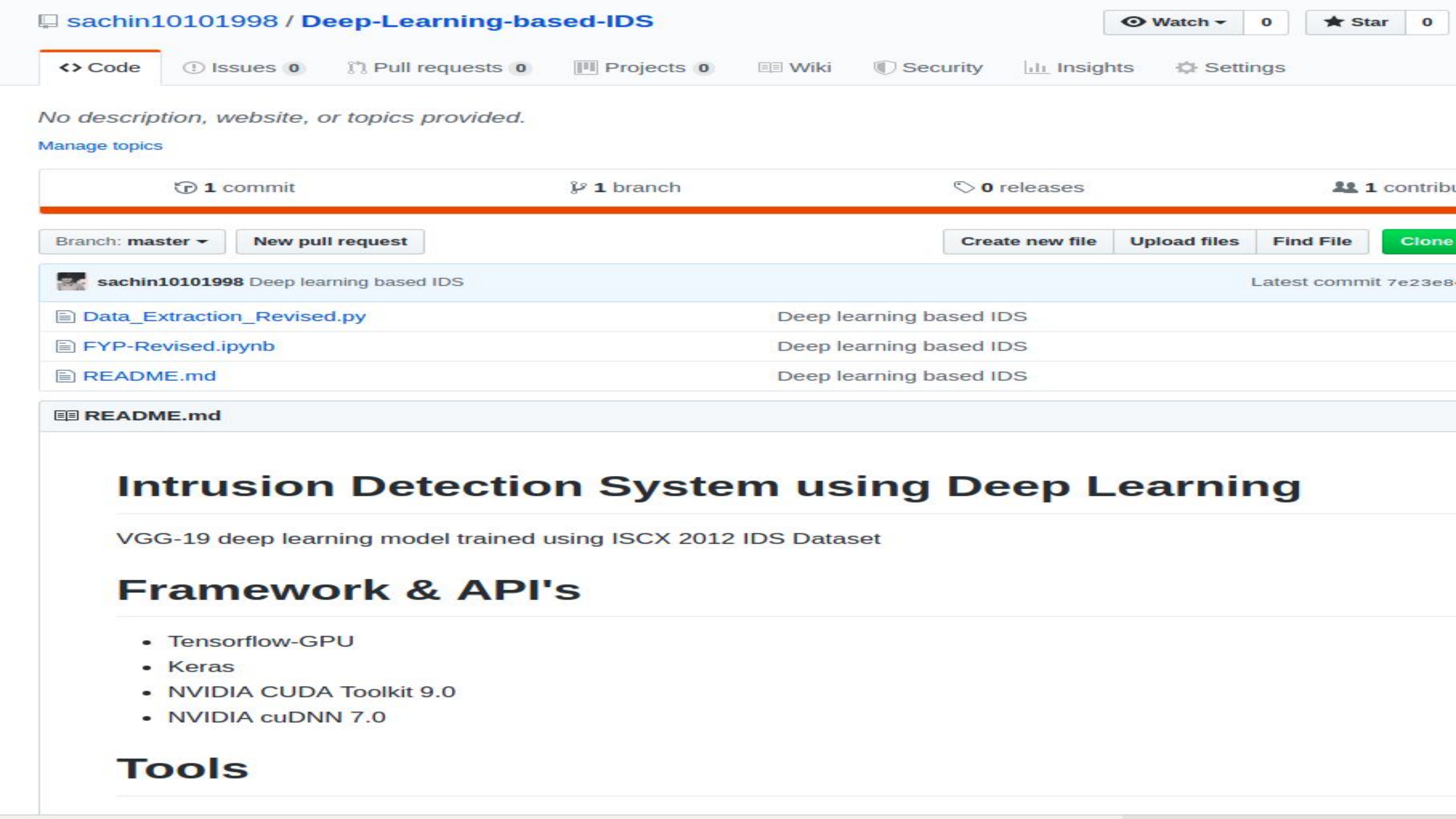
```
total length =  200699
Anomolies =  9453
Normal =  191246
```



```
<?xml version="1.0" encoding="UTF-8"?>
<dataroot xmlns:od="urn:schemas-microsoft-com:officedata"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  xsi:noNamespaceSchemaLocation="TestbedMonJun14Flows.xsd" generated="2014-03-11T18:21:14">
<TestbedMonJun14Flows>
<appName>Unknown_UDP</appName>
<totalSourceBytes>16076</totalSourceBytes>
<totalDestinationBytes>0</totalDestinationBytes>
<totalDestinationPackets>0</totalDestinationPackets>
<totalSourcePackets>178</totalSourcePackets>
<sourcePayloadAsBase64></sourcePayloadAsBase64>
<destinationPayloadAsBase64></destinationPayloadAsBase64>
<destinationPayloadAsUTF></destinationPayloadAsUTF>
<direction>L2R</direction>
<sourceTCPFlagsDescription>N/A</sourceTCPFlagsDescription>
<destinationTCPFlagsDescription>N/A</destinationTCPFlagsDescription>
<source>192.168.5.122</source>
<protocolName>udp_ip</protocolName>
<sourcePort>5353</sourcePort>
<destination>224.0.0.251</destination>
<destinationPort>5353</destinationPort>
<startDateTime>2010-06-13T23:57:19</startDateTime>
<stopDateTime>2010-06-14T00:11:23</stopDateTime>
<Tag>Normal</Tag>
</TestbedMonJun14Flows>
```



```
             precision    recall  f1-score

     normal       1.00      0.99      1.00
    anomaly       0.85      0.98      0.91

avg / total       0.99      0.99      0.99
```



