TEST Engineering & Management

May – June 2020
ISSN: 0193-4120 Page No. 15714 – 15719

Evaluation of Wireless Network Security Using Information System Security Assessment Framework (ISSAF) (Case Study: PT. Keberlanjutan Strategis Indonesia)

Muchamad Rusdan[1], Daniel T. H. Manurung[2], Franklin Kharisma Genta[3]
[1]Sekolah Tinggi Teknologi Bandung, Indonesia
[2]STIE Widya Gama Lumajang, Indonesia
[3]Institut Manajemen Koperasi Indonesia
Corresponding Author: rusdan@sttbandung.ac.id

Article Info
Volume 83
Page Number: 15714 – 15719
Publication Issue:
May - June 2020

Abstract:
The purpose of this study was conducted to determine the level of wireless network vulnerability using ISSAF with penetration testing and make plans, assessments, and evaluation reports of wireless network security that can be used as guidelines for conducting penetration testing on an organization or company. The study was conducted with an action research approach which was divided into several stages, namely diagnosing, action planning, intervention, evaluation, and reflection. Then for the wireless network security evaluation process by applying ISSAF Penetration Testing. The results of testing the level of wireless network vulnerability of PT. Keberlanjutan Strategis Indonesia using ISSAF with penetration testing shows that the overall results of the four types of testing show the average level of a vulnerability is 0.8, in other words, the overall wireless network at PT. Keberlanjutan Strategis Indonesia has a high level of vulnerability. The outputs from each phase, namely the planning and preparation phase, produce policy documents and agreements, the assessment phase, produce assessment documents, and the reporting, clean-up, and destroy artefacts phases, produce the evaluation documents. The output produced in each phase determines the next phase so that the three phases it is a series of processes that can not be separated.

Keywords: *Wireless Network Security, Information System Security Assessment Framework, Penetration Testing, Vulnerability.*

Article History
Article Received*: 1May 2020*
Revised*: 11 May 2020*
Accepted*: 20 May 2020*
Publication*: 24May 2020*

May – June 2020
ISSN: 0193-4120 Page No. 15714 – 15719

INTRODUCTION

The development of computer network technology makes it easier for people to meet their information needs[1]. One of the technologies developed is wireless media transmission technology. Wireless transmission media that are used for wireless networks are often found in various places that provide internet access. Nowadays, internet access services are made easier by the large number of communication tool products that provide wireless network features[2]. Wireless network infrastructure for internet access service needs is standardized with the IEEE 802.11 code[3].

Ease of users to be able to connect to a wireless network will certainly cause security problems that need attention, especially in an organization or company that cares about data security[4]. Wireless networks use radio waves as a transmission medium so that intruders and attacks from all directions will more easily enter the network[5]. On networks that are accessed together, such as wireless networks have a vulnerability to attacks or disruptions to the system so that the rules must be made to the wireless network system[5]. Some rules are applied to control the performance and condition of the wireless network so that the system runs as expected. To see the quality of wireless network security, it is necessary to evaluate the existing security system in the wireless network[6].

One of the frameworks that can be used in evaluating networks is by testing the system by simulating forms of attack on the network or commonly known as the Information System Security Assessment Framework (ISSAF). ISSAF has long been developed by several researchers in the field of information systems security and computer networks. ISSAF evaluates the network by taking penetration testing[7]. The act of penetration testing is an action that is harmful to the system[8]. Penetration testers are ethical hackers who are employed to conduct dangerous experiments on computer networks in companies to assess network or data security. If this activity is carried out in an organization or company by considering the risks of penetration testing, then it is necessary to have good planning to provide guarantees to the target parties and penetration actors[9]. This guarantee relates to the laws in force in the country regarding the use of information technology[10].

Associated with some understanding of wireless network security evaluation using the Information System Security Assessment Framework (ISSAF), this study was conducted to determine the level of wireless network vulnerability using ISSAF with penetration testing and make plans, assessments, and reports on evaluating wireless network security that can be used as guidelines to do penetration testing on an organization or company.

LITERATURE REVIEW

Wireless Network Concepts

Computer Network is a collection of computers consisting of two or more computers, each of which stands alone and is connected through a communication medium. Media that connects computers not only through copper cables, but can also through an optical fibre, radio waves, infrared, and satellite[11]. The transfer speed of a network is often referred to as bandwidth, the unit used in measuring this bandwidth can be bits per second or bytes per second. One byte consists of 8 data bits, whereas 1 kilobyte of data consists of 1024 bytes of data[12].

