IMPROVING RISK ASSESSMENT CONTENT IN PROCESS PHASE FOR LOW CAPACITY DEVICE

.

FATIN ZAHIDAH BINTI SHAMSUDIN

This report is submitted in partial fulfillment of the requirements for the Bachelor of Computer Science (Computer Network)

FACULTY OF INFORMATION AND COMMUNCATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2016

LAMPIRAN B: BORANG PENGESAHAN STATUS TESIS

BORANGPENGESAHAN STATUS TESIS

JUDUL: IMPROVING RISK ASSESSMENT CONTENT IN PROCESS PHASE FOR LOW CAPACITY DEVICE

SESI PENGAJIAN: 2015/2016

Saya FATIN ZAHIDAH BT SHAMSUDIN mengaku membenarkan tesis PSM ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaab seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

____	SULIT	(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)
/	TERHAD	(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)
____	TIDAK TERHAD	

(TANDATANGAN PENULIS)
Alamat tetap: LOT 961, KM5,
JLN MUAR, SEMABOK,
75050, MELAKA
Tarikh: 26th August 2016

(TANDATANGAN PNYELIA)
DR. NURUL AZMA BT ZAKARIA
Nama Penyelia
Tarikh: 26/8/2016

CATATAN: * Tesis dimaksudkan sebagai Laporan Akhir Projek Sarjana Muda (PSM)
** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

IMPROVING RISK ASSESSMENT CONTENT IN PROCESS PHASE FOR LOW CAPACITY DEVICE

.

FATIN ZAHIDAH BINTI SHAMSUDIN

This report is submitted in partial fulfillment of the requirements for the Bachelor of Computer Science (Computer Network)

FACULTY OF INFORMATION AND COMMUNCATION TECHNOLOGY

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2016

DECLARATION

I hereby declare that this project report entitled

IMPROVING RISK ASSESSMENT CONTENT IN PROCESS PHASE FOR LOW CAPACITY DEVICE

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : ______________________ Date: 26/8/2016
(FATIN ZAHIDAH BINTI SHAMSUDIN)

I hereby declare that I have read this project report and found this project report is sufficient in term of the scope and quality for the award of Bachelor of Computer Science (Computer Networking) With Honours.

SUPERVISOR : ______________________ Date: 26/8/2016
(DR.NURUL AZMA ZAKARIA)

DEDICATION

This work is dedicated to my beloved parents, Shamsudin bin Abdullah and Khadijah binti Abdul Rahman, and siblings who passed on a love of readings and respect for education.

The my supportive friends, Nur Adreena binti Ibrahim, Mubarakah binti Sualman and Mohammad Zahid bin Mohammad and my supervisor, thank you so much for assistance for help.

ACKNOWLEDGEMENTS

Bismillahirrahmanirrahim

Alhamdulillah, Thanks to Allah SWT, whom with His willing give me the opportunity to complete this Final Year Project with the title of Improving Risk Assessment Content in Process Phase for Low Capacity Device. First, I would like to express millions of thank you to my supervisor Dr. Nurul Azma Zakaria for guiding me throughout this project, thanks for being an open book and the inspiration for me to keep on going. Deepest thanks and appreciation to my fellow friends for always being there for me and to give a hand whenever I need it the most.

ABSTRACT

The research is about Improving Risk Assessment Content in Process Phase for Low Capacity Device. The research is focuses on the risk of low capacity device, Raspberry Pi that will be identified from the past literature review and provide the example research from other researcher.The testing will be done with port scanning and vulnerability test that will be conducted and will produce the rating of risk that contains threats and vulnerabilities. To document the guideline, the preliminary list of risk and recommendation is going to be shown. This will act as guideline of risk assessment for low capacity device in ISO Standard.

ABSTRAK

Kajian ini adalah mengenai meningkatkan kandungan penilaian risiko dalam fasa proses untuk peranti kapasiti rendah. Kajian ini memberi tumpuan kepada risiko peranti kapasiti yang rendah, Raspberry Pi yang akan dikenal pasti daripada kajian literatur yang lalu dan menyediakan penyelidikan contoh daripada kajian yang terdahulu.Selepas itu, ujian dilakukan dengan pengimbasan port dan ujian kelemahan yang akan dijalankan dan akan menghasilkan penarafan risiko yang mengandungi ancaman dan kelemahan. Untuk mendokumentasikan garis panduan, senarai awal risiko dan cadangan akan ditunjukkan. Ini akan bertindak sebagai garis panduan penilaian risiko untuk peranti kapasiti yang rendah dalam ISO Standard.

TABLE OF CONTENT

CHAPTER	CONTENT		PAGE
	DECLARATION		I
	DEDICATION		II
	ACKNOWLEDGEMENTS		III
	ABSTRACT		IV
	ABSTRAK		VI
	TABLE OF CONTENTS		VII
	LIST TABLE OF TABLES		X
	LIST TABLE OF FIGURE		XI
	LIST OF ABREVIATION		XIV
CHAPTER 1	INTRODUCTION		
	1.1	Introduction	1
	1.2	Problem Statement	2
	1.3	Project Question	3
	1.4	Project Objective	3
	1.5	Research Scope	4

1.6 Research Contribution 4

1.7 Thesis Organization 4

1.8 Conclusion 5

CHAPTER 2 LITERATURE REVIEW

2.1 Introduction 6

2.2 Related Work/Previous Work 8

2.2.1 Information Security 8

2.2.2 Access Control System 9

2.2.3 Physical Security 10

2.2.2 Analysis 28

2.2.2 Risk Assessment 30

2.3 Critical Review of Current Problem 17

2.3.1 Wireless Smoke Alarm Detector 17

2.3.2 Carbon Monoxide Alert System For Car 19

2.3.3 Cigarette Smoke Detector With Voice Alarm 20

2.4 Proposed Solution/Further Project 39

2.5 Conclusion 40

CHAPTER 3 METHODOLOGY

3.1 Introduction 41

3.2 Methodology 41

3.2.1 Phase1: Planning 42

3.2.2 Phase2 :Analysis: Literature Review 43

3.2.3 Phase3: Design & Implementation 44

3.2.4 Phase4: Testing 44

3.2.5 Phase5: Report/Documentation 45

3.3 Project Milestone 45

3.4 Conclusion 47

CHAPTER 4 DESIGN

4.1 Introduction 48

4.2 Logical and Physical Design of Testing Environment 48

4.2.1 Software Requirement 49

4.2.2 Hardware Requirement 51

4.3 Possible Scenario 53

4.4 Risk Assessment Analysis Step 54

4.5 Metric Measurement 56

4.6 List of Risk 56

4.7 Conclusion 57

CHAPTER 5 IMPLEMENTATION

5.1 Introduction 58

5.2 Environment Setup 59

5.2.1 Raspberry Pi Environment Setup and OS Installation 60

5.2.3 Zenmap Software 66

5.2.3 Vulnerability 68

5.3 Conclusion 71

CHAPTER 6 TESTING

6.1 Introduction 72

6.2 Results and Analysis Testing 72

6.2.1 Primary Data 73

6.2.3 Secondary Data 76

6.3 Risk on Low Capacity Device 88

6.4 Risk Classification 89

6.5 Propose Counter Measure For Identify Risk 90

6.5.1 Correlation from Past Research 91

6.6 Analysis Using Statistical Method 92

6.6.1 Operational Definition 94

6.6.2 Formation of hypothesis 94

6.6.3 Conceptual Framework 95

6.6 Conclusion 96

CHAPTER 7 CONCLUSION

7.1 Introduction 97

7.2 Project Summarization 97

7.3 Project Contribution 98

7.4 Project Limitation 99

7.5 Future Works 99

7.6 Conclusion 100

REFERENCES 101

APPENDICES 108

LIST OF TABLE

Table 1: List of threats (Protocols 2006) 13

Table 2: Smard Card roles (Vanderhoof n.d.) 19

Table 3: Differences between microprocessor and microcontroller 22

Table 4: Several types that used MPU and MCU 23

Table 5: Project Milestone 45

Table 6: Testing Description 72

Table 7: Testing Description 73

Table 8: Summarization of risks 85

Table 9: Level of risks 88

Table 10: Counter Measure of Identify High Risk 89

Table 11: Value for variable 91

Table 12: Non-Parametric Correlations 92

Table 13: Operational of definition 94

LIST OF FIGURE

Figure 1: Framework for Literature Review 7

Figure 2: Types of Biometric 15

Figure 3: Beaglebone 24

Figure 4: Raspberry Pi 25

Figure 5: Arduino 26

Figure 6: Process phase for risk assessment based on ISO 36

Figure 7: Flow diagram of this research 38

Figure 8: Process phase for Methodology 40

Figure 9: Network configuration test environment 43

Figure 10: Gantt chart of Project Milestone 44

Figure 11: Network configuration test environment 47

Figure 12: Kali-Linux 47

Figure 13: Zenmap Software 48

Figure 14: OpenVAS, vulnerabilities scanner 49

Figure 15: PC/ Laptop 50

Figure 16: Raspberry Pi 2 50

Figure 17: The example result of OpenVAS scan 53

Figure 18: Process phase for risk assessment based on ISO 54

Figure 19: Example of risk rating 55

Figure 20: List of Risk 56

Figure 21: Network configuration test environment 58

Figure 22: Environment setup 60

Figure 23: Choose SD Card to format. 61

Figure 24: Change format size adjustment ON 61

Figure 25: Choose OK to continue. 62

Figure 26: SD Card format complete. 62

Figure 27: Select KALI image and extract. 63

Figure 28: Use Win 32 Disk Imager to transfer KALI image to SD Card. 63

Figure 29: Choose Yes to continue 64

Figure 30: Write successful 64

Figure 31: To update and upgrade Kali Linux 65

Figure 32: Choose nmap in Vulnerability Analysis 66

Figure 33: Step to know current IP address 66

Figure 34: Scanning IP Address to test 67

Figure 35: Installation OPENVAS 67

Figure 36: To make sure all packages has been downloaded. 68

Figure 37: Openvas-check-setup 69

Figure 38: Openvas-check-setup (continue) 69

Figure 39: Netstat -antp to list out the state of port 70

Figure 40: Result from scan port testing. 72

Figure 41: Process to start the OpenVas 73

Figure 42: The real output to start the OpenVas. 74

Figure 43: The web was not appearing in the right browser. 74

Figure 44: The output from test Netcat 76

Figure 45: Output vulnerabilities testing in OpenVAS 77

Figure 46: Output for vulnerability testing in NeXpose CE 78

Figure 47: Port Scanning in Windows Server 79

Figure 48: Vulnerabilities scan for specific IP address. 79

Figure 49: Pie Chart for the result. 80

Figure 50: List Vulnerabilities 80

Figure 51: Description of vulnerability 81

Figure 52: Result from vulnerabilities testing. 82

Figure 53: Result from scanning port 83

Figure 54: Result from scanning vulnerabilities 83

Figure 55: List of open port 84

Figure 56: Summarize of risk 87

Figure 57: The conceptual framework of this research 95

LIST OF ABBREVIATIONS

SSH	-	Secure Shell
ICMP	-	Internet Control Message Protocol
FTP	-	File Transfer Protocol
TCP	-	Transmission Control Protocol
UDP	-	User Datagram Protocol
NTP	-	Network Time Protocol
ISO	-	International Organization for Standardization
HTTP	-	Hypertext Transfer Protocol
SMTP	-	Simple Mail Transfer Protocol
IP	-	Internet Protocol
SPSS	-	Statistical Package for the Social Science

CHAPTER I

INTRODUCTION

1.1 Introduction

Low capacity device contain low storage and has a low price in the market such as Beaglebone, Arduino and Raspberry Pi. It is widely used in technology related to Internet of Things (IoT). The IoT is an arrangement of interrelated registering gadgets, mechanical and advanced machines, articles, creatures or individuals that are given special identifiers and the capacity to exchange information over a system without obliging human-to-human or human-to-PC cooperation. Because it is widely used by the users, securities need to be considered and all threats need to minimize. The existence of security risks that would be harmful the use for this kind of device causes the need for risk assessment.

In this case, the study will focus on Raspberry Pi. It is very popular nowadays than others due to the benefits. The risk assessment is needed in the industry because of its effect can reduce the risks that are inherent in the environment. It has many of these

looInternational Federation of the National Standardizing Associations (ISO), Information Technology Infrastructure Library (ITIL), Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), Escal Institute of Advanced Technologies (SANS Institute) and National Institute of Standards and Technology (NIST). It provide guidance for cater the solutions in the use risk assessment.

1.2 Problem Statement (PS)

In this project, ISO Standard will be used since the government is using ISO Standard and it is widely used by industry. Therefore, this study was carried out to produce a guidance that relates to ISO Standard and low capacity device in this case is Raspberry Pi. Based on previous studies, there has no detail content relate to low capacity device in ISO Standard document. The ISO Standard focuses on equipment in general device but not for general low capacity device. Thus this motivates the development of this project in order to improve the content of ISO Standard to include the risk assessment information that provides guidance for analyzing security risk of the related device.

PS	**Problem Statement**
PS1	Lack of risk assessment content on low capacity device.

1.3 Research Question (RQ)

RQ	**Research Question**
RQ1	What is the list of threats related to the low capacity device?
RQ2	What are the vulnerabilities?

1.4 Project Objective (PO)

PO	**Objective**
PO1	To identify the risk of the low capacity device.
PO2	To analyze the identified risk.
PO3	To document the guideline.

Project Objective 1 (PO1)

To identify the risk of the low capacity device. From chapter 2, the risk of low capacity device will be identified from the past literature review and provide the example research from other researcher.

Project Objective 2 (PO2)

To analyze the identified risk. From chapter 4 and 5, the port scanning and vulnerability test will be conducted and will produce the rating of risk that contains threats and vulnerabilities.

Project Objective 3 (PO3)

To document the guideline. From this document, it will produce list of risk and recommendation to be solved. This will act as guideline of risk assessment for low capacity device in ISO Standard.

1.5 Research Scope

The scope in this research is focused on risk assessment in Raspberry Pi with ISO standard as guidance.

1.6 Research Contribution (RC)

With the establishment of this research, this study will help researchers in a study on the risk assessment for low capacity devices. This research also will improved ISO standard because existing standards focus on equipment in general.

1.7 Thesis Organization

In introduction, chapter 1, it will be focusing on introduction, project background, research problem research question, research objective, scope, project significant and report organization.

In this literature review, chapter 2, it will thrive more on the explanation and details of this project, supported with reading materials and conference paper. In this section, other related projects will also be included such as information security, physical security, risk assessment and ISO standard.

In this methodology, chapter 3, it will explain the method that will be used in this project. The method that is used in this project is the process phase. This will ease the task for implementing and organizing the research.

In this design, chapter 4, test environment will be showed. Hardware is coordinated to be used in implementing the project. The customization of the module will be conducted.

In this design, chapter 5, setup and installation of the process will be showed. Raspberry Pi is used as one of low capacity device and installation of Kali Linux will be held.

In this testing and analysis, chapter 6, it will test to scanning port and having vulnerabilities test on Raspberry Pi as primary data and test on secondary data.

In this conclusion, chapter 7, all project summarization, project contribution and project limitation will be explained. All the steps that have been made and that have been developed for this project will be listed briefly. In this last chapter also explain on additional work can be done in future.

1.8 Conclusion

As for conclusion, at the end of this project, the security in Raspberry Pi will be improved and an analysis will be improvement in ISO standard for risk assessment low capacity device. The next chapter will be focusing about literature review. Which will be covering about more detail about risk assessment and ISO standard for low capacity device.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

In previous chapter, the research problem, research questions and research objective of the research are clearly discussed. This chapter will be based on the phase. The purposes of the literature review are to provide the background and justification for undertaking research. The literature review provides example, case studies and other relevant works and that have been done in the past. The significance of the literature review is to allow the researcher to gain more information on their subject area. It also provides the researcher with the objectives, problem statements, scopes and other information on previous research. Theoretically, the researcher will produce a more efficient research which fulfills the user requirement of the previous research. The researcher will also know the limitations of the previous system which help the development of new and more advance system.

Figure 1 show the detail framework about the flow of getting content of risk assessment that will be used to guide in this chapter. This project will focus on identify the Risk Assessment and detail.

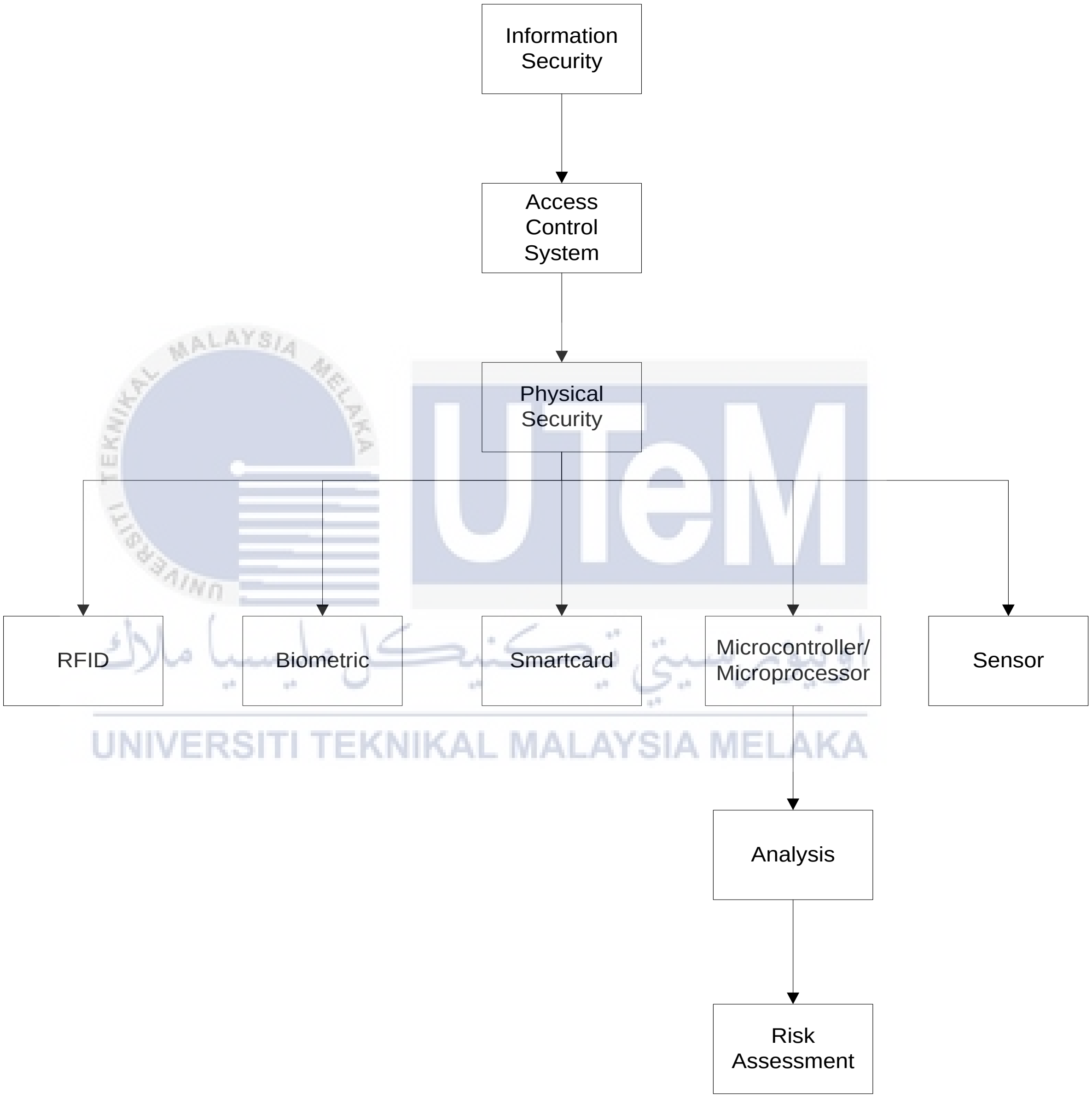


Figure 1: Framework for Literature Review

2.2. Related Work/Previous Work

2.2.1 Information Security

Information security (infosec) is formed from the words IT Security and Information Assurance. Information security is the order of business strategies that guarantees information assets paying little regard to how the information is composed or whether it is being taken care of, is in travel or is being secured. Based from Wikipedia, *"Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The terms information security, computer security and information assurance are frequently used interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms."*

From the text above, it means in infosec, there is three parts that can be separated, which is confidentiality, integrity and availability. **Confidentiality** means shielding data from being revealed to unapproved parties. As case for individual, when submitted to a site, your own information ought to just be utilized or got to solely by assigned staff in that organization for the reasons concurred. Nobody else ought to be permitted to utilize your information for unlawful purposes, or view the information just wondering. For business, Sensitive data, for example, deals figures or customer information, ought to just be gotten to by approved persons, for example, senior administration and the business group, and not different operations or offices. Trustworthiness implies shielding data from being changed by unapproved parties. Case for individual is when submitted to a site; your own information ought not be changed at all amid information transmission, or by the site organization. For business, the essential records or figures ought not be changed or modified by unapproved persons without earlier notice. Accessibility conveys intend to the accessibility of data to approved gatherings just when asked. The case for individual is the point at which you ought to have the capacity to get to and check your own information continued a site whenever. For business, approved senior administration faculty ought to have the capacity to get to deals figures when required; or customers ought to have the capacity to get to any of their information stayed with by the when they ask for it.

The significance of data security in a PC based environment has brought about an extensive stream of examination that spotlights on the specialized resistances (e.g., encryption, access control, and firewalls) connected with ensuring data and interruption location frameworks. Moreover, investigate has been quickly building up that spotlights on the behavioral parts of lessening data security ruptures. Interestingly, research concentrating on the financial parts of data security is fairly inadequate. The work that exists on, or identified with monetary parts of data security gives minimal nonspecific direction on the most proficient method to infer the best possible add up to contribute on such (Gordon & Loeb 2002).

2.2.2 Access Control System

The expression "access control" delineates any framework used to control area into or out of any district. The expression "access control structure" reliably infers a PC based, electronic card access control framework. The electronic card access control structure utilizes an exceptional "access card", as opposed to a metal key, to allow access into the secured area. There are two significant sorts of access control: physical and sensible. Physical access control limits access to grounds, structures, rooms and physical IT resources. Unsurprising access limits association with PC systems, structure records and information. Access control frameworks perform underwriting ID, assertion, access backing, and commitment of segments through login accreditations including passwords, individual perceiving confirmation numbers (PINs), biometric checks, and physical or electronic keys.

Access control is advancing from its customary host-driven worldview to assets and elements that execute over huge systems as wide as the Internet. The low-level access-control benefits of the essential read and compose of data are presently climbing a level higher to incorporate qualities that make up a profile for an element. These are the components that copy genuine client qualifications, for example, the benefit of having a keeping money account, having a charge card number, or being doled out a very much characterized part. The procedures expected to keep up substance profiling offered ascend to what is alluded to as character administration, which is in fact a prelude to any entrance control instrument. It is worried with the trusted techniques for overseeing and trading substance qualifications on different figuring frameworks and asset directors. Character administration shapes the establishment on which get to control is based (Benantar 2006)

2.2.3 Physical Security

Physical security describes attempt to build up wellbeing that are planned to deny unapproved access to workplaces, equipment and resources, and to shield work power and property from mischief or harm. Physical security incorporates the use of various layers of related structures which join CCTV perception, security screens, cautious impediments, locks, access control traditions, and various distinctive techniques. Physical security is frequently dismissed (and its essentialness considered little) for more particular and exciting issues, for instance, hacking, diseases, Trojans, and spyware. In any case, breaks of physical security can be finished with alongside zero particular learning regarding an attacker. Also, accidents and general catastrophes are a bit of normal life, and in the long separation, are unavoidable. There are three rule parts to physical security. In the first place, difficulty can be set in the system for potential assailants and regions can be established against failure and normal dissatisfaction. Such measures can join diverse locks, fencing, dividers, fire safe safes, and water sprinklers. Second, discernment and advised frameworks can be set up, for occasion, lighting, heat sensors, smoke identifiers, interruption pioneers, cautions, and cameras. Third, strategies can be executed to secure aggressors (ideally before any harm has been done) and to recover rapidly from episodes, flares, or basic disaster.

Physical security frameworks for ensured offices are by and large proposed to:

- deter potential intruders (e.g. advised signs and fringe markings);
- detect interferences and screen/record intruders (e.g. gatecrasher alerts and CCTV structures); and
- trigger fitting event responses (e.g. by security watches and police).

It is up to security fashioners, architects and specialists to alter security controls against risks, considering the costs of demonstrating, making, testing, completing, using, supervising, watching and keeping up the controls, close by more broad issues, for instance, feel human rights, prosperity and prosperity, and societal measures or customs. Physical access endeavors to build up wellbeing that are reasonable for a high security prison or a military site may not be right in an office, a home or a vehicle, disregarding the way that the measures are similar.

RFID means Radio-Frequency Identification is the utilization of radio waves to consider and escape on a name joined to a thing. A tag can be analyzed from up to two or three feet away and should not to be inside direct obvious pathway of per client to be taken after. A RFID structure is contained two portions: a tag or name and for every client. RFID names or stamps are presented with a transmitter and a recipient. The RFID piece on the imprints has two fragments: a microchip that stores and techniques data and a getting wire to get and transmit a sign. The tag contains the particular serial number for one particular thing. To start with exploration is from (Soon and Tieyan 2008), which expressed for the answers for handling the security and protection issues encompassing RFID. It can be arranged into three range which is label information assurance, per user trustworthiness, individual security. For label information insurance arrangements, secret word assurance on label memory, physical locking of label memory and confirmation of the "Creator" in label memory. For per user trustworthiness arrangements, it utilized per user assurance and read indicators. In individual security arrangements, it utilized kill label, faraday confine, dynamic sticking, "RSA" specific blocker tag and intelligent 'Hash-lock'.

In RFID system will support the appropriate security controls. This is taken from (Karygiannis et al. 2007) , the factors to consider which is :

- The general useful goal of the RFID innovation. For instance, does the framework need to decide the area of an article or the nearness of an item, verify a man, perform a money related exchange, or guarantee that specific things are not isolated?

- The nature of the data that the RFID framework forms or produces. One application may just need remarkable, static identifier esteem for each labeled item, while another application may need to store extra data about each labeled article after some time. The affectability of the data is additionally an imperative thought.

- The physical and specialized environment at the time RFID transactions occurs. This includes the distance between the readers and the tags, and the amount of time in which each transaction must be performed.

- The physical and specialized environment prior and then afterward RFID exchanges happen. For instance, human and natural dangers may posture dangers to labels' trustworthiness while the labeled items are away or in travel. A few applications require the utilization of labels with sensors that can track ecological conditions after some time, for example, temperature and mugginess.

