Internet of Thing Hacking Research Methodology Dharmendra

Table of Contents

[Chapter 3: Methodology 2](#_Toc109045391)

[Introduction 2](#_Toc109045392)

[Research Philosophy 2](#_Toc109045393)

[Shortcomings in the Literature 2](#_Toc109045394)

[Research Strategy 2](#_Toc109045395)

[IOT DOS and DDOS Dataset 3](#_Toc109045396)

[Dataset Features 3](#_Toc109045397)

[Python Libraries for preprocessing 3](#_Toc109045398)

[Machine Learning Programming 3](#_Toc109045399)

[Logistic Regression Model 3](#_Toc109045400)

[Random Forest Classifier 3](#_Toc109045401)

[SVC (Support Vector Classifier) 4](#_Toc109045402)

[Decision Tree 4](#_Toc109045403)

[Gaussian Naïve Bays Algorithm 4](#_Toc109045404)

[Result 4](#_Toc109045405)

[Ethical Hacking Kali Linux Hacking tools to Secure IOT 4](#_Toc109045406)

[Ethical Hacking on IOT Device Penetration Testing 5](#_Toc109045407)

[Mitigating Security Risk and Threats 5](#_Toc109045408)

[Analysis 6](#_Toc109045409)

[Ethical Concern 6](#_Toc109045410)

[References 7](#_Toc109045411)

# Chapter 3: Methodology

## Introduction

Research methodology of internet of thing system which are part of smart home solution, botnet is network IOT device which has infected by malware, hacker can playing botnet attack card to capture the IOT data easily by sending malware attack to the IOT system. Since botnet would be used to perform distributed denial of service attack, the hacking attack which steal data, send spam, which would allow the hacker and attacker to access the connected device hence typically the router is infected by malware and creates interrupt in the communication between the IOT network and mobile phone.

## Research Philosophy

Hacking was used in 1955, which major purpose to identify the technical term and knowledge which gives power to the hacker. Since the first internet hacker certainly identify media and produced first denial of service attack in 1989, the biggest hack in the history happened in 2013, 3 billion yahoo accounts hacked by hacker which was known as yahoo epic data breach. Since yahoo did not admit the problem due to its neglected the popularity. In May 2019 first American financial corporation real estate and mortgage insurer business which was exposed 900 customer file openly in the media.

Hence the internet of thing was coined in 1999 by the computer scientist Kevin Ashton. Since first IOT device was invented in 1993 namely toaster, which was on and off over the internet, the entire process for bread making which warms the bread on particular time period, beside this the IOT devices popularity increase in 2008 year.

ECHO IV first home automation device created by Westinghouse engineer in 1966. Which was the first true home automation device to control temperature and appliances.

## Shortcomings in the Literature

Several machine learning methods has been implemented in the past to scan and predict malware and hacking attack in the IOT system, some research generates diverse dataset, which are implements basic machine learning programing composed on decision tree method and Ada Boost.

Various research studies deploy security encryption method but left with no finding to meet the security requirement of IOT.

Some research studies deploy advance machine learning algorithm composed of dataset of IOT to identify malware and hacker in the network.

## Research Strategy

1. IOT Penetration testing (Kali Linux)
2. Machine learning method experiencing through the IOT dataset.
3. Encryption method

The research method concerned about denial of service attack of smart home IOT system which has evidently been driven by huge number of compromised internet connected devices. All of the internet connected devices are behind the router network system which easily hacked and captured by hacker.

## IOT DOS and DDOS Dataset

Internet of thing IOT device various vulnerability network attack occurred to violate the security of the system, the most frequent using of internet of thing devices which are captured through the internet network. The denial of service attack and distributed denial of service attack are reported in the IOT network, since the most frequency security system using the firewall method intrusion detection system which are unable to detect the complexity of DOS and DDOS attack.

