Dharmendra

Internet of Thing Hacking Result & Analysis

Table of Contents

[Chapter 4: Result & Analysis 3](#_Toc109316644)

[Python Machine learning programming 3](#_Toc109316645)

[Dataset information 3](#_Toc109316646)

[Network Traffic IOT dataset 3](#_Toc109316647)

[Python libraries 3](#_Toc109316648)

[Network traffic IOT DATA 4](#_Toc109316649)

[Wireshark PCAP FILE Network 5](#_Toc109316650)

[Data Preprocessing in Python Notebook 5](#_Toc109316651)

[Dataset Head 6](#_Toc109316652)

[Checking Missing values in dataset 6](#_Toc109316653)

[Dataset information 7](#_Toc109316654)

[Decision tree classifier 7](#_Toc109316655)

[Feature Selection 7](#_Toc109316656)

[Decision tree classifier to Detect IOT attack libraries 8](#_Toc109316657)

[Outcome 8](#_Toc109316658)

[Decision Tree Classification report 9](#_Toc109316659)

[Naïve Bays Model to DETECT IOT Attack 9](#_Toc109316660)

[Print data columns 9](#_Toc109316661)

[Naïve Bays Modeling 10](#_Toc109316662)

[Training and testing the dataset 10](#_Toc109316663)

[Naïve Bays Classification report 11](#_Toc109316664)

[Support Vector Machine modeling 11](#_Toc109316665)

[SVM Classification Report 12](#_Toc109316666)

[Kali Linux IOT Ethical Hacking Analysis: 12](#_Toc109316667)

[Firmware 12](#_Toc109316668)

[Bootloader 12](#_Toc109316669)

[Why examines the Firmware 13](#_Toc109316670)

[Features in firmware 13](#_Toc109316671)

[Security issues in IOT devices 13](#_Toc109316672)

[Static and Dynamic Analysis 13](#_Toc109316673)

[Static Analysis 13](#_Toc109316674)

[Dynamic Analysis 14](#_Toc109316675)

[Binwalk 14](#_Toc109316676)

[Binwalk Entropy Calculation 14](#_Toc109316677)

[Firmware analysis in Kali Linux 14](#_Toc109316678)

[Firmadyne 16](#_Toc109316679)

[Firmware Analysis Toolkit 17](#_Toc109316680)

[Firmware analysis toolkit directory 17](#_Toc109316681)

[Machine Learning VS Ethical Hacking for IOT Security 19](#_Toc109316682)

[Critical Analysis Ethical Hacking to Secure IOT devices 19](#_Toc109316683)

[References 20](#_Toc109316684)

# Chapter 4: Result & Analysis

## Python Machine learning programming

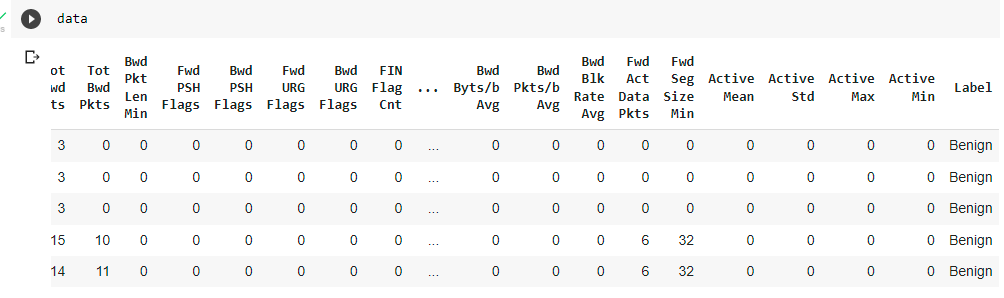
Using support vector machine classifier, Decision tree and Naïve bays modeling to predict the Internet of thing malware and hacking activity by using through the dataset.

## Dataset information

Dataset is based on different values in which to make predictions of internet thing attack.

Label columns is presenting the attack name and type.

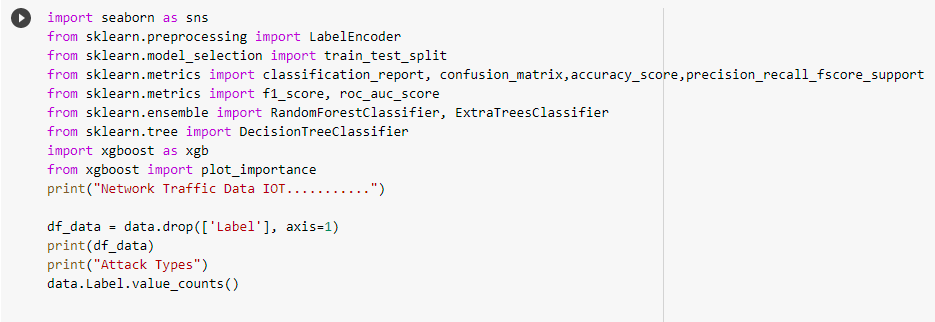
Dataset head:



## Network Traffic IOT dataset

Internet of thing devices data captured from Wireshark software by scanning the real time network PCAP network file, PCAP is data file created during scanning the network, the files contains the data & information which add to controlling the network traffic and defining the network. The PCAP extension file of Wireshark tool which enable them to identify the network data, identify the real time network data based on protocol. Hence the network used to analyze the network data by the cyber security analyst.

### Python libraries



The following network data library has been added to capture the real time network data of IOT system.

#### Seaborn:

Seaborn is known as python statistical library to graph by using the matplotlib functions hence seaborn is data visualization library which integrated on pandas data structure since visualize the data in the terms of x and y variable by separating the data and understand them in more meaningful way.

#### LabelEncoder:

Label Encoder library is common python library to handling the categorical variable hence this method in which each label is assigned unique value which based on integer value based on alphabetical order.

#### SKLEARN train test split:

In machine learning model evaluation and validation process there is needs to split the dataset into two phase train and test by using the x and y variable system. The train test and split library is python data science library scikit-learn, which splits data into subset & minimize the potential for bias on the basis of data evaluations and validation process.