- The financial aspects of the business procedure and RFID framework. The financial elements for RFID frameworks are not the same as those for conventional IT frameworks. For instance, numerous RFID labels offer few or no security highlights; selecting labels that fuse fundamental security usefulness essentially builds the expense of labels, particularly if encryption components are required. Likewise, the operational expense of some fundamental IT security controls, for example, setting one of a kind passwords and transforming them routinely, might be higher for RFID frameworks due to the logistical difficulties in overseeing security for thousands or a huge number of labels.

The third research is discussed about the security in RFID system (Protocols 2006). The table 1 shows the list of threats in RFID system:

List of threats	
Privacy	Physical attacks
Spoofing	Corporate Espionage
Data Integrity of Tags	Denial of Service

Table 1: List of threats (Protocols 2006)

After listing threats in table 1, the following are examples of situations when there are threats.

- An assaulter extorts a person for having certain stock in their ownership
- A criminal could make a copy tag with the same EPC number and give back a manufactured thing for an unapproved discount
- An aggressor pressure a person for having certain stock in their ownership
- A bomb in an eatery blasts when there are five or more individual of a specific country with RFID-empowered international IDs identified.

Biometrics is the estimation and factual examination of individuals' physical and behavioral qualities. The innovation is fundamentally utilized for recognizable proof and get to control, or for distinguishing people that are under reconnaissance. The fundamental reason of biometric verification is that everybody is one of a kind and an individual can be recognized by his or her inborn physical or behavioral attributes. (The expression "biometrics" is gotten from the Greek words "bio" which means life and "metric" intending to quantify.). In figure 2, it shows the types of biometric. There are two primary sorts of biometric identifiers:

1. Physiological attributes: The shape or constitution of the body.
2. Behavioral qualities: The conduct of a man.

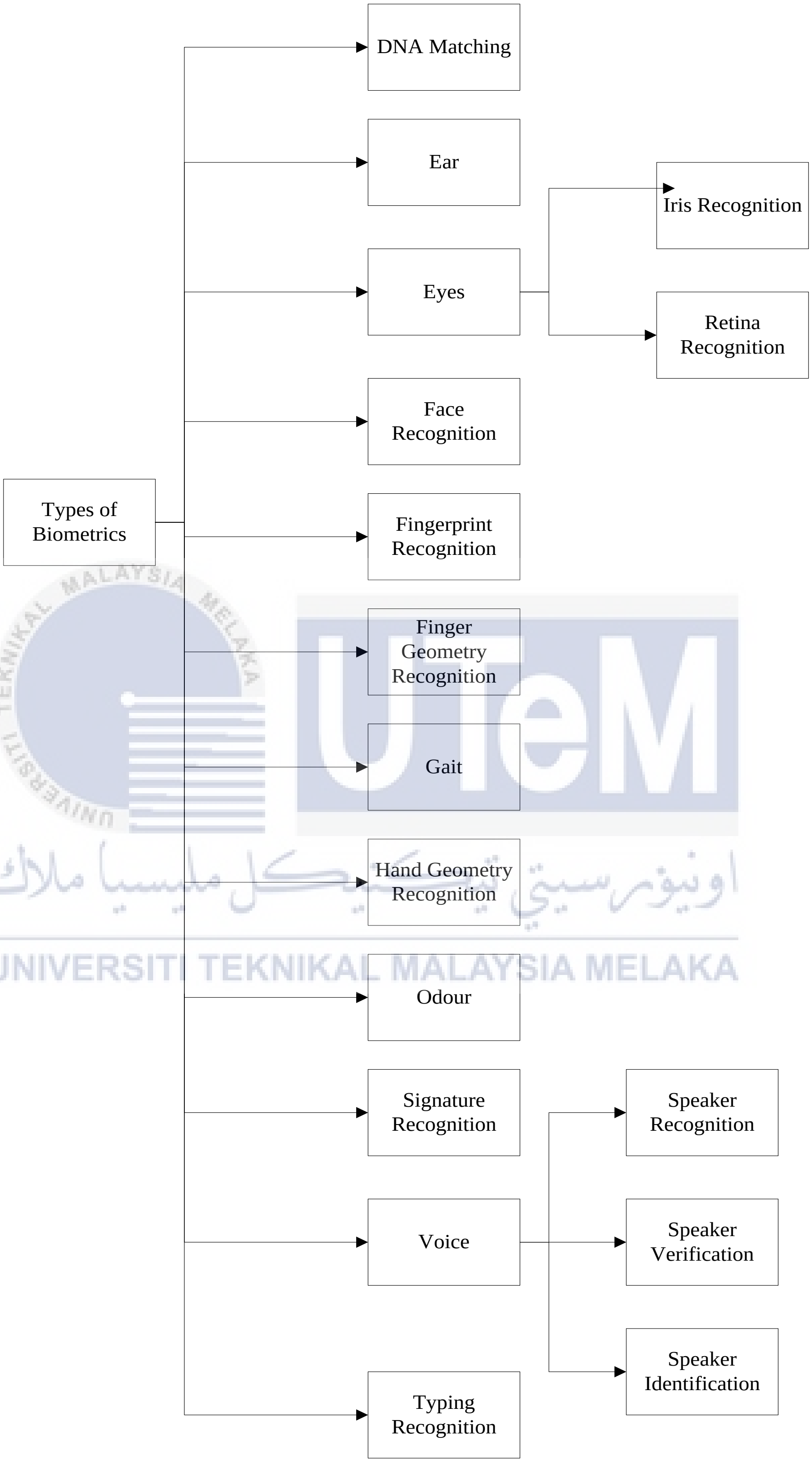


Figure 2: Types of Biometric

Physical access control refer to the technique that requires the physical qualities (Jain 2004). Be that as it may, then, smart access control is the arrangements, techniques and procedures which are used as a part of the structure. The refinement amongst honest to goodness and physical access control is little and it can be befuddled viably in light of the way that physical access control is controlled by sensible access control. Physical access control covers identity declaration frames which require customers to give physical qualities. It is used as a piece of high security ranges, for instance, recover offices, police base camp, and the military. Honest to goodness access control insinuates a strategy of an arrangement control over data records or PC programs. These contain individual or assurance information of an extensive variety of customers. Reliable access control is used by militaries and governments to guarantee their key data with high security structures using biometric advancement.

Biometrics can be used for some applications outside the degree of PC security (Republic 2002). Facial affirmation structures are frequently passed on at intermittently passed by spots to chase down guilty parties. Interesting finger impression structures (AFIS) are used to find a liable gathering according to trails left on the illicit spot. Infrared thermographs can point out people under effect of various medicines (unmistakable drugs react in different ways). Biometric structures adequately used as a piece of non-checking applications may moreover require not be viably used as a piece of affirming applications. The biometry consolidates all structures that make the interface between a PC system and a human(Orság & Drahanský n.d.). There is an extensive measure of characteristics that could be used for recognizing verification purposes. These qualities are fascinating for each person. Of those attributes, the extraordinary imprint was the first to be found and investigated. Everyone's finger passes on a surprising illustration. This illustration includes different circles, spirals and twists and is totally stood-out.

Smart card is a gadget that joins an introduced composed circuit that can be either a secured microcontroller or similar information with inward memory or a memory chip alone. The card partners with for each client with direct physical contact or with a remote contactless radio repeat interface. With an embedded microcontroller, splendid cards have the exceptional ability to store a great deal of data, do their own specific on-card limits (e.g., encryption and shared confirmation) and work together keenly with a brilliant card for each client. Insightful card advancement fits in with worldwide standards (ISO/IEC 7816 and ISO/IEC 14443) and is available in a combination of structure components, including plastic cards, key dandies, watches, endorser recognizing verification modules used as a piece of GSM cell phones, and USB-based tokens.

The restraint of Smart Card makes them impenetrable to ambush as they don't need to depend on possibly defenseless external resources. As an aftereffect of this, Smart Cards are as often as possible used as a piece of usages which require strong security protection and affirmation. Advancement and security are vehemently related. Saltines discover cutting edge ways to deal with get at to the extent anybody knows secure data on cards. Producers need to consider more mind boggling jolts and keys on cards. Wafers consider better strategies to evade these, in this way forming an interminable change circle, with both sides driving each other to use and improve advancement. There are four special parts of the Smart Card security:

- Communication
- Hardware
- Operating System (OS)
- Software

A smart card is a Mastercard estimated plastic card with a microchip chip implanted in the card that makes it smart (Fallis 2013). Contingent upon the kind of implanted chip, brilliant cards can be Java Cards, memory cards or processor cards.

- Java card - these card determinations empower Java innovation to keep running on smarts card and different gadgets with restricted memory. The greater part of telecom suppliers utilize this sort of card for their phone framework.

- Memory Cards-The chip goes about as a memory stockpiling gadget. Most utilization of this card sort is for telephone card and ticket. The card put away rechargeable esteem and can be utilized commonly.

- Processor cards - Smart cards with an undeniable microchip on board can work as a processor gadget that offer numerous capacities, for example, encryption, propelled security component, nearby information handling, complex figuring and other intelligent procedure.

To utilize Smart Cards as User Interface(UI) archives from one viewpoint and backing a wide assortment of collaboration gadgets (counting those with memory and CPU restrictions)(Schaefer et al. 2007), we needed to pick a UI portrayal group which is:

- Generic concerning the basic stage (e.g. methodology, toolbox, and so forth.)
- Easy process capable for low-CPU-customers
- Compact concerning memory requests for both the Smart Card and potential customers

So as to meet those limitations we picked the Dialog and Interface Specification Language DISL which is fundamentally an incline subset of the UIML 4.0 (User Interface Markup Language). The dialect predominantly comprises of an organized count of nonexclusive significance gadget and methodology independent–gadgets and a behavioral part which is utilized to indicate the exchange. As shown in table 2, in ID system, smart card has their own role such as (Vanderhoof n.d.):

Table 2:Smard Card roles (Vanderhoof n.d.)

A personal database	**A personal firewall**	**A personal terminal**
Store and defend data on an individual foundation	Smart gatekeeper of cardholder information – confirming that requestors are approved to get to data	Approval of the genuineness and dependability of card per users or terminals
Local, portable storage an individual's private information	Cardholder control of release of information	Intense acceptance of cardholder as legitimate owner of the ID card

A **sensor** is a gadget that distinguishes and reacts to some sort of contribution from the physical environment. The particular information could be light, warm, movement, dampness, weight, or any of an awesome number of other ecological wonders. The yield is for the most part a sign that is changed over to understandable presentation at the sensor area or transmitted electronically over a system for perusing or further preparing. Here are few of case of the wide range of sorts of sensors:

- In a mercury-based glass thermometer, the information is temperature. The fluid contained grows and contracts accordingly, bringing about the level to be higher or lower on the checked gage, which is intelligible.
- An oxygen sensor in an auto's discharge control framework identifies the fuel/oxygen proportion, as a rule through a compound response that produces a voltage. A PC in the motor peruses the voltage and, if the blend is not ideal, rearranges the equalization.
- Motion sensors in different frameworks including home security lights, programmed entryways and lavatory installations ordinarily convey some kind of

vitality, for example, microwaves, ultrasonic waves or light pillars and identify when the stream of vitality is hindered by something entering its way.

- A photo sensor identifies the nearness of unmistakable light, infrared transmission (IR), and/or bright (UV) vitality.

There are sure elements which must be considered when we pick a sensor. They are as given underneath:

i. Accuracy
ii. Environmental condition - generally has limits for temperature/dampness
iii. Range - Measurement farthest point of sensor
iv. Calibration - Essential for the vast majority of the measuring gadgets as the readings changes with time
v. Resolution - Smallest augmentation distinguished by the sensor
vi. Cost
vii. Repeatability - The perusing that changes is more than once measured under the same environment

Sensors are another answer for measuring streams and voltages required for insurance and checking in medium voltage power frameworks (Anon n.d.). Certain solid patterns have been available in the middle of the entire time of electrical gear fabricating: a nonstop reduces of hardware size, a constant change of hardware execution and a persistently scoring requirement for standardization. Nonetheless, in some writes of gear the noticeable impact of those patterns has, amid drawn out stretches of time, been generally little. A run of the mill case is the transformer, including instrument transformers. The characteristic properties of the delicate iron center, as maximal changeability thickness and absence of linearity in the excitation bend, have set points of confinement for the conceivable outcomes to lessen the transformer measure and to utilize the transformer in a more extensive scope of uses. As a result, most instrument transformer units have been electrically perfectly customized for one certain application and an extensive standardization has never been figured it out.

This disservice can be vanquished with the presentation of sensors taking into account elective standards like the Rogowski curl and resistive or capacitive dividers for current and voltage detecting individually. These standards are a long way from new; they are for the most part as old as the standards of customary inductive instrument transformers. Notwithstanding, the usage of the standards has not been conceivable to complete – with the exception of in extraordinary applications – because of the absence of exact and economical electronic gadgets required. Not as of recently, with the presentation of flexible electronic transfers, has it been conceivable to make utilization of the favorable properties of sensors.

Following of Mr. Irv Smietan, (East 1997), inside dynamic infrared sensors are comprised of a transmitter and collector encased inside a solitary lodging unit. The transmitter utilizes a laser to make a location zone. The laser plane is anticipated onto an extraordinary retro-intelligent tape that characterizes the end/edge of the security zone. Vitality is reflected off the tape back to the recipient, which is situated in the same lodging unit as the transmitter. After achieving the recipient the vitality goes through a gathering lens that centers the vitality onto a gathering cell, which changes over the infrared vitality to an electrical sign. The recipient screens the electrical flag and creates an alert when the sign drops underneath a preset edge for a particular timeframe. A gatecrasher going through the field of identification will interfere with the sign and briefly cause the sign to fall beneath the edge esteem. For sensor in fiber optic, it has their own classifications (Gerhard et al. 2008) which are:

- Sensing area: Intrinsic versus Outward

  - Intrinsic fiber optic sensor has a detecting area inside the fiber and light never leaves the fiber.
  - In outward sensors, light needs to leave the fiber and achieve the detecting area outside and after that returns to the fiber.

- Optical adjustment system

  - Intensity adjusted
  - Phase adjusted
  - Wavelength adjusted
  - Polarization adjusted

A **microprocessor** typically refers specifically to the device/component whose job it is to fetch commands, interpret the command opcodes, and execute the commands. In a modern microprocessor, this basically means the ALU, the register set, instruction pipeline, and the microprocessor control circuitry to perform the Von-neumann "fetch-decode-execute" cycle. One generalization is that microprocessors require an external bus and discreet memory devices to interface with (separate from internal registers, and whatever built in caching memory the microprocessor contains).

Microcontrollers are more generalized devices which contain a microprocessor, a main system bus, ram, rom/flash, and typically a set of other devices such as a programmable interrupt controller, analog/digital converters, any number of general purpose IO devices, communications interfaces. The term chip and microcontroller have dependably been mistaken for each other. The two have been intended for continuous application. They share numerous regular components and in the meantime they have noteworthy contrasts. Both the IC's i.e., the chip and microcontroller can't be recognized by taking a gander at them. They are accessible in various renditions beginning from 6 pin to as high as 80 to 100 sticks or significantly higher relying upon the elements. Table 3 shows the differences between microcontroller and microprocessor.

Microprocessor(MCU)	**Microcontroller(MPU)**
Bit taking care of guideline is less, maybe a couple sort only	Many kind of bit taking care of direction
Quick developments of code and information between outer memory and MP	Rapid developments of code and information inside MC
It is utilized for configuration broadly useful advanced PCs system	They are utilized for planning application particular devoted framework.

Table 3: Differences between microprocessor and microcontroller (Gaillard & Eieland 2013)

From the network point of view (Gaillard & Eieland 2013) , most MCU and MPU gadgets are accessible, with all the basic prevalent fringe interfaces. In any case, fast correspondence peripherals, for example, HS USB 2.0, numerous 10/100 Ethernet ports or Gigabit Ethernet port are for the most part just found on MPU in light of the fact that they are better skilled to handle and process a lot of information. Whether there are sufficient appropriate channels and transfer speed to handle the information activity is a key inquiry. Contingent upon the correspondence conventions utilized, the effect on code space utilizing outsider stacks ought to be checked. Applications requesting rapid network particularly in mix with utilizing OS-based stacks will require a MPU-based configuration. There are a few sorts that utilizing single-board as MPU and MCU. There are:

Microprocessor	**Microcontroller**
Beaglebone	Arduino
SolidRun	Wiring
Raspberry Pi	

Table 4: Several types that used MPU and MCU

1. Beaglebone

Declared toward the end of October 2011, the BeagleBone is a barebone improvement board with a Sitara ARM Cortex-A8 processor running at 720 MHz, 256 MB of RAM, two 46-pin development connectors, on-chip Ethernet, a microSD opening, and a USB host port and multipurpose gadget port which incorporates low-level serial control and JTAG equipment investigate associations, so no JTAG emulator is required. Various BeagleBone "Capes" have as of late been discharged. These capes are extension loads up which can be stacked onto the BeagleBone Board (up to four at one time). BeagleBone capes incorporate yet are not constrained to:

- LCD touchscreen capes (7" and 3.5")
- DVI-D point
- Breakout point
- Breadboard point
- CAN bus point
- RS-232 point
- Battery point

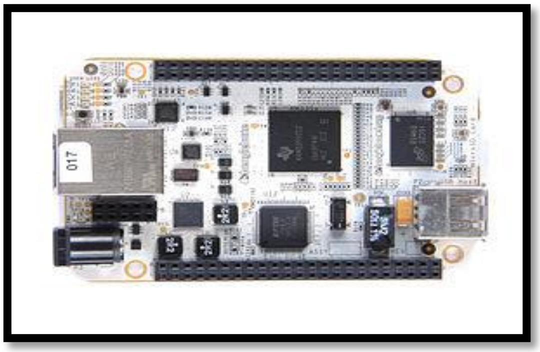


Figure 3: Beaglebone

2. SolidRun

It actually is a "carrier" board with a processing board on top. The processor board (MicroSOM) can be removed and exchanged. This setup is kind of like the Compute Module and Development board just released. The processors available are single core or dual core at 1GHz and the memory is 64bit 512MB or 1GB. Prices range from $44.99 to $116.99. These prices depend on whether you buy a micro SD and power adapter with the board. It uses a Micro USB power adapter. It claims 1Gbit on the i2eX MicroSOM Ethernet but it is limited to 470Mbps, the other two versions are 10/100. It has two USB in the same place as the RasPi and two internal USB on a header. The primary connectors (HDMI, USB, Ethernet, Coax, earphone) are located in the same positions as the RasPi. So is the SD except it is a Micro SD. It contain slight speed gain and 64 bit memory. It uses Linux and has quite a few distributions available;

- Android
- ArchLinux
- Debian
- Fedora
- GeeXboX
- Gentoo

3. Raspberry Pi

The Raspberry Pi is a minimal effort, charge card measured PC that attachments into a PC screen or TV, and utilizations a standard console and mouse. It is a skilled little gadget that empowers individuals of any age to investigate registering, and to figure out how to program in dialects like Scratch and Python. It's equipped for doing all that you'd anticipate that a desktop PC will do, from scanning the web and playing top quality video, to making spreadsheets, word-preparing, and playing diversions. There are about eight product of Raspberry Pi; Raspberry Pi 3 model B, Raspberry Pi 2 model B, Raspberry Pi 1 model A+, Raspberry Pi zero, Raspberry Pi touch display, Raspberry Pi case, Sense hat and compute module development kit.

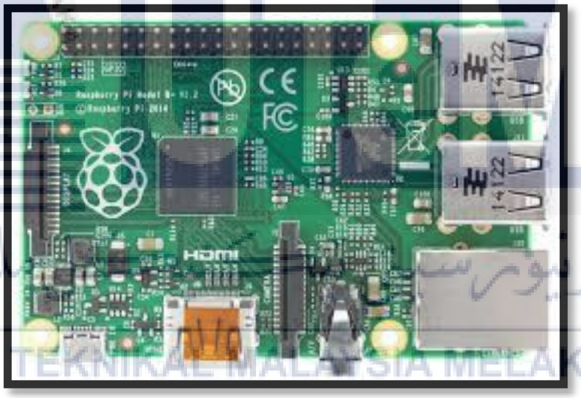


Figure 4: Raspberry Pi

4. Arduino

It is a product organization, undertaking, and client group that outlines and makes PC equipment, open-source programming, and microcontroller-based units for building advanced gadgets and intelligent items that can sense and control physical gadgets. The task depends on microcontroller board plans, delivered by a few sellers, utilizing different microcontrollers. These frameworks give sets of computerized and simple I/O sticks that can interface to different development sheets (termed shields) and different circuits. The sheets highlight serial correspondence interfaces, including Universal Serial Bus (USB) on some demonstrates, for stacking programs from PCs. For programming the microcontrollers, the Arduino venture gives a coordinated improvement environment (IDE) taking into account a programming dialect named Processing, which likewise underpins the dialects, C and C++. The primary Arduino was presented in 2005, expecting to give a minimal effort, simple path for beginners and experts to make gadgets that cooperate with their surroundings utilizing sensors and actuators. Normal case of such gadgets planned for amateur specialists incorporate basic robots, indoor regulators, and movement finders. Arduino sheets are accessible economically in preassembled structure, or as do-it-without anyone's help packs. The equipment plan particulars are straightforwardly accessible, permitting the Arduino sheets to be created by anybody. Adafruit Industries evaluated in mid-2011 that more than 300,000 authority Arduinos had been economically created, and in 2013 that 700,000 authority sheets were in clients' grasp.

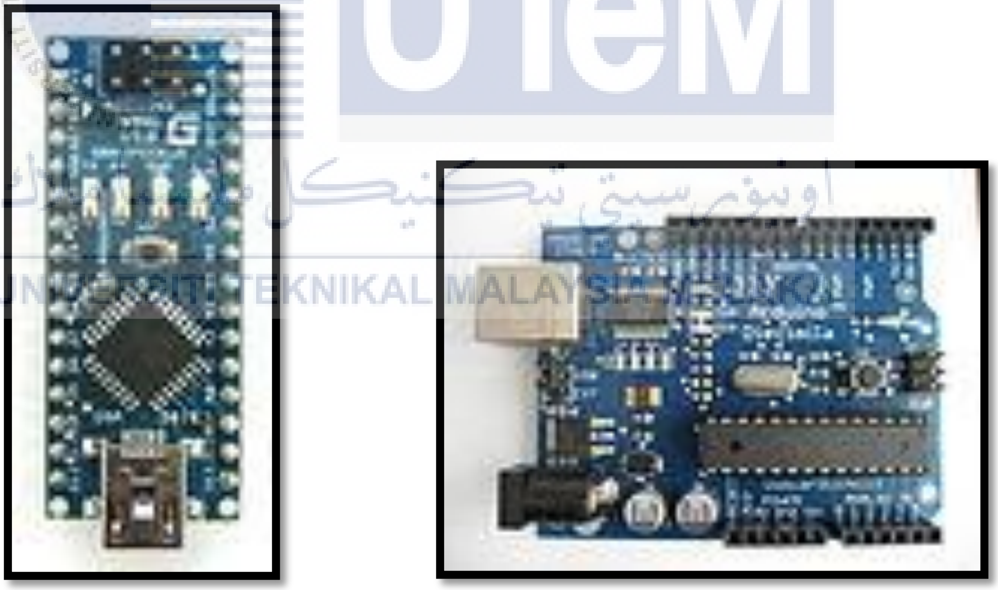


Figure 5: Arduino

5. Wiring

Wiring is an open-source hardware prototyping stage made out of a programming dialect, a coordinated improvement environment (IDE), and a solitary board microcontroller. It was produced beginning in 2003 by Hernando Barragán. Barragán began the venture at the Interaction Design Institute Ivrea. The task is right now created at the School of Architecture and Design at the Universidad de Los Andes in Bogotá, Colombia. Wiring expands on Processing, an open venture started by Casey Reas and Benjamin Fry, both some time ago of the Esthetics and Computation Group at the MIT Media Lab. The Wiring IDE is a cross-stage application written in Java which is gotten from the IDE made for the Processing programming dialect. It is intended to present programming and drawing with hardware to specialists and originators. It incorporates a code editorial manager with components, for example, language structure highlighting, prop coordinating, and programmed space fit for aggregating and transferring projects to the board with a solitary snap. The Wiring IDE accompanies a C/C++ library called "Wiring", which makes normal info/yield operations much simpler. Wiring projects are composed in C/C++, in spite of the fact that clients just need to characterize two capacities to make a runnable system:

- setup() – a capacity run once toward the begin of a project which can be utilized to characterize beginning environment settings
- loop() – a capacity called over and over until the board is fueled off

2.2.4 Analysis

The Physical Security Assessment utilizes an organized, formal investigation handle that permits us to build up a profound comprehension of a business, working conditions, corporate society, and one of a kind security risks and dangers. While customer inclusion is essential to achievement, our specialists encourage the evaluation at all times, venture on track, and ensuring that extremely critical components are inspected. The Security Assessment is exclusively customized for every venture, except ordinarily incorporates the accompanying errands:

- Risk recognizable proof and investigation
- Threat and powerlessness evaluation
- Review of site and office security
- Analysis of wrongdoing information including misfortune history, police calls for administration, wrongdoing insights, and wrongdoing estimate reports.
- Review of level of consistence with perceived CPTED (Crime Prevention Through Environmental Design) principals
- Review of level of consistence with security necessities that are particular to your industry. These may incorporate C-TPAT (Customs-Trade Partnership Against Terrorism), FISMA (Federal Information Security Management Act), HIPAA (Health Insurance Portability and Accountability Act), PCI (Payment Card Industry), Joint Commission, and security necessities forced by administrative offices.
    - Review of office working strategies
    - Review of physical security frameworks
    - Review of electronic security frameworks
    - Review of design security
    - Review of security arrangements and strategies
    - Review of security administration
    - Review of security work force
    - Evaluation of present security system and distinguishing proof of any shortcomings and vulnerabilities
    - Development of suggestions for security enhancements
    - Identification of transient and long haul costs
    - Prioritization of proposals and improvement of execution arrangement

- Preparation of composed Security Assessment Report

An affectability coefficient is a subordinate: the adjustment in some result as for an adjustment in some information. Regardless of the possibility that the likelihood of a specific danger can't be resolved absolutely, affectability examination can be utilized to figure out which variables have the best impact on the danger. Since an essential capacity of danger examination is to separate the issue into key components that can be tended to by administration, affectability investigation can be extremely valuable in figuring out what choices the supervisor ought to make to get the coveted results or to stay away from undesired results. Without hard information, affectability investigation can be extremely valuable in surveying the legitimacy of danger models.

In this research, it will focus on Raspberry Pi 2. In this study, the Raspberry Pi will be used since it already began to be known and used by many people. Raspberry Pi has also been done as between the famous search.

2.2.5 Risk Assessment

Security hazard evaluations are performed to permit associations to survey, distinguish and change their general security act and to empower security, operations, hierarchical administration and other staff to team up and see the whole association from an assailant's point of view. This procedure is required to get authoritative administration's dedication to distribute assets and execute the proper security arrangements. An extensive venture security hazard evaluation likewise decides the estimation of the different sorts of information created and put away over the association. Without esteeming the different sorts of information in the association, it is about difficult to organize and dispense innovation assets where they are required the most. To precisely survey hazard, administration must recognize the information that are most important to the association, the capacity systems of said information and their related vulnerabilities.

