

BORANG PENGESAHAN STATUS TESIS

JUDUL: UTeM Security Audit via Penetration Testing

SESI PENGAJIAN: - 2007/2008

Saya MOHD NABIL BIN CHE ZAM FADZILAH mengaku membenarkan tesis PSM ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalah hakmilik Kolej Universiti Teknikal Kebangsaan Malaysia.
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)

X/ TERHAD (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

_____ TIDAK TERHAD



(TANDATANGAN PENULIS)

Alamat Tetap: No 6, Jln Kelab Ukay 11
Tmn Kelab Ukay, 68000 Ampang.

Selangor D.E

Tarikh: 2/05/2007



(TANDATANGAN PENYELIA)

Prof. Dr. Shahrin bin Sahibuddin @ Sahib

Tarikh: 2/05/2007

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

UTeM SECURITY AUDIT via PENETRATION TESTING

MOHD NABIL B. CHE ZAM FADZILAH

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


**FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA**

DECLARATION


I hereby declare that this project report entitled
UTeM SECURITY AUDIT via PENETRATION TESTING

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

STUDENT

:  _____ Date: 2/05/08
(MOHD NABIL B. CHE ZAM FADZILAH)

SUPERVISOR

: ^{10/p}  _____ Date: 2/5/08
(Prof. Dr SHAHRIN SAHIBUDIN @ SAHIB)

DEDICATION

To my beloved mom, dad and my family, you meant world to me.

To my friends, thanks for supporting me on this

ACKNOWLEDGEMENTS

Bismillahirrahmannirrahim.

Firstly, Alhamdulillah and Thank You Allah S.W.T that finally I have completed my PSM II.

I would like to take this opportunity to thank my PSM supervisor, Prof.Dr. Shahrin Sahabudin for his guidance throughout the period of PSM. I am much appreciating his assistance and all the valuable knowledge provided in helping me to complete the documentation.

Special acknowledgement and appreciation to my parents, Che Zam Fadzilah bin Abd. Kahar and Norsiah bte Mohd Nor and not forgetful to my adored family members for their moral support, full understanding and patience to be completion of my final year project.

Finally, I wish to thank to my work partner, classmate and all friends for their cooperation, comments, advised contribution and support. I also express my deep gratitude to those who directly or indirectly helped me in completing this PSM documentation.

May ALLAH S.W.T always bless you.Wassalam.

Thank you.

ABSTRACT

Penetration testing is a one of the technique that being used to evaluate network security posture installed in organizations. The idea is to execute penetration testing here in UTeM. A person who wanted to execute the testing must equip himself/herself with large knowledge on computer network and security in order to smooth the works while avoiding committing computer crime. Contribution, project strength and weakness and also improvement after executing the task are included in conclusion area.

ABSTRAK

Penetration Testing merupakan salah satu teknik yang digunakan untuk menilai tahap keselamatan rangkaian di sesebuah organisasi. Setiap bab mengkhususkan kepada pengkelasan yang tersendiri. Kekuatan dan kelemahan projek dapat dirumuskan pada bab terakhir (rumusan). Selain dari kekuatan dan kelemahan, sumbangan serta pembaikan dapat disertakan pada akhir bab. *Penetration Testing* mengkehendaki seseorang itu mempunyai kebolehan serta pengetahuan dalam bidang keselamatan dan rangkaian bagi memudahkan kerja serta mengelakkan insiden-insiden yang melibatkan jenayah perkomputeran.

TABLE OF CONTENTS

CHAPTER	SUBJECT	PAGE
	DECLARATION	i
	DEDICATION	ii
	ACKNOWLEDGEMENTS	iii
	ABSTRACT	iv
	ABSTRAK	v
	TABLE OF CONTENTS	vi
	LIST OF TABLES	x
	LIST OF FIGURES	xi
CHAPTER I	INTRODUCTION	
	1.1 Project Background	1
	1.2 Problem Statement	2
	1.3 Objective	2
	1.4 Scopes	3
	1.5 Project Significance	3
	1.6 Expected Output	4
	1.7 Conclusion	4
CHAPTER II	LITERATURE REVIEW AND PROJECT METHODOLOGY	
	2.1 Introduction	5
	2.2 Fact and Finding	6
	2.2.1 Domain	8
	2.2.2 Existing Method	10