#### Classification Report confusion matrix:

Classification report in python machine learning measures the quality of predictions from the classification programing method hence predictions are based on true positive and false positive and true negative and false negative outcome, which predicts the performance metrics of training and testing data and produce classification report.

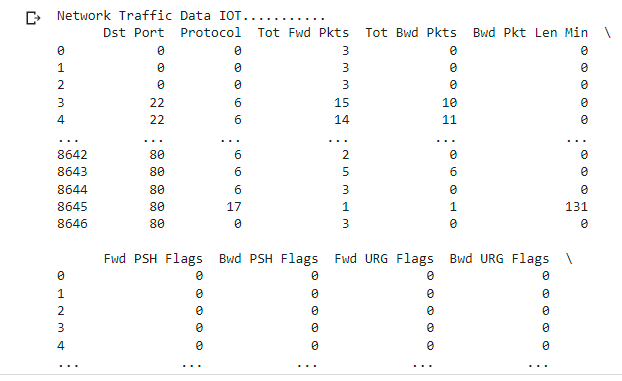
#### Precision Recall and Accuracy score:

The meaningful method to identify the dataset score based on the measurement validation. The outcomes are presented to identify the F1 score and precision recall score. The better score of Naïve bays SVM and decision tree is 90% score.

#### RandomForestClassifier:

In python programing the random forest classifier library which the random forest estimate the fits a number of decision tree classifier on various sub samples of the dataset and uses the averaging to improve the predictive accuracy and control over fitting.

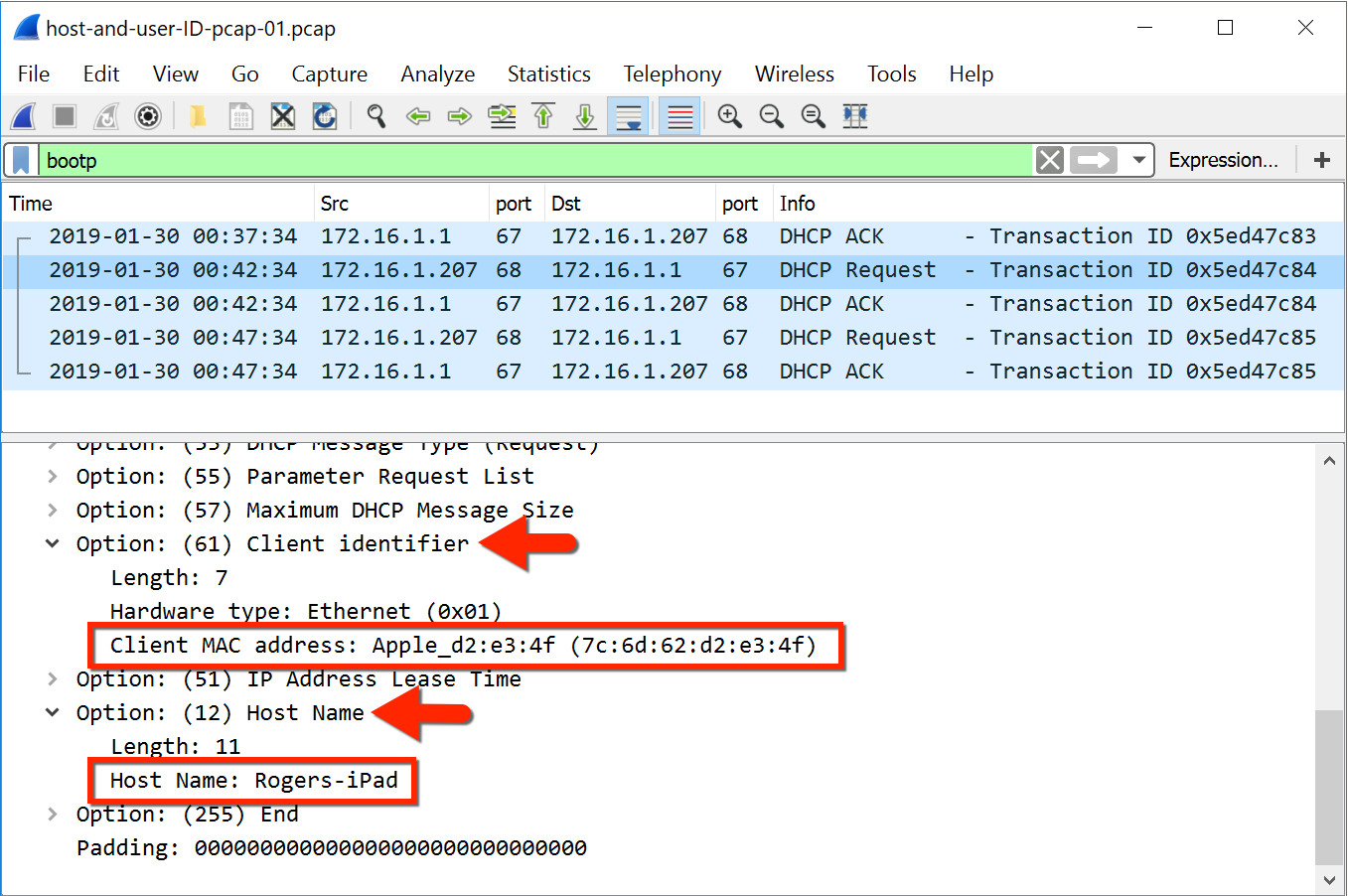
## Network traffic IOT DATA



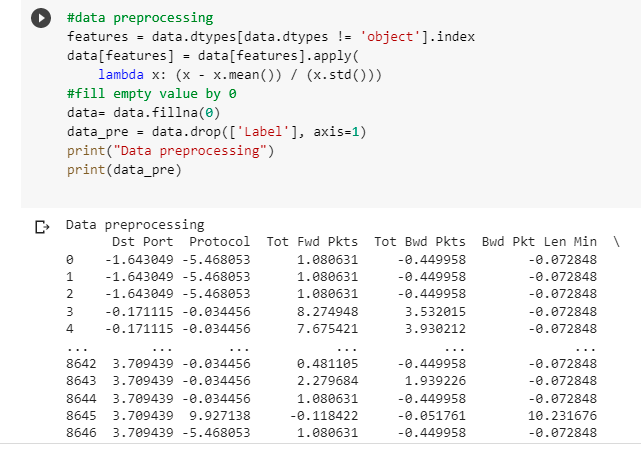
## Wireshark PCAP FILE Network

PCAP file is part of real time network analysis file which are composed of real time network analysis file, hence the TCPDUMP file which are program to identify the real time network monitoring analysis. The PCAP icon file in which to view all packets information of IOT device in real time.