In practical terms, a threat assessment is a comprehensive look at your workplace to recognize those things, circumstances, structures, et cetera that may realize harm, particularly to people. After ID is made, you evaluate how likely and genuine the perils are, and subsequently pick what measures should be set up to suitably keep or control the harm from happening. Hazard appraisal is the procedure of recognizing variables that can possibly contrarily affect an association's capacity to direct business. In a substantial undertaking, a danger appraisal is normally directed by the Chief Risk Officer (CRO). Hazard evaluations are vital as they shape a vital part of a decent word related wellbeing and security administration arrangement. They help to:

- Create familiarity with perils and dangers.
- Identify who might be at danger (representatives, cleaners, guests, temporary workers, people in general, and so on).
- Determine if existing control measures are satisfactory or if more ought to be finished.
- Prevent wounds or ailments when done at the outline or arranging stage.
- Prioritize perils and control measures.

A risk assessment can be quantitative or a subjective. In a quantitative danger evaluation, the CRO allots numerical qualities to the likelihood an occasion will happen and the effect it will have. These numerical qualities can then be utilized to ascertain an occasion's danger component, which thusly can be mapped to dollar sums. Subjective danger evaluations, which are utilized all the more frequently, don't include numerical probabilities or forecasts of misfortune. The objective of a subjective methodology is just to rank which dangers represent the most risk.

Quantitative danger investigation strategies use scientific and measurable devices to speak to hazard (Karabacak & Sogukpinar 2005) . In subjective danger investigation strategies, danger is broke down with the assistance of descriptors as opposed to utilizing science. Hazard examination strategies that utilization concentrated quantitative measures are not appropriate for now's data security hazard investigation. Rather than the previous decades, today's data frameworks have a convoluted structure and an across the board use. Subsequently, escalated numerical measures used to model danger for complex situations make the procedure more troublesome. Figuring performed amid the danger examination procedure are additionally extremely mind boggling. Quantitative strategies will be unable to model today's unpredictable danger situations. The quantitative technique measures the unmistakable potential effect of a danger activating or abusing a particular powerlessness, utilizing a numeric quality connected with asset cost (Portability 2007) . This might include resource costs, such as repair costs to information systems or the replacement cost for an asset that is lost or stolen. The quantitative method provides valuable information for cost-benefit analysis associated with risks. However, it is generally difficult to assign numeric values to intangible losses. Therefore, all potential impacts generally cannot be determined using this method. In this work (Karabacak & Sogukpinar 2006) a quantitative overview technique is proposed for ISO 17799 consistence checks. Proposed strategy has some extraordinary elements. Its usability and adaptability are essential focal points. Specialized faculty can without much of a stretch change the quantity of inquiries, answer decisions, and alter new numerical estimations of them. Consistence investigation does not take much time by utilizing our technique. The expense of our model is low contrasted with the product devices in business sector.

The accomplishment of our strategy relies on upon the answers of surveyors. Precisely addressed inquiries lead to exact consistence results. A few activities assume essential part to enhance exactness. Firstly, part construct access control help seriously in light of exactness. Just related surveyors answer the devoted inquiries. Besides, unique consideration is paid while planning answer decisions and the weight estimations of inquiries (controls) and their answers. Thirdly, contingent upon the sort of the association, and the kind of the procedures inside the association, a few provisions and the few inquiries in the conditions can be overlooked. Fourthly, before every consistence check, surveyors ought to be orientated. All these activities ought to be performed to enhance the exactness of the studies before beginning any review procedure.

The subjective technique rates the extent of the potential effect coming about because of a danger activating or misusing a particular defenselessness on a scale, for example, high, medium and low. The subjective strategy is the most widely recognized measure used to gauge the effect of danger. This strategy permits the secured substance to quantify all potential effects, whether substantial or immaterial. For instance, an elusive misfortune, for example, lost open certainty or loss of validity, can be measured utilizing a high, medium or low scale. Hazard investigation techniques in light of subjective measures, are more reasonable for now's mind boggling hazard environment of data frameworks. In any case, one essential disadvantage for subjective danger investigation strategies is their temperament that yields conflicting results. Since subjective techniques don't utilize devices like arithmetic and measurements to demonstrate the danger, the consequence of strategy is inconceivably relied on upon the thoughts of individuals who direct the danger investigation. There is a danger of giving subjective results while utilizing subjective danger examination techniques.

The name ISO is used the world over to show the connection with, in this manner keeping up a key separation from the mix of truncations that would come to fruition on account of the translation of "Worldwide Organization for Standardization" into the unmistakable national vernaculars of people. In any country, the ISO standard may be used for the development of a country. Risk impacting connection with can have results similarly as monetary execution and master reputation, and natural, security and societal results. Thus, regulating risk effectively helps relationship to perform well in a circumstance stacked with defenselessness.

ISO 31000:2009 gives gages and non-specific principles on danger association. ISO 31000:2009 can be used by any open, private or gathering undertaking, association, social event or individual. Along these lines, ISO 31000:2009 is not specific to any industry or region. ISO 31000:2009 can be associated for the term of the life of an affiliation, and to a broad assortment of activities, including systems and decisions, operations, shapes, limits, wanders, things, organizations and assets. ISO 31000:2009 can be associated with a threat, whatever its demeanor, whether having positive or negative results. Notwithstanding the way that ISO 31000:2009 gives flat principles, it is not anticipated that would propel consistency of risk organization across over affiliations. The setup and execution of peril organization courses of action and frameworks ought to consider the changing needs of a specific affiliation, its particular objectives, association, structure, operations, shapes, limits, wanders, things, organizations, or assets and specific practices used. It is proposed that ISO 31000:2009 be used to orchestrate hazard administration forms in existing and future models. It gives a typical methodology in backing of models managing particular dangers and/or segments, and does not supplant those gauges. ISO 31000:2009 is not planned with the end goal of confirmation. ISO is utilized due to its wide use all through the around the world. In ISO 31000:2009, there are 11 Principles of risk management (Australian Government 2009) which is:

1) **Creates and secures esteem**

   Great danger administration adds to the accomplishment of an office's goals through the nonstop survey of its procedures and frameworks.

2) **Be a vital piece of authoritative procedures**

   Hazard administration should be incorporated with an organization's administration system and turn into a piece of its arranging forms, at both the operational and key level.

3) **Be piece of basic leadership**

   The procedure of danger administration helps chiefs to settle on educated decisions, recognize needs and select the most proper activity.

4) **Explicitly address vulnerability**

By distinguishing potential dangers, offices can actualize controls and medications to boost the shot of increase while minimizing the possibility of misfortune.

5) **Be efficient, organized and opportune**

The procedure of danger administration ought to be predictable over an office to guarantee effectiveness, consistency and the unwavering quality of results.

6) **Based on the best accessible data**

To adequately oversee hazard it is imperative to comprehend and consider all accessible data significant to an action and to know that there might be restrictions on that data. It is then imperative to see how this data educates the danger administration process.

7) **Be custom-made**

An office's danger administration structure needs to incorporate its danger profile, and in addition think about its inner and outer working environment.

8) **Take into record human and social components**

Hazard administration needs to perceive the commitment that individuals and society have on accomplishing an organization's destinations.

9) **Be straightforward and comprehensive**

Drawing in partners, both interior and outer, all through the danger administration process perceives that correspondence and interview is critical to recognizing, investigating and observing danger.

10) **Be dynamic, iterative and receptive to change**

The procedure of overseeing hazard should be adaptable. The testing environment we work in obliges organizations to consider the setting for overseeing hazard and also keeping on recognizing new dangers that develop, and rationalize those dangers that no more exist.

11) **Facilitate the consistent change of associations**

Organizations with an experienced danger administration society are those that have contributed assets after some time and can show the constant accomplishment of their destinations.

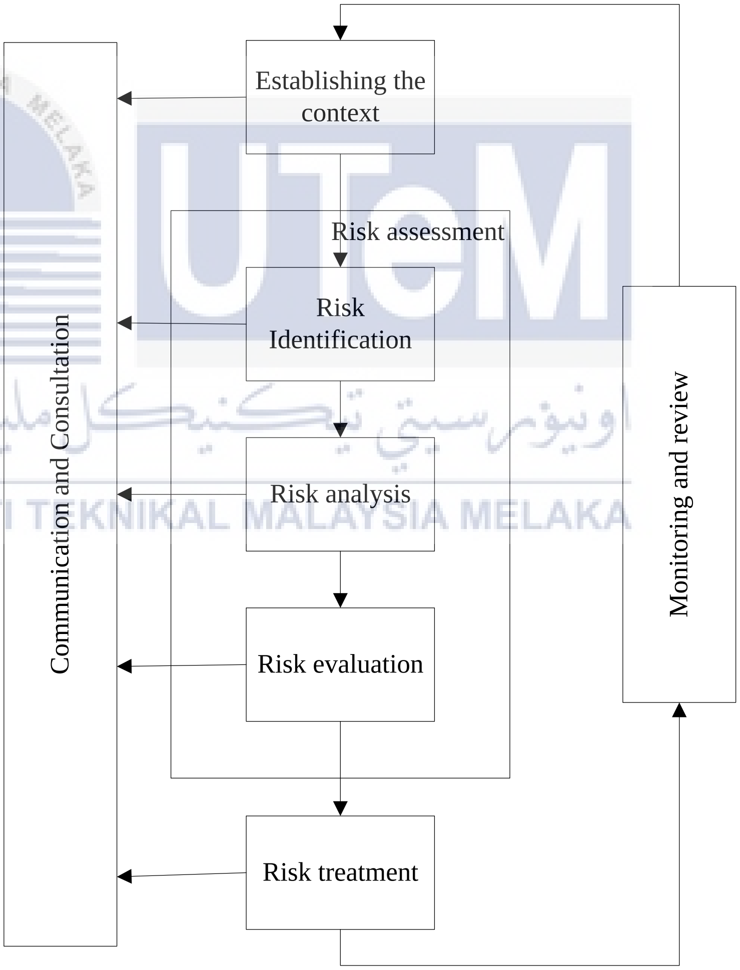


Figure 6: Process phase for risk assessment based on ISO (ISO - The International Organization for Standardization 2009)

Based from Figure 6, it is the process phase for risk assessment based ISO 31000:2009. Building up the connection characterizes the extension for the danger administration process and sets the criteria against which the dangers will be surveyed. The extension ought to be resolved inside the setting of the association's authoritative destinations. Dangers are instabilities that influence the accomplishment of business destinations, so hazards can't completely be distinguished if these targets and systems are indistinct. The determination of key destinations inside the business ought to be driven by an assessment of the outside and interior variables that may right now affect the firm. A survey of both the outer and inner connection at the beginning of the danger appraisal arranging helps with recognizing the procedures which might be liable to expanded dangers and, all things considered, would get the best esteem from the danger evaluation. Dangers can emerge because of outside or inward impacts:

- External dangers are exposures that outcome from ecological conditions that the firm generally can't impact, for example, the administrative environment and economic situations.
- Internal dangers are exposures that get from basic leadership and the utilization of interior and outer assets, including the company's operations and its destinations.

Hazard acknowledgment is the method of choosing perils that could keep the framework, undertaking, or hypothesis from finishing its destinations. It joins documenting and granting the stress. The objective of risk ID is the early and endless ID of events that, if they happen, will inconsistency influence the assignment's ability to perform execution or capacity result goals. They may begin from inside the endeavor or from external sources.

Hazard examination is the strategy of describing and separating the risks to individuals, associations and government workplaces posed by potential trademark and human-made unfavorable events. In IT, a risk examination report can be used to change advancement related destinations to an association's business targets. A threat examination report can be either quantitative or subjective.

Risk assessment is a procedure that is utilized to contrast hazard investigation results and hazard criteria keeping in mind the end goal to figure out if or not a predetermined level of danger is satisfactory or bearable. As such, hazard assessment is determination of danger administration needs through foundation of subjective and/or quantitative connections amongst advantages and related dangers.

Risk treatment is a peril change process. It incorporates selecting and realizing one or more treatment decisions. Once a treatment has been executed, it transforms into a control or it modifies existing controls. You have various treatment decisions. You can avoid the threat, you can lessen the peril, you can empty the wellspring of the risk, you can conform the outcomes, you can change the probabilities, you can confer the peril to others, you can basically hold the peril, or you can even grow the peril with a particular deciding objective to look for after an open entryway.

Perceive and review should be a masterminded part of the danger organization handle and incorporate ordinary checking or perception. The results should be recorded and reported remotely and inside, as appropriate. The results should in like manner be a commitment to the review and steady change of the organization's threat organization structure. Commitments with respect to checking and review should be clearly described. The organization's checking and overview strategies should fuse all parts of the threat organization process for the inspirations driving:

- Ensuring that controls are capable and gainful in both blueprint and operation

- Obtaining extra information to improve danger evaluation
- Analyzing and taking in lessons from peril events, including close misses, changes, examples, triumphs and frustrations
- Detecting changes in the external and inside association, including changes to peril criteria and to the threats, which may require remedy of danger pharmaceuticals and necessities
- Identifying rising dangers.

2.3 Proposed Solution/further project

In proposed solution, based on from Figure 7, this research is going to be focus on risk assessment based on qualitative in ISO standard. From the qualitative method that will be used, it will produced list of security issues especially in Raspberry Pi and it is be validated content of risk assessment model.

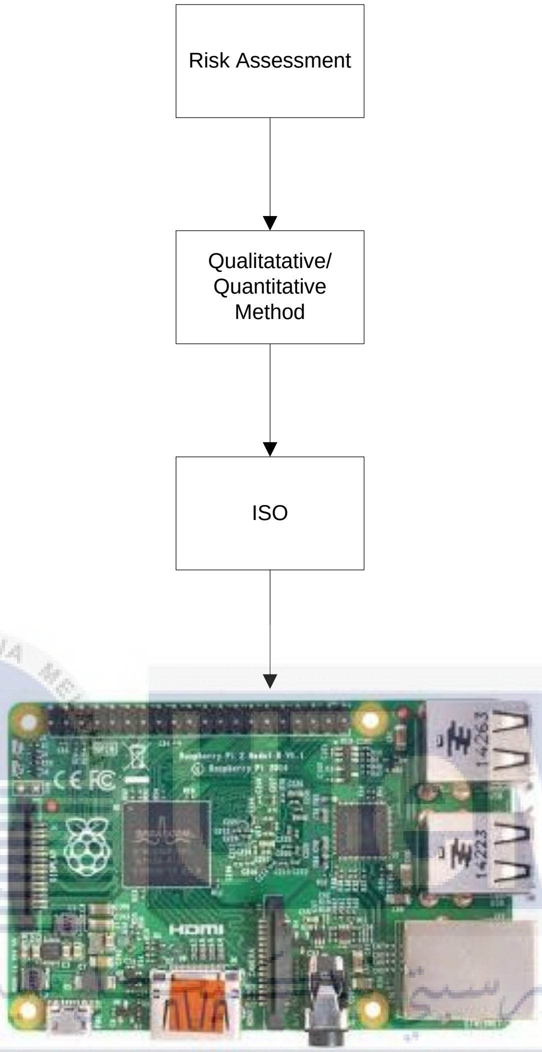


Figure 7: Flow diagram of this research

2.4 Conclusion

In conclusion, this chapter has provided a literature review of this project. This is to make sure that it enables the research to be implemented in a proper manner. This chapter will be used to help analysis in the next phase of this project.

CHAPTER III

PROJECT METHODOLOGY

3.1. Introduction

This chapter will briefly explain about the design of process phase in ISO according from discussion in chapter 2. This process phase will be a guide to produce this chapter. The content of this chapter are methodology and project milestone for risk assessment model in process phase for low capacity device.

3.2. Methodology

For the methodology part of this project, it is divided into 5 stage of process phase. The first stage is planning, the second stage is analysis, the third stage is design, the fourth stage is testing and the last stage is documentation. Figure 8 shows the process of phase in project methodology.

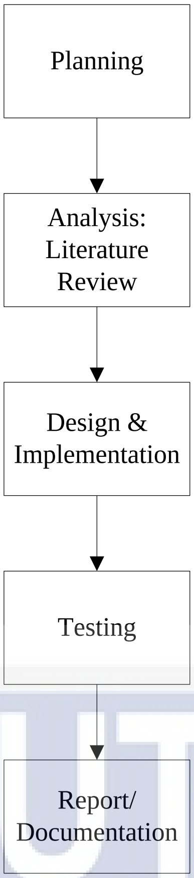


Figure 8: Process phase for Methodology

3.2.1 Phase 1: Planning

The principal stage identifies with the arranging environment around the Security Management Plan (Commission 2010). These are fused pretty much as heading; in any case, if other organizing contraptions exist then those should be used. It has four sections:

1. **Rationale:** Why a Security Management Plan is suggested for the Asset and the historical backdrop of the basic framework assurance in the European Union. In this section, risk assessment is important because the risks can be managed by eliminating, isolating or controlling them.

2. **Stakeholder Analysis:** Gives a progression of structures to use keeping in mind the end goal to recognize who the key inward and outer Stakeholders are, their level of interest and impact over the advancement and execution of the Security Management Plan. In this section, framework for this research was provided. It is to guide the researcher to do the research.

3. **Securing the Enterprise:** Discloses how to evaluate the risk administration system inside the proprietor/administrator and distinguish how best to position the Security Management Plan inside it. In this section, the framework of risk assessment will be guide by ISO for low capacity device.

4. **Planning:** These are incorporated just as direction; be that as it may, if other arranging apparatuses exist then those ought to be utilized. In this section, through planning, the research will provide from the past literature review and do the differences about risk assessment. In the last, tools like Raspberry Pi will be used to complete the research.

3.2.2 Phase 2: Analysis: Literature Review

In this phase, it will be a summary from literature review in chapter 2. Overall, from there, there will be two important things that can get, which are:

- **Information seeking**: information that can get from the past research about the flow from information security until risk assessment in detail.
- **Critical appraisal**: The main thing to do this chapter is to tell the content of risk assessment itself through ISO that been usually in Malaysia.

3.2.3 Phase 3: Design & Implementation

In this phase, design that will be used is about using risk assessment from ISO. From there, it will guide how to write in sequences. This research also is going to do with qualitative method that already been explain in chapter before this. By using qualitative, data from past research will be taking down and will be comparison to create the content of risk assessment following the title. This research also will be specifically focus on Raspberry Pi as example to implement the risk to prevent for an attack.

This risk evaluation on the Raspberry Pi dissects and surveys the dangers and vulnerabilities inherent with a stock non-solidified Raspberry Pi. Dynamic procedures and administrations, their need, and whether debilitating them is an alternative is resolved. Results introduced are in a subjective structure that considers an unprejudiced assessment and to guarantee that the appraisal without much of a stretch be duplicated with comparable discoveries ought to an alternate evaluation group rehash this study. The outcomes are subjective and are broke down and checked on by means of the subjective guidelines.

3.2.4 Phase 4: Testing

The testing will be test on the Raspberry Pi port. For this risk analysis, two port sweeps and one weakness output were directed. The gear used amid this stage incorporated an Asus portable workstation running VM Player, supporting Kali-Linux 1.10. A Raspberry Pi running Debian 7.0 (Wheezy) was specifically associated with the Wi-Fi switch, and was connected to a DSL modem.

The consequences of the defenselessness check recognized just two data reviews. These two vulnerabilities are SSH and ICMP. Both are low-level occasions. Raspberry Pi effectively breezed through this helplessness test. Figure 9, appears, the system arrangement test environment for testing the Raspberry Pi.

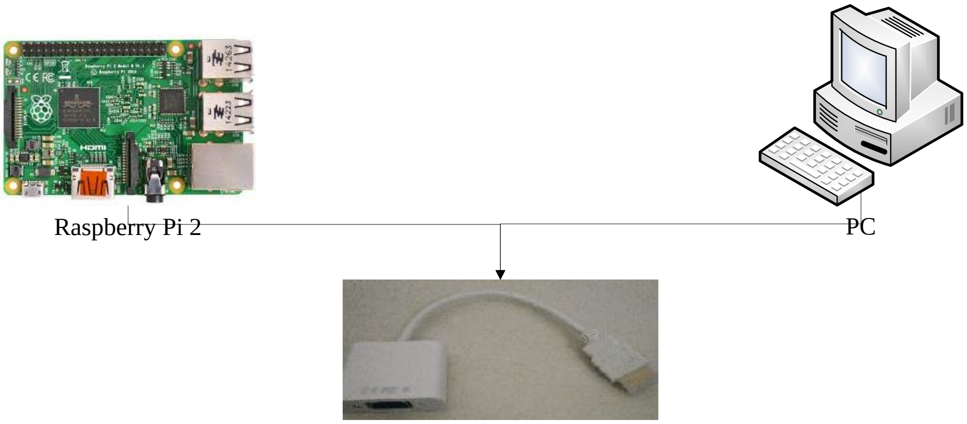


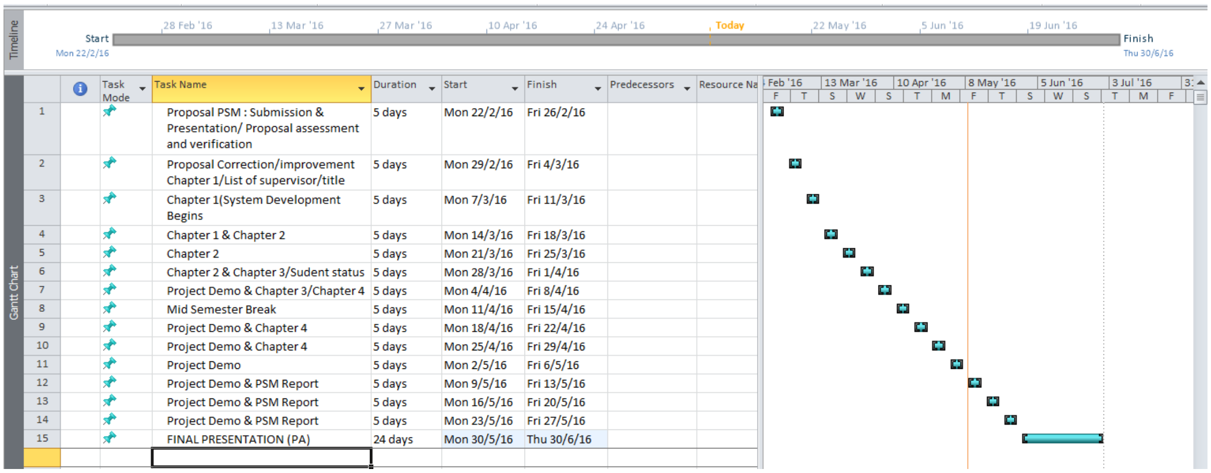
Figure 9: Network configuration test environment

3.2.5 Phase 5: Report/Documentation

After all configurations have been made, risk will be shown; list and content of risk will be documented.

3.3. Project Milestones

Project milestone is use to mark specific points along with a project timeline. Project milestone is focus on major progress point that must be reaching to achieve success. Figure 10 shows the project milestone that being use in this project. Project milestone help to manage time to determine the project is on schedule or not. It started in week 1 until week 15.



	Task Mode	Task Name	Duration	Start	Finish	Predecessors	Resource Na
1		Proposal PSM : Submission & Presentation/ Proposal assessment and verification	5 days	Mon 22/2/16	Fri 26/2/16		
2		Proposal Correction/improvement Chapter 1/List of supervisor/title	5 days	Mon 29/2/16	Fri 4/3/16		
3		Chapter 1(System Development Begins	5 days	Mon 7/3/16	Fri 11/3/16		
4		Chapter 1 & Chapter 2	5 days	Mon 14/3/16	Fri 18/3/16		
5		Chapter 2	5 days	Mon 21/3/16	Fri 25/3/16		
6		Chapter 2 & Chapter 3/Sudent status	5 days	Mon 28/3/16	Fri 1/4/16		
7		Project Demo & Chapter 3/Chapter 4	5 days	Mon 4/4/16	Fri 8/4/16		
8		Mid Semester Break	5 days	Mon 11/4/16	Fri 15/4/16		
9		Project Demo & Chapter 4	5 days	Mon 18/4/16	Fri 22/4/16		
10		Project Demo & Chapter 4	5 days	Mon 25/4/16	Fri 29/4/16		
11		Project Demo	5 days	Mon 2/5/16	Fri 6/5/16		
12		Project Demo & PSM Report	5 days	Mon 9/5/16	Fri 13/5/16		
13		Project Demo & PSM Report	5 days	Mon 16/5/16	Fri 20/5/16		
14		Project Demo & PSM Report	5 days	Mon 23/5/16	Fri 27/5/16		
15		FINAL PRESENTATION (PA)	24 days	Mon 30/5/16	Thu 30/6/16		

Figure 10: Gantt chart of Project Milestone

Activity	**Responsibility**	**Week**
Submission proposal	Student and Supervisor	Week 1
Proposal Correction/improvement Chapter 1/List of supervisor/title	Student, AJK PSM and Supervisor	Week 2
Chapter 1(System Development Begins	Student and Supervisor	Week 3
Chapter 1 & Chapter 2	Student	Week 4
Chapter 2	Student	Week 5
Chapter 2 Chapter 3	Student and Supervisor	Week 6
Project Demo & Chapter 3 Chapter 4	Student	Week 7
Project Demo & Chapter 4	Student and Supervisor	Week 9
Project Demo & Chapter 4	Student and Supervisor	Week 10
Project Demo	Student	Week 11
Project Demo & PSM	Student and Supervisor	Week 12

Report		
Project Demo & PSM Report	Student and Supervisor	Week 13
Project Demo & PSM Report	Student and Supervisor	Week 14
FINAL PRESENTATION (PA)	Student, Supervisor and Evaluator	Week 15

Table 5: Project Milestone

3.4. Conclusion

In conclusion, to develop a system project methodology, schedule and milestones are important to organized time well. The time that has been organized need to be followed to make it consistent and well-manage. In the next chapter, Design of this system will be discussed in details.

CHAPTER IV

DESIGN

4.1 Introduction

This chapter was focusing more on the analysis design and implementation of project. In this chapter discussed about the software and hardware requirement that were going to use and the implementation in ISO standard for low capacity device. There were many standards that have been introduced, but ISO standard will be discussed in this project. In this chapter also will be shown the progress of analysis design in detecting risk on Raspberry Pi. The final result will be produced list of risk.

4.2 Logical and Physical Design of Testing Environment

Figure 11 shows the network configuration test environment. This section will introduce in detail of software and hardware that going to be used in this project.