## Dataset Features

Data contains the following values which contains in csv file.

pkSeqID stime flgs flgs\_number proto proto\_number saddr sport daddr dport pkts bytes state state\_number ltime seq dur mean stddev sum min max spkts dpkts sbytes dbytes rate srate drate TnBPSrcIP TnBPDstIP TnP\_PSrcIP TnP\_PDstIP TnP\_PerProto TnP\_Per\_Dport AR\_P\_Proto\_P\_SrcIP AR\_P\_Proto\_P\_DstIP N\_IN\_Conn\_P\_DstIP N\_IN\_Conn\_P\_SrcIP AR\_P\_Proto\_P\_Sport AR\_P\_Proto\_P\_Dport Pkts\_P\_State\_P\_Protocol\_P\_DestIP Pkts\_P\_State\_P\_Protocol\_P\_SrcIP attack category subcategory

## Python Libraries for preprocessing

Dataset to detect anomalies in the IOT network and this dataset contains seven different attack scenear4io such as brute force Heartbleed Botnet Dos and DDOS attack web attacks and infiltration of the network from inside , we have used various kinds of libraries in this regard such as the SKLEARN is also known as scikit-learn which has huge and very useful machine learning library which features various algorithms like support vector machine, random forest, k nearest neighbors classification regression, k-means hence it also support python numerical and scientific libraries such as numpy and scipy hence numpy libraries support large multi-dimensional arrays and metrics are used in this project.

## Machine Learning Programming

(Guizani, M., 2020) Label encoder which is part of SKLEARN which is used to convert the label into numeric form so as to convert them into machine readable form hence another part is sklearn is known as standard scalar which is standardize the features of the data such that its distribution will have a mean value 0 and standard deviation 1. Which has useful function in the data which has negative values.

## Logistic Regression Model

(Ghoneim, A. and Alrashoud, M., 2020) Logistic regression modeling which is also known to be part of machine learning python sklearn library which has used to predict the probability of a categorical dependent variable or binary variable that contains one or zero.

## Random Forest Classifier

(Otoum, Y. and Nayak, A., 2020, ) Random forest is supervised machine learning algorithm that is widely used in classification and regression for problems which estimated the which builds the number of decision tree classifier on various samples from the dataset and used averaging to predict to improve the predictive accuracy.

## SVC (Support Vector Classifier)

(Alrajeh, N.A. and Alsolami, F., 2020) Support vector classification is another interesting machine learning algorithm which classify based on support vector classification method, and solved regression problem which detect classification regression and outlier detection. Since the implementation of four different kernel parameter that is linear, polynomial, RVF and Sigmoid and hence the RBF kernel type is used by default and if the kernel type to be used by algorithm is not mentioned.

## Decision Tree

(Du, X. and Guizani, M., 2020) Decision tree which is supervised machine learning programming which uses multiple algorithm to split data into two or more nodes according to certain parameter in which we used the parameter criteria based on entropy whose function is to be measure the quality of the split.

## Gaussian Naïve Bays Algorithm

(Moh, M. and Raju, R., 2018, ) It is used for conditional probability purpose that is to estimate the mean and standard deviation from theta, and in this programming the use of matplotlib library for visualization purposes which will used during the execution part to visualized the confusion matrix and heatmap.

## Result

(Moh, M. and Raju, R., 2018) Dataset will generate performance metrics which will show the accuracy, precision, recall score. Since the classification model is defined as percentage of correct predictions for the test data, these values are represented in the confusion matrix which gives the accuracy ratio and precision is defined as a rate of correctly classified positives or true positives and its gives us the precision ratio. Hence recall is the metric that quantifies how many of the actual positives were found or recalled it is also very important metric as undetective positive might have serious consequences in some areas for example a model that does not recall the cases of DDOS attacks means that malicious network traffic will go on unnoticed increase the potential harm of the system and its users.

