Implementing IT Security Penetration Testing in Higher Education Institute: A Case of University Teknologi MARA (UiTM) Pahang

Zulazeze Sahri
Mohamad Affendi Abdul Malek
Muhd Eizan Shafiq Abd Aziz
Roslan Jamaludin
Roger Canda

ABSTRACT

The higher educational industry has unique information security requirements as the organization holds critical data and information of students, employees, research findings as well as other university's main agenda information. This paper proposed an enhanced process flow for web deployment by implementing IT security penetration testing practices in University Teknologi MARA (UiTM) Pahang, Campus Jengka, as a way to early detection, reduce and prevent the institution's information security and services. This empirical research is based on qualitative data analysis which applied action research and interviews that requires researcher to study the existing university's IT security policy, infrastructure and available services. The development of the penetration testing process flow is guided by various industry standard penetration testing frameworks and literature review.

Keyword: *Penetration Testing, IT Security in UiTM, Computer Security, Hacking*

Introduction

With the increasing importance of information systems in today's complex virtual environment, university's have to perform a higher level of due diligence to ensure the confidentiality, integrity and availability of the customer information and university's IT services. University Teknologi MARA, Campus Jengka is one of Malaysian Government Higher Education Institute located in the state of Pahang, eastern Malaysia. As one of the fast growing university in terms of number of graduated students and latest research developments and findings, the university's holds critical and real time data for its stakeholders such as student information, administration information, research findings and other web applications. Unfortunately, in 2012, a couple of successfully compromised and exploited attacks were reported in the university's server that led to the misuse of the server as the phishing activities (Ibrahim, Personal Interview, 2013). The university's management personnel believed that the attacker could be from internal or external of the target environment. The lack of awareness for securing universities' information and network infrastructure is reported by experts in computer security which agree that, related to computer, universities are among the least secure places in the universe (Foster, 2001). In addition, North et al., (2006) in their research shows that audits of the university security systems reveal a large number of weaknesses. Therefore, the safeguard and prevention of the university's IT infrastructure and services must be enhanced.

In order to prevent and reduce such critical attacks from occur in the future, this paper proposed the implementation of Penetration Testing that can be applied in some of the university's IT infrastructure and services. Penetration testing is the process to find security vulnerabilities in a target environment that could let an attacker penetrate the network or computer systems (Skoudis, 2008). A penetration testing usually conducted by trusted individual which purposely assigned and conducting attack that are similarly used by a real attacker (Wai, 2002). Therefore, the proposed penetration testing processes is believed can achieve the research objectives to minimize security issues in the university's environment by reducing, preventing and safeguard the institution's application and services at early stage.

Literature Review

I. Penetration Testing Defined

Penetration testing is a way to identify vulnerabilities that exists in a system or network that has an existing security measures in place (Wai, 2002). Penetration testing also helps in identifying which vulnerability is exploitable. A penetration testing usually involves the use of attacking methods conducted by trusted individual that are similarly used by hostile intruders or hackers. It means, the penetration tester will 'think like an attacker' and devise test cases which try to break the system's integrity by exposing vulnerabilities such as SQL injection, cross-site scripting and error message information leakage (Austin et al., 2010). The benefits of penetration testing are more than finding and indentifying exploits and vulnerabilities in organization's IT infrastructure and services (Rahmat et al., 2004). It also can helps to confirm whether the current security measures implemented is effective, or not, and also can gives a bird-eye perspective on current and future security level in the organization. The results of these tests or attacks will be documented and presented as a report to the owner of the system and the vulnerabilities found can then be resolved.

Many companies are now offering penetration services to identify vulnerabilities in system and the surrounding process (Moyer, 2001). According to Wai (2002), penetration testing is normally done for two reasons. This is either to increase upper management awareness of security issues or to test intrusion detection and response capabilities. In many industries, a penetration testing has become a required audit (Sans, 2001). It is also become the commodity characterized by the performance of a series of substantive test procedures. Therefore, this statement shows the important of having penetration testing practices in all industries in order to enhance security and prevent attacks. However, recent report by the Malaysian Communications and Multimedia Commission (2011) stated that 91 websites, 51 of which are the government based website and Malaysian university's website has been hacked and defaced by unknown hackers. The question remains unanswered whether or not the educational industry in Malaysia is aware with the penetration testing practice that can help to safeguard and prevent any attacks especially to their website and back-end server.