2.2.3 Technique	11
2.3 Project Methodology	12
2.4 Project Requirement	16
2.4.1 Software Requirements	16
2.4.2 Hardware Requirements	20
2.4.3 Other Requirements	20
2.5 Project Schedule and Milestones	21
2.6 Conclusion	22
CHAPTER III ANALYSIS	
3.1 Introduction	23
3.2 Problem Analysis	24
3.3 Requirement Analysis	25
3.4 Conclusion	27
CHAPTER IV DESIGN	
4.1 Introduction	28
4.2 Network Architecture	29
4.3 Logical Design	31
4.3.1 Planning Stage	31
4.3.2 Reconnaissance	32
4.3.3 Scanning	33
4.3.4 Verify Vulnerabilities	34
4.3.5 Gaining Access	34
4.3.6 Clearing Track	35
4.3.7 Prepare and Delivering reports	36
4.4 Physical Design	38
4.5 Conclusion	39
CHAPTER V IMPLEMENTATION	
5.1 Introduction	40
5.2 Detail Design	41
5.2.1 Reconnaissance	41

5.2.1.1 Intelligence Gathering	42
5.2.1.2 Footprinting	48
5.2.1.3 Verification	23
5.2.2 Enumeration	58
5.2.2.1 Fingerprinting	60
5.2.2.2 Web Site Enumeration	69
5.2.3 Gaining Access	71
5.2.3.1 RPC Access	71
5.2.3.2 Email Forging	74
5.2.3.3 FTP Attack	76
5.3 Conclusion	77

CHAPTER VI COUNTERMEASURES

6.1 Introduction	78
6.2 Classes of Countermeasures	79
6.2.1 OS Security Issue	79
6.2.1.1 LM vs NTLM	79
6.2.2 Web Server Security	90
6.2.2.1 SQL Injection Attack	94
6.2.2.2 Email Security	98
6.2.2.3 Lockdown Policy	100
6.2.2.4 Other Web Server Security Issues	101
6.2.3 General Security Issues	102
6.2.3.1 Perimeter Security	102
6.2.3.2 Password Policy	102
6.2.3.3 Other Issues	103
6.3 Conclusion	104

CHAPTER VII PROJECT CONCLUSION

7.1 Observation on Weaknesses and Strengths	105
7.2 Propositions for Improvement	108
7.3 Contribution	109
7.4 Conclusion	109

REFERENCES**110****APPENDICES****112**

LIST OF TABLES

TABLE	TITLE	PAGE
2.1	The Most Critical Cyber Security Threats	7
2.2	Future Cyber Security Threats	7
2.3	Project Schedule	21
4.1	Banner Grabber Info	31
5.1	Different type of DNS Records	53
5.2	nmap options and scan type	58
5.3	Default TTL value	61
5.4	Host with IP address	62

LIST OF FIGURES

FIGURES	TITLE	PAGE
2.1	Methodology	15
3.1	Banner Grabber	26
4.1	WHOIS UTeM	30
4.2	Testing Steps	37
4.3	Outside Penetration Testing	38
5.1	Google search for “UTeM”	42
5.2	Kart00 result for www.utem.edu.my	43
5.3	Kart00 result for Universiti Teknikal Malaysia Melaka	44
5.4	Kart00 result for UTeM	44
5.5	nslookup for www.utem.edu.my	46
5.6	Whois lookup for www.utem.edu.my	46
5.7	Primay and secondary name server for UTeM	47
5.8	Netcraft on www.utem.edu.my	47
5.9	Mail sent to non-existing-user@utem.edu.my	49
5.10	Mail bounce with IP address (10.1.3.10)	49
5.11	Result for <i>host -l utem.edu.my</i>	50
5.12	Result for <i>host -t ns utem.edu.my</i>	51
5.13	Result fot <i>host -t mx utem.edu.my</i>	52
5.14	Result for <i>dig utem.edu.my MX</i>	52
5.15	nmap with ICMP ping scan	54
5.16	Hostname www.utem.edu.my	55
5.17	IP address http://58.139.248.103	56
5.18	<i>ping</i> command on 10.1.3.10	63
5.19	smtp.utem.edu.my OS type	64
5.20	kutkm.edu.my OS type	64