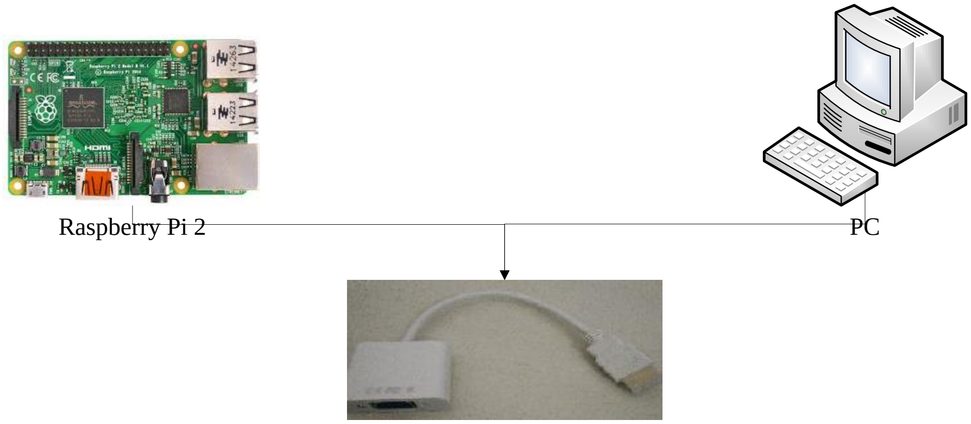


Figure 11: Network configuration test environment

4.2.1 Software Requirement

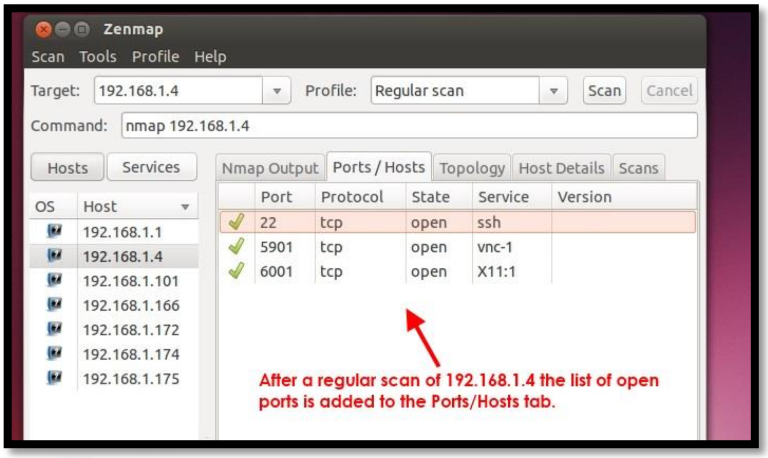
i. **Kali-Linux 1.10**

KALI LINUX™
"the quieter you become, the more you are able to hear"
Kali Linux 1.1.0 Installation Guide

Figure 12: Kali-Linux

Kali Linux is a Debian-based Linux conveyance went for cutting edge Penetration Testing and Security Auditing. Kali contains a few hundred apparatuses went for different data security assignments, for example, Penetration Testing, Forensics and Reverse Engineering. In this project, Kali-Linux will be used as software to run in laptop or pc.

ii. Zenmap Software



Target: 192.168.1.4

Profile: Regular scan

Command: nmap 192.168.1.4

OS	Host
	192.168.1.1
	192.168.1.4
	192.168.1.101
	192.168.1.166
	192.168.1.172
	192.168.1.174
	192.168.1.175

	Port	Protocol	State	Service	Version
✓	22	tcp	open	ssh	
✓	5901	tcp	open	vnc-1	
✓	6001	tcp	open	X11:1	

After a regular scan of 192.168.1.4 the list of open ports is added to the Ports/Hosts tab.

Figure 13: Zenmap Software

Zenmap is the power Nmap Security Scanner GUI. It is a multi-stage free and open source application which hopes to make Nmap basic for learner to use while giving impelled components to experienced Nmap customers. A great part of the time used yields can be saved as profiles to make them easy to run more than once. A charge creator grants instinctive generation of Nmap request lines. Channel results can be saved and saw later.Spared check results can be contrasted with each other with perceive how they vary. The consequences of late outputs are put away in a searchable database. In this project, Zenmap software will be used as scanning all port that will be detect in Raspberry Pi.

iii. OpenVAS

Figure 14: OpenVAS, vulnerabilities scanner

The Open Vulnerability Assessment System (OpenVAS) is a structure of a few administrations and devices offering an extensive and effective powerlessness filtering and defenselessness administration arrangement. The genuine security scanner is went with a frequently redesigned food of Network Vulnerability Tests (NVTs), more than 47,000 altogether (as of June 2016). All OpenVAS items are Free Software. Most parts are authorized under the GNU General Public License (GNU GPL).

4.2.2 Hardware Requirement

i. **Laptop / PC**

Figure 15: PC/ Laptop

Laptop or PC is a hardware that is going to use to conduct the project. It used to install software and place for write coding.

ii. Raspberry Pi 2

Figure 16: Raspberry Pi 2

The Raspberry Pi 2 Model B is the second generation Raspberry Pi. It replaced the original Raspberry Pi 1 Model B+ in February 2015.The specification of Raspberry Pi as below:

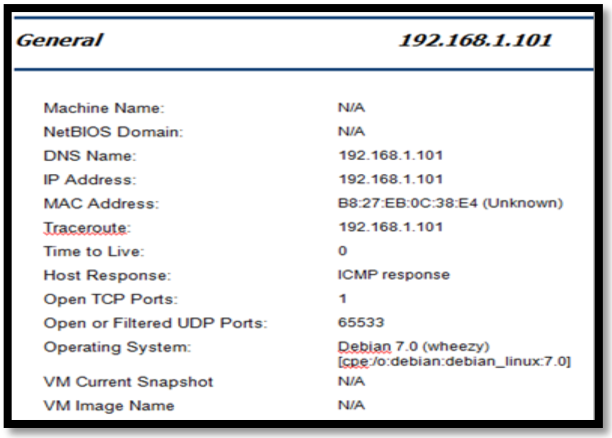
- A 900MHz quad-core ARM Cortex-A7 CPU
- 1GB RAM
- 4 USB ports
- 40 GPIO pins
- Full HDMI port
- Ethernet port
- Combined 3.5mm audio jack and composite video
- Camera interface (CSI)

- Display interface (DSI)
- Micro SD card slot
- VideoCore IV 3D graphics core
- ARMv7 processor, it can run the full range of ARM GNU/Linux distributions, including Snappy Ubuntu Core, as well as Microsoft Windows 10

4.3 Possible Scenario

In this project, the outcome will be port scanning and vulnerabilities test. In port scanning, all port will be scan and will be detect which were filtered, open and closed. During scanning port, Zenmap also will be detecting on total of packets was sent during scanning is happened. The scanning port will be conduct two times which is for the first time, it will scan all the ports that open and for the second time, the open port will be reduced which only allow installation and configuration to be done in Raspberry Pi.

For the vulnerabilities test, OpenVAS software will be used to scan the vulnerabilities in Raspberry Pi. Once the test had been done for getting the result, the vulnerabilities test will be declared as success. The result will be showed as Figure 19 below.



General	192.168.1.101
Machine Name:	N/A
NetBIOS Domain:	N/A
DNS Name:	192.168.1.101
IP Address:	192.168.1.101
MAC Address:	B8:27:EB:0C:38:E4 (Unknown)
Traceroute:	192.168.1.101
Time to Live:	0
Host Response:	ICMP response
Open TCP Ports:	1
Open or Filtered UDP Ports:	65533
Operating System:	Debian 7.0 (wheezy) [cpe:/o:debian:debian_linux:7.0]
VM Current Snapshot	N/A
VM Image Name	N/A

Figure 17: The example result of OpenVAS scan

4.4 Risk Assessment Analysis Step

In this section, it will refer from chapter 2.Figure 20 below is the process phase for risk assessment based ISO 31000:2009. Establishing the context defines the scope for the risk management process and sets the criteria against which the risks will be assessed.

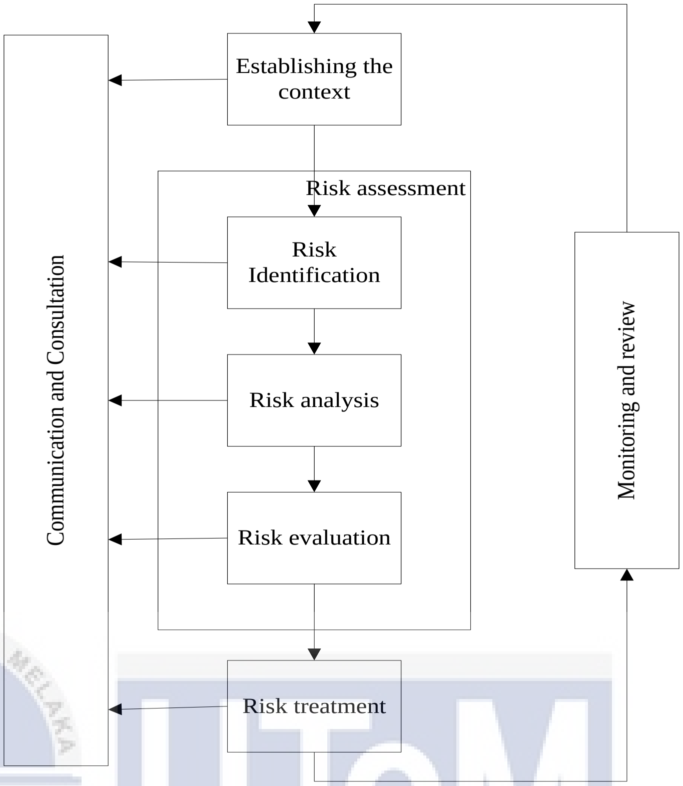


Figure 18 : Process phase for risk assessment based on ISO

From the process phase, this project is focusing on risk assessment. On this chapter, the result of risk will only get from literature review as preliminary list. The preliminary list was get from the process in software requirement that implement in hardware requirement. Risk analysis will be produced due to port scanning and vulnerability test that had been discussed in possible scenario above. The design also can be refer to test environment that had been introduced in other chapter before.

All possible in risk evaluation in this project will be evaluated and be rated. After the risks been listed, the recommendation will be listed. The types of vulnerability also be listed that could be used against Raspberry Pi. The finalize work from all testing and the result that get for risk assessment will be documented.

4.5 Metric Measurement

For metric measurement, ratings will be used to populate the risks. The rating consists of low, medium and high. The example is shown below in Figure 21. This represent of measurement due to ISO standards (ISO - The International Organization for Standardization 2009) . Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered.

Risk Rating			
High			
Medium			
Low			

Figure 19: Example of risk rating

4.6 List of Risk

From Figure 20, it shows the preliminary list of data that produced from scanning port and vulnerability test.

List of Risk
Perform border system survey/filtering
Perform system sniffing of uncovered systems
Perform observation and survey of the focused on gadget

Embed untargeted malware into downloadable programming and/or into business data innovation items
Exploit act as of late found vulnerabilities
Manage wireless crowd assaults
Conduct focused on Denial of Service (DoS) assaults
Conduct non-focused on zero-day assaults.
Acquire tricky data through system sniffing of outer systems.

Figure 20: List of Risk

4.7 Conclusion

In this chapter, discusses the testing environment following phase process flow. Testing scenario made on Raspberry Pi is port scanning and vulnerability test. From the tests, it will produce list of risks that will give harmful to the Raspberry Pi. The results of the risk will be rated according to ISO standard as guidance.

For the next chapter, the topics will be contributed on the testing for risk and vulnerabilities test and ratings the result for the risk analysis to get specific stage of risks. This is the most important chapter in this project which will test of scanning port in detail.

CHAPTER V

IMPLEMENTATION

5.1 Introduction

This chapter was focusing more on the activity that being implement in this project. In this chapter discussed about the requirement that were going to use following in ISO standard for Raspberry Pi. In this chapter also will be shown in detail the process of design to detect risk on Raspberry Pi. The final result will be used for testing the project.

5.2 Environment Setup

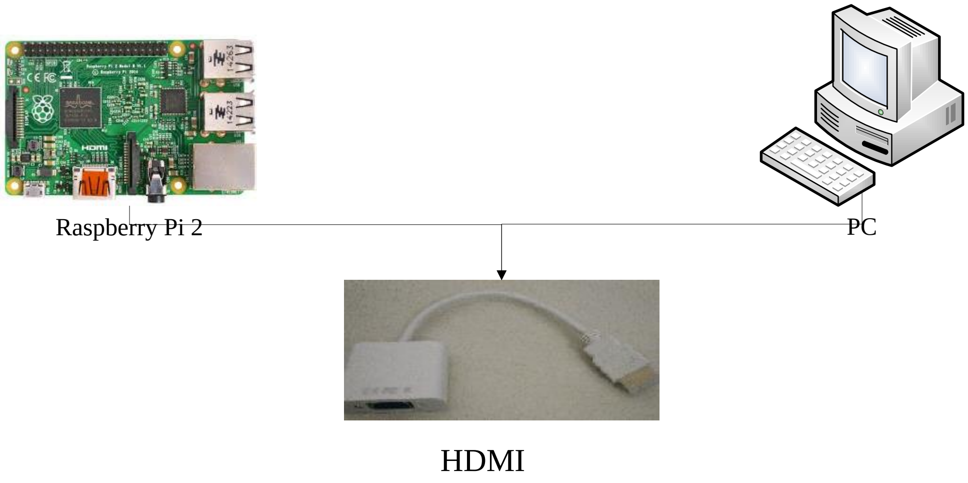


Figure 21: Network configuration test environment

From the network environment above, this chapter is focusing on implementation of test environment. The early stage that is needed to start is to prepare and setup the environment which listed below:

1. Raspberry Pi Environment Setup

In this Raspberry Pi Environment Setup, will find on how Raspberry Pi being setup from the earliest starting point until the complete project and will be clarified in subtle elements how the working framework has been introduce and designed.

2. Installation Software Scanning

In this section, the software will be installed and explain in details about the steps in installing software. It will be installed by using Raspberry Pi and will scan the Raspberry Pi to detect the ports and vulnerabilities.

5.2.1 Raspberry Pi Environment Setup and OS Installation

5.2.1.1 Raspberry Pi Environment Setup

In this project Raspberry Pi one of the main platform that gone be used to make this project succeed. Raspberry Pi need to be setup the hardware and software, including their main operating system setup. The hardware needed to setup this project is Raspberry Pi, power supply for the Pi, SD card, HDMI monitor, HDMI cable, WIFI USB dongle / Ethernet connection, USB mouse and USB Keyboard.

Detailed implementation steps as listed below:

Steps:

1. Setting up the raspberry pi board by embedding the SD card into the space and after that associate the HDMI link to both screen and Pi. Likewise, connect to the force supply to the Pi and after that switch on the Pi.
2. Install the operating system which is Kali Linux. The Kali Linux is an operating system that set of a security programs and utilities that make Raspberry Pi run.
3. Plug in the keyboard and the mouse to the USB port on the Raspberry Pi for the first time booting, it is required that mouse and keyboard to be attached to the Raspberry Pi.
4. Raspbi-config screen shows up first time booting which the setting can be changed on the screen.
5. Restart the Pi in order to activate the entire configuration that has been made during an operating system installation.

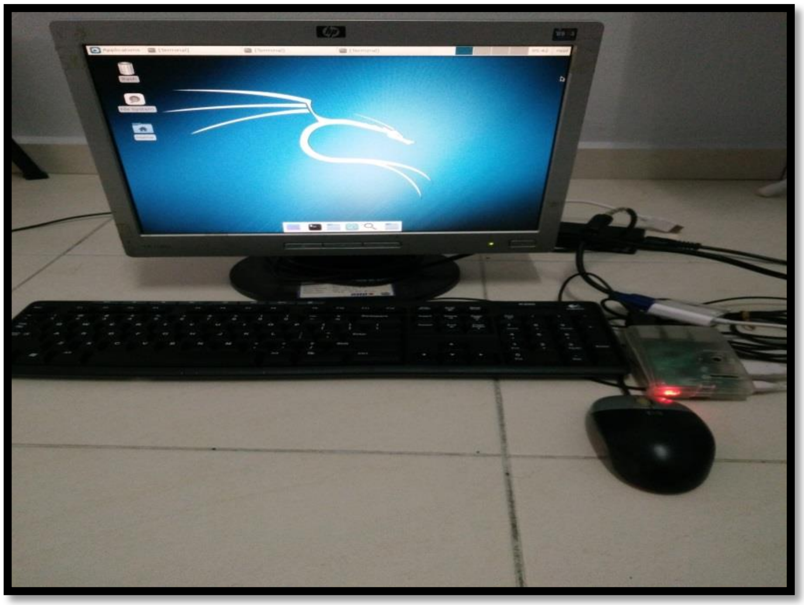
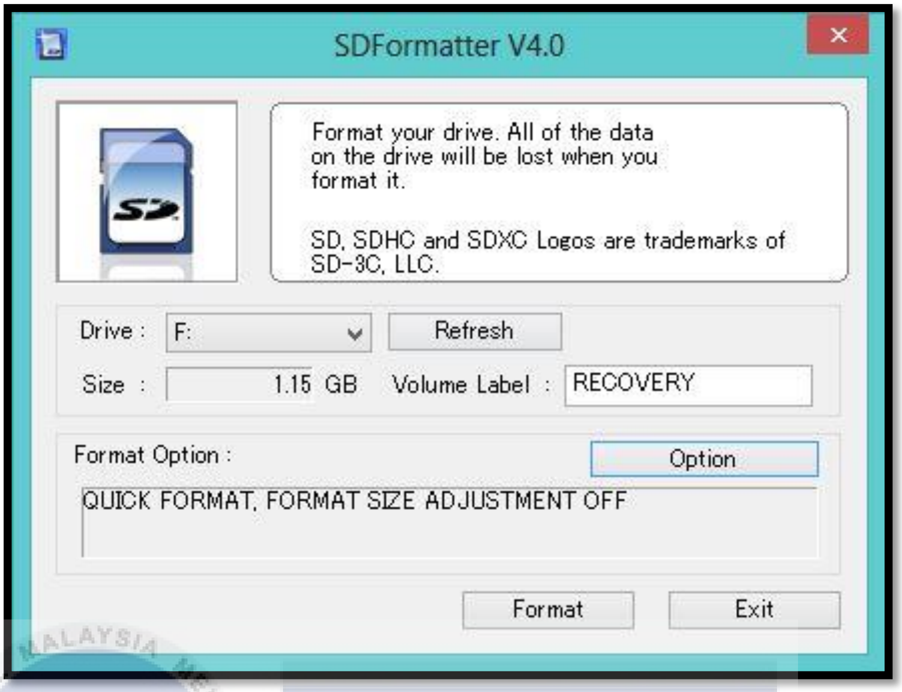


Figure 172: Environment setup

6. Environment setup of Raspberry Pi success.

5.2.1.2 OS Installation

This section, operating system (OS) in Raspberry Pi is being installed. Before OS being installed, the process of empty the SD Card needs to be done before it being used. The SD Card will be inserting in Raspberry Pi for installation process. All installation been made in Windows.



Format your drive. All of the data on the drive will be lost when you format it.

SD, SDHC and SDXC Logos are trademarks of SD-3C, LLC.

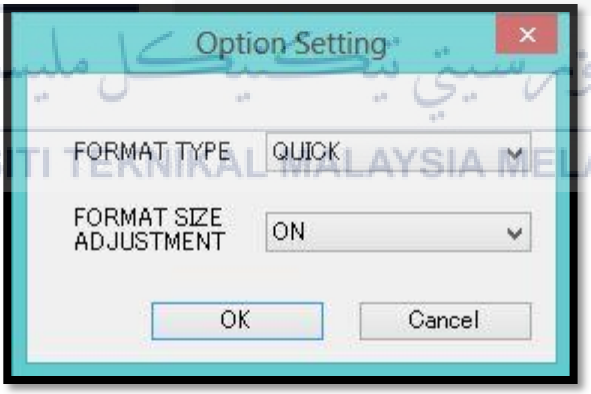
Drive : F:

Size : 1.15 GB Volume Label : RECOVERY

Format Option :

QUICK FORMAT, FORMAT SIZE ADJUSTMENT OFF

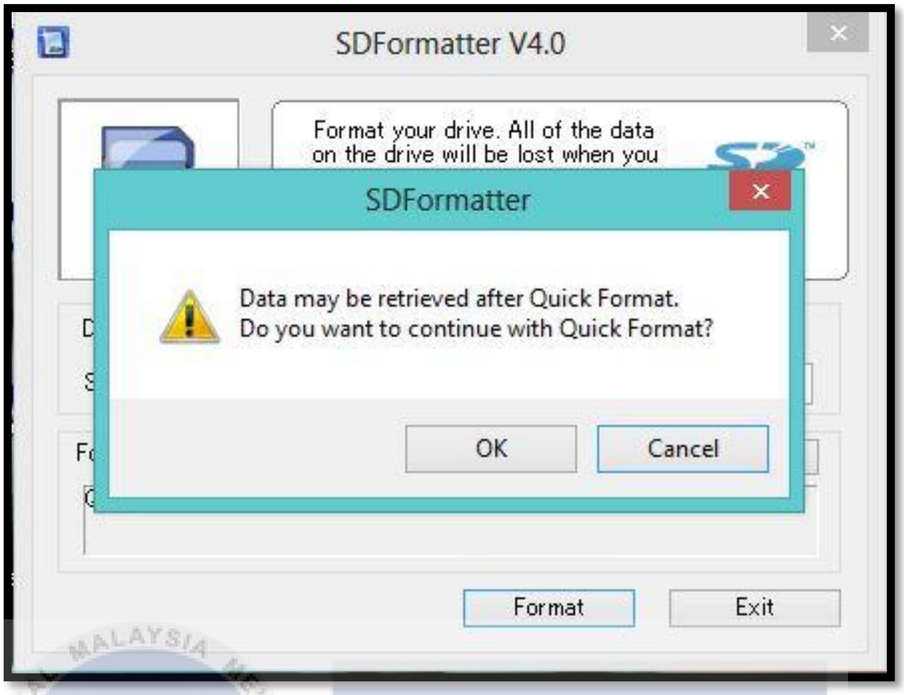
Figure 23: Choose SD Card to format.



FORMAT TYPE QUICK

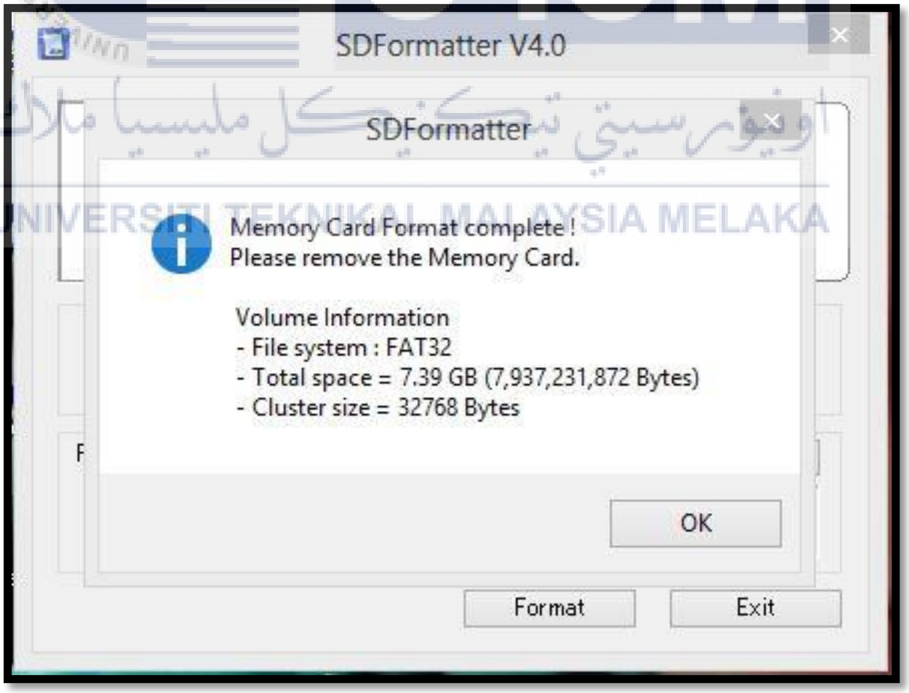
FORMAT SIZE ADJUSTMENT ON

Figure 24: Change format size adjustment ON.


SDFormatter V4.0
Format your drive. All of the data
on the drive will be lost when you
SDFormatter
OK
Cancel
Format
Exit

Data may be retrieved after Quick Format.
Do you want to continue with Quick Format?

Figure 25: Choose OK to continue.



Memory Card Format complete !
Please remove the Memory Card.

Volume Information
- File system : FAT32
- Total space = 7.39 GB (7,937,231,872 Bytes)
- Cluster size = 32768 Bytes

Figure 26: SD Card format complete.