II. Types of Penetration Testing

The variation of penetration testing can be classified based on the source of information that the test team has been given prior to start a test (Wang & Kou, 2012) and the location which the test is conducted (Rajeev & Eugene, 2001). According to Wang & Kou (2012), there are two types of penetration testing which are internal and external. Internal penetration testing refers to test conducted against host inside the organization's internal network. External penetration testing refers to test conducted against internet facing host. The classification of the test also can be based on the penetration team who conduct the test, whether from internal organization team or conducted by third-party organization. This can be referred as in-house penetration testing and out-source penetration testing. In-house penetration testing is refer as penetration testing activity that conducted by organization's security expert, whereas, the out-source penetration testing is conducted by trusted individual that can be hired from any security based company.

III. Phases in Penetration Testing

Several authors have suggested a common and reliable penetration testing phase's activities. According to Wang & Kou (2012), there are three phases in a penetration testing activities that a tester can use which are Pre-Attack Phase, Attack Phase and Post-Attack Phase, as shown in Figure 1. The pre-test phase involves an attempt to investigate and explore the potential target. Meanwhile, the attack phase involves the actual performing of an attack to the defined target. This activity may exploit logical or physical vulnerabilities. Finally, the post-attack phase focuses on returning any modified system(s) to the pretest state. In addition, Wai (2012) has recommend a detail penetration process to support the three general phases by Wang & Kou (2012) which covers Planning and Preparation, Information Gathering and Analysis, Vulnerability Detection, Penetration Attempt, Analysis and Reporting and Cleaning Up. Figure 2 illustrates the penetration process suggested by Wai (2012).

Figure 1: The three phases in a penetration testing by Wang & Kou (2012)

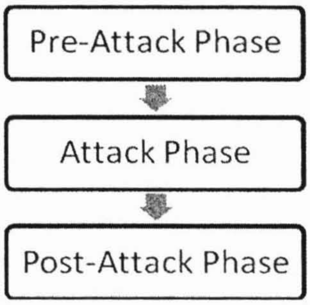
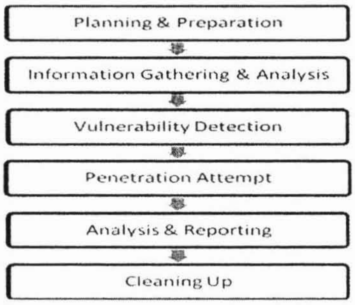


Figure 2: Penetration testing process by Wai (2012)



Similarly, Graves (2007) in his book *'Official Certified Ethical Hacker'* has suggested five phases in penetration testing that hackers generally follow in hacking a system as in Figure 3.

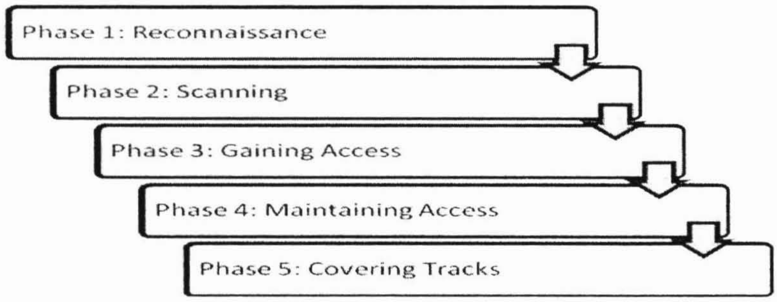


Figure 3: Five phases of penetration testing by Graves (2007)

Generally, reconnaissance involve initial information gathering and analysis of a target machine, then, in phase 2, the information gathered during phase 1 is use to examine the overall network or target system for further action. Gaining access is the phase where the attacker exploits whatever vulnerabilities found in phase 1 and 2 to gain an access. Upon successful attacks require the attacker try to keep that access for future exploitation and attacks. Final phase suggest to cover the attacker track to avoid detection by system owner, to remove evidence of hacking and to avoid legal action.

IV. Major Areas in Penetration Testing

Organization that plan to conduct a penetration testing must have a good preparation concerning the scope and objective of the penetration test (Wai, 2002). The research suggests that understanding major area and scope of the IT infrastructure and available services in the organization that need to test is the first priority in planning the penetration test activities. According to Olson (2010), there are six major areas that penetration testing can be applied namely; network topology, network perimeter device, wireless devices, web-based application, commercial-off the shelf test and In-house developed application test. Meanwhile, Burrows (2002) suggested that penetration testing involve performing reconnaissance scan towards perimeter defenses, boundary routers, firewalls, switches, network devices, servers, and workstation. Understanding the types and major areas in penetration testing is importance in planning and designing the penetration testing model and process flows.