TPC/UDP packet information by scanning through the Wireshark tool.



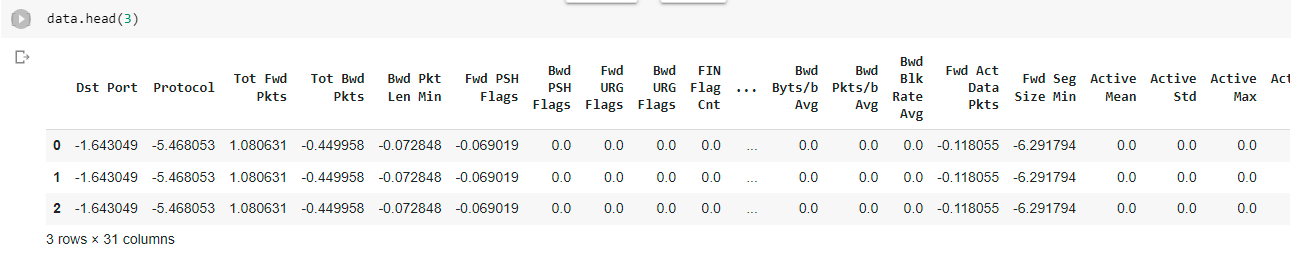
## Data Preprocessing in Python Notebook



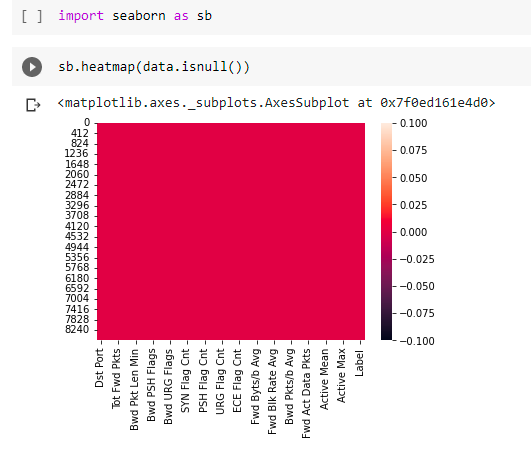
Data preprocessing in python in order to achieve the data cleaning and dataset optimization process to remove the data redundancy through data preprocessing steps

Dataset to be cleaned and optimized by determining the dataset labels in which the IOT attack occurred.

### Dataset Head

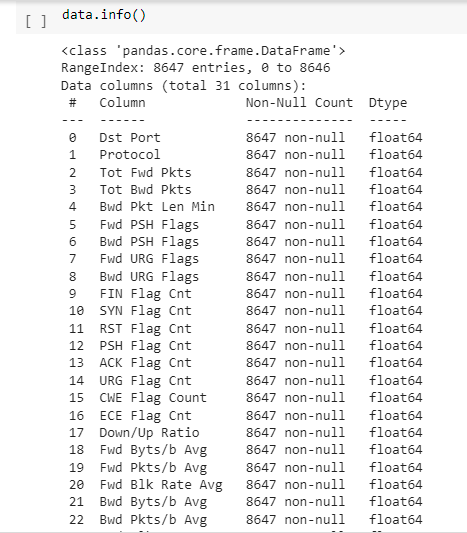


### Checking Missing values in dataset

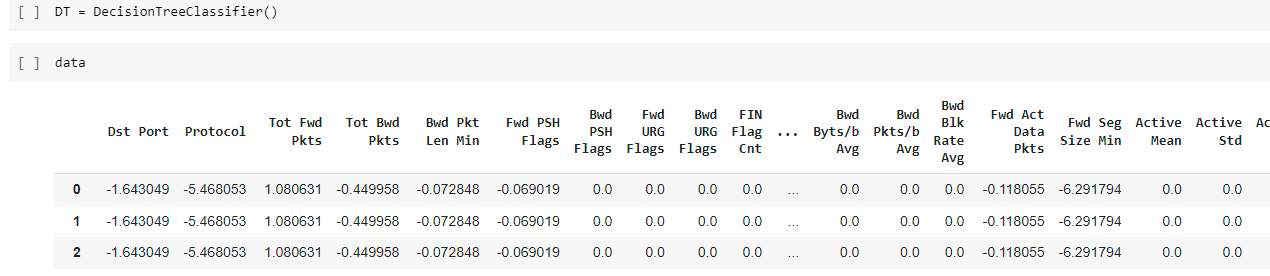


Predicting any missing value in the dataset to determine the values of the dataset, since the data cleaning is the organized process in which the various processing has been optimized. Dataset organized and managed through the python preprocessing library.

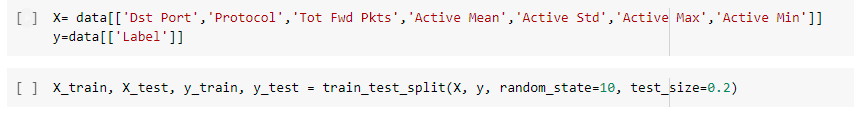
### Dataset information



## Decision tree classifier

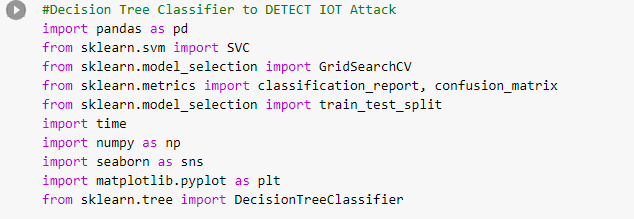


### Feature Selection

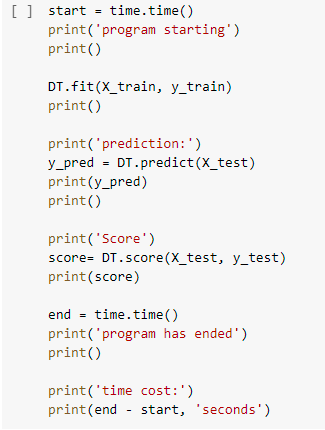


Separating the dataset feature turns into the variable into x and y to determine the variable outcome.