5.21	kutkm05.kutkm.edu.my OS type	65
5.22	utem10.utem.edu.my OS type	65
5.23	kutkm13.kutkm.edu.my OS type	66
5.24	kutkm22.kutkm.edu.my OS type	66
5.25	Kutkm14.kutkm.edu.my OS type	67
5.26	Utem21.utem.edu.my OS type	67
5.27	Gallery.utem.edu.my OS type	68
5.28	Mysql.utem.edu.my OS type	68
5.29	Banner Grabber on http://www.utem.edu.my	89
5.30	Banner Grabber on http://portal.utem.edu.my	70
5.31	Banner Grabber on http://eftmk.utem.edu.my	70
5.32	IPC shares	72
5.33	Net view failed	73
5.34	Null Session established	73
5.35	Net view success	74
5.36	Attempting an email forging	75
5.37	FTP sites	76
5.38	FTP browsing	77
6.1	LM to NTLM	80
6.2	DontDisplayLastUserName registry value	82
6.3	Setting new minimum password length	83
6.4	Minimum password length	83
6.5	Disable password caching	84
6.6	Disabling Internet Password cache	85
6.7	DisablePasswordCache value	86
6.8	Enforced login authentication	87
6.9	ForceUnlockLogon DWORD value	87
6.10	Disabling registry tools	88
6.11	DisableRegistryTools value	89
6.12	New Virus signatures distributed	90
6.13	http://eftmk.utem.edu.my	91
6.14	eftmk databases	91
6.15	Log on http://eftmk.utem.edu.my	92
6.16	No password for root access	92

6.17	Tables name give hint	93
6.18	Username&Password	93
6.19	SQL statement	95
6.20	Overwrite SQL statement	96
6.21	Executed SQL statement	96
6.22	Administrator SQL command	97
6.23	Executed administrator SQL query	97
6.24	Email checking status prompt	99
6.25	Email status	99
6.26	MyNIC contacts	104

CHAPTER I

INTRODUCTION

1.1 Project Background

All the organization is encouraged to execute penetration testing because of penetration testing is proved to be an excellent ways to discovered network weaknesses. Currently, penetration testing is not implemented widely because of many organization did not realize how important the test is and scared of critical information will be leaking out during the test.

Normally, network security policies are implemented solely based on network administrator knowledge. It is possible sometimes network administrator missed something important and as a result, it may jeopardize organization critical information because of there is too many burden on administrators that must be carried out. So there must be a person who is specializing on discovered network weakness and once again it is important to execute penetration testing.

SLA (Service Level Agreement) is a contract agreement that describes the terms of the penetration testing will be executed must be signed by the organization and by signing the agreement, penetration tester given approval to execute the test. This approval is a must because the nature of penetration testing, failure to get this approval might result in committing computer crime, despite the best intentions. Countermeasures will be recommended right after completing the test based on weaknesses and vulnerabilities for organization acknowledgement.

1.2 Problem Statements

When there are problems, there must be solutions and there must be statements that encourage penetration testing to be executed. The problems are:

- Security weakness in a Target of Evaluation (ToE) due to failures in analysis, design implementation or operation
- Weakness in an information system or component (e.g system security procedures, hardware design or internal controls) that could be exploited to produce information misfortune
- Vulnerability in the presence of a weakness, design or implementation error that can cause unexpected and desirable event and jeopardize the security of a system, network, applications or protocols
- Security policies implemented to certain organization usually based on the needs and also administrator knowledge and possibly missed something important and maybe some critical policies.

1.3 Objectives

The major objective of Penetration testing is to address vulnerabilities before they can be utilized by unauthorized individual and the objectives of implementing the testing here in UTeM are:

- To improve UTeM network security
By executing penetration testing, penetration tester may discover vulnerabilities that missed by administrator and new approach will be implemented based on discovered vulnerabilities.
- Discover UTeM network vulnerabilities and weakness
Pentest is aim to discover network vulnerabilities and weakness and by doing that, new assessment of vulnerabilities and weaknesses gathered before proceed into actions.

- Re-evaluate UTeM network security policies

Studied current network security policies that implemented in UTeM and verify either current policy is suitable or not based on security triangle that consist of Ease of Use, Security and Functionality.

1.4 Scope

All the penetration testing process will be executed based on certain ranged and the ranges of penetration testing are:

- Internal Network

Penetration testing will be executed from inside the organization itself and performed from several network access points including logical and physical segments

- External Network

Try to penetrate organization from outside and simulate the real-world attack that may happen when someone try to penetrate the organization.