Methodologies

This research employs qualitative data analysis methodologies which has adopted action research and interviews in collecting the required data. Four (4) interviews session has been conducted with the university's network and infrastructure administrator from the Information Technology Unit (InfoTech), who responsible in managing, maintaining and safeguard the overall UiTM Pahang IT infrastructure. The interviews and data collection involves the study of existing university's IT security policy, scope of infrastructure and services managed by InfoTech, attack history, mitigation and incident handling response. The findings will be further discusses in result and discussion section along with the propose penetration testing process and model for the university. The scope of the research is focusing on securing the web application hosted in UiTM Pahang only. This is because UiTM Pahang is one of the branches that have limited access in terms of managing and maintaining overall IT infrastructure and services. Most of the IT infrastructure currently managed centralizes by the main campus Information Technology Division in UiTM Shah Alam, Malaysia. Figure 4 illustrates the scope of penetration testing in this research.

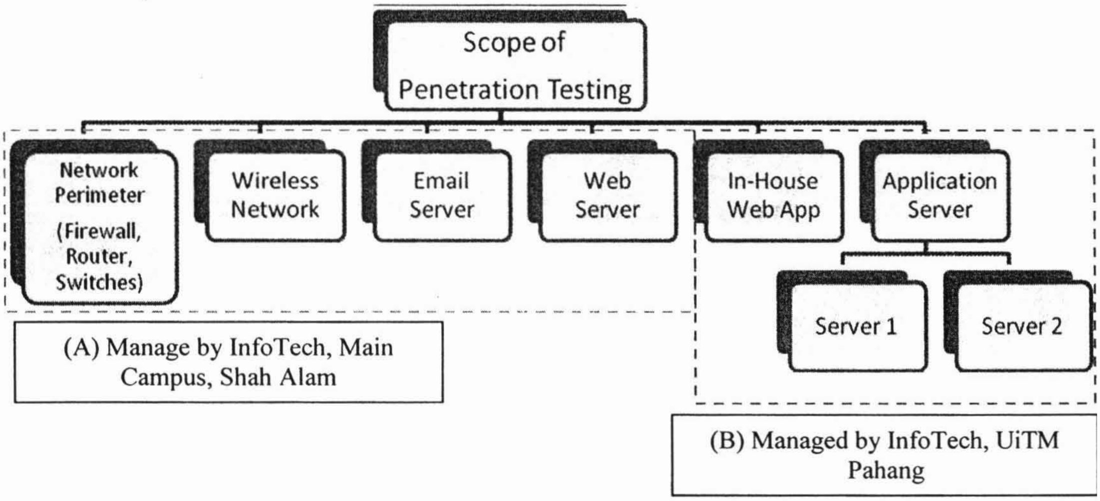

Scope of Penetration Testing
Network Perimeter (Firewall, Router, Switches)
Wireless Network
Email Server
Web Server
In-House Web App
Application Server
Server 1
Server 2
(A) Manage by InfoTech, Main Campus, Shah Alam
(B) Managed by InfoTech, UiTM Pahang

Figure 4: Scope of Penetration Testing in UiTM Pahang

Based on Figure 4, the scope of the research is focusing on securing the server and in-house web application as in area (B).

Result and Discussion

The interview session and analysis of data collected shows in 2011 to 2012, one of the web application server has been compromised and a couple of successfully exploited towards in-house web application own by the university has been recorded (Ibrahim, Personal Interview, 2013). This is due to there is no policy that requires security assessment and penetration testing to the web application to find vulnerabilities before it being deployed in the web application server. Therefore, the research propose an enhanced web deployment business process flow which focusing on the implementation of web application security assessment before it being deployed to the production server. The scope of penetration testing is limited to in-house developed web applications and branch application server because all internal web application is maintained and managed by InfoTech UiTM Pahang. This penetration testing business flow is expected to be implemented internally by the administrator of InfoTech, UiTM Pahang, which formally known as internal penetration tester. Detail illustration and discussion on the enhanced web application deployment business flow as in figure 5.