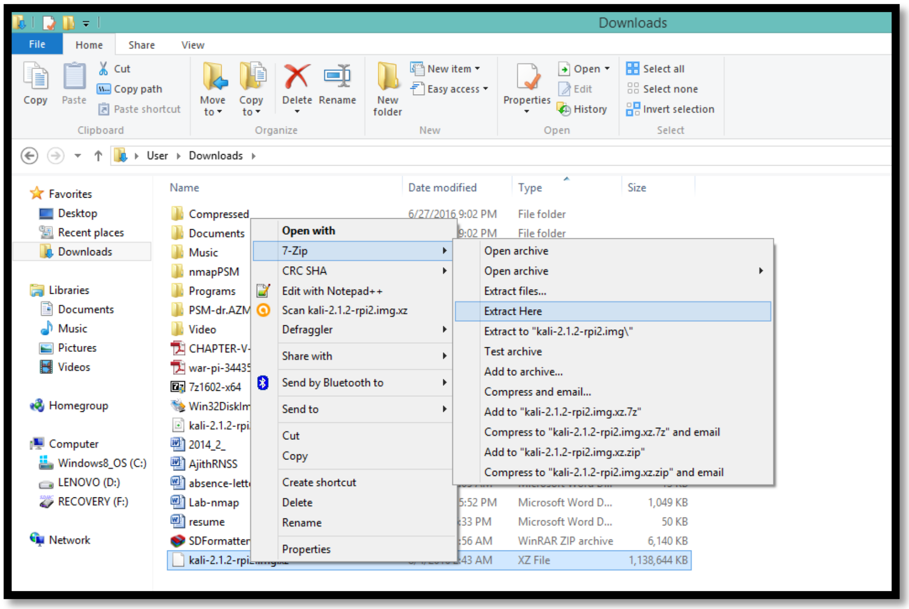
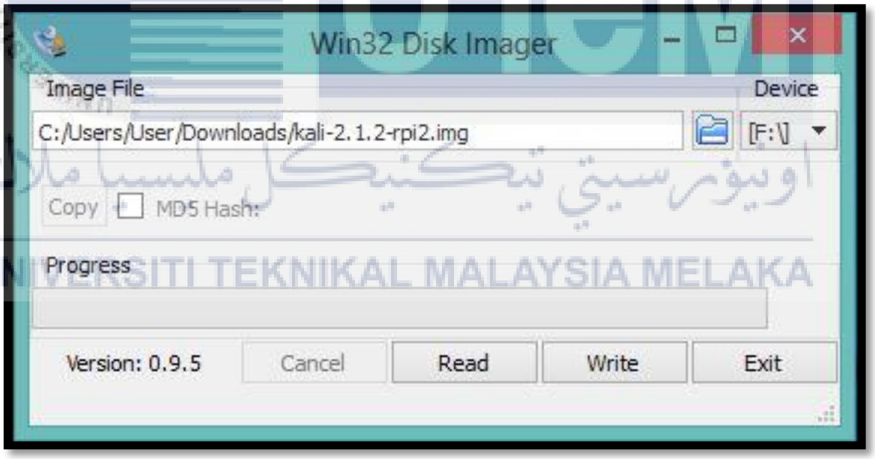
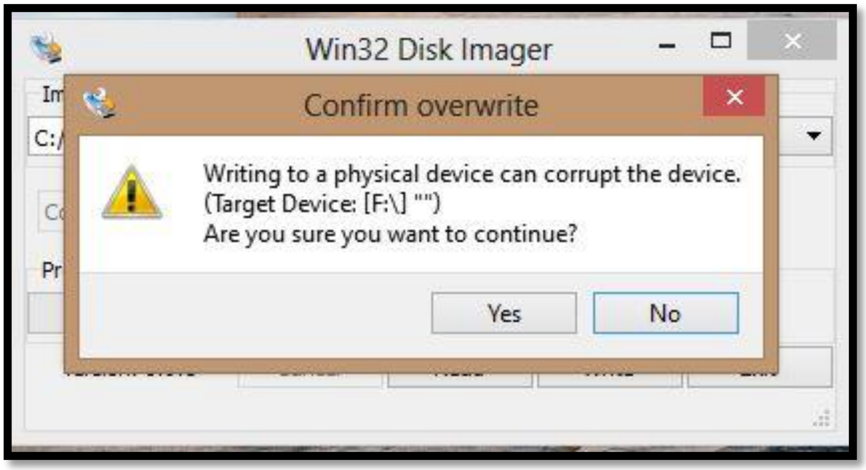


Figure 27: Select KALI image and extract.



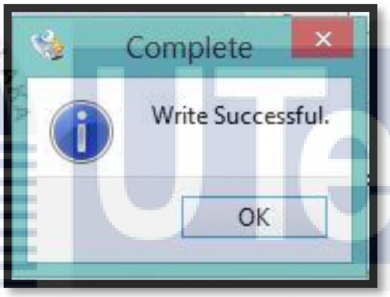
C:/Users/User/Downloads/kali-2.1.2-rpi2.img

Figure 28: Use Win 32 Disk Imager to transfer KALI image to SD Card.



Writing to a physical device can corrupt the device.
(Target Device: [F:\] "")
Are you sure you want to continue?

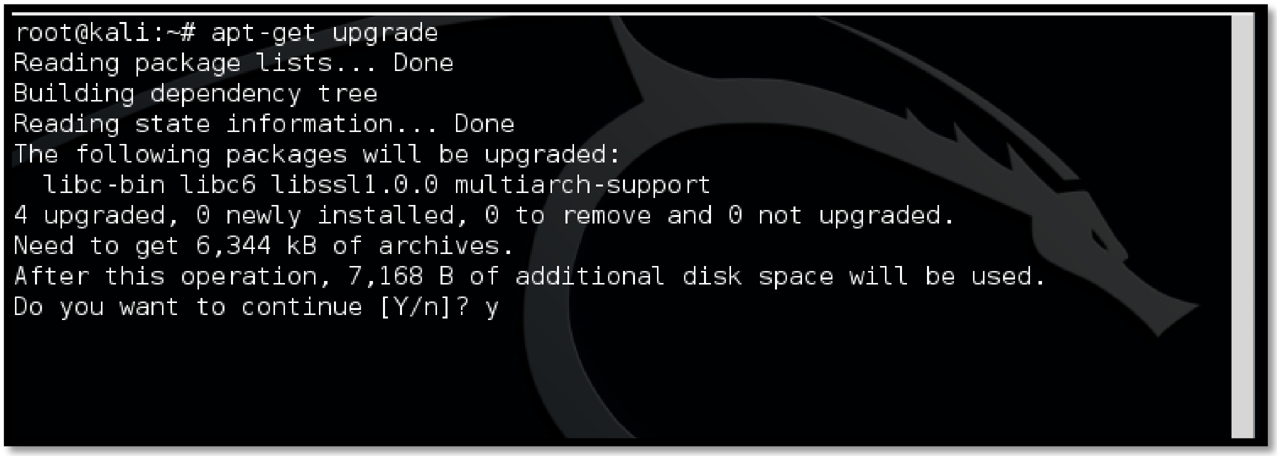
Figure 29: Choose Yes to continue



Write Successful.

Figure 30: Write successful

After installation in SD Card been successful, transfer the SD Card to Raspberry Pi to been installed. To get the latest update for OS, those command need to be write. These commands always need to be written after installation so that Kali Linux will always be updated.



```
root@kali:~# apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be upgraded:
  libc-bin libc6 libssl1.0.0 multiarch-support
4 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 6,344 kB of archives.
After this operation, 7,168 B of additional disk space will be used.
Do you want to continue [Y/n]? y
```

Figure 31: To update and upgrade Kali Linux

5.2.2 Zenmap Software

Zenmap is the official Nmap Security Scanner GUI. It is a multi-platform (Linux, Windows, Mac OS X, BSD, etc.) free and open source application which aims to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users. Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines. Scan results can be saved and viewed later. Saved scan results can be compared with one another to see how they differ. The results of recent scans are stored in a searchable database.

After Kali Linux been updated, Nmap will be automatically been installed under Vulnerability analysis.

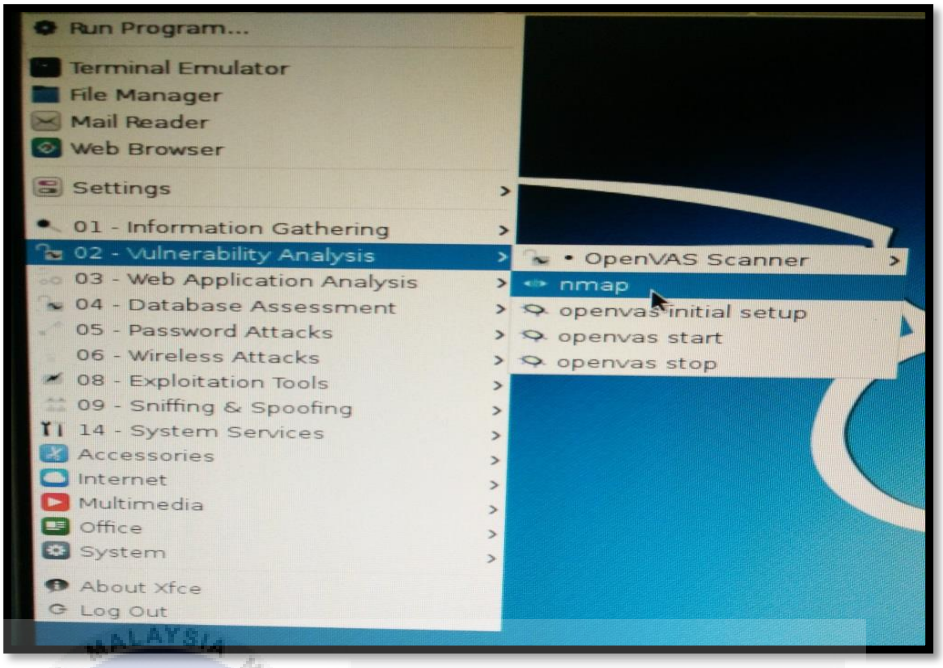
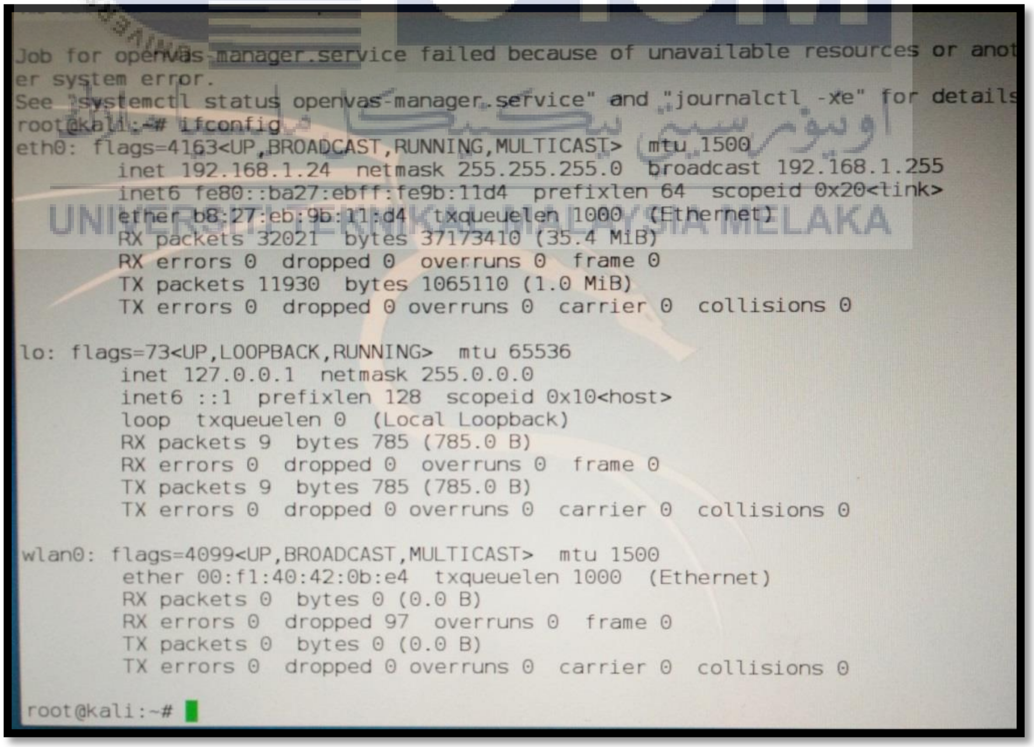
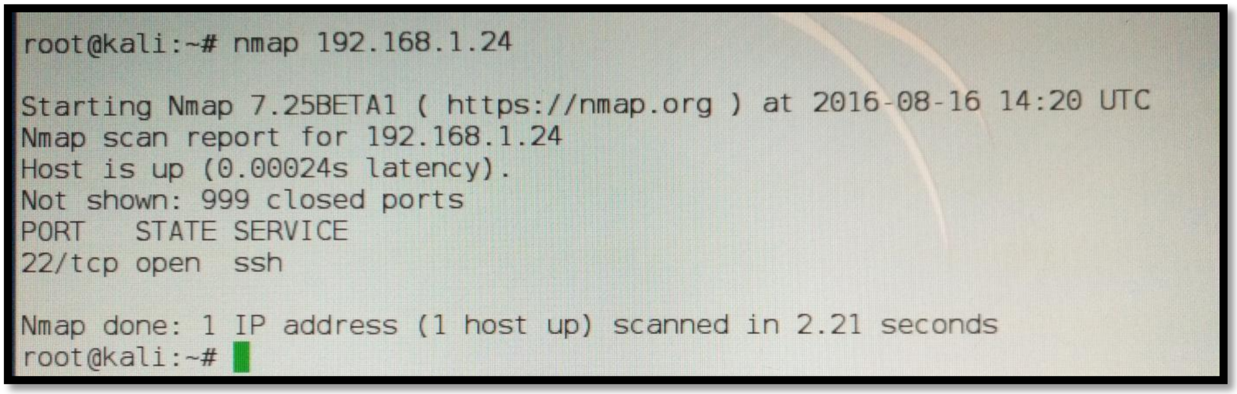


Figure 32: Choose nmap in Vulnerability Analysis



```
Job for openvas-manager.service failed because of unavailable resources or anot
er system error.
See "systemctl status openvas-manager.service" and "journalctl -xe" for details
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.24  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::ba27:ebff:fe9b:11d4  prefixlen 64  scopeid 0x20<link>
        ether b8:27:eb:9b:11:d4  txqueuelen 1000  (Ethernet)
        RX packets 32021  bytes 37173410 (35.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11930  bytes 1065110 (1.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 0  (Local Loopback)
        RX packets 9  bytes 785 (785.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9  bytes 785 (785.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 00:f1:40:42:0b:e4  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 97  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# 
```

Figure 33: Step to know current IP address

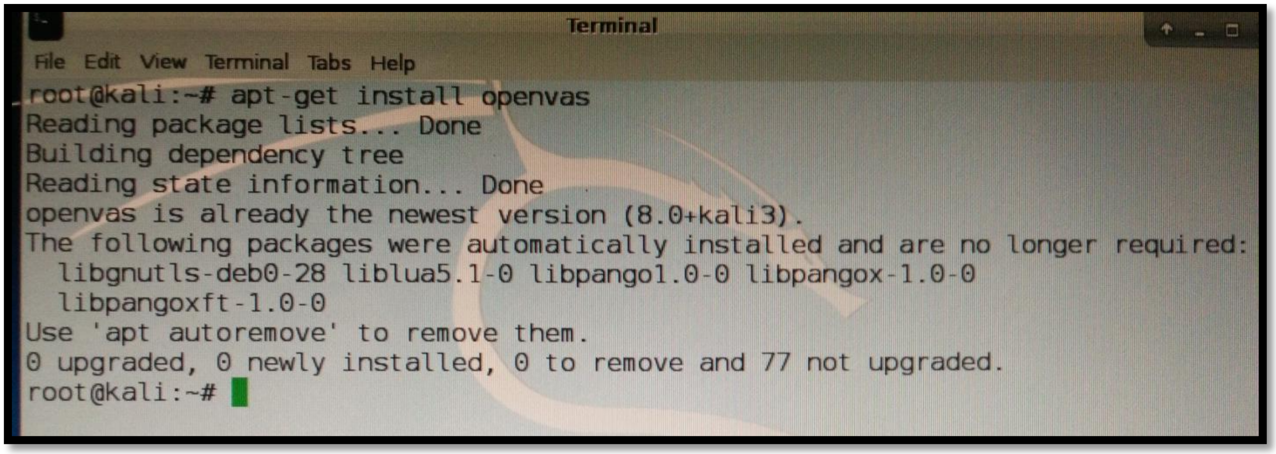


```
root@kali:~# nmap 192.168.1.24

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-08-16 14:20 UTC
Nmap scan report for 192.168.1.24
Host is up (0.00024s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 2.21 seconds
root@kali:~# 
```

Figure 34: Scanning IP Address to test

5.2.3 Vulnerability

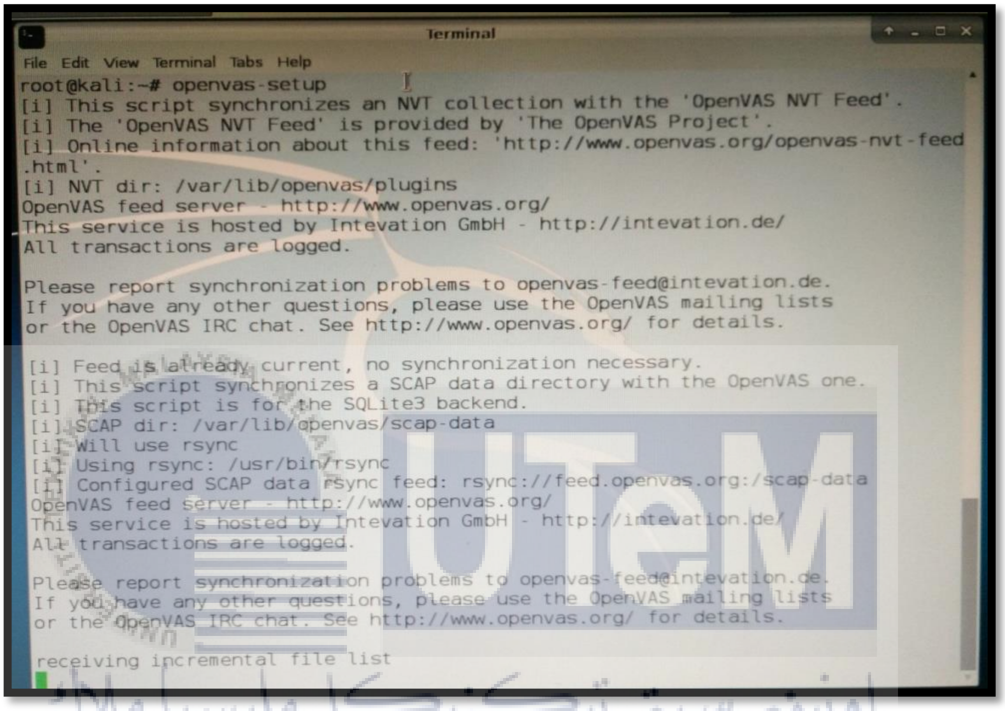
Vulnerability scanning is a crucial phase of a penetration test and having an updated vulnerability scanner in your security toolkit can often make a real difference by helping you discover overlooked vulnerable items. For this reason, we've manually packaged the latest and newly released OpenVAS 8.0 tool and libraries for Kali Linux. Although nothing major has changed in this release in terms of running the vulnerability scanner, we wanted to give a quick overview on how to get it up and running.



```
root@kali:~# apt-get install openvas
Reading package lists... Done
Building dependency tree
Reading state information... Done
openvas is already the newest version (8.0+kali3).
The following packages were automatically installed and are no longer required:
  libgnutls-deb0-28 liblua5.1-0 libpango1.0-0 libpangox-1.0-0
  libpangoxft-1.0-0
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 77 not upgraded.
root@kali:~# 
```

Figure 35: Installation OPENVAS

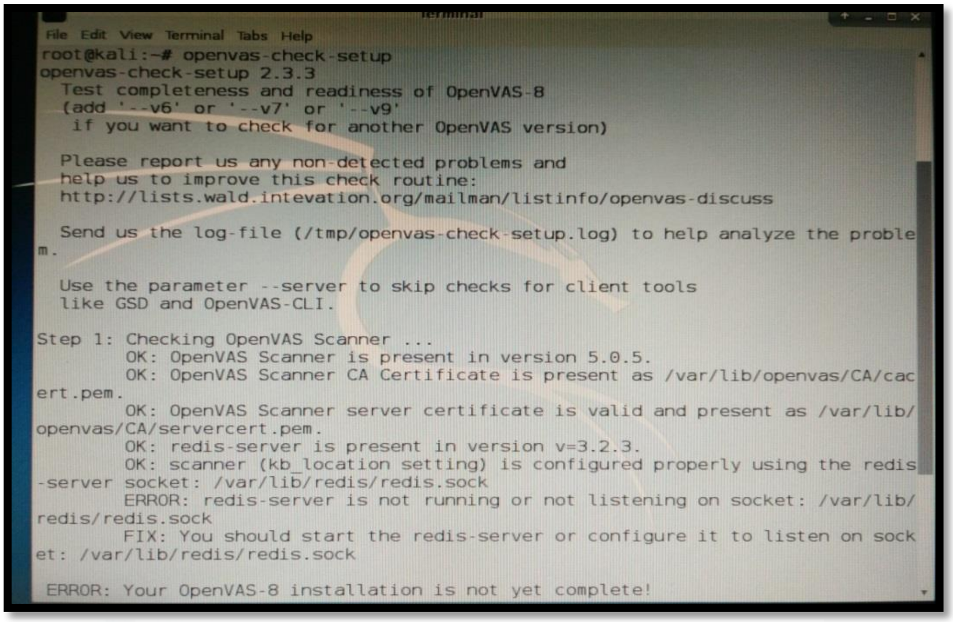
Figure 37 shows first process to install OpenVas. All the package that in the OpenVas will be downloaded using internet. The latest OpenVas is been downloaded accordingly following the latest version.



```
root@kali:~# openvas-setup
[i] This script synchronizes an NVT collection with the 'OpenVAS NVT Feed'.
[i] The 'OpenVAS NVT Feed' is provided by 'The OpenVAS Project'.
[i] Online information about this feed: 'http://www.openvas.org/openvas-nvt-feed
.html'.
[i] NVT dir: /var/lib/openvas/plugins
OpenVAS feed server - http://www.openvas.org/
This service is hosted by Intevation GmbH - http://intevation.de/
All transactions are logged.

Please report synchronization problems to openvas-feed@intevation.de.
If you have any other questions, please use the OpenVAS mailing lists
or the OpenVAS IRC chat. See http://www.openvas.org/ for details.

[i] Feed is already current, no synchronization necessary.
[i] This script synchronizes a SCAP data directory with the OpenVAS one.
[i] This script is for the SQLite3 backend.
[i] SCAP dir: /var/lib/openvas/scap-data
[i] Will use rsync
[i] Using rsync: /usr/bin/rsync
[i] Configured SCAP data rsync feed: rsync://feed.openvas.org:/scap-data
OpenVAS feed server - http://www.openvas.org/
This service is hosted by Intevation GmbH - http://intevation.de/
All transactions are logged.

Please report synchronization problems to openvas-feed@intevation.de.
If you have any other questions, please use the OpenVAS mailing lists
or the OpenVAS IRC chat. See http://www.openvas.org/ for details.

receiving incremental file list
```

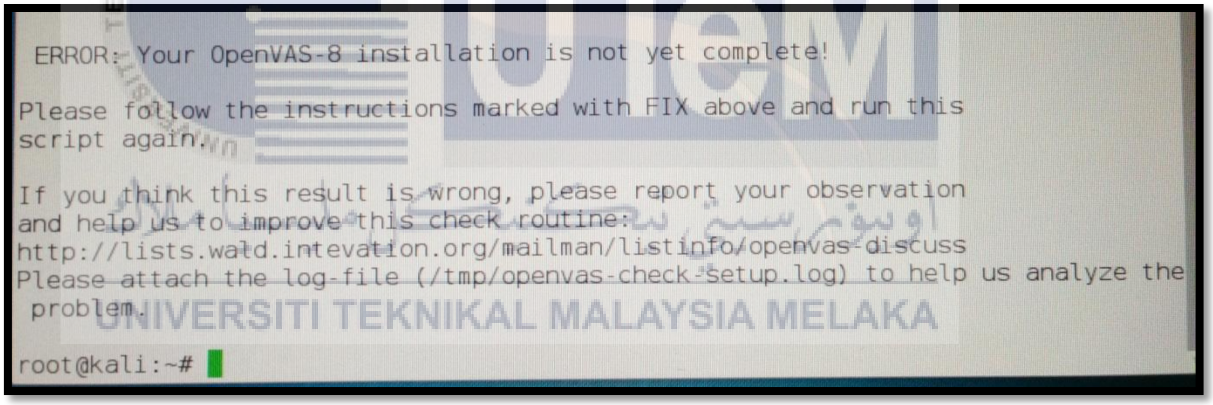
Figure 36: To make sure all packages has been downloaded.

Once done, run the **openvas-setup** command to setup OpenVAS. The last command is setting up OpenVAS and is synchronizing the NVT feed with the NVT collection on your machine. Depending on your connection speed this might take a while to finish.



```
root@kali:~# openvas-check-setup
openvas-check-setup 2.3.3
  Test completeness and readiness of OpenVAS-8
  (add '--v6' or '--v7' or '--v9'
   if you want to check for another OpenVAS version)

  Please report us any non-detected problems and
  help us to improve this check routine:
  http://lists.wald.intevation.org/mailman/listinfo/openvas-discuss

  Send us the log-file (/tmp/openvas-check-setup.log) to help analyze the proble
m.

  Use the parameter --server to skip checks for client tools
  like GSD and OpenVAS-CLI.

Step 1: Checking OpenVAS Scanner ...
        OK: OpenVAS Scanner is present in version 5.0.5.
        OK: OpenVAS Scanner CA Certificate is present as /var/lib/openvas/CA/cac
ert.pem.
        OK: OpenVAS Scanner server certificate is valid and present as /var/lib/
openvas/CA/servercert.pem.
        OK: redis-server is present in version v=3.2.3.
        OK: scanner (kb_location setting) is configured properly using the redis
-server socket: /var/lib/redis/redis.sock
        ERROR: redis-server is not running or not listening on socket: /var/lib/
redis/redis.sock
        FIX: You should start the redis-server or configure it to listen on sock
et: /var/lib/redis/redis.sock

 ERROR: Your OpenVAS-8 installation is not yet complete!
```

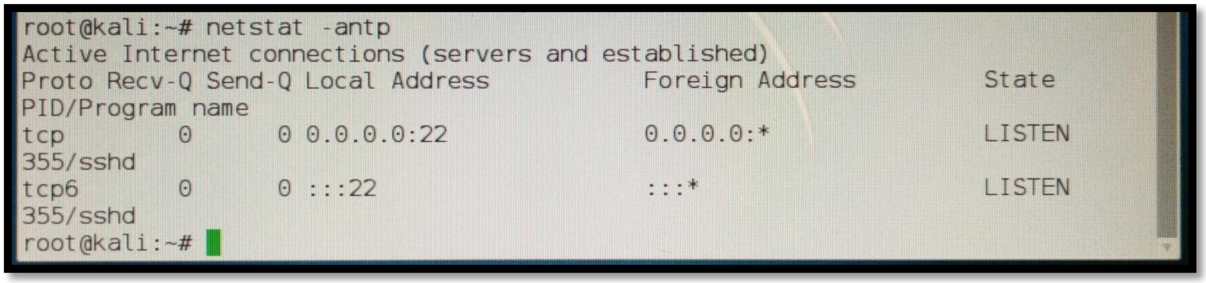
Figure 37: Openvas-check-setup



```
 ERROR: Your OpenVAS-8 installation is not yet complete!

Please follow the instructions marked with FIX above and run this
script again.

If you think this result is wrong, please report your observation
and help us to improve this check routine:
http://lists.wald.intevation.org/mailman/listinfo/openvas-discuss
Please attach the log-file (/tmp/openvas-check-setup.log) to help us analyze the
 problem.

root@kali:~# 
```

Figure 38: Openvas-check-setup (continue)

Openvas-check-setup is to analyze the state of OpenVAS installation and propose fixes should it detect any errors or misconfigurations. It will also check if all required OpenVAS services are running and listening on the correct ports.



```
root@kali:~# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
355/sshd
tcp6       0      0 :::22                   :::*                    LISTEN
355/sshd
root@kali:~# 
```

Figure 39: Netstat -antp to list out the state of port

Figure 41 shows to display all port whether the services in listen state. The usual port will be displayed which is TCP and SSH and also the local address.

5.3 Conclusion

In this chapter, discusses the installation of environment following the design network. Installation on Raspberry Pi was the most important because the process of scanning will be held on Raspberry Pi. Testing scenario will be made on Raspberry Pi is port scanning and vulnerability test on next chapter. From the tests, it will produce list of risks that will give harmful to the Raspberry Pi. The results of the risk will be rated according to ISO standard as guidance.