Wireless networks are computer networks that do not use cable media but use radio waves to interact or communicate between devices that support wireless connections[13]. Works at 2.4 GHz (802.11 b / g / n / ac) or 5 GHz (802.11 a / n / ac). Backbone wireless networks usually use cable, with one or more access points[13].

May – June 2020
ISSN: 0193-4120 Page No. 15714 – 15719

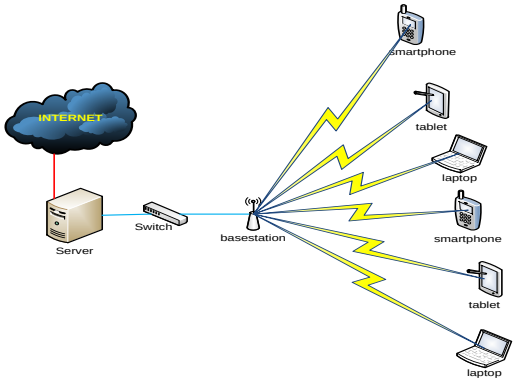

Figure 1. Wireless Network Topology[14]

Wireless Network Security

Security aims to avoid unexpected eavesdropping and theft. Security is very important for protecting data communications so that confidentiality, integrity, and availability are guaranteed[15]. Wireless network transmission media has a higher potential to be attacked than cable media thus increasing threats to wireless networks[16]. Wireless network security as a combination of wireless channel security and network security. Wireless network challenges such as interference with radio frequency signals, confidentiality data, data integrity, and data availability[17].

Wireless network security assessments are carried out based on the level of vulnerability using values as specified in ISSAF[18]. The parameters used in providing vulnerability level values can be explained in table 1.

Table 1. Vulnerability Level Value

Vulnerability Level	Assigned Value
Extremely	1
Highly	0.8
Average	0.6
Low	0.4
Extremely Low	0.2

Information System Security Assessment Framework (ISSAF)

One of the frameworks that can be used to do penetration testing is the Information System Security Assessment Framework (ISSAF). This framework was developed by the Open Information System Security Group (OISSG). ISSAF Penetration Testing is designed in conducting evaluations using a three-phase approach, namely[18]:

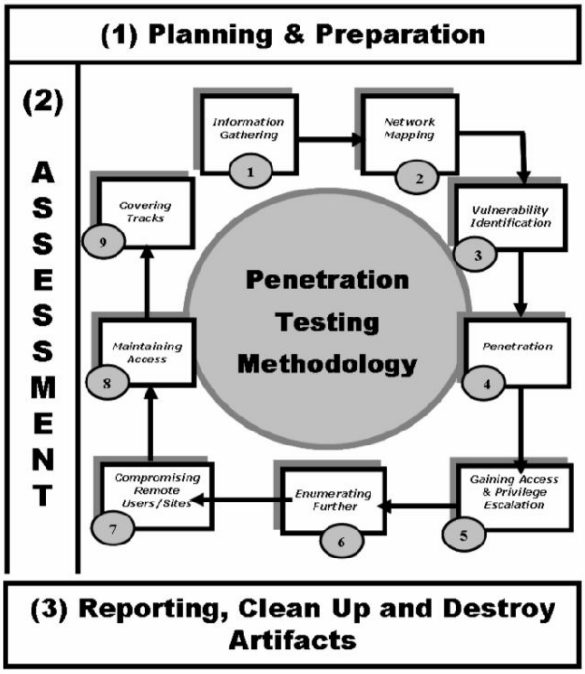

Figure 2. Approach and Methodology ISSAF[6]

1)Planning and Preparation

This stage is the stage of introduction and adjustment between the perpetrators of penetration and the parties who will be the object by exchanging information. Agreement between the two parties is needed for mutual legal protection. This stage also determines the team involved in testing, the right time plan and other rules.

2)Assessment

This stage is a stage of penetration testing consisting of several layered approaches. The layers here are Information Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access & Privilege Escalation, Enumerating Further, Compromise Remote Users / Sites, Maintaining Access, and Covering Tracks.

3)Reporting, Clean-up and Destroy Artefacts

The final stage of testing by making several reports of findings during penetration testing. After taking action, it is necessary to

May – June 2020
ISSN: 0193-4120 Page No. 15714 – 15719

delete logs that can harm the system that can be used by others.

RESEARCH METHODS

The study was conducted with an action research approach which was divided into several stages, namely diagnostic, action planning, intervention, evaluation, and reflection[19]. Then for the wireless network security evaluation process by applying ISSAF Penetration Testing. The stages of the research are as follows[19]:

1)Diagnostic

The initial stage is carried out by identifying problems related to wireless network systems through interviews and observations.

