International Journal of Engineering & Technology, 8 (1.9) (2019) 359-363

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Security Analysis System E-learning at one of the University in Indonesia

Entik Insanudin[1], Bambang Pudjoatmodjo[2]

School of Applied Science, Telkom University, Bandung 40257, Indonesia
**Corresponding author E-mail: insanudin@tass.telkomuniversity.ac.id*

Abstract

E-learning is one of the services that were developed massively in education. Therefore the application of the system security is also very taken into account, this is done in order to user comfort e-learning system mainly reflects the e-learning system for on-line or better known by the term e-learning. In this research, the authors attempted to analyze the security system e-learning at one of the universities in Indonesia by using the tools sniffing cain and abel to detect the vulnerability when a user e-learning while doing logged if the username and password is visible and tools Acunetix Web vulnerability scanner to analyze more remote security loopholes contained in e-learning system at one of the universities in Indonesia, In additions Acunetix Web Vulnerability scanning tools can inform the whole of each vulnerability found on e-learning system at one of the universities in Indonesia located on level 3 High, this shows that e-learning on one of the university is very vulnerable to threats.

Keywords: *E-learning, System Scurity, Vulnerability, Sniffing.*

1. Introduction

Technology is a key success factor in the implementation of the-learning process [2]. Since the information technology (IT) and information systems (IS) used as a strategic resource, the organization is actually required to have specific formulations for the implementation of IT / IS in the strategic policy as an effort to improve the quality of service [9].

Universities in Indonesia changing panorama over the last decade. Panorama changes may include a change of paradigm, management, competition, and so on. The paradigm change was primarily driven by IT developments such as e-learning, e-university, and the like [3]. Panorama is happening in the Universities is further reinforced by the standard-setting financing, facilities and infrastructure, as well as one grain SI accreditation standard for Universities by Badan Akreditasi Nasional Perguruan Tinggi (BAN-PT) (Anonymous, 2008a).

The program to improve the quality of service on the universities with the implementation of IT / IS actually do not forget the other important aspect is the safety factor to be integrated in any IT infrastructure / IS no exception to the e-learning system that is used to accelerate the achievement of the objectives of teaching and learning.

According to Gollmann (2000), the security of computer systems relating to the prevention and detection actions unauthorized by the user computer system. Furthermore Whitman and Mattord (2010) stated that in the perspective of security of information systems there are some critical aspects that need to be protected, namely Confidentiality (secrecy), Integrity, and Availability. Then these three aspects are considered to have a strong relevance as a feature that should be owned by the e-learning system. This paper discusses security analysis e-learning system used in one of the universities in Indonesia.

2. The Scurity of Information System

This information system security can be defined is one of the efforts to secure information on disposal. Information security consists of protection against the following aspects:

1. Confidentiality (confidentiality) aspects that ensure the confidentiality of data or information, ensuring that information can only be accessed by authorized persons and ensure the confidentiality of data sent, received and stored.

2. Integrity aspect which ensures that data is not changed without a permit authorized parties (authorized), maintain the accuracy and integrity of information and methods of the process to ensure the integrity of this aspect.

3. Availability aspect which ensures that data will be available when needed, ensuring legitimate users can use the information and related devices (assets associated if necessary). Security of information obtained by implementing a set of tools decent control, which could be policies, practices, procedures, organizational structures and software.

Information security protects information from a wide threats to ensure business continuity, minimize loss of the company and maximize return on investment and business opportunities. Management information system allows data to be distributed electronically, so that the necessary systems to ensure the data has been sent and received by the correct user.

The survey results ISBS (Information Security Breaches Survey) in 2000 showed that most of the data or information is not sufficiently maintained / protected so unwarranted insecurity. The survey results related to this can be seen in the following figure 1:

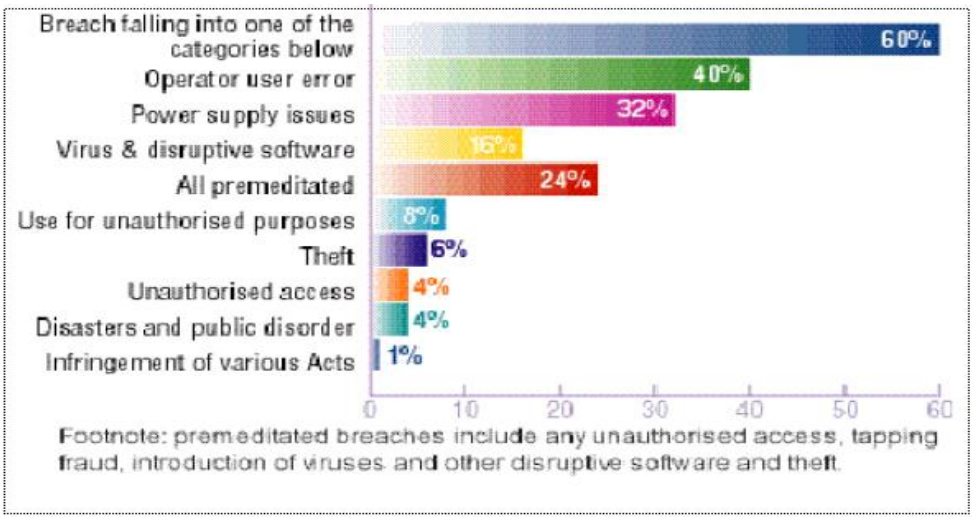

Fig.1: Percentage graph Information Systems Security Threats

The survey also showed that 60% of organizations have experienced seizures or destruction of data because of a weakness in the security system. Security system failure caused more by internal factors than by external factors. The internal factors include errors in the operation of the system (40%) and discontinuities power supply (32%).

Information security has several aspects that must be understood to be applicable. Some of these aspects, the first three are called C.I.A (Confidentiality, Integrity and Availability) "triangle model", as described in point 2.1 of Information Security (discussion). Another aspect mentioned by Dr. Michael E.Whitman and Herbert J. Mattord in his book Management Of Information Security is:

1. Privacy Information collected, used, and stored by organizations is used only for certain purposes, especially for the owner of the data when the information is collected. Privacy ensures data security for the owner.

2. Integrity (integrity) aspect which ensures that data is not changed without a permit authorized parties (authorized), maintain the accuracy and integrity of information and methods of the process to ensure the integrity of this aspect.

3. Availability (availability) aspect which ensures that data will be available when needed, ensuring legitimate users can use the information and related devices related assets.

4. Identification System has the characteristic identification information if it can identify individual users. Identification is the first step in obtaining the right of access to information is secured. Identification is generally performed in the use of your user name or user ID.

Authentication Authentication occurs when the system can prove that the user is really the person who has the identity they claim.

3. E-Learning

E-learning instructional media is now not a privilege for every college and for schools. e-Learning or electronic learning is now increasingly recognized as one way to address the issue of education, both in developed countries and in developing countries. Many people use the terms that vary with e-learning, but in principle an e-learning is learning to use electronic services as supporting equipment.

e-Learning is a learning technology is relatively new in Indonesia. To simplify the term, the electronic learning shortened to e-learning. This word consists of two parts, namely 'e' stands for 'electronica' and 'learning' which means 'learning'. So e-learning means learning by using electronic devices assistance services. So in the implementation of e-learning using the services of audio, video or computer device or a combination of all three. In the literature, e-learning is defined as follows:

e-Learning is a generic term for all technologically supported learning using an array of teaching and learning tools as phone bridging, audio and videotapes, teleconferencing, satellite transmissions, and the more recognized web-based training or computer aided instruction also commonly referred to as online courses (Soekartawi, Haryono dan Librero, 2002).

Therefore, e-learning is learning that its implementation is supported by technological services such as telephone, audio, vidiotape, satellite transmissions or computer

4. Methodology

Step-by-step analysis of the study e-learning system security begins by analyzing the real system that simultaneously aligned with the theoretical studies and then identify the factual issues. To set the focus of the study, the formulation of objectives and continued on the preparation of an analytical framework using Cain and Abel applications as well as web vulnerability scanner Acunetic as an analytical

tool to identify the status of the user at login time and know the security holes in the system of e-learning. The next stage is the implementation of the framework for analysis, documentation of the results as well as discussing the results of the analysis which concludes with a summary. Schematically the whole stage can be seen in Figure 2:

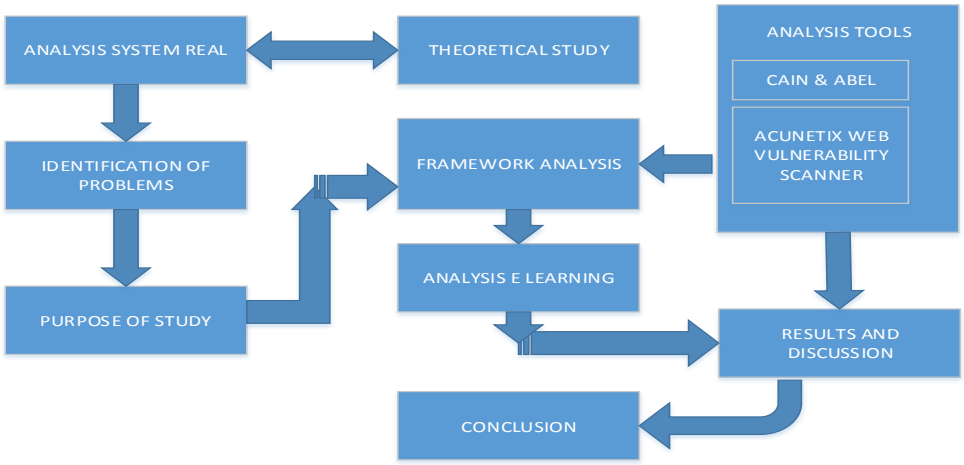

Fig. 2: Methodology

Another thing in conducting this study using literature study and analysis of the application of methods and stages of work steps as follows:

1. The safety analysis refers to the analysis of e-learning system security

2. Identify the problem is one of the main measures undertaken by tracing the background of the problem, determine the formulation of the problem, create a destination empirically, the benefits of research, the scope of research, determines the problem definition, design research methods, as well as making the stages of systematic discussion on system security analysis e-learning on one University.

3. The study of literature is the next stage which is carried out with regard to the topics done in analyzing the e-learning system on one University.

4. Melakukan kajian analisis sistem keamanan menggunakan program sniffing menggunakan tools Chain, Abel and aquatix web vulnerability scanner.

5. Implementation of the study results of the safety analysis of e-learning on one of the University, by using a sniffing program uses tools Chain, Abel and aquatix web vulnerability scanner is done by means of experimental trials on a server MORA e-learning on one University.

6. The final stage in drawing conclusions from the results of the study analyzes the security of e-learning system on one of university from the findings of this study and the conclusions of the study results analysis of the security system of e-learning on one University in Indonesia.

5. Results and Discussion

5.1. Status User Security

Technically, initial steps were taken to analyze the security of e-learning system at one of the colleges are doing sniffing test involving 72 students as sample testing and using an account on a certain course. All students start sniffing the user's status to one another, with the target of identifying a user name and password respectively. The results obtained at the end of the activity are all students were tested successfully to know the user name and password to each other at the time of log-in on e-learning. This leads to the security status of users who are vulnerable to unauthorized user activity. Shown in Figure 3 one result sniffing is done by the students.

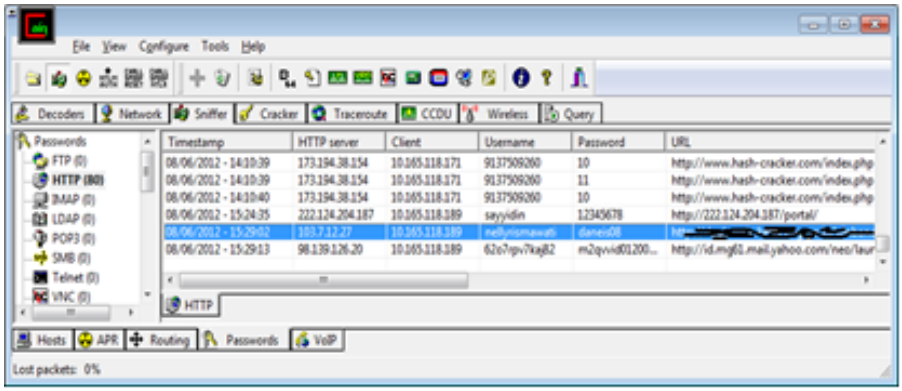

Fig.3: one result sniffing is done by the students

5.2. Security Gap E-Learning Systems

5.2.1. Summary of level of vigilance

a. 1 alert at level 3 (high level): a very high level of vigilance found in Apache 2.2.14 mod_isapi Dangling pointer.

b. 9 warning there is at level 2 (Medium level): a medium alert level contained in the Apache 2.x version older than 2.2.9 (1 warning), Apache httpd remote denial of service (1 warning), apache httpOnly cookie Disclosure (1 warning), the HTML form without CSRF protection (2 warnings), PHP hangs on particular parsing strings as floating point number (1 warning), user credetial are sent in clear text (3 warnings);

c. 3 warnings contained in level 1 (Low level): there is a low level of awareness on the Apache 2.x version older than 2.2.10 (1 warning), Login page password-guessing attack (1 warning), TRACE method is enabled (1 warning);

d. 2 warnings contained in the informational level 0 level: the level of vigilance for notification purposes only. When the scan is done first by trying to login, the system generates a notification type Password input with autocomplete enabled (2 warnings). As shown in Figure 4.