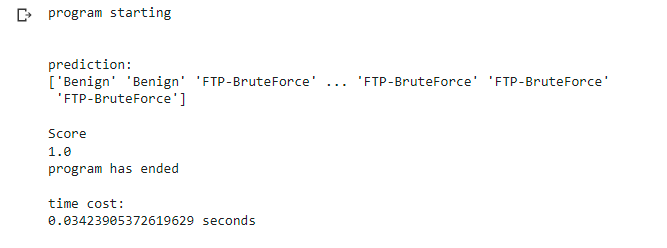
## Decision tree classifier to Detect IOT attack libraries



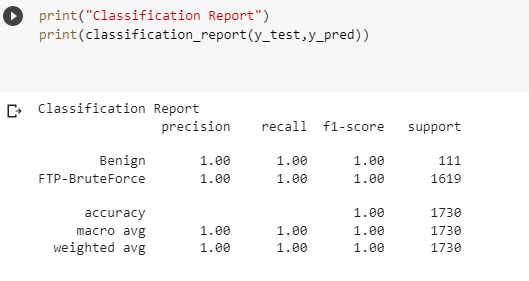
This section taken from (GitHub 2022. )



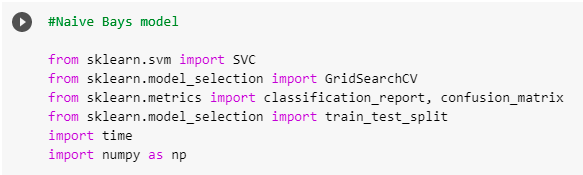
### Outcome



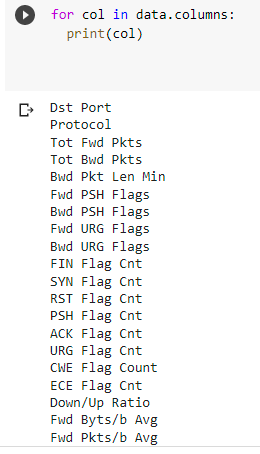
### Decision Tree Classification report

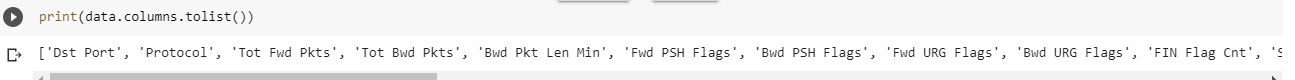


## Naïve Bays Model to DETECT IOT Attack



### Print data columns

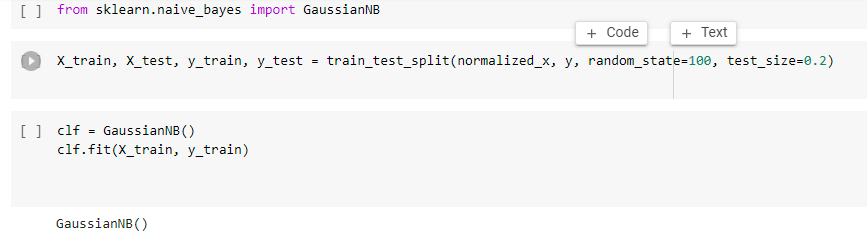


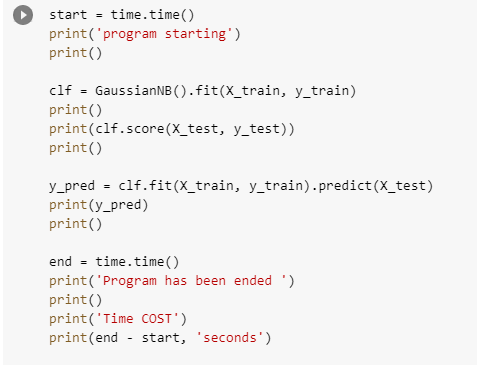


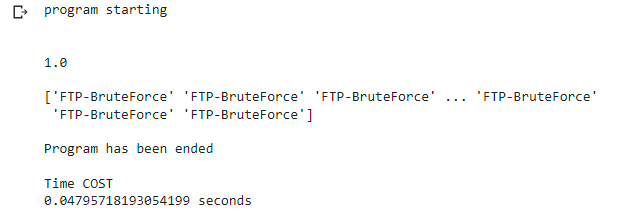
### Naïve Bays Modeling



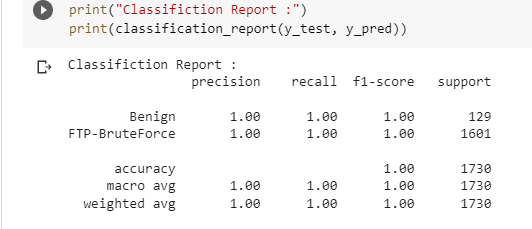
### Training and testing the dataset



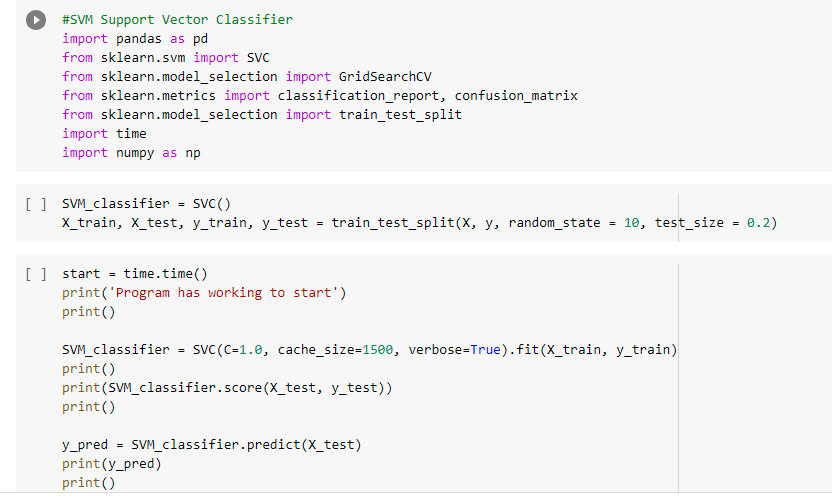


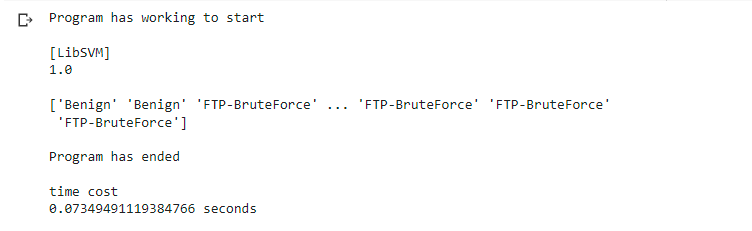


### Naïve Bays Classification report

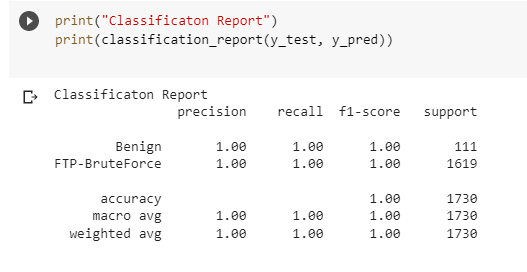


## Support Vector Machine modeling





### SVM Classification Report



# Kali Linux IOT Ethical Hacking Analysis:

What’s an IOT device anyhow? Hence the term given to non-standard device connected to the internet usually the embedded operating system (Firmware) which interface them since the embedded sensor in the IOT device which can send, collect and exchange data

1. Security Camera
2. Smart Home Devices such as outlets, light, switches, electronic devices
3. Raspberry PI
4. Connected appliances such as washers, dryers, ovens, etc.
5. Wireless router
6. Wearable : apple watch, Pedometers, heart monitors
7. Autonomous ag equipment and cars

## Firmware

Code running on hardware which is critical to hardware operations. Provides the necessary actions on how the device is supported to work, it makes the IOT device work and what the manufacturer intended to do it.

## Bootloader

The bootloader the piece of code and software that runs before any operating system loaded into the memory. Bootloader usually contains several ways to boot the operating system kernel and also contains commands for debugging and modifying the kernel environment.

The common bootloader:

1. U-BOOT
2. RedBOOT
3. BareBox
4. BusyBox

