

UNIVERSITI TEKNOLOGI MARA

**SECURITY POSTURE ASSESSMENT FOR
SHAPADU CORPORATION SDN.BHD**

EDIWARMAN BIN MOHAMAD TAHER

IT Project submitted in partial fulfilment
of the requirements for the degree of

Master of Science (Information Technology)

Faculty of Computer and Mathematical Sciences

July 2013

ABSTRACT

Information is the critical asset of any organizations. Data captured, recorded and shared every day is the heartbeat of an organization to secure its relationships with vendors and customers, as well as the foundation for its internal operations and business processes. Having specific, relevant and correct information can make a huge difference to an organization's efficiency as its survival. To protect the information from misuse, abuse and destruction, organizations are willing to spend on technical solutions and comprehensive monitoring tools. However, organizations will still be at risk if they are unable to perform any security assessment of their infrastructure especially on their network, system, application and its infrastructure. The purpose of this study is to identify any vulnerability that may arise in external or internal of Shapadu Corporation Sdn. Bhd's premise. This study also proposes method and technique in order to perform vulnerability assessment and host assessment. The implementation tool has been used in the experimental design which is Nessus scanner. The outcome of this study is a result of the finding, analysis and the recommendation that can be used to rectify the vulnerability and issue in order to ensure ICT infrastructure is secured and to avoid a malevolent individual from exploit vulnerability or execute a denial of service attack to Shapadu Corporation's ICT infrastructure.

ACKNOWLEDGEMENT

Alhamdulillah. My foremost gratitude to Allah for giving me the strength, guidance and will to complete the dissertation. Special thanks to my dearest supervisor Dr. Fakariah Hani Hj Mohd Ali and En. Shamsudin Md Sarif for the patience and guidance in showing the right way of doing the IT Project. Thank you also to Dr. Wan Adilah Wan Adnan the coordinator for IT Project (SYS798). Not to forget, my beloved family members; wife and parents as well as my colleagues for their motivation, support and prayers throughout the process. May Allah grant all of you happiness and prosperity in this world and hereafter.

TABLE OF CONTENTS

	Page	
STUDENT'S DECLARATION	i	
ABSTRACT	ii	
ACKNOWLEDGEMENT	iii	
TABLE OF CONTENTS	iv	
LIST OF TABLES	viii	
LIST OF FIGURES	ix	
CHAPTER ONE: INTRODUCTION		
1.1	Background	1
1.2	Problem Statement	2
1.3	Research Questions	3
1.4	Objectives	4
1.5	Significance	4
1.6	Project Scope	5
	1.6.1 Vulnerability Assessment	5
	1.6.2 Host Assessment	5
1.7	Report Outline	6
CHAPTER TWO: LITERATURE REVIEW		
2.1	Introduction	7
2.2	Computer and Information Security	7
	2.2.1 Confidentiality	9
	2.2.2 Integrity	9
	2.2.3 Availability	9
2.3	Type of Vulnerability and Threat	10
2.4	Incident of Vulnerabilities in Malaysia	11
2.5	Security Tools	12
	2.5.1 Port Scanner	12
	2.5.2 Vulnerability Scanner	13
	2.5.3 Password Cracker	13

2.5.4	Intrusion Prevention System (IPS)	13
2.5.5	Intrusion Detection System (IDS)	13
2.5.6	Firewall	14
2.6	Security Posture Assessment	14
2.6.1	Method of Security Posture Assessment	15
2.6.2	Type of Security Posture Assessment	17
2.6.2.1	Vulnerability Assessment (VA) is scanning a group of hosts or network for known vulnerable service.	17
2.6.2.2	Host Assessment	18
2.6.3	Scope of Security Posture Assessment	20
2.7	Vulnerability Scanning Tool	20
2.8	How is a Security Posture Assessment Different from a Security Audit	22
2.9	Related Works	23
2.10	Summary	30

CHAPTER THREE: METHODOLOGY

3.1	Introduction	31
3.2	Project Methodology Framework	31
3.2.1	Information Gathering and Planning Phase	33
3.2.2	Vulnerability Assessment	34
3.2.3	Host Assessment	34
3.2.4	Analysis and Findings	35
3.2.5	Documentation	35
3.3	Experimental Design of Vulnerability Assessment	36
3.3.1	Vulnerability Assessment Definition	36
3.3.2	Scope of Assessment	38
3.3.3	Expected Vulnerability	39
3.3.4	Expected Results	41
3.4	Experimental Design of Host Assessment	42
3.4.1	Host Assessment	43
3.4.2	Scope of Assessment	43
3.4.3	Expected Vulnerability	46