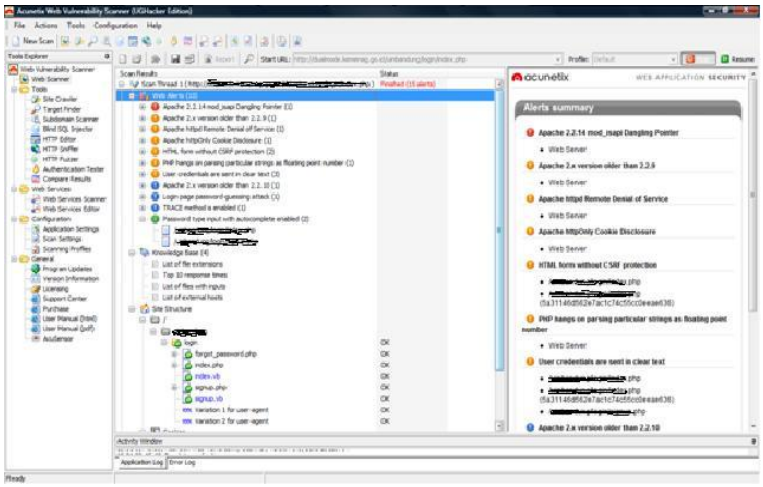

Fig.4: Scan Results aquapix e-learning using web vulnerability scanner

5.3. Target Informasion

a) Response true/ yes;

b) Web server banner apache/2.2.8 (win32) Dav/2 mod_ssl OpenSSL/0.9.8g Mod_autoindex_color PHP/5.2.5;

c) The operating system used windows;

d) Web server apache 2.x;

e) The technology used php, mod_ssl, OpenSSL.

5.4. Statistics Made 8665 Requests

a) Scanning duration is 1 minute 31 seconds;

b) Total demand by 8665;

c) average response time 1257.81 seconds.

5. Conclusion

The conclusion that can be drawn from this study showed that in the management relating to the security of this system, as a whole in order to use sniffing tools cain and abel to use network features snifer password, shows sightings account username and password for all users of e-learning. As a whole shows that to reduce the level of vulnerability or security holes contained in e-learning system is necessary maintenance and application upgrades on an ongoing basis, this is done to reduce the risk of attack from unauthorized persons, and threats to e-learning at one of the colleges it is located on level 3 High, this shows that e-learning on one of university is very vulnerable to threats, especially in apache 2.2.14 mod_isapi Dangling pointers that can pitch on a web server.

References

[1] Anonymous. 2008. Accreditation Standards and Procedures Undergraduate Studies Program. Ministry of Education, National Accreditation Board for Higher Education, Jakarta.

[2] Ramdhani, M. A, dan Wulan, E. R. (2012). The Analysis of Determinant Factors In Software Design For Computer Assisted Instruction. IJSTR, 1 (8), 69-73.

[3] Indrajit, R. E., dan R. Djokopranoto. 2004. College of Modern Management. School of Information Management and Computer PERBANAS, Jakarta.
[4] Pernul, G. (1997). Database Security and Internet Systems, Department of Information Systems University of Essen.
[5] Raharjo, B. (2002). "Internet-Based Information System Security". PT Insan Indonesia – Bandung dan PT INDOCISC – Jakarta.
[6] Sasongko, A. (2011). "Web Server Security Guide". The Ministry of Communication and Information of the Republic of Indonesia, Information Security Directorate, The Directorate-General for Informatics Applications.
[7] MSI Labs. A Real World Review,"ACUNETIX WEB VULNERABILITI SCANNER". http://www.acunetix.com.
[8] Date, C.J. (2000). An Introduction To Database Systems, Seventh Edition, Addison-Wesley.
[9] Slamet, C. (2012). The Implementation of Strategic Planning for Information System in Educational Foundation. International Journal of Basic and Applied Science, Vol. 01, No. 01, July 2012, 89-94.
[10] Martin, J. (1975). Computer Data-Base Organization. Prentice Hall National Computer Security Center, A Guide To Understanding Discretionary Access Control in Trusted Systems, Version 1, National Computer Security Center, 30 September 1987.
[11] Sutanta, E. (2008). "Security Analysis System Application (Application E-learning Case Studies in IST AKPRIND YOGYAKARTA"
[12] Date, C.J. (2000). An Introduction To Database Systems, Seventh Edition, Addison-Wesley.
[13] Akbar, M. dan Perdana, I. "Comparative Analysis Between Web Application Vulnerability Scanner Acunetix and Nikto.
[14] Lukito, R. B. (2008), Analysis and Security Policy Studies, A Case Study System E-learning At University BCD.
[15] Michael E. Whitman, Herbert J. Mattord. (2010). Management of Information Security 3rd Edition, Boston, USA.
[16] Ellis, J. dan Speed, T. (2003). Internet Security : "A Jumpstart for Systems Administrators and IT Managers"