No description, website, or topics provided.

sachin10101998 Deep learning based IDS — Latest commit 7e23e8

Data_Extraction_Revised.py	Deep learning based IDS
FYP-Revised.ipynb	Deep learning based IDS
README.md	Deep learning based IDS

README.md

Intrusion Detection System using Deep Learning

VGG-19 deep learning model trained using ISCX 2012 IDS Dataset

Framework & API's

- Tensorflow-GPU
- Keras
- NVIDIA CUDA Toolkit 9.0
- NVIDIA cuDNN 7.0

Tools

Into the future

WHAT DOES CYBEROPS LOOK FORWARD TO!

@cogoport

SURICATA + KIBANA MAGIC

A Sample Timeline

SURICATA

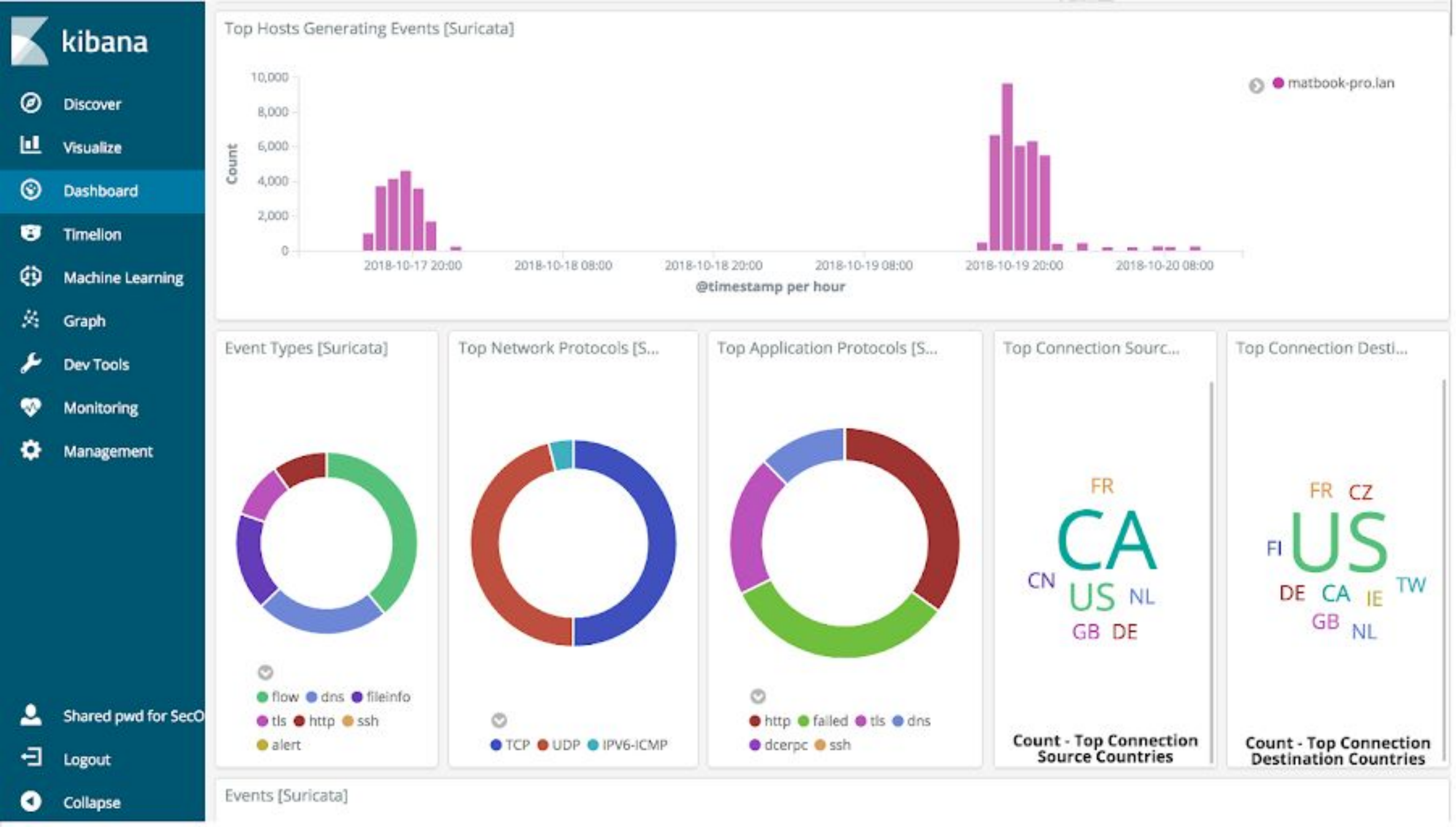
The Suricata engine is capable of real time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM) and offline pcap processing.