For the next chapter, the topics will be contributed on the testing for risk and vulnerabilities test and ratings the result for the risk analysis to get specific stage of risks. This is the most important chapter in this project which will test of scanning port in detail. All possible in risk evaluation in this project will be evaluated and be rated. After the risks been listed, the recommendation will be listed. The types of vulnerability also be listed that could be used against Raspberry Pi. The finalize work from all testing and the result that get for risk assessment will be documented.

CHAPTER VI

TESTING AND ANALYSIS

6.1. Introduction

In the previous chapter, we have briefly discussed about the implementation of the project. Now that we have implemented the project we will now continue to discuss and review the testing of this project. Testing of a project is crucial in order to ensure that the project is completed and met the requirements of the project; the result in testing the port scanning and vulnerabilities scanning in Raspberry Pi as one of the low capacity device reporting will be included as we go through this chapter.

6.2. Results and Analysis Testing

The motivation behind information gathering is to get data, to continue record of the information, to settle on choices about imperative issues and to pass data on to others. The information had been grouping and comprises of two sorts which is essential information and auxiliary information.

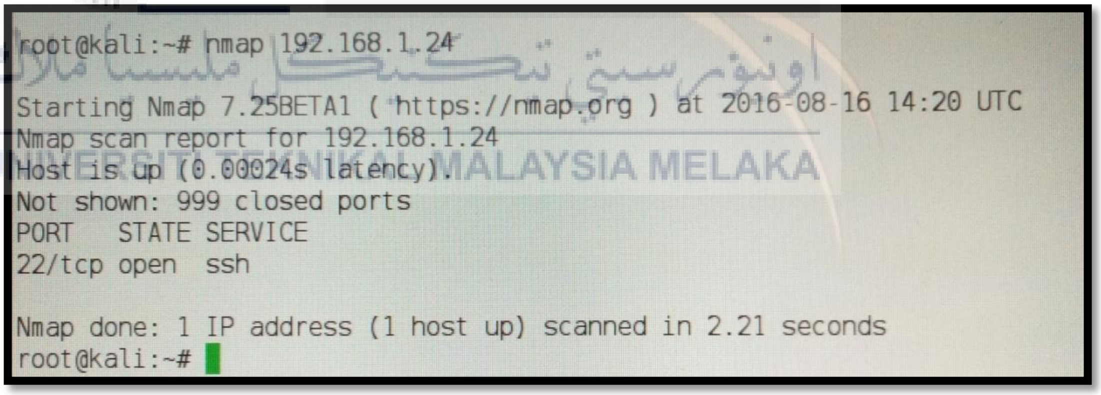
6.2.1. Primary Data

This strategy is about information that gather from genuine testing that had been done in this examination. It is called essential information. At the end of the day, specialists gather the information themselves, utilizing reviews, meets and direct perceptions. Generally, the inquiries the scientists request that are custom-made evoke the information that will help them with their study.

6.2.1.1 Port Scanning

Table 6: Testing Description

Test	Scanning port on IP address of network that connects using Raspberry Pi.
Test Purpose	To detect port that opened and closed.
Test Environment	Apply on Kali Linux and used Nmap .
Test Setup	Enter the IP address was 192.168.1.24 and start the scanning.

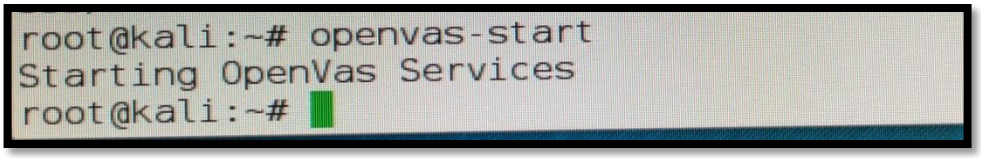
Expected Result	
	`root@kali:~# nmap 192.168.1.24`
	
	`Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-08-16 14:20 UTC`
	`Nmap scan report for 192.168.1.24`
	`Host is up (0.00024s latency).`
	`Not shown: 999 closed ports`
	`PORT   STATE SERVICE`
	`22/tcp open  ssh`
	
	`Nmap done: 1 IP address (1 host up) scanned in 2.21 seconds`
	`root@kali:~#`
	Figure 40: Result from scan port testing.
	• It shows that the host is up within 0.00024s latency.
	• The total port that will be scanned was 1000 TCP port while the result shows closed ports was 999 ports and the opened port was listed which only port 22 that is SSH port.
	• The shut port may can be consider blocking such ports with a firewall and it

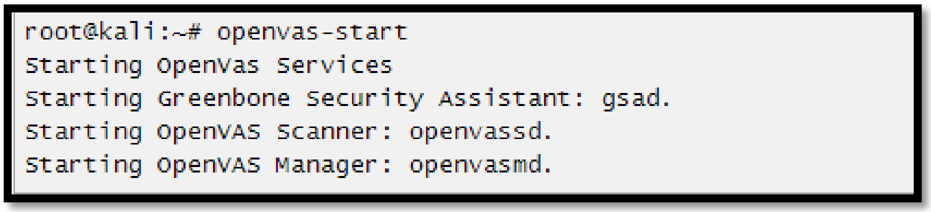
	would be show up in the sifted state, future works. For the opened port, the outcome is regularly for the essential objective of port filtering.

6.2.1.2 Vulnerabilities Testing

Table 7: Testing Description

Test	Scanning vulnerabilities on IP address of network that connects using Raspberry Pi.
Test Purpose	To detect vulnerability exists.
Test Environment	By using OpenVas as tool.

Test Setup	• Once the Raspberry Pi running, the disk expansion procedure was employed to expand the Kali installation to the nearly entire available disk space on the SD card.
	• With available space, additional tools could now be loaded. However after several times tried to install OpenVAS, the SD card was full.
	
	`root@kali:~# openvas-start`
	`Starting OpenVas Services`
	`root@kali:~#`
	Figure 41: Process to start the OpenVas
	• Figure 41, shows the command to run the OpenVas. It is the one of the process to scan the vulnerability in the network by using Raspberry Pi. It is the continuous from the last chapter that explained about installation.

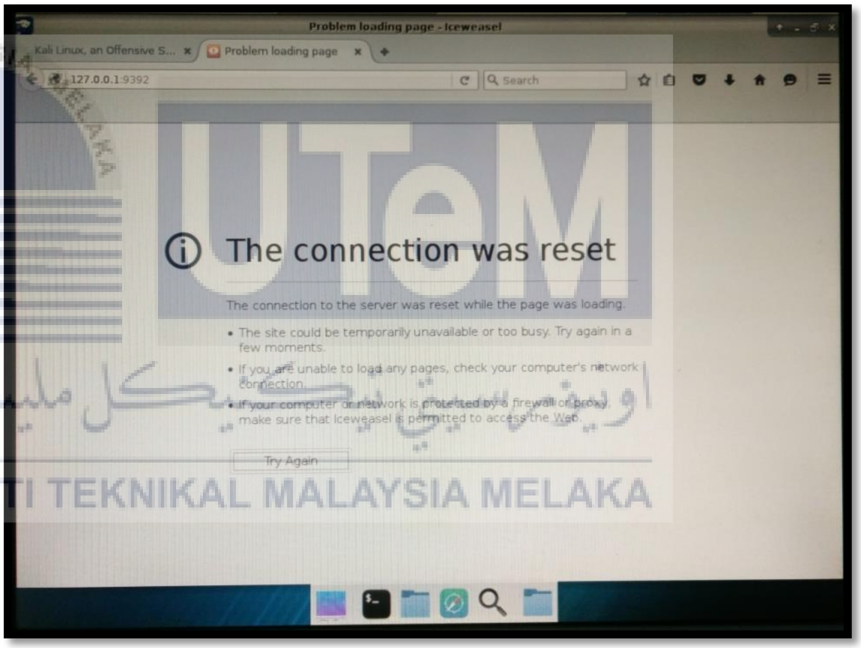
<table>
<tr>
<td><b>Expected
Result</b></td>
<td>


```
root@kali:~# openvas-start
Starting OpenVas Services
Starting Greenbone Security Assistant: gsad.
Starting OpenVAS Scanner: openvassd.
Starting OpenVAS Manager: openvasmd.
```

<b>Figure 42: The real output to start the OpenVas.</b>

- Figure 42, is the exactly output after start the OpenVas. It is not same with the real testing because during the testing was held, a problem was occurred.
</td>
</tr>
<tr>
<td><b>Remark</b></td>
<td>

- Unfortunately the testing had been failed due to circumstances problem.



Problem loading page - Iceweasel
Kali Linux, an Offensive S...
Problem loading page
127.0.0.1:9392
Search

The connection was reset

The connection to the server was reset while the page was loading.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Iceweasel is permitted to access the Web.

<b>Figure 183: The web was not appearing in the right browser.</b>

- Figure 43, shows the errors that appear on the browser.
- Website link, https://127.0.0.1:9392, was entered to plug in the credentials for the admin user.
- This is proven that testing by using OpenVas to scan vulnerability was failed and was back up with secondary data.
</td>
</tr>
</table>

6.2.2. Secondary Data

This term alludes to information that is gathered routinely as a major aspect of the everyday operations of an association, foundation or office. Contrasted with essential information, optional information has a tendency to be promptly accessible and modest to acquire. What's more, managerial information has a tendency to have expansive examples, on the grounds that the information accumulation is exhaustive and schedule. Besides, information (and numerous sorts of optional information) are gathered over a long stretch. That permits specialists to distinguish change after some time.

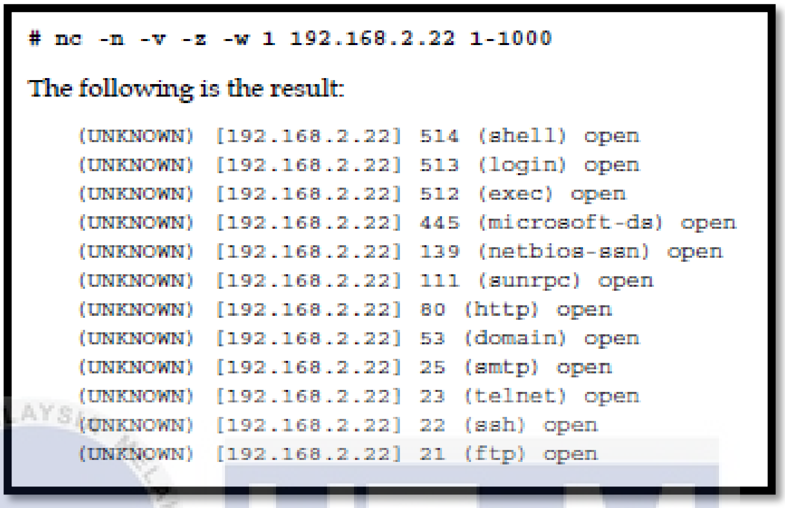
Based experiment done by (Hunt n.d.), the examination is utilizing Raspberry Pi, was chosen as it is a cheap advancement ARM stage that is straightforwardly bolstered by Kali Linux. In this examination, the firewall was opened any discretionary port and forward it to an inside gadget without validation. This is on the grounds that they make a presumption that all hubs on the LAN are trusted. For the synopsis in this exploration, it presume that all ports were opened and the vulnerabilities were exist in light of the fact that with access to LAN gadgets' movement, the assailant can profile the gadgets particularly, increasing point by point information about gadget forms and administrations that can be abused. The assailant may utilize Metasploit for an immediate assault upon a found weakness.

In addition, (Allen et al. 2014a), checking ports instrument that been utilized is DMitry (Deepmagic Information Gathering Tool), Hping3 device, Nmap, Netcat. Every one of the tolls had been connected in low limit gadget. The outcome is a few beneath:

- From Dmitry device, the former summon, it was found that the objective host is utilizing a gadget to do parcel separating. It just permits approaching associations with port 80, which is ordinarily utilized for a web server.
- From Hping3 instrument, the previous yield, we can take note of that the

objective machine is alive on the grounds that it has answered to our ICMP reverberation demand.

- The output from Netcat instrument.



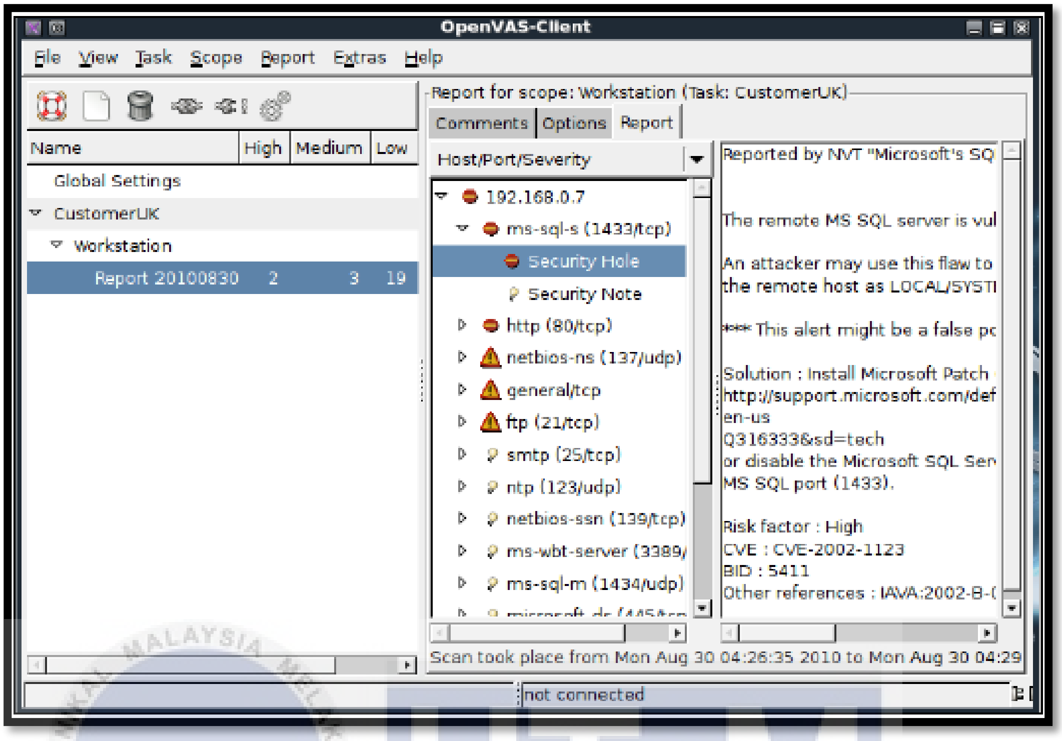
```
# nc -n -v -z -w 1 192.168.2.22 1-1000
```

The following is the result:

```
    (UNKNOWN) [192.168.2.22] 514 (shell) open
    (UNKNOWN) [192.168.2.22] 513 (login) open
    (UNKNOWN) [192.168.2.22] 512 (exec) open
    (UNKNOWN) [192.168.2.22] 445 (microsoft-ds) open
    (UNKNOWN) [192.168.2.22] 139 (netbios-ssn) open
    (UNKNOWN) [192.168.2.22] 111 (sunrpc) open
    (UNKNOWN) [192.168.2.22] 80 (http) open
    (UNKNOWN) [192.168.2.22] 53 (domain) open
    (UNKNOWN) [192.168.2.22] 25 (smtp) open
    (UNKNOWN) [192.168.2.22] 23 (telnet) open
    (UNKNOWN) [192.168.2.22] 22 (ssh) open
    (UNKNOWN) [192.168.2.22] 21 (ftp) open
```

Figure 44: The output from test Netcat

For the vulnerabilities testing, Open Vulnerability Assessment System (**OpenVAS**) and NeXpose Vulnerability Scanner Community Edition (**NeXpose CE**) are the tools that been used to scan the vulnerability. NeXpose CE is a free vulnerability scanner from Rapid7 that scans devices for vulnerabilities. It can also be integrated with the Metasploit exploit framework. These are the result from using the tools.



Name	High	Medium	Low
Global Settings			
CustomerUK			
Workstation			
Report 20100830	2	3	19

Report for scope: Workstation (Task: CustomerUK)

```
192.168.0.7
  ms-sql-s (1433/tcp)
    Security Hole
    Security Note
  http (80/tcp)
  netbios-ns (137/udp)
  general/tcp
  ftp (21/tcp)
  smtp (25/tcp)
  ntp (123/udp)
  netbios-ssn (139/tcp)
  ms-wbt-server (3389/
  ms-sql-m (1434/udp)
```

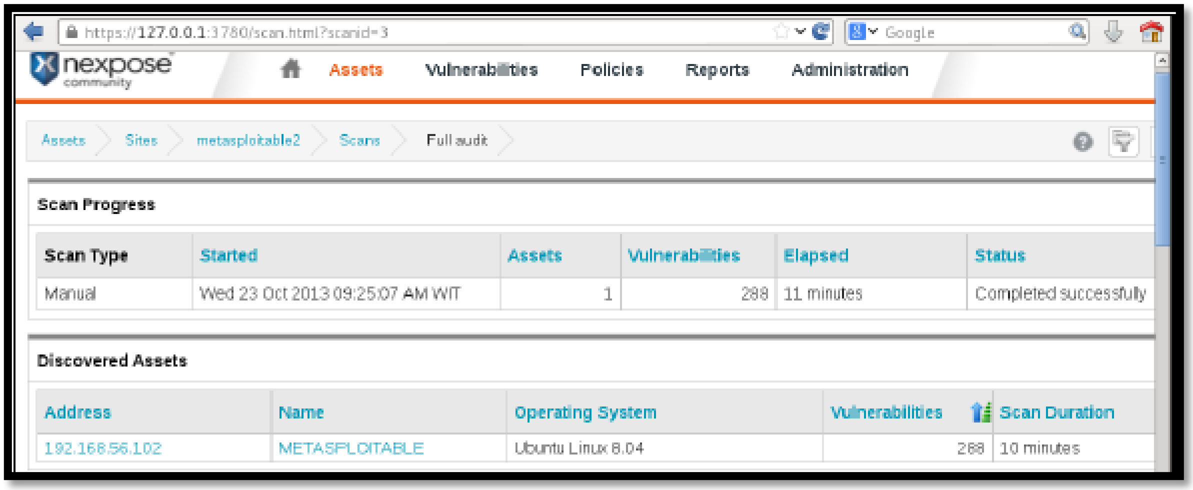
```
Reported by NVT "Microsoft's SQ

The remote MS SQL server is vul

An attacker may use this flaw to
the remote host as LOCAL/SYSTI

*** This alert might be a false pc

Solution : Install Microsoft Patch
http://support.microsoft.com/def
en-us
Q316333&sd=tech
or disable the Microsoft SQL Ser
MS SQL port (1433).

Risk factor : High
CVE : CVE-2002-1123
BID : 5411
Other references : IAVA:2002-B-(
```

Scan took place from Mon Aug 30 04:26:35 2010 to Mon Aug 30 04:29

not connected

Figure 45: Output vulnerabilities testing in OpenVAS

Figure 45 shows the result of vulnerabilities testing in OpenVas that appear in web browser. It is the report that listed out the vulnerabilities for IP address '192.168.0.7'.


https://127.0.0.1:3780/scan.html?scanid=3
Google
nexpose community
Assets
Vulnerabilities
Policies
Reports
Administration
Assets > Sites > metasploitable2 > Scans > Full audit

Scan Progress

Scan Type	Started	Assets	Vulnerabilities	Elapsed	Status
Manual	Wed 23 Oct 2013 09:25:07 AM WIT	1	288	11 minutes	Completed successfully

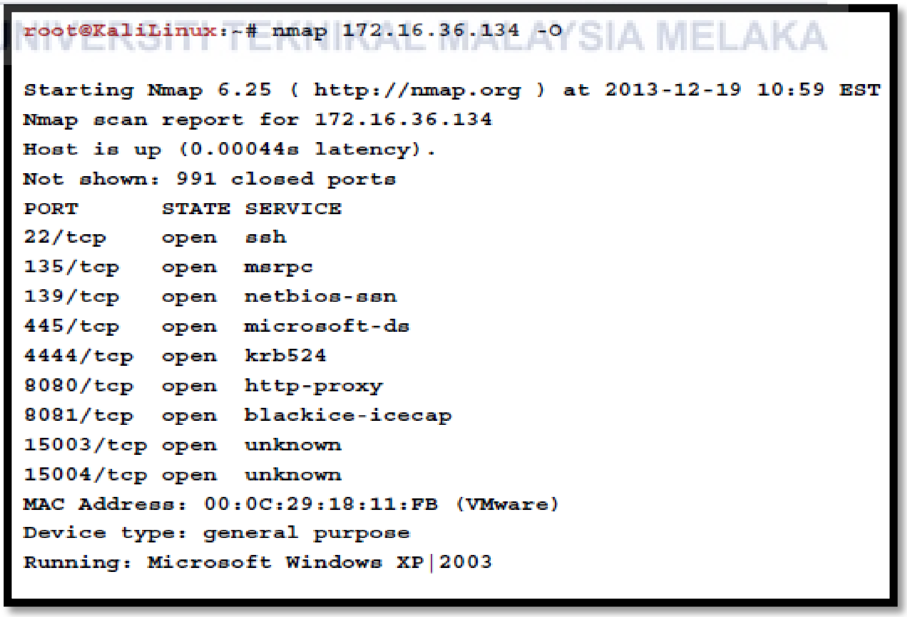
Discovered Assets

Address	Name	Operating System	Vulnerabilities	Scan Duration
192.168.56.102	METASPLOITABLE	Ubuntu Linux 8.04	288	10 minutes

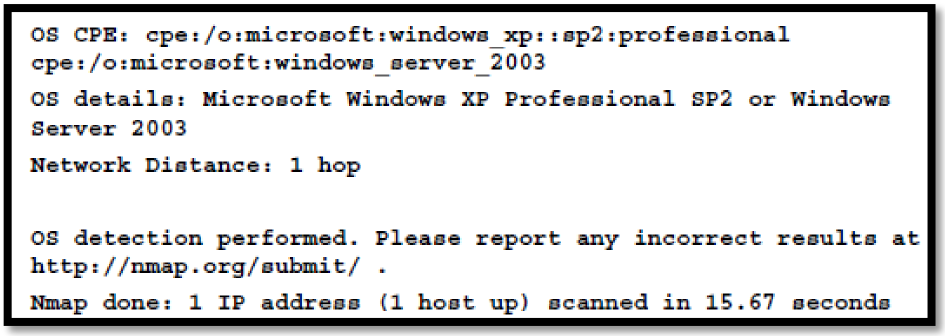
Figure 46: Output for vulnerability testing in NeXpose CE

Figure 46 shows the result after test on vulnerabilities was done. It was tested by using NeXpose CE as scanning tool.

In (Hutchens 2014), Nmap was used to scan the port that been applied in Windows Server on suitable low capacity device. '-o' was used to specifically on IP address.



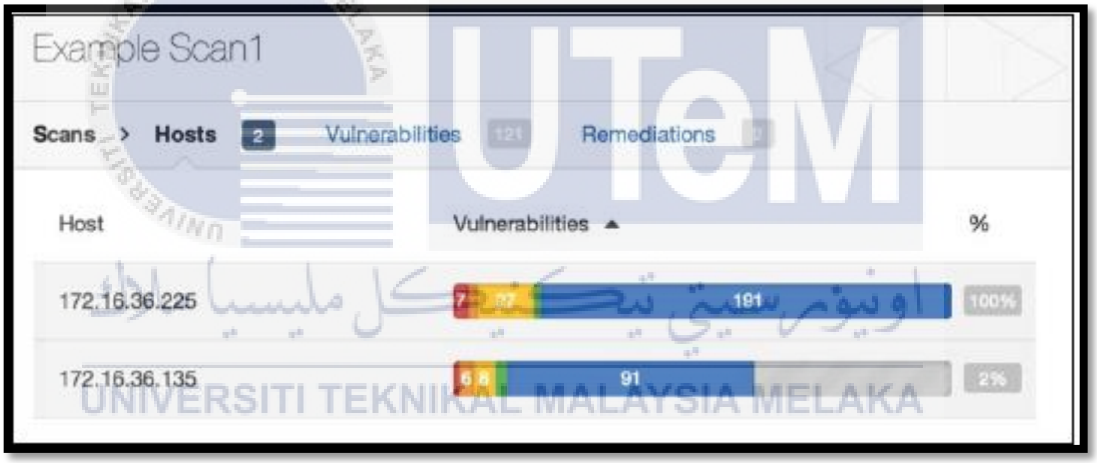
```
root@KaliLinux:~# nmap 172.16.36.134 -O

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-19 10:59 EST
Nmap scan report for 172.16.36.134
Host is up (0.00044s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
4444/tcp  open  krb524
8080/tcp  open  http-proxy
8081/tcp  open  blackice-icecap
15003/tcp open  unknown
15004/tcp open  unknown
MAC Address: 00:0C:29:18:11:FB (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
```



```
OS CPE: cpe:/o:microsoft:windows_xp::sp2:professional
cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP Professional SP2 or Windows
Server 2003
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.67 seconds
```

Figure 47: Port Scanning in Windows Server

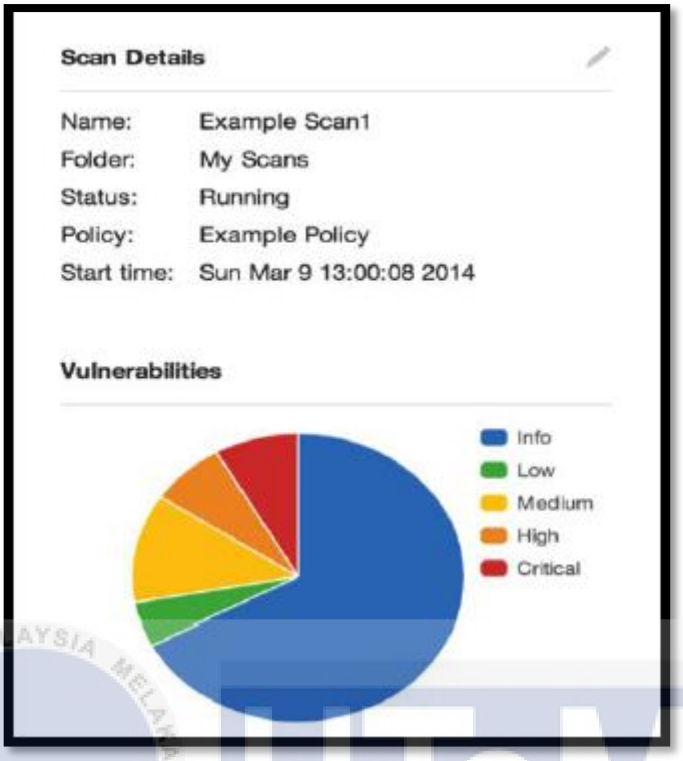
For the vulnerabilities, this researcher is used Nessus to scan the vulnerability. The result can be showed until the explanations for the vulnerabilities.