- Wireless Network

Penetration from wireless access points also being executed. The reason to execute Pentest from wireless points is to ensure wireless integrity.

UTeM selected as the subject and all the test will be conducted in controlled environment which mean it will not disrupt UTeM daily business and all the information gathered during the test is confidential.

1.5 Project Significance

UTeM is guaranteed to get the benefits from penetration testing because Pentest is designed to simulate methods that intruders use to gain unauthorized access to an organization and the different between penetration tester and a hacker is their intention to discover vulnerabilities in the network and not to exploits them.

By executing Pentest also proved to it can improve current network security assessment to an organization and after implementing new network security assessment, all the organization confidential information well kept from an intruders for a long times and when the time comes, the information maybe useless and expired. This is because if hacker wants to get inside your system, he will and there nothing you can do about it and the only ways is to make it harder for him to get in.

1.6 Expected Output

The expected output from penetration testing is to bring benefits to UTeM itself based on vulnerabilities gathered and countermeasures provided during the testing period. After implementing new security policies based on provided countermeasure, hopefully it can make UTeM network tougher and harder to penetrate by attacker with any intends to disrupt UTeM networked computer.

Penetration testing also proved to avoid the cost of network downtime. Why am I saying that? It is because recovering from a security breach can cost millions and jeopardize corporate image and customer loyalty if the organization provides internet marketing as their core business.

1.7 Conclusion

As the conclusion, penetration testing can give corporate lots of benefits and all steps involve in PenTest will be list out later. All the devices, software and also hardware with justification are listed out in the next chapter.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

All the software, hardware and other requirement needed will be listed out in order to execute the project here in this chapter. Also in this chapter project methodology and also technique involved will be discuss. The objective of this chapter is to prove and also clarify by doing some research on related topics, citation, and also conclusion.

What literature review mean? Literature review translated in Wikipedia (http://en.wikipedia.org/wiki/Literature_review) as a body of text that aims to review the critical points of current knowledge on a particular topic. According to Cooper (1988) "A literature review uses as its database reports of primary or original scholarship, and does not report new primary scholarship itself. The primary reports used in the literature may be verbal, but in the vast majority of cases reports are written documents. The types of scholarship may be empirical, theoretical, critical/analytic, or methodological in nature. Second a literature review seeks to describe, summarize, evaluate, clarify and/or integrate the content of primary reports".

In order to execute Pentest, the entire requirements, technique involved and current process needs to be identified and also project milestone also being provided in this chapter. This chapter consists of Fact and Finding, Domain, Existing Method /

Process, Project Methodology, Project Requirement, Project Schedule also Conclusion and all of it will be describe in detail later in this chapter.

2.2 Fact and Finding

Fact and Finding is an attempt to discover some argument or citation that support for supporting my final project which is *Security Audit in UTeM via Penetration Testing*.

There are lots of terms associate with Penetration Testing such as according to CoreSecurity (<http://www.coresecurity.com>) Penetration Testing is a “proactive and authorized attempt to compromise network security and access sensitive information by taking advantage of vulnerabilities.” Also, Penetration described in Wikipedia (http://en.wikipedia.org/wiki/Penetration_Testing) as a “method of evaluating the security of a computer system or network by simulating an attack by a malicious user” and commonly the objective of penetration testing is to discover vulnerabilities in network by compromising the network itself. Ethical hacking also identical with Penetration Testing because of it share same objective by meant to impose as and malicious user and try to compromise certain network.

Differentiate between Ethical Hacker/Penetration Tester and Hacker/Cracker is their aim in compromising network. Malicious user aim to exploit founded vulnerabilities into their own goods and compromising network without permission (illegal) but Penetration Tester aims to fix founded vulnerabilities and also have permission plus support in compromising network.

Security Audit described as “A search through a computer system for security problems and vulnerabilities.” by Texas State Library and Archives Commission (<http://www.tsl.state.tx.us/ld/pubs/compsecurity/glossary.html>).