## Why examines the Firmware

The control on firmware which control the IOT devices, since various vulnerability hacking attacked occurred in internet of thing device, it allows the device to work and configured the common mistakes in the programming , IOT device which easily entry point of hacker which attack the entire network and swivel from.

## Features in firmware

Firmware contains hardcoded based on:

1. Credentials
2. Keys
3. Network values

Encryption not used for sensitive information and updates are not encrypted and update are not verified before upload and install.

## Security issues in IOT devices

1. Weak Guessable and hardcoded password
2. Insecure network service
3. Insecure ecosystem interfaces
4. Lack of secure update mechanism
5. Use of insecure obsolete machineries
6. Insufficient privacy protection
7. Insecure data transfer and storage
8. Lack of device management
9. Insecure default settings
10. Lack of corporeal inurement

## Static and Dynamic Analysis

The static analysis looks on firmware while using the IOT operation.

* Analyze the file system and inspect bootloader
* Looks for hardcoded item
* Use tools firmadyne, Binwalk, Firmwalker etc.
* Dynamic operation looking the process of operation, involuntary static analysis which not exactly often confused them.
* Need to have device which needs to access them
* The virtualize operation on internet of thing device using the penetration testing process in Kali Linux such as NMAP, Metasploit.

## Static Analysis

The static analysis are based on Firmware, which extract the Binwalk file system and uncompressed the file system and component if required. The firmware looking the binaries which presents on the firmware and analyze them according to them and identify vulnerability. Hence the common binaries such as busybox, corresponding to exploit on the given version. Since analyze binaries based on disassembly on IDA.

## Dynamic Analysis

The firmware running on the system which extract the physical device, virtualize device, QEMU. Since the penetration testing tools in Kali Linux

1. NMAP
2. Metasploit
3. TCPDUMP NETCAT
4. Wireshark

## Binwalk

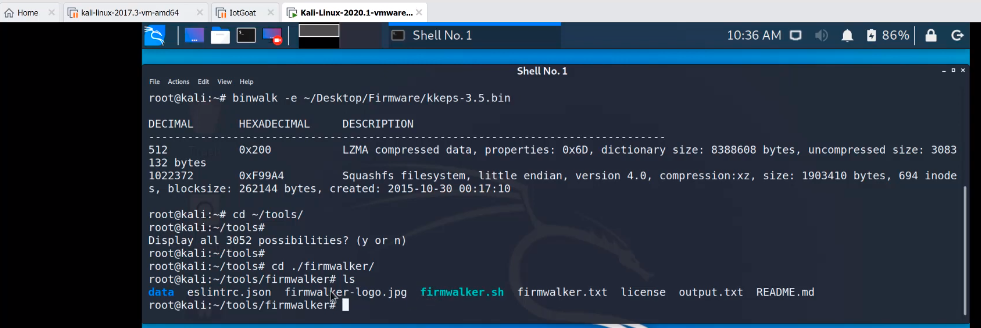
(Zhao, W. and Shi, Z., 2019) Binwalk is tool for searching a firmware image embedded files and executable code, hence Binwalk professional tool also available on cloud based.