Host	Vulnerabilities	%
172.16.36.225	7 27 191	100%
172.16.36.135	6 8 91	2%

Figure 48: Vulnerabilities scan for specific IP address.

Figure 48 shows the process of scanning and the total of vulnerabilities on each host. The result has been categorized into level of risks according to the color. For 192.16.36.225, it detect that seven high level risk, 27 medium level risk and 191 for low level risks. For 172.16.36.135, the process of scanning process is working. Usually it contain HTTP,UDP and FTP.



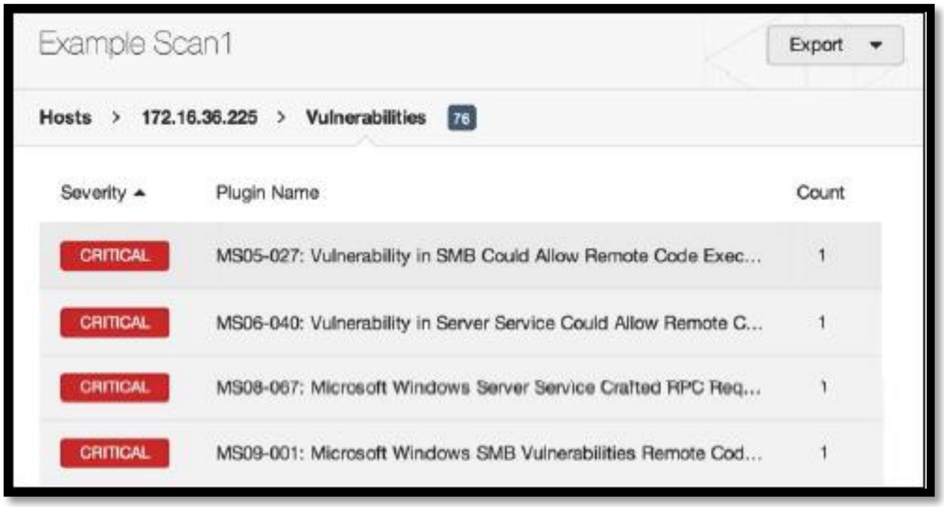
Scan Details

Name: Example Scan1
Folder: My Scans
Status: Running
Policy: Example Policy
Start time: Sun Mar 9 13:00:08 2014

Vulnerabilities

Figure 49: Pie Chart for the result.

Figure 49 shows the result of scanning vulnerabilities in pie chart. It has been divided into five levels which is info, low, medium, high and critical.



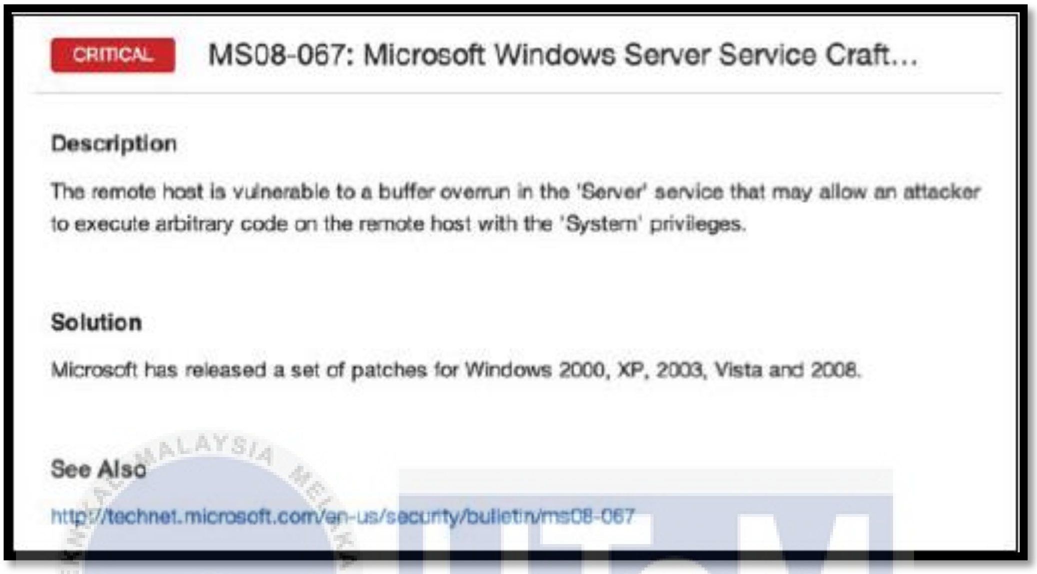
Example Scan1

Hosts > 172.16.36.225 > Vulnerabilities 76

Severity ▲	Plugin Name	Count
CRITICAL	MS05-027: Vulnerability in SMB Could Allow Remote Code Exec...	1
CRITICAL	MS06-040: Vulnerability in Server Service Could Allow Remote C...	1
CRITICAL	MS08-067: Microsoft Windows Server Service Crafted RPC Req...	1
CRITICAL	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Cod...	1

Figure 50: List Vulnerabilities

Figure 50 shows list of vulnerabilities following the severity based on specific host. It is more detail because due to the severity, plugin name that scan held on and the total of risk on each plugin.


CRITICAL MS08-067: Microsoft Windows Server Service Craft...

Description

The remote host is vulnerable to a buffer overrun in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with the 'System' privileges.

Solution

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008.

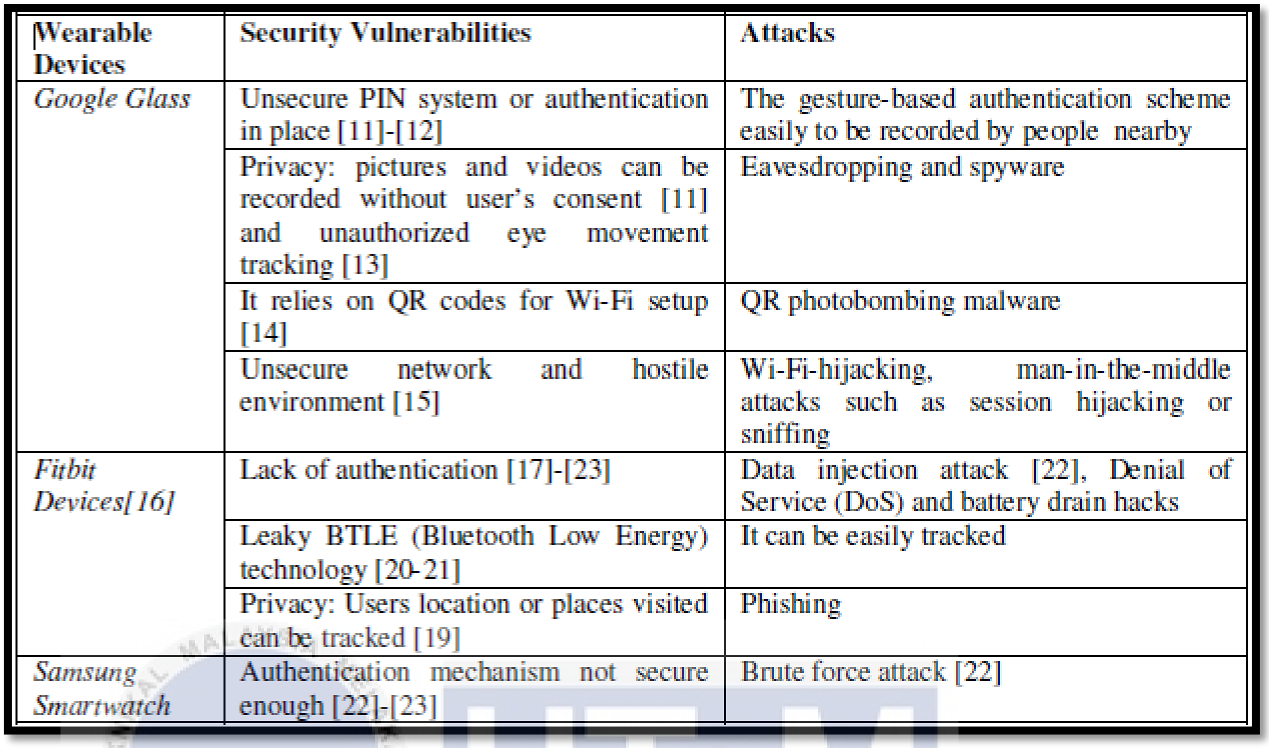
See Also

http://technet.microsoft.com/en-us/security/bulletin/ms08-067

Figure 51: Description of vulnerability.

In Figure 51, the detail of description about the each vulnerabilities was listed and the solution for the problem also be listed. It shows that the risk can be secure by using the solution.

In next research, (Ching & Singh 2016) was tested only for vulnerabilities for wearable devices as one of low capacity devices. The figure below shows the result after detection of the vulnerability:

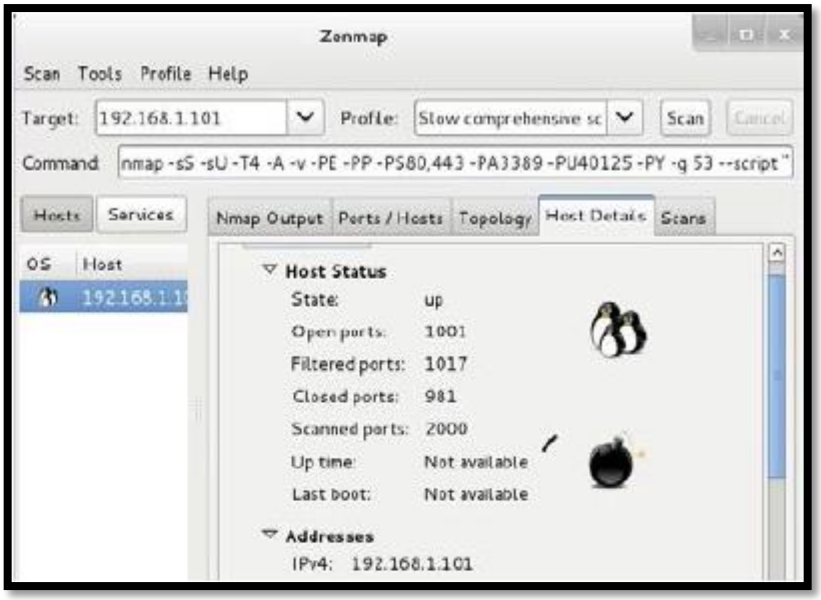


Wearable Devices	Security Vulnerabilities	Attacks
Google Glass	Unsecure PIN system or authentication in place [11]-[12]	The gesture-based authentication scheme easily to be recorded by people nearby
	Privacy: pictures and videos can be recorded without user's consent [11] and unauthorized eye movement tracking [13]	Eavesdropping and spyware
	It relies on QR codes for Wi-Fi setup [14]	QR photobombing malware
	Unsecure network and hostile environment [15]	Wi-Fi-hijacking, man-in-the-middle attacks such as session hijacking or sniffing
Fitbit Devices[16]	Lack of authentication [17]-[23]	Data injection attack [22], Denial of Service (DoS) and battery drain hacks
	Leaky BTLE (Bluetooth Low Energy) technology [20-21]	It can be easily tracked
	Privacy: Users location or places visited can be tracked [19]	Phishing
Samsung Smartwatch	Authentication mechanism not secure enough [22]-[23]	Brute force attack [22]

Figure 52: Result from vulnerabilities testing.

The wearable gadgets were partitioned into three segments which is Google Glass, Fitbit Devices and Samsung Smartwatch. The assaults were being recognized after the security vulnerabilities were identified for every wearable gadget.

According (Williams 2015), this examination contained two port sweeps and one defenselessness output were led. The hardware used amid this stage incorporated an Asus portable workstation running VM Player, supporting Kali-Linux 1.10. A Raspberry PI running Debian 7.0 (Wheezy) was specifically associated with the Wi-Fi switch, and was connected to a DSL modem. Zenmap is utilized as instrument to filter the port and it contains 2000 ports. For vulnerabilities filtered, Retina was utilized to distinguish the vulnerabilities that exist.



Target: 192.168.1.101

Profile: Slow comprehensive sc

Command: nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script"

Host Status

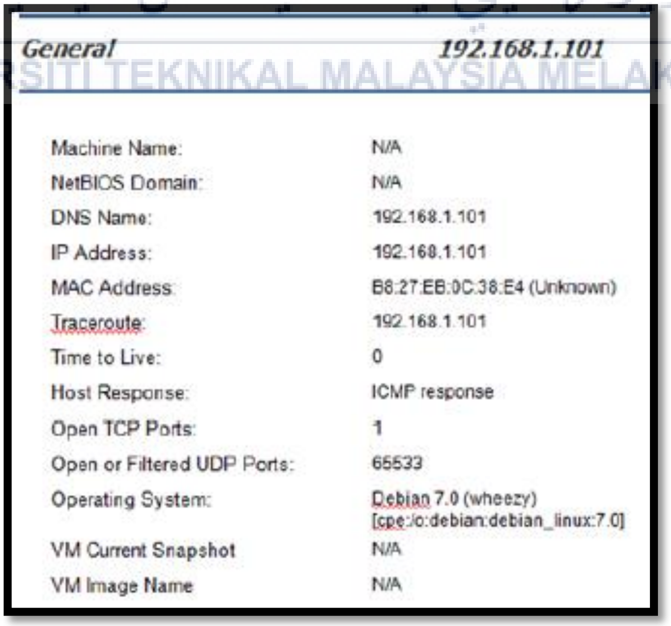
State:	up
Open ports:	1001
Filtered ports:	1017
Closed ports:	981
Scanned ports:	2000
Up time:	Not available
Last boot:	Not available

Addresses

IPv4: 192.168.1.101

Figure 53: Result from scanning port

From figure above, from 2000 ports that been scanned, 1001 ports was opened and 981 ports was closed. From the total open and closed ports, 1017 ports have been filtered.



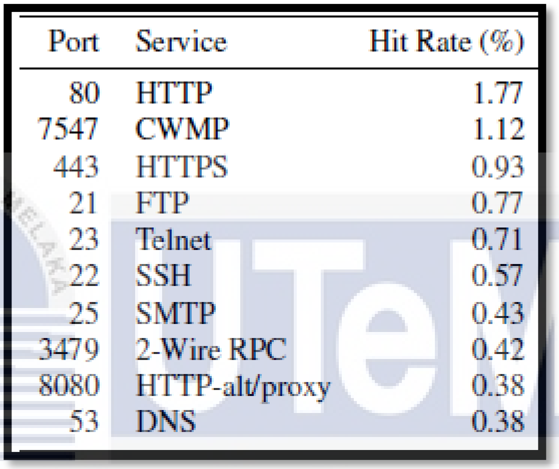
General *192.168.1.101*

Machine Name:	N/A
NetBIOS Domain:	N/A
DNS Name:	192.168.1.101
IP Address:	192.168.1.101
MAC Address:	B8:27:EB:0C:38:E4 (Unknown)
Traceroute:	192.168.1.101
Time to Live:	0
Host Response:	ICMP response
Open TCP Ports:	1
Open or Filtered UDP Ports:	65533
Operating System:	Debian 7.0 (wheezy) [cpe:/o:debian:debian_linux:7.0]
VM Current Snapshot	N/A
VM Image Name	N/A

Figure 54: Result from scanning vulnerabilities

From result above, there are two vulnerabilities that were SSH Local Access Audit ID No. 2264 and ICMP Timestamp Request Audit ID No. 3688. Both are finish up as low-level occasions.

Due to (Durumeric et al. 2013), Zmap is an open-source system scanner that empowers analysts to effortlessly perform all-inclusive system contemplates. It is additionally can be connected in any of low limit gadget particularly in Raspberry Pi.



Port	Service	Hit Rate (%)
80	HTTP	1.77
7547	CWMP	1.12
443	HTTPS	0.93
21	FTP	0.77
23	Telnet	0.71
22	SSH	0.57
25	SMTP	0.43
3479	2-Wire RPC	0.42
8080	HTTP-alt/proxy	0.38
53	DNS	0.38

Figure 55: List of open port

Based on this research, Zmap was scanned 2.15 million hosts on TCP ports 0–9175 and observed what fraction was listening on each port. Figure 57 shows 10 ports that been scanned. HTTP port shows the highest rate 1.77% if compared to others. HTTP was frequently used because the port is used for web browser.

On the vulnerabilities testing, UPnP weakness was discovered larger part which it at last affected 1,500 merchants and 6,900 items, all of which can be misused to perform discretionary code execution with a solitary UDP bundle. This output discovered 15.7 million freely open UPnP gadgets, of which 2.56 million (16.5%) were running helpless variants of the for UPnP Devices, and 817,000 (5.2%) utilized powerless adaptations of MiniUPnPd.2 Leveraging strategy like ZMap, it would just have taken a matter of hours from the season of exposure to taint each freely accessible defenseless host.

Furthermore, Weak Public Key was found that 44,600 special declarations used factorable RSA keys and is served on 51,000 hosts, a 20% reduction from 2011. Four of these testaments were program believed; the latter was marked in August 2012. Also, on this examination it can be discovered 2,743 special endorsements that contained Debian feeble keys, of which 96 were program believed, a 34% reduction from 2011. The last program trusted endorsement containing a Debian feeble key was marked in January 2012. We additionally watched a 67% lessening in the quantity of program trusted authentications that contained default open keys utilized for Citrix remote access items.

Table 8: Summarization of risks

Scanning Port	**Vulnerabilities scanning**	**Author**
• UDP • SSH	• UPnP • ICMP • SMTP	Hunt n.d
• HTTP port • ICMP port • Shell • Login • Exec • Microsoft-DS • Netbios-SSN • Sunrpc • HTTPS • SNTP • TELNET	• TCP (6) • HTTP (1) • UDP (3) • FTP (1) • SMTP • NTP • Netbios-SSN	Allen et.AL 2014

• SSH • FTP		
• 991 • SSH • MSRPC • KRB524 • Netbios-SSN • Microsoft-DS • HTTP-PROXY • TCP • Blackice-icecap	• HTTP • UDP • FTP • ICMP	Hutchens (2014)
Not Applicable	• Unsecure Authentication • Unsecure Network • Location can be tracked • Authentication mechanism not secure	Ching & Singh 2016
• TCP • SSH	• SSH • ICMP	William 2015
• HTTP • HTTPS • TELNET • SMTP • HTTP(alt/proxy) • DNS • FTP • SSH • 2-Wire RPC	• UPnP • Weak Public Key	Durumeric et al. 2013

6.3.Risk on Low Capacity Device

In this section, risk on low capacity device was short list to usually exist in any process scanning due to previous research. After finish the process of analyze the risks, there are ten risks that been found due to frequency occurrence at scanning risks.

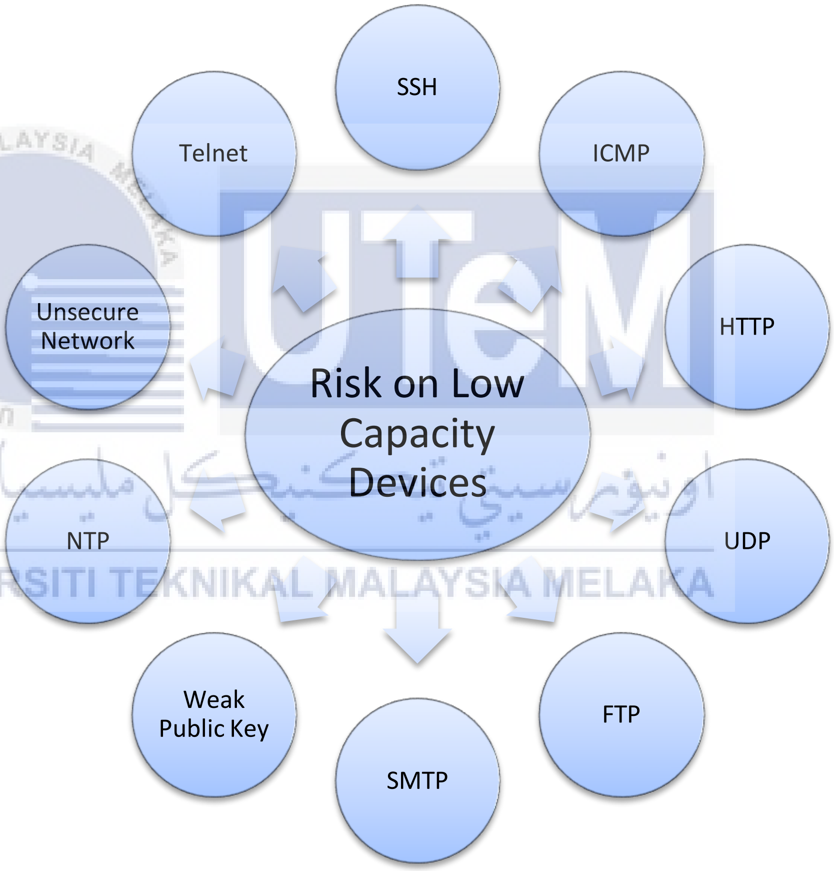


Figure 56: Summarize of risk

Figure 58 above shows summarize of risks after all the result had been produced. These are the result after been identifying from the testing and based from research from another journal.

6.4.Risk Classification

This area clarifies the danger levels (high, medium and low) utilized as a part of the report. These levels ought to obviously separate and highlight the specialized security presentation as far as seriousness.

The level of danger is depending to analyst to level it in view of the checking test. This permits the benefit proprietor to settle on keen choices with respect to tolerating the danger. The capacity to signoff is resolved taking into account the level of danger. Typically high dangers must be acknowledged by administration of an association, while little dangers can be acknowledged by resource proprietors (Reeves 14AD). In this research, the level of risks is based on the higher the level depends on the frequency occurrence on low capacity device.

Table 9: Level of risks

Level of Risk	Risks
Low (Frequency Occurrence– 1)	Unsecure Network, NTP, Weak Public Key
Medium (Frequency Occurrence– 2-3)	Telnet, SMTP, FTP
High (Frequency Occurrence- 4-5)	SSH, ICMP, HTTP, UDP

Table 9 above shows the level of risk according to frequency occurrence in research result. For low level, the frequency occurrence is 1 and it usually happened for unsecure network, NTP and weak public key. For the medium level, it usually occur in 2 until 3 times that is telnet, SMTP and FTP. For the high level, the frequency occurrence is happened between 4 until which is SSH, ICMP, HTTP and UDP.

6.5. Propose Counter Measure For Identify Risk

Table 10: Counter Measure of High Risk

List of threats/risks	Counter Measure	Citation
SSH	• Through middlemen • Switch to Pure Key-based Authentication	• (Sebastian,Grenville,Philip 2007)
ICMP	• Loki, which tunnelled data in the payload of ICMP echo messages. • Zelenchuk implemented an indirect IP over ICMP tunnel	• (Sebastian,Grenville,Philip 2007)
HTTP	• Transfer the risk • Implementing and enforcing a policy directive that forbids the use of protocols with known susceptibilities to eavesdropping	• (Allen et al. 2014b)
UDP	• Proposed using its presence or absence to signal one bit of covert information per UDP packet	• (Sebastian,Grenville,Philip 2007)

This section is about the list of risk that categorized as high level above. Because of the vulnerability is too risky to low capacity device, the counter measure has been listed to overcome the risk in vulnerability that can reduce any harmful to low capacity device. This list is also included the author to make another researcher easy to search the journal.

6.5.1. Correlation from Past Research

SPSS relationship test is a method for testing whether two metric variables are straightly related in some populace. The degree to which they are is generally communicated by a number, called the relationship coefficient. The invalid theory infers that no straight connection at all is available in the middle of the variables, which infers a relationship of 0.

Table 11: Value for variable

Variable	Cronbach's Alpha value
Scan Port	.752
Vulnerability scan	.752

From Table 11, Cronbach’s Alpha values for scan port and vulnerability scan are .752 respectively which means if a variable value less than 0.7, it will be dropped out. Considering the result is more than 0.7, the result is acceptable to continue with analyze the correlation. This is the result for item analysis using Cronbach’s Alpha as shown.

Table 12: Non-Parametric Correlations

Correlations

			total	Scan Port	Vulnerability Scan
Spearman's rho	total	Correlation Coefficient	1.000	.779**	.991**
		Sig. (2-tailed)	.	.005	.000
		N	11	11	11
	Scan Port	Correlation Coefficient	.779**	1.000	.699*
		Sig. (2-tailed)	.005	.	.017
		N	11	11	11
	Vulnerability scan	Correlation Coefficient	.991**	.699*	1.000
		Sig. (2-tailed)	.000	.017	.
		N	11	11	11

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

From table 12, Site vulnerability scan is significantly correlated with scan port but very strong with .991**.So, for the conclusion, it is proven that vulnerability scan is more risky towards risk on low capacity device.

6.6. Analysis Using Statistical Method

In this section, method that had been used to analyze the scan port and vulnerability scan to find the correlation was SPSS. SPSS is the acronym of Statistical Package for the Social Science. SPSS is a standout among the most mainstream measurable bundles which can perform exceedingly complex information control and investigation with basic guidelines. It is intended for both intelligent and non-intuitive (batch) employments. It can take information from a record and utilize them to create classified reports, graphs, and plots of appropriations and patterns, unmistakable measurements, and complex factual examination.

This analyze process is intend to find the correlation between scan port and vulnerability scan, which may prove what is more dangerous to risk in low capacity device. Before this research continues with correlation, the reliability of the data needs to identify. The most common use to identify the reliability by using Cronbach's alpha. Cronbach's alpha is a measure used to evaluate the unwavering quality, or inner consistency, of an arrangement of scale or test things. At the end of the day, the dependability of any given estimation alludes to the degree to which it is a predictable measure of an idea, and Cronbach's alpha is one method for measuring the quality of that consistency.

Correlation is a bivariate examination that measures the qualities of relationship between two variables. In insights, the estimation of the relationship coefficient shifts amongst +1 and - 1. At the point when the estimation of the connection coefficient lies around ± 1, then it is said to be an impeccable level of relationship between the two variables. As the connection coefficient esteem goes towards 0, the relationship between the two variables will be weaker.

There are three types of correlation that can be used which is Pearson correlation, Kendall rank correlation and Spearman correlation. Pearson r correlation is generally utilized as a part of insights to gauge the level of the relationship between direct related variables. For instance, in the share trading system, in the event that we need to gauge how two products are identified with each other, Pearson r correlation is utilized to quantify the level of relationship between the two wares.

Kendall rank correlation is a non-parametric test that measures the quality of reliance between two variables. In the event that we consider two specimens, an and b, where every example size is n, we realize that the aggregate number of pairings with a b is n(n-1)/2.

Spearman rank correlation is a non-parametric test that is utilized to quantify the level of relationship between two variables. It was produced by Spearman, in this manner it is known as the Spearman rank connection. Spearman rank connection test does not expect any presumptions about the dissemination of the information and is the proper relationship examination when the variables are measured on a scale that is at any rate ordinal.