## Ethical Hacking Kali Linux Hacking tools to Secure IOT

1. Wireshark

(Abdalla, P.A. and Varol, C., 2020) Network scanning tool which scans the internet of thing smart home connected devices in real time. Wireshark tool which enable them to identify them to communicate with external router which captures packets and debug network. The beauty of Wireshark tool is export pcap file in system hence PCAP data attacker attempt to identify them the sniffing protocol attack, this method identify the packet attack and protocol attack in the system.

1. Binwalk

(Sheng, Q. and Huang, X., 2016, ) In Kali Linux Bin Walk is firmware extraction tool its support ethical hacker to identify the IOT device firmware, Binwalk firmware support smart home internet of thing devices which enable them to identify the contents of file system which extracted the data, Binwalk managing the libmagic library which compatible with python, which extracts the vulnerability in the IOT network.

1. Firmwalker

(Haddad, R.J., 2019, ) Firmwalker is based on bash script which scans the files and extracted the information form the IOT firmware and see the vulnerability in the network. The tool extracted the data into the text file since the tools works amazingly to highlight the potential issues.

1. OWASP ZAP (Zed Attack Proxy)

Web based interface which support ethical hackers to identify any vulnerability in the internet network in the real situation. ZED attack allows hackers to perform proxy ethical hacking attack in the system. The fuzzy security system attack the web interface and find potential susceptibility

1. Metaspolit

(Moravec, J., 2018) In Kali Linux Operating system to predict the hacking attack in the real time which allows ethical hacker to make penetration testing segments and test the attack in IOT app. Metaspolit tool allows them to perform attack on IOT apps. Metaspolit app which perform certain attack on them to identify them the target attack. The vulnerability black hat attack hacker’s exploits.

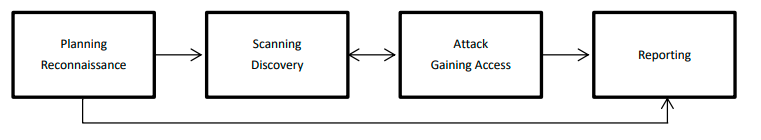


Figure 1: the four stages of penetration testing

## Ethical Hacking on IOT Device Penetration Testing

(Lakshmi, H. and MJ, P.K., 2022) Cyber-attacks are becoming more popular due to capturing the sensitive information in the Internet of thing based system. Since internet of thing system easily captured and hacked through the external router of the smart home network. Kali Linux penetration testing is wide range of ethical hacking security solution tool which enable the ethical hacker to protect the internet of thing system by deploying them towards the method of various security tools. The objective of this research to validate and evaluate the internet thing devices security by deploying the ethical hacking system.

## Mitigating Security Risk and Threats

(Toutsop, O., Das, S. and Kornegay, K., 2021) Lessening threats security attack involves by reviewing them to identify the critical function of the system the internet of thing system dividing them into different component by simplifying them the complex system. Since the potential threats composed of identify them the mitigation schemes of the internet thing network. Acquiring firmware for IOT devices according to penetration testing cook book which defined the four relevant approaches as follows:

1. Obtain firmware from vendor website
2. Mirror or proxy network traffic when updating the device
3. Googling/ Researching
4. Decompiling associated mobile applications

Kali Linux is Debian driven Linux distribution which helps in cyber security investigation by doing penetration testing, it support to identify the man in the middle attack in the internet of thing network. TCPDUMP tool which has piped the network protocol and sniff the packets in the network. Beside this Ettercap is the kali Linux tool which support active and passive examination protocol including encrypted exchange communication between the networks. Another tool Macchanger which implements in Linux which aids in network to capture the fake network and fake hardware device by detecting the fake MAC address, it’s possible through the possible network.

## Analysis

The investigation of this research proposed on machine learning and second method proposed on ethical hacking Kali Linux method, since machine learning method is not completely secure the smart home internet of thing devices beside this Kali Linux system is purely designed for cyber security analysis. Its enable them to identify the network traffic rules and it detect all hacking attack based on router and real time internet network. Cyber security solution are composed of development of security protocol method to secure the smart home system through ethical hacking platform. Various ethical hacking tools and technique are available in Kali Linux and parrot operating system which enable the smart security solution which deeply concerned to secure the smart home devices from the hacking attack and any suspicious activity attack in real situation. Parrot is another turn of security solution which combines works on Kali Linux.