According to Prinya Hom-anek ACIS (Advanced Certified Information Security) Professional Centre Co. Ltd. Thailand on his “The Ten Most Critical Cyber Security Threats 2007” presentation, he has list out the most security threats in the year of 2007 and the future cyber security threats that may happen in the year of 2007-2008. All the threats listed out below:

Table 2.1 – The Most Critical Cyber Security Threats

The Ten Most Critical Cyber Security Threats 2007	
1	Malware attack with Social Engineering Tactics
2	SPAM
3	DoS and DDoS attack
4	Phishing and Pharming (Identity Theft and DNS attack)
5	Botnets
6	IM attack (SPIM) and P2P attack
7	Mobile and Wireless attack (Wi-Fi and Bluetooth)
8	Rootkits
9	Web application attack
10	Hacking with google

Table 2.2 – Future Cyber Security Threats

The Future Cyber Security Threats 2007-2008	
1	Web 2.0 Attack
2	RFID Attack
3	VoIP Attack
4	Web Service and SOA Attack
5	Removable Storage Data Leakage (USB Attack)
6	IP Storage Security Vulnerabilities (iSCSI Attack)
7	Virtualized Exploit/Trojan/RAT Attack (MOSVM)
8	Completely Anonymity:TOR (The Onion Router)
9	Rainbow attack and Zero-Day Attack
10	Critical Infrastructure

Some of the attack featured in the Future Cyber Security Threats already happen such as USB attack and the most popular technique is *Pod Slurping*. iPod has been used as the hacking tool by exploiting the used of it. Beside IPOD, USB modules (USB Drive) also been used as the tools and with the growth of U3 technologies, USB attack (Information Stealing) runs covertly when the device plugged. USB Drive with U3 technologies act as smart drives that enable user to install an application and also execute it known as portable application. If it is use in

a good manner, it was a great technology to implement but hackers always exploits the advantages and turns it into vulnerabilities.

According to NISER (National ICT Security and Emergency Response centre) in January 2007, they have reported that intrusion and fraud as the highest scores collected from organization in Malaysia. This is serious factor because both of them can jeopardize organization that can cause bankruptcy. Also to remind that 80% of intrusion came from inside the organizations probably disgruntle employee and just only 20% of it came from outside and maybe driven by political issues and fame. For sure fraud came from inside the organization itself and commonly involved banking sector.

Based on the fact listed above, there are needs to improve and harden organization network in order to prevent all of tragedy happens that can ruins organization, economy and definitely cost lots of money and one from many ways to do it is by Penetration testing.

2.2.1 Domain

Every organization uses different types of security assessments to validate the level of security on its network resources. Organization needs to choose the assessment method that suite their situations appropriately. Different assessment methods require different skills.

Security audits is one from three assessment method that typically focus on people and processes used to design, implement and manage security on a network. There is baseline involved for processes and policies within an organization. The policies auditor and the organizations security policies and procedures use the specific baseline to audit the organization and usually initiates IT security audits by IT management. There is also IT security audit manual and associated toolset to conduct the audit provided by NIST (National Institute of Standard Technology).

Vulnerability assessment also known as method of assessment besides security audits and also penetration testing. Vulnerability assessments works in

scanning a network for known security weakness. Vulnerability scanners are capable on detecting device configuration including OS versions, IP protocols and TCP/UDP ports that are listening and also applications that are installed on computers. Additionally , vulnerability scanners can detect CVE (common vulnerabilities & exposures) and as and examples, it can identify common security mistakes such as accounts that have weak passwords, weak permissions in file and folder also common security mistakes during configurations in applications. Vulnerability scanners can test systems and network devices for exposures to common attacks but results gather after scanning may includes many false positives.

Penetration testing goes a step beyond vulnerability scanning in the assessments category. Penetration testing assesses the security model of the organization as a whole and reveals the security weakness that a typical vulnerability scanning misses. Besides revealing potential consequences of a real attacker breaking into the network and point out vulnerabilities, it also will document how the weakness can be exploited and how several minor vulnerabilities can be escalated by an attacker to compromise network and computer.

Most vulnerability assessments are carried out solely based on software and cannot assesses security that is not related to technology. Using social engineering, penetration testing practices such as patch management cycles can be evaluated. Once again, it must be pointed out that a penetration tester is differentiated from an attacker only by his intent and lack of malice. Penetration testing helps organizations reach a balance between technical and business functionality from the perspective of potential security breaches. This can help in disaster recovery and business continuity planning. The irony of penetration testing is the fact that the inability to breach a target does not indicate that the absence of vulnerability and even the network is secured 100%, there is no patches for human stupidity which mean that social engineering skills can be applied.

“Security is not a product that can be purchased off the shelf, but consists of policies, people, processes, and technology.”

-www.kevinmitnick.com-