KIBANA

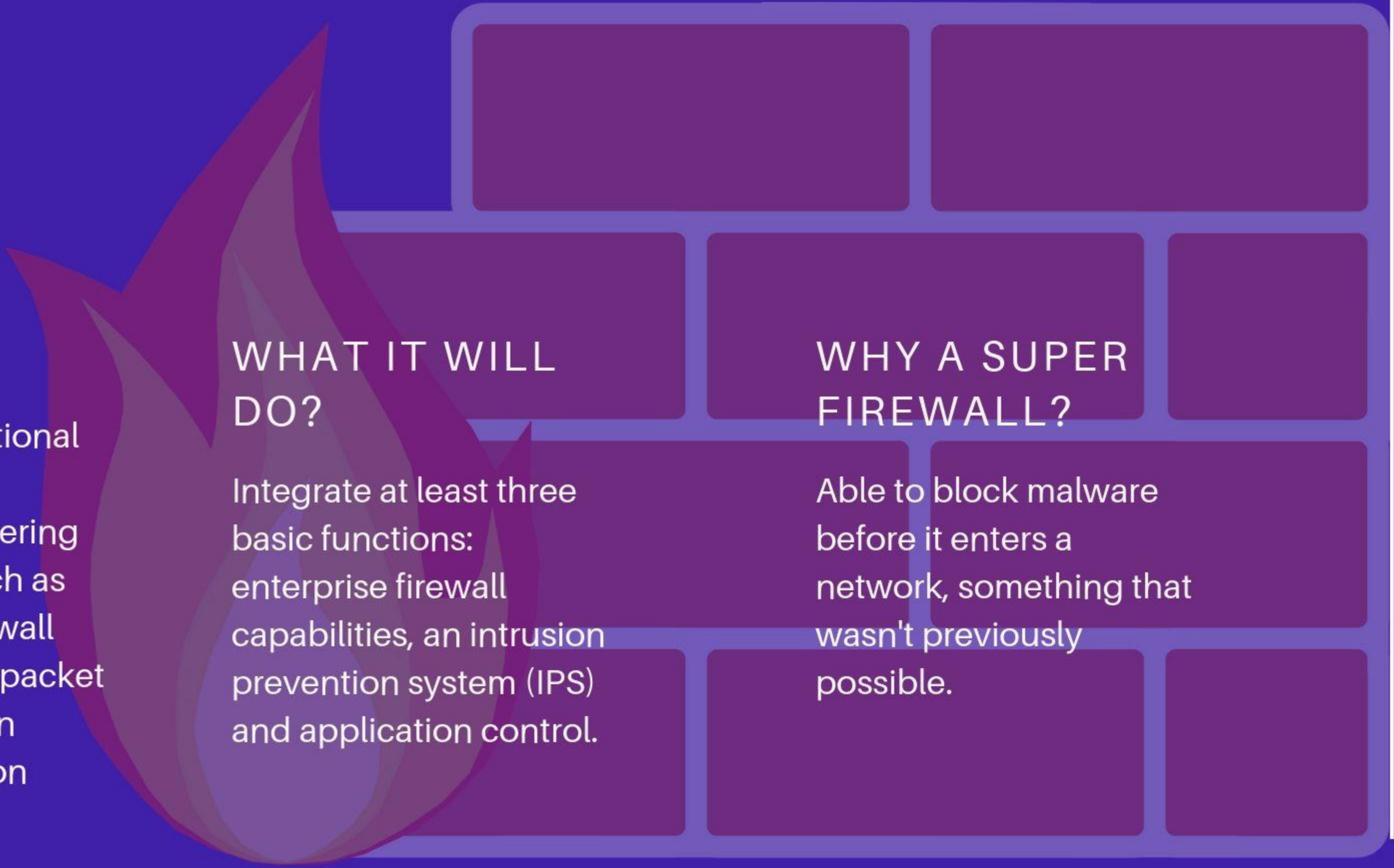
Kibana lets you visualize your Elasticsearch data and navigate the Elastic Stack

FILEBEAT

Filebeat is a lightweight shipper for forwarding and centralizing log data. Installed as an agent on your servers, Filebeat monitors the log files or locations that you specify, collects log events, and forwards them to either to Elasticsearch or Logstash for indexing.


kibana
Discover
Visualize
Dashboard
Timelion
Machine Learning
Graph
Dev Tools
Monitoring
Management
Shared pwd for SecO
Logout
Collapse
Top Hosts Generating Events [Suricata]
10,000
8,000
6,000
4,000
2,000
0
Count
2018-10-17 20:00
2018-10-18 08:00
2018-10-18 20:00
2018-10-19 08:00
2018-10-19 20:00
2018-10-20 08:00
@timestamp per hour
● matbook-pro.lan
Event Types [Suricata]
● flow ● dns ● fileinfo
● tls ● http ● ssh
● alert
Top Network Protocols [S...
● TCP ● UDP ● IPV6-ICMP
Top Application Protocols [S...
● http ● failed ● tls ● dns
● dcerpc ● ssh
Top Connection Sourc...
FR
CA
CN
US
NL
GB
DE
Count - Top Connection Source Countries
Top Connection Desti...
FR
CZ
FI
US
TW
DE
CA
IE
GB
NL
Count - Top Connection Destination Countries
Events [Suricata]

CONCEPTUALIZING SUPER FIREWALL



WHAT IS IT?

Combining a traditional firewall with other network device filtering functionalities, such as an application firewall using in-line deep packet inspection (DPI), an intrusion prevention system (IPS).

WHAT IT WILL DO?

Integrate at least three basic functions: enterprise firewall capabilities, an intrusion prevention system (IPS) and application control.

WHY A SUPER FIREWALL?

Able to block malware before it enters a network, something that wasn't previously possible.

CYBEROPS

DEVOPS

CREDITS

SACHIN CHOPRA

@CYBEROPSGUY

SANAT TALWAR (MENTOR)

@DEVOPSGUY