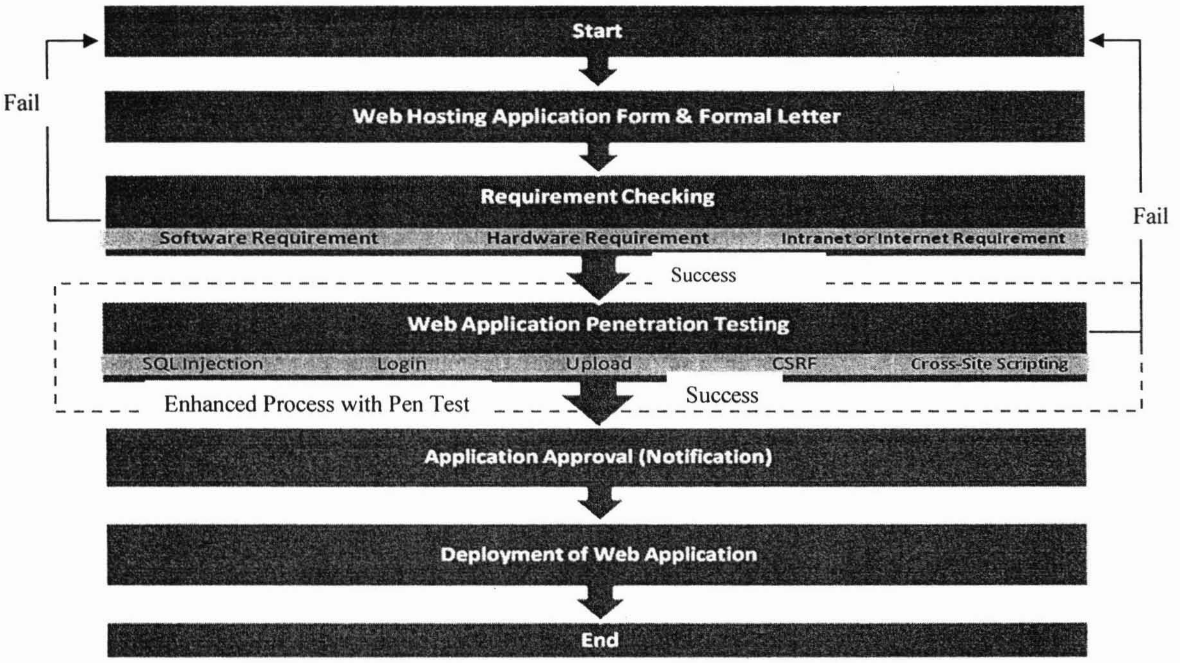

Start
Fail
Web Hosting Application Form & Formal Letter
Requirement Checking
Fail
Software Requirement
Hardware Requirement
Intranet or Internet Requirement
Success
Web Application Penetration Testing
SQL Injection
Login
Upload
CSRF
Cross-Site Scripting
Enhanced Process with Pen Test
Success
Application Approval (Notification)
Deployment of Web Application
End

Figure 5: UiTM Pahang Web Deployment Process Flow with added Penetration Testing

The enhanced web deployment business process flow is based on current practices where all in-house developed web application is require filling up an application form along with a formal letter that request hosting and deployment of the web application in the university's infrastructure to InfoTech. Current process only focusing on the assessment of hardware and software requirement whether or not the web application follows the technical specification as stated in the policy. This is to ensure that the web application can be deployed and run in the web application server without any technical errors. This research proposed to add a significant penetration testing business process where all web application is required to go through a penetration testing phase to check any vulnerabilities and possible loop hole that will allow cracking and unauthorized activities to the web application in the future. The strict penetration testing will focus on common security vulnerabilities in web application as suggested by Robinson (2005) which are;

a) SQL injection
b) Login and Upload pages (bypass authentication)
c) Cross-site scripting
d) CSRF

The paper suggest to adopt the general penetration testing process suggested by Wai (2012) as per discusses in the literature review. However, this paper recommends focusing in *vulnerability detection and penetration attempt* phases during the pen test process to ensure each of security parameter defined above is free from any vulnerabilities. Figure 6 shows UiTM Pahang web application penetration testing process.