## Binwalk Entropy Calculation

Internet of thing is hardware based eco system connected with wireless internet network in real time backend the mobile and smart devices also connected on all smart home internet of thing devices. Since firmware updates are always delivered based on compressed file. In order to determine the encryption firmware file which are composed of entropy compressed file. To process the analysis composed of decompressed and encrypted form.

## Firmware analysis in Kali Linux

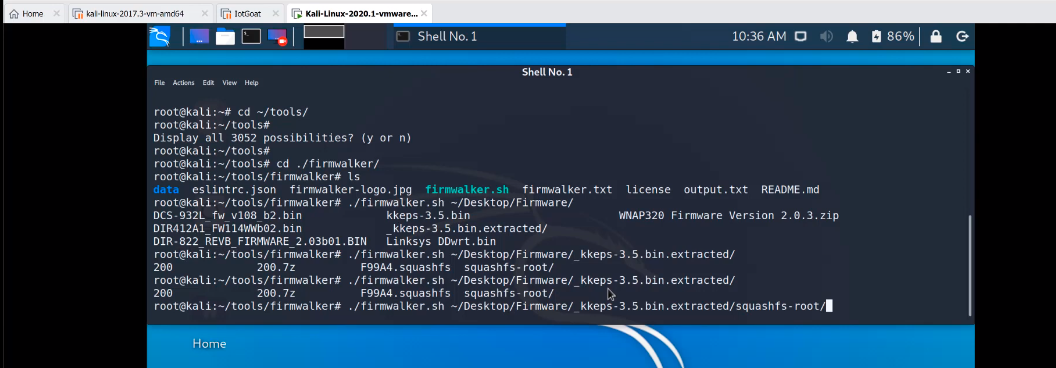
Smart IOT device firmware download from Google GitHub



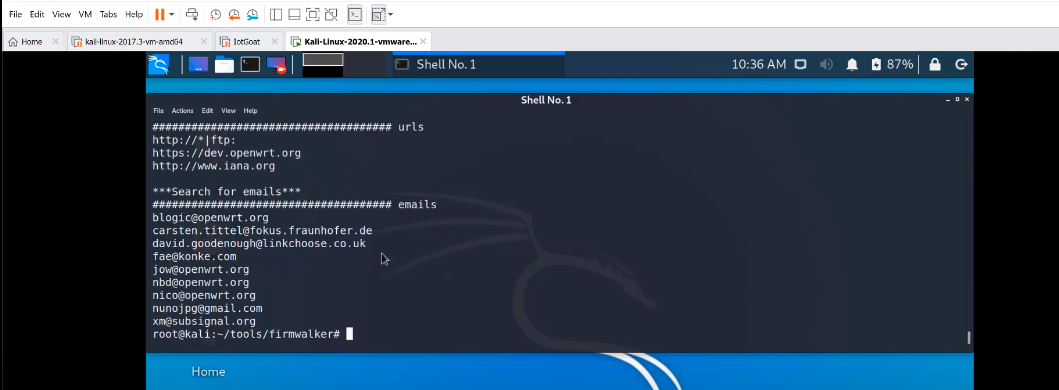
To executes firmwalker.sh file in order to optimize the performance of IOT device hardware.

Extracted the KKEP bin file in Kali Linux operating system.

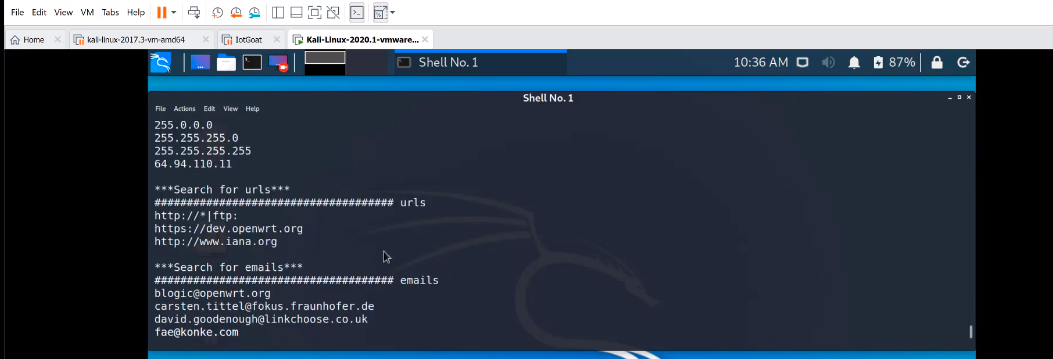
Now extracted the squashed root file in the system



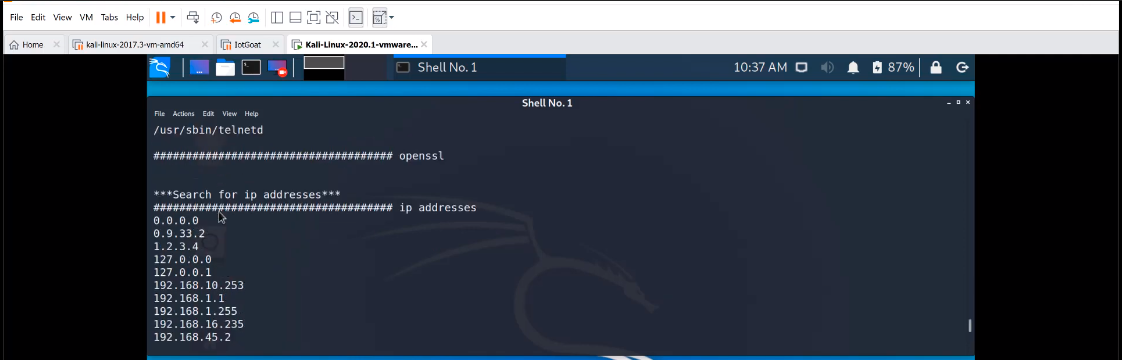
Squashed root file searching the email address in IOT system



