

**UNIVERSITI TEKNOLOGI MARA**

**LOW COST NETWORK  
PENETRATION DEVICE USING  
RASPBERRY PI**

**ADAM BIN IBRAHIM**

Dissertation submitted in partial fulfillment of the  
requirements for the degree of  
**Master of Science in Telecommunication and  
Information Engineering**

**Faculty of Electrical Engineering**

July 2015

## **ABSTRACT**

Network penetration testing basically known as the proses of actively and systematically testing a deployed network in order to determine the security weakness of the network and what vulnerabilities may be present. Based on the penetration test report, the action can be taken to mitigate or resolve the vulnerabilities of the network. The portable penetration device are quiet costly and penetration tester commonly use a laptop with Kali Linux installed to performed the test in order to save cost without purchasing any portable penetration device. This paper presented how to setup the low cost penetration device by using Raspberry Pi and Kali Linux. By installing Kali Linux at the Raspberry Pi board, a simple penetration test is being conducted with virtual penetration lab that have been created by using GNS3 and verified that Raspberry pi with Kali Linux are suitable acting as penetration device. This experiment also shown the performance between Raspberry Pi and Laptop are quiet similar in term of scanning time of Nmap tool when performing Discovery Scanning, Port Scanning, Fingerprinting and Vulnerability Scanning.

## **ACKNOWLEDGEMENTS**

I would like to gratefully and sincerely thank Prof.Madya Dr Mat Ikram Bin Yusof for his guidance, understanding, patience, and most importantly, his friendship during my studies at UiTM.

Finally, I would like to thanks to my wife and family for supporting me during my studies and during the time to finish this project successfully. With their support and encouragement, I can able to finish my Master successfully even a lot of barriers and difficultness during my Master.

## TABLE OF CONTENTS

<b>ABSTRACT</b>	<b>I</b>
<b>ACKNOWLEDGEMENTS</b>	<b>II</b>
<b>LIST OF TABLES</b>	<b>V</b>
<b>LIST OF FIGURES</b>	<b>VI</b>
<b>CHAPTER ONE: INTRODUCTION</b>	<b>1</b>
1.1 Project Background	1
1.2 Problem Statement	3
1.3 Objectives Of The Study	3
1.4 Scope Of The Study	4
1.5 Structure Of The Thesis	4
<b>CHAPTER TWO: LITERATURE REVIEW</b>	<b>5</b>
2.1 Raspberry Pi	5
2.1.1 History Of Raspberry Pi	5
2.1.2 Hardware Of Raspberry Pi	7
2.2 Kali Linux	10
2.2.1 History Of Kali Linux	11
2.2.2 Kali Linux Tool Categories	11
2.3 Nmap Tool	13
2.4 Ettercap Tool	15
2.5 Related Research Based On Raspberry Pi	19
<b>CHAPTER THREE: RESEARCH METHODOLOGY</b>	<b>21</b>
3.1 Installing Kali Linux On Raspberry Pi As Operating System	21

3.2	Creating Virtual Lab Using Gns3 And Virtualbox	24
3.3	Network Scanning And Man In The Middle Attack	27
3.3.1	Discovery Scanning	27
3.3.2	Port Scanning	28
3.3.3	Udp Scanning	28
3.3.4	Tcp Scanning	29
3.3.5	Fingerprinting	30
3.4	Man In The Middle Attack	32
<b>CHAPTER FOUR: RESULT AND DISCUSSION</b>		<b>33</b>
4.1	Network Scanning Result	33
4.1.1	Discovery Scanning	33
4.1.2	Port Scanning	36
4.1.3	Fingerprinting	38
4.2	Man In The Middle Attack	40
<b>CHAPTER FIVE: CONCLUSION AND FUTURE WORK</b>		<b>42</b>
5.1	Conclusion	42
5.2	Future Work	42
<b>REFERENCES</b>		<b>43</b>
<b>APPENDIX A</b>		<b>2</b>