2)Action Planning

The next stage is the planning and preparation needed in the study. The problem that will be raised in the evaluation of wireless networks using the Penetration Testing method. This stage uses the planning and preparation phase in ISSAF which includes activities such as identifying penetration actors and people from the company responsible for the network system, confirming with management regarding the scope of the test and testing approach and methodology to be used, making agreements and a formal agreement that can provide legal guarantees to penetration actors and the company being targeted for penetration.

3)Intervention

After the planning is made next take action by implementing it on the research object. This stage is an assessment stage in ISSAF where the method used, namely information gathering process of data collection by scanning the network, analyzing and researching the data obtained then analyzing, evaluating the results of each test action by involving the network manager to discuss matters relating to wireless network security settings, and the final reflection of the cycle sequence and the method used is the reporting phase of ISSAF.

RESULTS AND DISCUSSION

This study uses ISSAF as a security system evaluation framework with penetration testing methods. The evaluation process is divided into three phases, namely, planning and preparation, assessment, and reporting[18]. The results of this study will generally produce policies, agreements, assessment documents, and evaluation documents. Each process and output determine and influence each other processes so that a methodology that is built is an inseparable unity in this research—the results obtained from testing wireless networks at PT. Keberlanjutan Strategis Indonesia can be presented in table 2.

Table 2. Wireless Network Test Results PT. Keberlanjutan Strategis Indonesia

Penetration Testing Measures	AP_KSI1	AP_KSI2	AP_KSI3	AP_KSI4	AP_KSI5
DoS Attack	1	1	1	1	1
MITM Attack	1	1	1	1	1
Cracking the encryption	0,8	0,8	0,8	0,8	0,8
Bypassing Authentication	0,6	0,6	0,6	0,6	0,6

The overall results obtained from the four types of testing show the average level of a vulnerability is 0.8 in other words overall, the wireless network at PT. Keberlanjutan Strategis Indonesia has a high level of vulnerability. Wireless network test results are obtained from the assessment process, but to do the process must be preceded by previous processes which in this study are included in the planning and preparation phase. Without an agreement between the perpetrators and the organization or company, penetration testing should not be done because they do not have legal guarantees from each party.

The evaluation documents produced were obtained from the two previous phases, namely planning and preparation and assessment. The contents of the document consist of data from the evaluation activities

May – June 2020
ISSN: 0193-4120 Page No. 15714 – 15719

from the beginning to the end. There is an evaluation document for companies that need it, especially for the management of the wireless network. In addition to administrative data, the contents of the document are a clear description of the wireless network security vulnerabilities that PT. Keberlanjutan Strategis Indonesia so that managers are expected to be able to take policies to improve wireless network security better.

Methodologies that include the planning and preparation, assessment, and reporting phases, clean-up and destroy artefacts can be used as guidelines for conducting penetration testing on an organization or company. The output of each phase is as follows 1) Planning and preparation phase, producing policy documents and agreements, 2) Assessment Phase, produces assessment documents, and 3) Reporting, Clean-Up, and Destroy Artefacts Phase, produces an evaluation document. Output generated from each phase determines the next phase so that the three phases constitute a series of processes that cannot be separated.

CONCLUSION

Based on data analysis and discussion of Wireless Network Security Evaluation Using the Information System Security Assessment Framework (ISSAF) case study at PT. Keberlanjutan Strategis Indonesia, several conclusions can be drawn, such as the following:

1)The results of testing the wireless network vulnerability level of PT. Keberlanjutan Strategis Indonesia using ISSAF with penetration testing shows that the overall results of the four types of testing show the average level of a vulnerability is 0.8, in other words, the overall wireless network at PT. Keberlanjutan Strategis Indonesia has a high level of vulnerability.

2)Making planning documents, assessments, and evaluation reports of wireless network security that can be used as guidelines for conducting penetration testing at PT. Keberlanjutan Strategis Indonesia is derived from the two previous phases, namely planning and preparation and assessment. The contents of the document consist of data from the evaluation activities from the beginning to the end. The content of the document is a clear picture of the wireless network security vulnerability owned by PT. Keberlanjutan Strategis Indonesia so that managers are expected to be able to take policies to improve wireless network security better. Methodologies that include the planning and preparation, assessment, and reporting phases, clean-up and destroy artefacts can be used as guidelines for conducting penetration testing on an organization or company. The outputs from each phase, namely the planning and preparation phase, produce policy documents and agreements, the assessment phase, produce assessment documents, and the reporting, clean-up, and destroy artefacts phases, produce the evaluation documents. The output produced in each phase determines the next phase so that the three phases it is a series of processes that can not be separated.