In order to use the suitable correlation in SPSS, The Spearman's rank-order correlation is the most suitable because Spearman is non-parametric alternative that been used in this research than Pearson is for parametric alternative test. Spearman also is to measure the degree of association than Kendall that is to measure the quality of reliance.

6.6.1 Operational Definition

Table 13: Operational of definition

Variable	Meaning
Scan Port	Port Scanning is the name for the technique used to identify open ports and services available on a network host.
Vulnerability Scan	Vulnerability scan is a security method used to recognize security shortcomings in a PC framework. Weakness filtering can be utilized by people or system executives for security purposes, or it can be utilized by programmers attempt to increase unapproved access to PC frameworks.

6.6.2 Formation of Hypothesis

Theories that propose a causal relationship include no less than one free variable and no less than one ward variable; as it were, one variable which is dared to influence the other.

- H1 - Is the risk on low capacity device affect by scan port?
- H2 – Is the risk on low capacity device affect by vulnerability scan?

In hypothesis 1, the scan port has been questioned whether it affects towards risk on low capacity device. From the testing result, scan port gives effect to risk on low capacity device because the value that gets from the result in statistical test is telling that the value is enough to give an effect.

In hypothesis 2, the vulnerability scan has been questioned whether it affects towards risk on low capacity device. From the testing result, vulnerability scan gives effect to risk on low capacity device because the value that gets from the result in statistical test is telling that the value is enough to give an effect. For the conclusion, the value of vulnerability is more risky than scan port.

6.6.3 Conceptual Framework

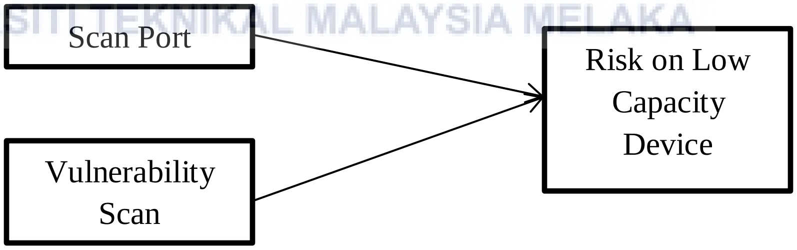


Figure 57: The conceptual framework of this research

Figure 57 shows the conceptual of framework between scan port and vulnerability scan towards risk on low capacity device. This conceptual framework is to clarify concepts of this research and explain of observation on the flow of this research.

6.6.3.1 Independent and Dependent Data

Independent and dependent data means to find out the relationship between the data of scan port and vulnerability scan towards the risk of low capacity device. The independent data is consists of scan port and vulnerability scan and the dependent data is for risk of low capacity device. From the result of the testing, the independent data is depend to dependent data that is the scan port and vulnerability scan is reliable to the risk.

6.6.3.2 Item Analysis

In item analysis, Cronbach's alpha is used because it is one method for measuring the quality of that consistency. The alpha coefficient for the two items is .752, suggesting that the items have relatively high internal consistency. (Note that a reliability coefficient of .70 or higher is considered "acceptable" in most social science research situations.) this can conclude that the item that has high correlation is accepted.

6.7. Conclusion

As for conclusion, all of the objectives of this project nearly achieved which that we have manage to produced and list out the risk from low capacity device, we have also develop a vulnerability and port scanned reporting and we also manage to perform an port scanning on Raspberry Pi using Kali Linux. From the result, it shows in the next chapter, we will cover about the conclusion of the whole project development.

CHAPTER VII

PROJECT CONCLUSION

7.1. Introduction

In this part we will examine about the outline of the project, project commitment, project confinement and future works of the task.

7.2. Project Summarization

Based on from all research that had been done, the entire objective has achieved such as following:

Through first objective, it is to identify the risk of the low capacity device. From chapter 2, the risk of low capacity device will be identified from the past literature review and provide the example research from other researcher.

From the second objective, it is to analyze the identified risk. Through here, it has been achieved through the testing from the primary data and supported by secondary data. The results of list of risk from both data are produced from chapter 6.

From the third objective, it is to document the guideline. From this document, it will produce list of risk and recommendation to be solved. This will act as guideline of risk assessment for low capacity device in ISO Standard. This third objective also has been achieved with the list of risk and the counter measure to overcome the risk in the same time produced a guideline.

- Project Strength and Weakness

Through the research, the strength that produced is this content of research can help following in the content of ISO. Nowadays, a lot of people use low capacity device as tools for communication despite of the technology today use a lot more on IOT devices. This research can help in based on security to develop relate to device. The lists of risk get to be validating using actual relationship.

For the weaknesses, this research does not be able to do test completely. It happened while installing processed had to be done. The results from this result are more focuses on secondary data.

7.3. Project Contribution

With the establishment of this research, this study will help researchers in a study on the risk assessment for low capacity devices. This research also will improved ISO standard because existing standards focus on equipment in general.

7.4. Project Limitation

There are several limitations of while doing this research. Firstly, the latest version had release of Kali Linux for Raspberry Pi but it does not suit for this research, so this research has been used old Kali Linux so that it can run smoothly. Secondly, the problem that has to face is the limitation of space in SD card. Although the size has been upgraded into 16 GB, it still produces a problem. Due to the problem, installation of OpenVas cannot be continued.

Finally, while analyze the risk in SPSS, the result only show for correlation. For regression, it does not come out as perfect result because of insufficient data. Despite from insufficient data, input for detail analysis analytical cannot be key in because of the data is too small.

7.5. Future Works

For the future works, the problem that we faced while this research on going may can be solved including:

- especially the problem while installing OpenVas in Kali Linux. Another researcher also can try another low capacity device such as microcontroller devices or Arduino. Through different approach also can be done so that can get some data that can help another developer such as using questionnaire.

7.6. Conclusion

For the conclusion, finally we can conclude that all the research objectives of project have been achieved. We have successfully study the risk that exist in low capacity device is not dangerous to user. The Raspberry Pi that been used as this research device also save to use because of the existence of counter measure to overcome the list of risk.

REFERENCES

Anon, Sensor Technology.

Australian Government, C., 2009. As / Nzs Iso 31000 : 2009. , (August), pp.3–5.

Benantar, M., 2006. *Access Control Systems: Security, Identity Management and Trust Models*, Available at: https://books.google.com/books?id=dpjsXA5SPPwC&pgis=1.

Commission, E., 2010. A Reference Security Management Plan for Energy Infrastructure Prepared by the Harnser Group for the European Commission.

East, N., 1997. Perimeter Security Sensor Technologies Handbook.

Fallis, A.., 2013. No Title No Title. *Journal of Chemical Information and Modeling*, 53(9), pp.1689–1699.

Gaillard, F. & Eieland, A., 2013. Microprocessor (MPU) or Microcontroller (MCU)? *Atmel*, pp.1–2. Available at: http://www.atmel.com/Images/MCU_vs_MPU_Article.pdf.

Gerhard, E., Lorenz, T. & Heiliger, R., 2008. Fiber optic sensor technology. *Biomedizinische Technik. Biomedical engineering*, 44(1-2), pp.25–30. Available at: http://www.ncbi.nlm.nih.gov/pubmed/10194882.

Gordon, L. a. & Loeb, M.P., 2002. The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4), pp.438–457.

ISO - The International Organization for Standardization, 2009. ISO 31000:2009 - Risk management - Principles and guidelines. *Iso 31000:2009*, 2009, p.24.

Jain, R., 2004. Abstract : Keyword : Table of Contents : 2-Application Fields for Biometrics Technology. , (Id), pp.1–10.

Karabacak, B. & Sogukpinar, I., 2006. A quantitative method for ISO 17799 gap analysis. *Computers and Security*, 25(6), pp.413–419.

Karabacak, B. & Sogukpinar, I., 2005. ISRAM: information security risk analysis method. *Computers & Security*, 24(2), pp.147–159.

Karygiannis, T., Eydt, B. & Barber, G., 2007. Guidelines for securing radio frequency identification (RFID) systems. *NIST Special* .... Available at: http://www.fali.unsri.ac.id/userfiles/SP800-98_RFID-2007.pdf.

Orság, F. & Drahanský, M., Biometric Security Systems : Fingerprint and Speech Technology Design of Biometric Security System.

Portability, H.I., 2007. Security Topics 1. *Risk Management*, 2, pp.1–20.

Protocols, S., 2006. Security Issues in RFID Systems RFID Systems tag. *Security*.

Republic, C., 2002. Biometric Authentication — Security and Usability. *Advanced communications and multimedia security IFIP TC6TC11 Sixth Joint Working Conference on Communications and Multimedia Security September 2627 2002 Portorož Slovenia*, 100, pp.1–13. Available at: http://www.ecom-monitor.com/papers/biometricsTR2000.pdf.

Schaefer, R., Mueller, W. & López, A.M., 2007. Using Smart Cards for Secure and Device Independent User Interfaces. , 07, pp.743–750.

Vanderhoof, R., Smart Card Technology Roadmap for Secure ID Applications Smart Card Alliance. *Agenda*.

Anon, Sensor Technology.

Australian Government, C., 2009. As / Nzs Iso 31000 : 2009. , (August), pp.3–5.

Benantar, M., 2006. *Access Control Systems: Security, Identity Management and Trust Models*, Available at: https://books.google.com/books?id=dpjsXA5SPPwC&pgis=1.

Commission, E., 2010. A Reference Security Management Plan for Energy Infrastructure Prepared by the Harnser Group for the European Commission.

East, N., 1997. Perimeter Security Sensor Technologies Handbook.

Fallis, A.., 2013. No Title No Title. *Journal of Chemical Information and Modeling*, 53(9), pp.1689–1699.

Gaillard, F. & Eieland, A., 2013. Microprocessor (MPU) or Microcontroller (MCU)? *Atmel*, pp.1–2. Available at: http://www.atmel.com/Images/MCU_vs_MPU_Article.pdf.

Gerhard, E., Lorenz, T. & Heiliger, R., 2008. Fiber optic sensor technology. *Biomedizinische Technik. Biomedical engineering*, 44(1-2), pp.25–30. Available at: http://www.ncbi.nlm.nih.gov/pubmed/10194882.

Gordon, L. a. & Loeb, M.P., 2002. The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4), pp.438–457.

ISO - The International Organization for Standardization, 2009. ISO 31000:2009 - Risk management - Principles and guidelines. *Iso 31000:2009*, 2009, p.24.

Jain, R., 2004. Abstract : Keyword : Table of Contents : 2-Application Fields for Biometrics Technology. , (Id), pp.1–10.

Karabacak, B. & Sogukpinar, I., 2006. A quantitative method for ISO 17799 gap analysis. *Computers and Security*, 25(6), pp.413–419.

Karabacak, B. & Sogukpinar, I., 2005. ISRAM: information security risk analysis method. *Computers & Security*, 24(2), pp.147–159.

Karygiannis, T., Eydt, B. & Barber, G., 2007. Guidelines for securing radio frequency identification (RFID) systems. *NIST Special* …. Available at: http://www.fali.unsri.ac.id/userfiles/SP800-98_RFID-2007.pdf.

Orság, F. & Drahanský, M., Biometric Security Systems : Fingerprint and Speech Technology Design of Biometric Security System.

Portability, H.I., 2007. Security Topics 1. *Risk Management*, 2, pp.1–20.

Protocols, S., 2006. Security Issues in RFID Systems RFID Systems tag. *Security*.

Republic, C., 2002. Biometric Authentication — Security and Usability. *Advanced communications and multimedia security IFIP TC6TC11 Sixth Joint Working Conference on Communications and Multimedia Security September 2627 2002 Portorož Slovenia*, 100, pp.1–13. Available at: http://www.ecom-monitor.com/papers/biometricsTR2000.pdf.

Schaefer, R., Mueller, W. & López, A.M., 2007. Using Smart Cards for Secure and Device Independent User Interfaces. , 07, pp.743–750.

Vanderhoof, R., Smart Card Technology Roadmap for Secure ID Applications Smart Card Alliance. *Agenda*.

Anon, Sensor Technology.

Australian Government, C., 2009. As / Nzs Iso 31000 : 2009. , (August), pp.3–5.

Benantar, M., 2006. *Access Control Systems: Security, Identity Management and Trust Models*, Available at: https://books.google.com/books?id=dpjsXA5SPPwC&pgis=1.

Commission, E., 2010. A Reference Security Management Plan for Energy Infrastructure Prepared by the Harnser Group for the European Commission.

East, N., 1997. Perimeter Security Sensor Technologies Handbook.

Fallis, A.., 2013. No Title No Title. *Journal of Chemical Information and Modeling*, 53(9), pp.1689–1699.

Gaillard, F. & Eieland, A., 2013. Microprocessor (MPU) or Microcontroller (MCU)? *Atmel*, pp.1–2. Available at: http://www.atmel.com/Images/MCU_vs_MPU_Article.pdf.

Gerhard, E., Lorenz, T. & Heiliger, R., 2008. Fiber optic sensor technology. *Biomedizinische Technik. Biomedical engineering*, 44(1-2), pp.25–30. Available at: http://www.ncbi.nlm.nih.gov/pubmed/10194882.

Gordon, L. a. & Loeb, M.P., 2002. The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4), pp.438–457.

ISO - The International Organization for Standardization, 2009. ISO 31000:2009 - Risk management - Principles and guidelines. *Iso 31000:2009*, 2009, p.24.

Jain, R., 2004. Abstract : Keyword : Table of Contents : 2-Application Fields for Biometrics Technology. , (Id), pp.1–10.

Karabacak, B. & Sogukpinar, I., 2006. A quantitative method for ISO 17799 gap analysis. *Computers and Security*, 25(6), pp.413–419.

Karabacak, B. & Sogukpinar, I., 2005. ISRAM: information security risk analysis method. *Computers & Security*, 24(2), pp.147–159.

Karygiannis, T., Eydt, B. & Barber, G., 2007. Guidelines for securing radio frequency identification (RFID) systems. *NIST Special* .... Available at: http://www.fali.unsri.ac.id/userfiles/SP800-98_RFID-2007.pdf.

Orság, F. & Drahanský, M., Biometric Security Systems : Fingerprint and Speech Technology Design of Biometric Security System.

Portability, H.I., 2007. Security Topics 1. *Risk Management*, 2, pp.1–20.

Protocols, S., 2006. Security Issues in RFID Systems RFID Systems tag. *Security*.

Republic, C., 2002. Biometric Authentication — Security and Usability. *Advanced* *communications and multimedia security IFIP TC6TC11 Sixth Joint Working Conference on Communications and Multimedia Security September 2627 2002 Portorož Slovenia*, 100, pp.1–13. Available at: http://www.ecom-monitor.com/papers/biometricsTR2000.pdf.

Schaefer, R., Mueller, W. & López, A.M., 2007. Using Smart Cards for Secure and Device Independent User Interfaces. , 07, pp.743–750.

Vanderhoof, R., Smart Card Technology Roadmap for Secure ID Applications Smart Card Alliance. *Agenda*.

Allen, L., Heriyanto, T. & Ali, S., 2014a. *Kali Linux – Assuring Security by Penetration Testing*, Available at: http://linkinghub.elsevier.com/retrieve/pii/S1353485814700777.

Allen, L., Heriyanto, T. & Ali, S., 2014b. Kali Linux – Assuring Security by Penetration Testing. *Network Security*, 2014(August), p.4. Available at: http://linkinghub.elsevier.com/retrieve/pii/S1353485814700777.

Ching, K.W. & Singh, M.M., 2016. Wearable Technology Devices Security and Privacy Vulnerability Analysis. *International Journal of Network Security & Its Applications*, 8(3), pp.19–30. Available at: http://aircconline.com/ijnsa/V8N3/8316ijnsa02.pdf.

Durumeric, Z., Wustrow, E. & Halderman, J.A., 2013. ZMap: Fast Internet-wide Scanning and Its Security Applications. *Proceedings of the 22nd USENIX Security Symposium*, (August), pp.605–619. Available at: https://zmap.io/paper.pdf.

Hunt, A., Raspberry MoCA : an Automated Penetration Platform.

Hutchens, J., 2014. *Kali Linux Network Scanning Cookbook*,

Internet, H.W.A., 2007. a S Urvey of I Ntegrating. *Communications*, 6(3), pp.14–30.

Reeves, S., 14AD. InfoSec Reading Room. *Information Security*, (Vm), p.9.

Williams, M.G., 2015. A Risk Assessment on Raspberry PI using NIST Standards. , 15(6), pp.22–30.

APPENDICES

1. Guideline Risk Assessment Content In Process Phase For Low Capacity Device

1.1. Introduction of guideline

"Material that supplements the content of the paper, but would be distracting or inappropriate to include in the body of the paper is to be placed in an appendix." This includes "materials that are relatively brief and that are easily presented in print format" (*Publication Manual of the APA*, section 2.13). In this section, the material that was used in the research is low capacity device that contained low storage and has a low price in the market such as Beaglebone, Arduino and Raspberry Pi. It is widely used in technology related to Internet of Things (IoT). This study was carried out to produce a guidance that relates to ISO Standard because of there has no detail content relate to low capacity device in ISO Standard document and low capacity device in this case is focuses on Raspberry Pi. ISO that was used is ISO 31000:2009. It is proposed that ISO 31000:2009 be used to orchestrate hazard administration forms in existing and future models. It gives a typical methodology in backing of models managing particular dangers and/or segments, and does not supplant those gauges. ISO 31000:2009 is not planned with the end goal of confirmation. ISO is utilized due to its wide use all through the around the world.

1.2. Risk Assessment

Risk assessment is a procedure that is utilized to contrast hazard investigation results and hazard criteria keeping in mind the end goal to figure out if or not a predetermined level of danger is satisfactory or bearable. As such, hazard assessment is determination of danger administration needs through foundation of subjective and/or quantitative connections amongst advantages and related dangers. In ISO 31000:2009, risk assessment is provided in process phase form. Building up the connection characterizes the extension for the danger administration process and sets the criteria against which the dangers will be surveyed.

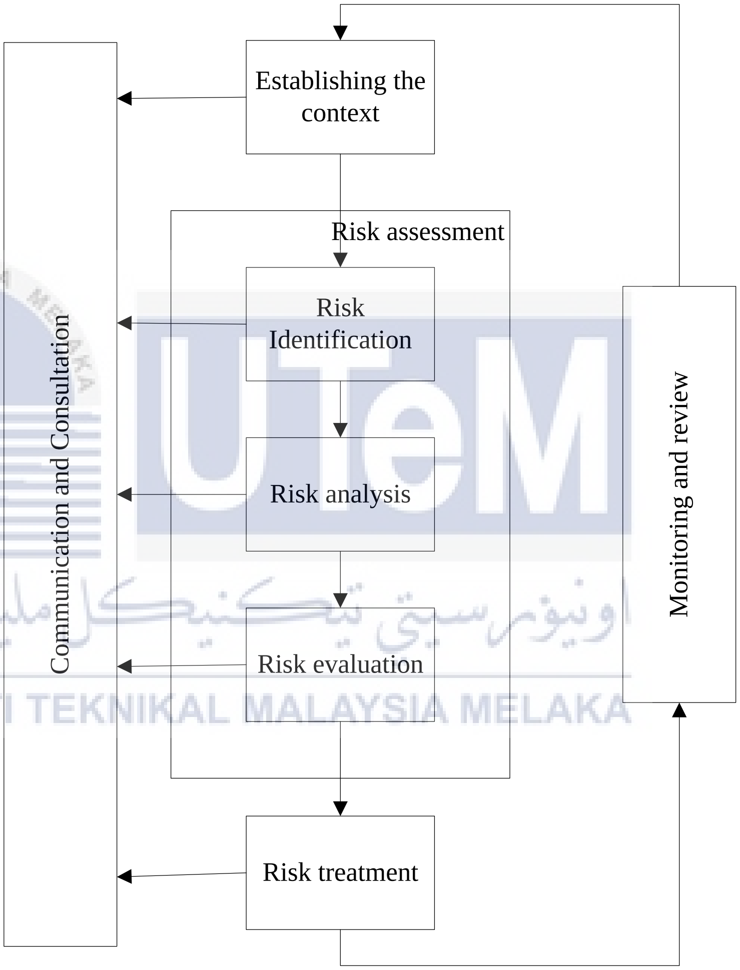


Figure 19: Process phase for risk assessment based on ISO (ISO - The International Organization for Standardization 2009)

In this process phase, this research was more focusing more on content for low capacity device which is in process phase risk assessment area that contained risk identification, risk analysis and risk evaluation. These three processes will be leading this research until finished.

1.2.1. Risk Identification

The objective of risk identification is to identify all possible risks, not to eliminate risks from consideration or to develop solutions for mitigating risks—those functions are carried out during the risk assessment and risk mitigation steps. Based on from research through experiment and based from previous work, risk will be identify in this section which is through testing in scanning port and vulnerability testing.

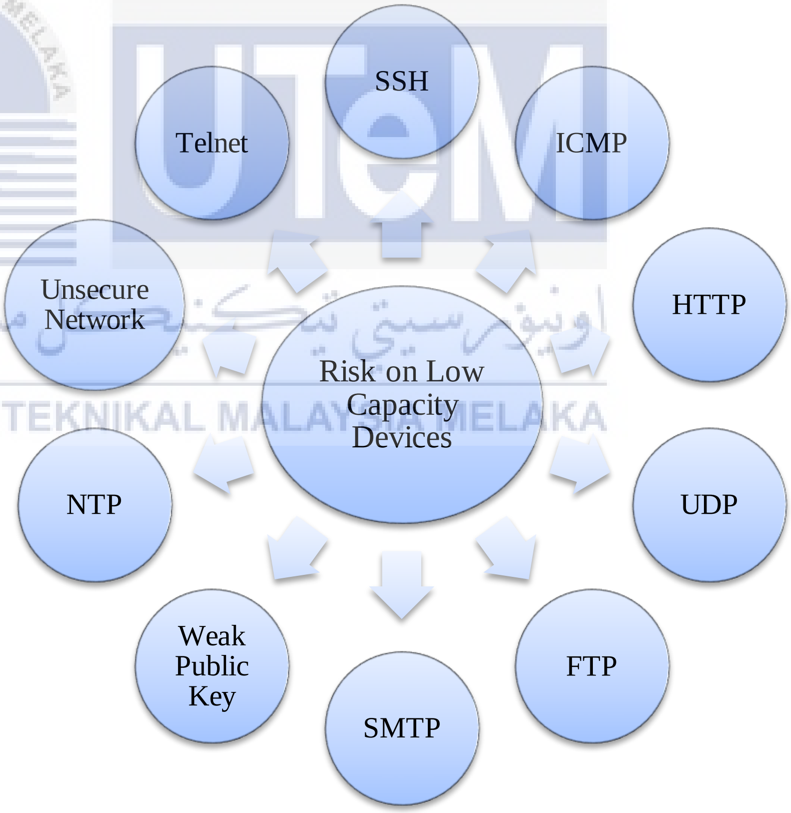


Figure 20: Summarize of risk

Figure 2 above shows summarize of risks after all the result had been produced. These are the result after been identifying from the testing and based from research from another journal.

1.2.2. Risk Analysis

In risk analysis, the risk would be analyze and classify according to frequency occurrence. This area clarifies the frequency occurrence into three levels (high, medium and low) utilized as a part of the report. These levels ought to obviously separate and highlight the specialized security presentation as far as seriousness. In this research, the level of risks is based on the higher the level depends on the frequency occurrence on low capacity device.

Table 5: Level of risks

Level of Risk	**Risks**
Low (Frequency Occurrence– 1)	Unsecure Network, NTP, Weak Public Key
Medium (Frequency Occurrence– 2-3)	Telnet, SMTP, FTP
High (Frequency Occurrence- 4-5)	SSH, ICMP, HTTP, UDP

Table 1 above shows the level of risk according to frequency occurrence in research result. For low level, the frequency occurrence is 1 and it usually happened for unsecure network, NTP and weak public key. For the medium level, it usually occurs in 2 until 3 times that are telnet, SMTP and FTP. For the high level, the frequency occurrence is happened between 4 until which are SSH, ICMP, HTTP and UDP.

1.2.3. Risk Evaluation

In risk evaluation, risk will be evaluated by using SPSS. This evaluation is to aim the correlation between the scanning ports and vulnerability test that more influence to risk on low capacity device.

Table 6: Value for variable

Variable	Cronbach's Alpha value
Scan Port	.752
Vulnerability scan	.752

From Table 2, Cronbach’s Alpha value for scan port and vulnerability scan are .752 respectively. This is the result for item analysis using Cronbach’s Alpha. The value means both of the variable is accepted to continue the process for using in correlation process.

Table 7: Non-Parametric Correlations

Correlations

			ScanPort	Vulnerability	RiskofLCD
Spearman's rho	ScanPort	Correlation Coefficient	1.000	.699*	.779**
		Sig. (2-tailed)	.	.017	.005
		N	11	11	11
	Vulnerability	Correlation Coefficient	.699*	1.000	.991**
		Sig. (2-tailed)	.017	.	.000
		N	11	11	11
	RiskofLCD	Correlation Coefficient	.779**	.991**	1.000

	Sig. (2-tailed)	.005	.000	.
	N	11	11	11

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

From table 3, Site vulnerability scan is significantly correlated with scan port but very strong with .991** other than result in scan port which is .699*. The value in vulnerability is bigger than value in scan port and for the conclusion; it is proven that vulnerability scan is more risky towards risk on low capacity device.

From the evaluation process, we can say that focusing on the high risk especially it is high risk for low capacity device. This risk need to be in high consideration to put on the product. After the high risk been recognizing, the counter measure for all risk will be listed.

Table 8: List of counter measure according to risk

List of high risks	**Counter Measure**	**Citation**
SSH	• Through middlemen • Switch to Pure Key-based Authentication	• (Sebastian,Grenville,Philip 2007)
ICMP	• Loki, which tunneled data in the payload of ICMP echo messages. • Zelenchuk implemented an indirect IP over ICMP tunnel	• (Sebastian,Grenville,Philip 2007)
HTTP	• Transfer the risk	• (Allen et al. 2014b)

	- Implementing and enforcing a policy directive that forbids the use of protocols with known susceptibilities to eavesdropping	
UDP	- Proposed using its presence or absence to signal one bit of covert information per UDP packet	- (Sebastian,Grenville,Philip 2007)

This section is about the list of risk that categorized as high level above. Because of the vulnerability is too risky to low capacity device, the counter measure has been listed to overcome the risk in vulnerability that can reduce any harmful to low capacity device. This list is also included the author to make another researcher easy to search the journal.

LIST OF ABBREVIATIONS

SSH	-	Secure Shell
ICMP	-	Internet Control Message Protocol
FTP	-	File Transfer Protocol
TCP	-	Transmission Control Protocol
UDP	-	User Datagram Protocol
NTP	-	Network Time Protocol
ISO	-	International Organization for Standardization
HTTP	-	Hypertext Transfer Protocol
SMTP	-	Simple Mail Transfer Protocol
IP	-	Internet Protocol
SPSS	-	Statistical Package for the Social Science