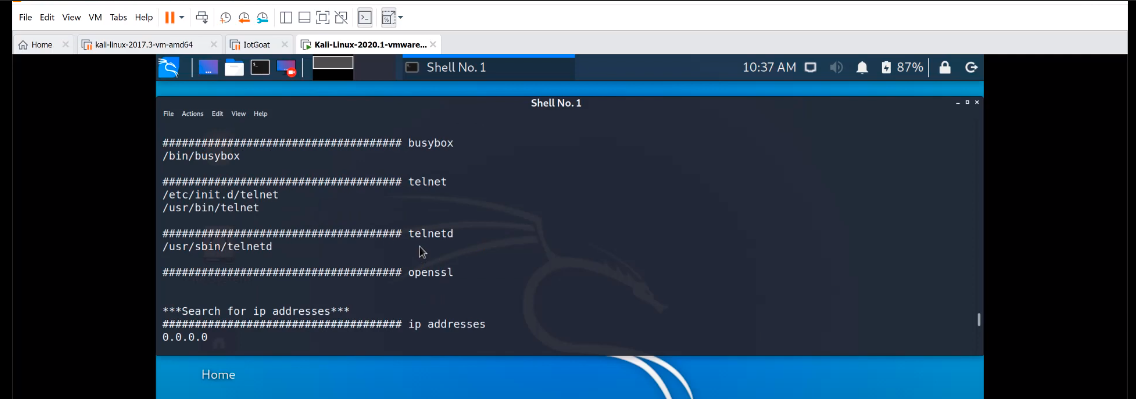
Searching for URL



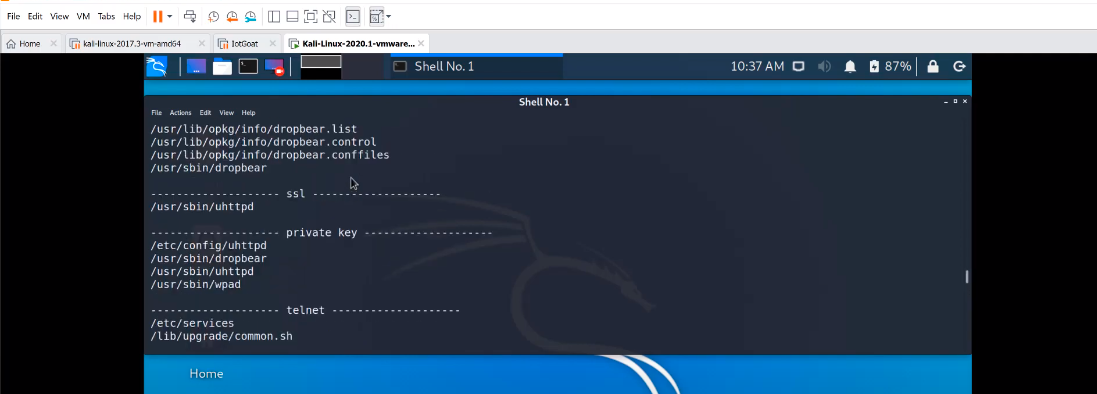
Searching for Encoded IP Address



Searching for OPEN SSL



Searching for telnet with private key



So Binwalk is used to extract the file system of firmware IOT hardware device to execute the internal firmware data.

## Firmadyne

Firmadyne is automated and scalable system for performing emulation and dynamic analysis of Linux based firmware embedded system.

It makes use of Binwalk and QEMU

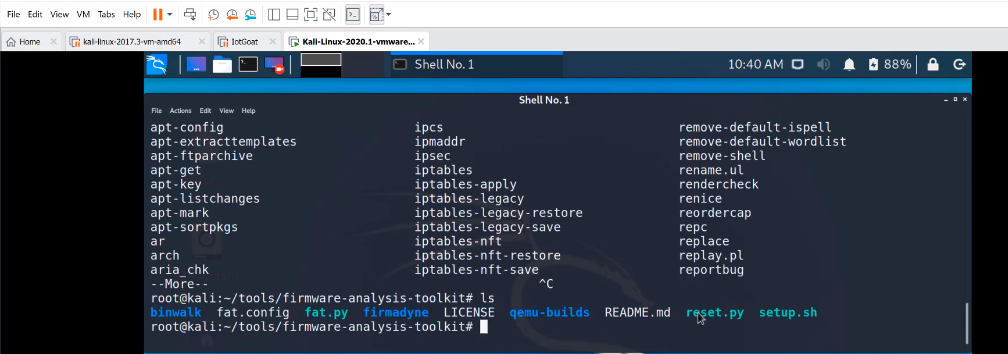
It includes the extracted file from kernel file system and stores in the database system.

1. 3 basic automatic analysis has been performed using the Firmadyne system. It used to access the web pages and this script iterate through the each file within the file system of firmware and image that appear to be served by a webserver and aggregates the results based whether they appear to required authentication.
2. SNMP information dumps contents of public and private SNMP V2c without credit, hence the vulnerability check this script test based on tests for the presence of 60 known vulnerability exploit from Metasploit.

## Firmware Analysis Toolkit

(Doshi, R., Apthorpe, N. and Feamster, N., 2018) Simply the script to automate Firmadyne which is the tool used for firmware emulation. Hence the firmware filename as an argument to the script hence the script display the IP address which are assigned to the created network interfaces. The firmware boots up PING the IP which was shown in the browser.