REFERENCES

[1] W. Cascio and R. Montealegre, “How Technology Is Changing Work and Organizations,” *Annu. Rev. Organ. Psychol. Organ. Behav.*, vol. 3, pp. 349–375, Mar. 2016, DOI: 10.1146/annurev-orgpsych-041015-062352.

[2] S. Song and B. Issac, “Analysis of WiFi and WiMAX and Wireless Network Coexistence,” *Int. J. Comput. Networks Commun.*, vol. 6, Nov. 2014, DOI: 10.5121/ijcnc.2014.6605.

[3] S. Banerji and R. Chowdhury, “On IEEE 802.11: Wireless Lan Technology,” *Int. J. Mob. Netw. Commun. Telemat.*, vol. 3, Jul. 2013, DOI: 10.5121/ijmnct.2013.3405.

May – June 2020
ISSN: 0193-4120 Page No. 15714 – 15719

[4] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device Fingerprinting in Wireless Networks: Challenges and Opportunities," *IEEE Commun. Surv. Tutorials*, vol. 18, Jan. 2015, DOI: 10.1109/COMST.2015.2476338.

[5] L. Mohammed and B. Issac, "Detailed DoS Attacks in Wireless Networks and Countermeasures," *IJAHUC*, vol. 2, pp. 157–166, Jan. 2007, DOI: 10.1504/IJAHUC.2007.012417

[6] S. Sharma, R. Mishra, and K. Singh, *A Review on Wireless Network Security*. 2013.

[7] T. Klima, "PETA: Methodology of Information Systems Security Penetration Testing," *Acta Inform. Pragensia*, vol. 5, pp. 98–117, Dec. 2016, DOI: 10.18267/j.aip.88.

[8] T. Dimkov, A. van, W. Pieters, and P. Hartel, *Two methodologies for physical penetration testing using social engineering*. 2010.

[9] A. Bacudio, X. Yuan, B. Chu, and M. Jones, "An Overview of Penetration Testing," *Int. J. Netw. Secure. Its Appl.*, vol. 3, pp. 19–38, Nov. 2011, DOI: 10.5121/ijnsa.2011.3602.

[10] M. Caselli and F. Kargl, *A Security Assessment Methodology for Critical Infrastructures*. 2016.

[11] D. Bertoglio and A. Zorzo, "Overview and open issues on a penetration test," *J. Brazilian Comput. Soc.*, vol. 23 Dec. 2017, DOI: 10.1186/s13173-017-0051-1.

[12] M. Rusdan, "Design of Wireless Network System for Digital Village Using Wireless Distribution System (Case Study: Cijambe Village)," *J. Informatics, Inf. Syst. Softw. Eng. Appl.*, vol. 1, no. 2, pp. 51-059, 2019, DOI: 10.20895/INISTA.V1I2.

[13] A. Zappone, M. Di Renzo, and mérouane Debbah, "Wireless Networks Design in the Era of Deep Learning: Model-Based, AI-Based, or Both?," *IEEE Trans. Commun.*, vol. PP, p. 1, Jun. 2019, DOI: 10.1109/TCOMM.2019.2924010.

[14] M. Rusdan and M. Sabar, "Analisis dan Perancangan Jaringan Wireless Dengan Wireless Distribution System Menggunakan User Authentication Berbasis Multi-Factor Authentication," *Jt. (Journal Inf. Technol.*, vol. 02, no. 01, pp. 17–24, 2020.

[15] M. Rusdan and D. T. Manurung, "Designing of User Authentication Based on Multi-factor Authentication on Wireless Networks," *J. Adv. Res. Dyn. Control Syst.*, vol. 12, no. 1, pp. 201–209, Feb. 2020, DOI: 10.5373/JARDCS/V12I1/20201030.

[16] G. Ijemaru, I. Adeyanju, K. Olusuyi, T. Ofusori, and E. Ngharamike, "Security Challenges of Wireless Communications Networks: A Survey," *Int. J. Appl. Eng. Res.*, vol. 13, Apr. 2018.

[17] Y. Zou, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends," *Proc. IEEE*, vol. 104 May, 2015, DOI: 10.1109/JPROC.2016.2558521.

[18] T. Wilhelm, *Professional Penetration Testing, Second Edition: Creating and Learning in a Hacking Lab*, 2nd ed. Syngress Publishing, 2013.

[19] K. Petersen, C. Gencel, N. Asghari, dejan baca, and S. Betz, *Action research as a model for industry-academia collaboration in the software engineering context*. 2014.