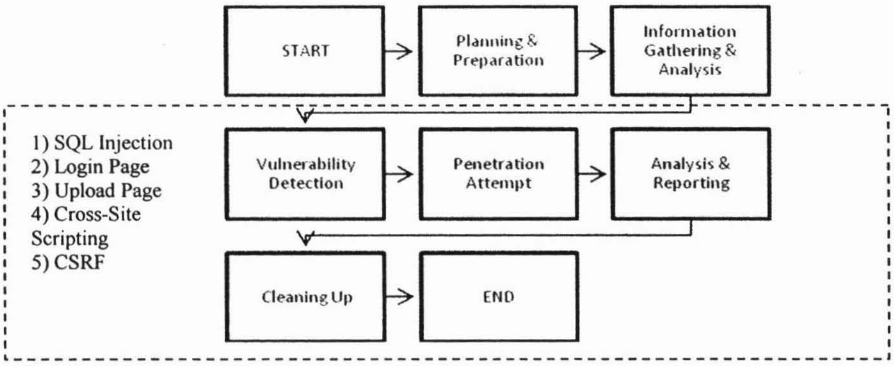


Figure 6: UiTM Pahang web application penetration testing process

In order for a web application is able to be hosted inside the university's web application server, the web application must first successfully passes with ZERO vulnerabilities in all web application security assessment checkpoint as mentioned above. This penetration testing business flow which will thoroughly check vulnerabilities on the web application before it being deployed is expected to be enforced and supported by the top management and InfoTech.

Conclusion

Most of mature IT and non-IT based industries has aware with the importance of penetration testing activities as a way for early detection and prevention of security leaked in their organization. This paper has learned and takes initiative by which current research in security field and industries practices in safeguarding information security. The result is to get in par for enhancing IT security in higher educational institute by proposing the implementation of IT security penetration testing in the university's web application deployment business flow. The implementation of the penetration testing is guided by various research findings and industry white paper. The penetration testing process for web application in early stage is expected will reduce the chances of the web application being exploited as the internal penetration tester must check for any vulnerabilities found in the web application before it being deployed in the server. The vulnerabilities found must be corrected and the re-check process has to be done so that only ZERO vulnerabilities and validated web application can be hosted in the university's server.

References

Austin, A., Smith, B. & Williams, L. (2010). Towards Improved Security Criteria for Certification of Electronic Health Record System. SEHC'10, May 3–4, 2010, Cape Town, South Africa.

Burrows, D. (2002). Penetration Testing 101 – Introduction to becoming a Penetration Tester, Sans Institute.

Foster, A., L. (2004).Insecure and Unaware, The Chronicle of Higher Education, May 7, 2004.

Graves, K. (2007). Official Certified Ethical Hacker, Wiley Publishing, Inc, Indianapolis, Indiana.

Ibrahim, M., I. (2013). Personal Interview with InfoTech.

North, M., George, R., and North, S. (2006) Computer Security and Ethics Awareness in University Environments: A Challenge for Management of Information Systems. ACM SE'06, March 10-12 2006, Melbourne, Florida, USA.

Malaysian Communications and Multimedia Commissions (MCMC) (2011). Retrieved October, 2012 http://www.skmm.gov.my/skmmgovmy/files/attachments/110616_Follow%20Up%20Press%20Release-Hacking%20of%20Government%20Websites-2.pdf.

Moyer, P. (2001). What to Demand from Penetration Testers, Computer Security Alert. URL: http://www.gocsi.com/penet.htm (13 August, 2001).

Olson, C. (2010). Penetration Testing in the Financial Services Industry, Sans Institutes.

Rahmat, B., Sureswaran, R., Azman, S., and Salah, N. (2004). Development of Penetration Testing Model for Increasing Network Security, IEEE.

Rajeev, G., and Eugene, H.,S.(2001). A Framework for Distributed Intrusion Detection Using InterestDriven Cooperating Agents.

Robinson, S. (2005).The Art of Penetration Testing, Şecurity of Distributed Control Systems, 2005. LogicaCMG, London, UK.

Skoudis, E. (2008). Planning, Scoping and Recon. Proceedings of the Network penetration testing and ethical hacking course (pp. 12-16). The SANS Institute. V120708.

Sans Institute.(2001).Guidelines of Developing Penetration Rules of Behavior.

Wai, T., C. (2002). Conducting a Penetration Test on an Organization, Sans Institute 2002.

Wang, L., F., and Kou, H., Z. (2012). A Research of Behavior-Based Penetration Testing Model of the Network, 2012 International Conference on Industrial Control and Electronic Engineering. IEEE.

ZULAZEZE SAHRI, MOHAMAD AFFENDI ABDUL MALEK, MUHD EIZAN SHAFIQ ABD AZIZ, ROSLAN JAMALUDIN, ROGER CANDA.
Universiti Teknologi MARA (Pahang).
Azeze@pahang.uitm.edu.my, maffendi@pahang.uitm.edu.my, eizan@pahang.uitm.edu.my, roslan961@pahang.uitm.edu.my, rogercanda@pahang.uitm.edu.my