## Ethical Concern

This research does not harm any human being during the research finding, its follow the all rules and regulations of research ethics, the deeply concerned to avoid plagiarism during the research finding. Ethical hacking platform using the Kali Linux which is free operating system distribution which enables them to capture them network vulnerability attack and hacking attack during the discovery of hacking attack. Machine learning programing only enable to capture the dataset related issues during the network scanning tools. The development with python programing which might be able to identify the dataset malicious activity during the internet of thing vulnerability attack. It identify them to capture the machine learning accuracy score with precision and recall.

# References

Al-Garadi, M.A., Mohamed, A., Al-Ali, A.K., Du, X., Ali, I. and Guizani, M., 2020. A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Communications Surveys & Tutorials*, *22*(3), pp.1646-1685.

Makkar, A., Garg, S., Kumar, N., Hossain, M.S., Ghoneim, A. and Alrashoud, M., 2020. An efficient spam detection technique for IoT devices using machine learning. *IEEE Transactions on Industrial Informatics*, *17*(2), pp.903-912.

Otoum, Y. and Nayak, A., 2020, July. On securing IoT from deep learning perspective. In *2020 IEEE Symposium on Computers and Communications (ISCC)* (pp. 1-7). IEEE.

Rahman, A., Hossain, M.S., Alrajeh, N.A. and Alsolami, F., 2020. Adversarial examples—Security threats to COVID-19 deep learning systems in medical IoT devices. *IEEE Internet of Things Journal*, *8*(12), pp.9603-9610.

Shafiq, M., Tian, Z., Bashir, A.K., Du, X. and Guizani, M., 2020. CorrAUC: a malicious bot-IoT traffic detection method in IoT network using machine-learning techniques. *IEEE Internet of Things Journal*, *8*(5), pp.3242-3254.

Moh, M. and Raju, R., 2018, July. Machine learning techniques for security of Internet of Things (IoT) and fog computing systems. In *2018 International Conference on High Performance Computing & Simulation (HPCS)* (pp. 709-715). IEEE.

Moh, M. and Raju, R., 2018, July. Machine learning techniques for security of Internet of Things (IoT) and fog computing systems. In *2018 International Conference on High Performance Computing & Simulation (HPCS)* (pp. 709-715). IEEE.

Abdalla, P.A. and Varol, C., 2020, June. Testing IoT security: The case study of an ip camera. In *2020 8th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-5). IEEE.

Liang, L., Zheng, K., Sheng, Q. and Huang, X., 2016, December. A denial of service attack method for an iot system. In *2016 8th international conference on Information Technology in Medicine and Education (ITME)* (pp. 360-364). IEEE.

Overstreet, D., Wimmer, H. and Haddad, R.J., 2019, April. Penetration Testing of the Amazon Echo Digital Voice Assistant Using a Denial-of-Service Attack. In *2019 SoutheastCon* (pp. 1-6). IEEE.

Zitta, T., Neruda, M., Vojtech, L., Matejkova, M., Jehlicka, M., Hach, L. and Moravec, J., 2018, December. Penetration testing of intrusion detection and prevention system in low-performance embedded IoT device. In *2018 18th International Conference on Mechatronics-Mechatronika (ME)* (pp. 1-5). IEEE.

Gururaj, H.L., Soundarya, B.C., Janhavi, V., Lakshmi, H. and MJ, P.K., 2022, April. Analysis of Cyber Security Attacks using Kali Linux. In *2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)* (pp. 1-6). IEEE.

Toutsop, O., Das, S. and Kornegay, K., 2021, October. Exploring The Security Issues in Home-Based IoT Devices Through Denial of Service Attacks. In *2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI)* (pp. 407-415). IEEE.