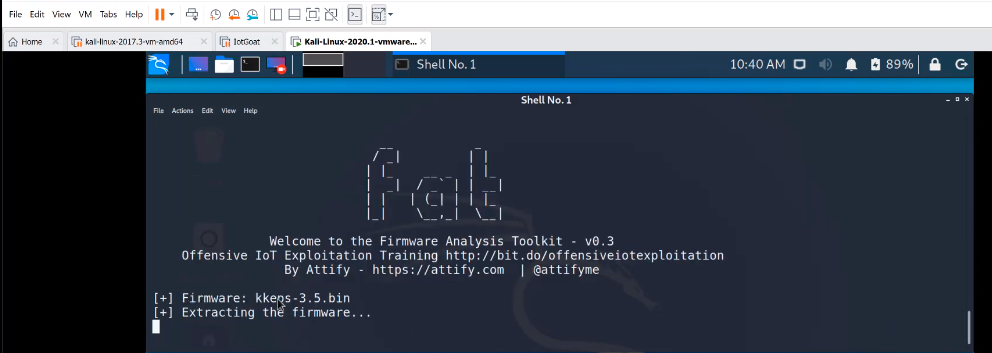
### Firmware analysis toolkit directory



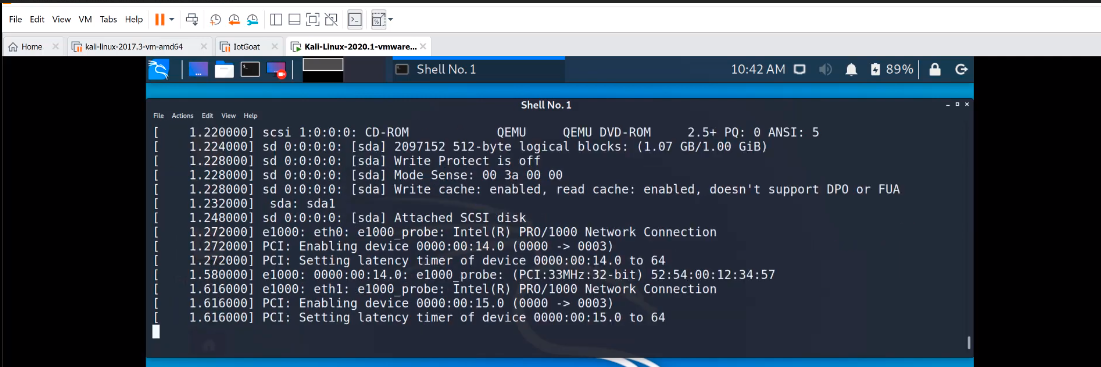
Reset.py this file should be run analyzing the firmware.

Fat is firmware toolkit analysis toolkit, offensive IOT Exploitation training the offensive threads.

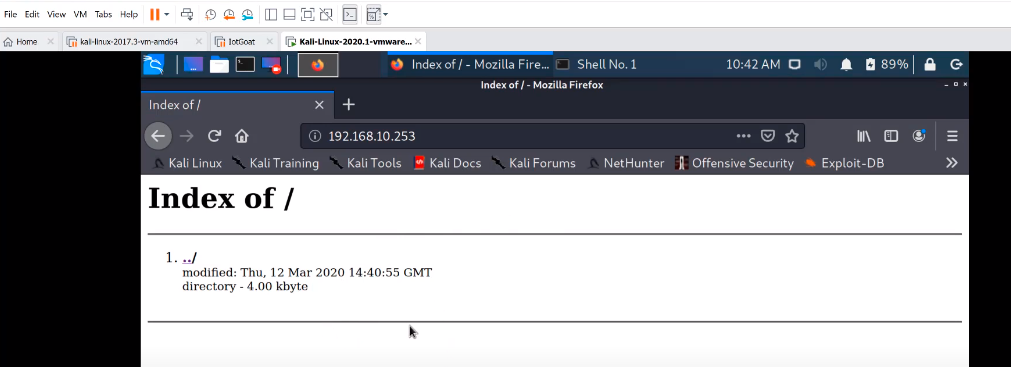
it includes the Firmware: KKEP-3.5.bin and the extracted firmware file.



IOT device Firmware file has been extracted

Now test the file in browser: 

The IP address: 192.168.10.256 extracted from IOT device and executes in web browser.



## Machine Learning VS Ethical Hacking for IOT Security

(Strecker, S., Haaften, W.V. and Dave, R., 2021) It has been determined and analyzed that the ethical hacking Kali Linux method is very good, machine learning modeling is not good to secure because its only work to analyze the PCAP Wireshark data to view the infected network data packets by experience through the machine learning modeling.

Ethical Hacking by using the Kali Linux operating system which enable the smart home user to determine the real time ethical process in which the various security tools has been attached to secure the IOT device through the firmware analysis.

So it is strongly recommended by various researcher that Kali Linux security is the only way to secure smart home IOT devices.

## Critical Analysis Ethical Hacking to Secure IOT devices

(Mukundini, K. and Karthi, R., 2020) Kali Linux operating system freely available for everyone, which organized the smart internet of thing security system. Various IP address based security in which encryption method adapted to hide the device and secure the device. Security method of Kali Linux is an organized method to predict the infected IOT system.

So it was noted that the internet of thing system secure through the Kali Linux operating system, the security method is very easily to deploy in real time, such as

1. Secure the Internal router through Kali Linux tool
2. Secure the internet WIFI through Kali Linux tool
3. Hide the Internet of thing device through Kali Linux tool security
4. Hide the location and IP address of smart IOT device through Kali Linux system

(Alzahrani, T. and Karimian, N., 2021) So it has been observed carefully and predicted that the machine learning method does not support in fully cooperation to secure the internet of thing devices from hacking attack and malware attack. Kali Linux is the best way to organized security in more appropriate manner.

# References

Kiran, K.S., Devisetty, R.K., Kalyan, N.P., Mukundini, K. and Karthi, R., 2020. Building a intrusion detection system for IoT environment using machine learning techniques. *Procedia Computer Science*, *171*, pp.2372-2379.

Sahu, K., Kshirsagar, R., Vasudeva, S., Alzahrani, T. and Karimian, N., 2021, January. Leveraging Timing Side-Channel Information and Machine Learning for IoT Security. In *2021 IEEE International Conference on Consumer Electronics (ICCE)* (pp. 1-6). IEEE.

Strecker, S., Haaften, W.V. and Dave, R., 2021. An analysis of IoT cyber security driven by machine learning. In *Proceedings of International Conference on Communication and Computational Technologies* (pp. 725-753). Springer, Singapore.

Doshi, R., Apthorpe, N. and Feamster, N., 2018, May. Machine learning ddos detection for consumer internet of things devices. In *2018 IEEE Security and Privacy Workshops (SPW)* (pp. 29-35). IEEE.

Ma, Y., Han, L., Ying, H., Yang, S., Zhao, W. and Shi, Z., 2019, May. SVM-based instruction set identification for grid device firmware. In *2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)* (pp. 214-218). IEEE.