RES MILITARIS
REVUE EUROPEENNE D ETUDES EUROPEAN JOURNAL OF MILITARY STUDIES
Social Science Journal

Comparative Study of Computer Security Methodologies for Countering Cyber Attacks

By

Francisco Manuel Hilario Falcón
Universidad César Vallejo, Lima, Perú
Email: fhilariof@ucvvirtual.edu.pe

Milner David Liendo Arévalo
Universidad César Vallejo, Lima, Perú
Email: mliendoa@ucvvirtual.edu.pe

Giancarlo Sanchez Atuncar
Universidad César Vallejo, Lima, Perú
Email: gsanchezat@ucvvirtual.edu.pe

Ivan Crispin Sanchez
Universidad César Vallejo, Lima, Perú
Email: icrispin@ucvvirtual.edu.pe

Abstract

Nowadays, computer security ensures the absence of risks in any of the elements of a system such as hardware, software, computer-human resources, networks, users, data, and procedures, interrupting that any user or personnel without authorization can have access to the information contained in the system and avoiding modifying, damaging, altering, eliminating and/or giving it any treatment that is not authorized. That is why large organizations or IT researchers developed methodologies ((a) ISSAF Methodology, (b) OSSTMM Methodology, and (c) OWASP Methodology) that were implemented in different organizational environments and were effective in countering anomalies and cyber attacks. Therefore, the objective of the present research is the comparison of computer security methodologies to counter cyber attacks with the following criteria: Year of inception, Country of development, definition, characteristics, method, phases, benefits. These criteria were fundamental to compare the information of each development methodology presented to evaluate their functions and classify which one is more efficient to avoid some anomalies in an entity. As a recommendation, it is proposed to continue developing this research in different variables of evaluation based on the methodologies of computer security that help to encourage students to develop scientific articles based on computer security, information security, and mong others.

Keywords: OWASP, ISSAF, OSSTMM, computer security, computer auditing.

Introduction

Nowadays, technological components and principles (computers, network services, technological tools, telecommunications, etc.) are fundamental elements of Information Technology (IT). Are fundamental elements that are proper of Information Technology (IT) since they are common aspects in the life of a person (social, economic, technological and daily), oriented to cyber security (CS) that seeks the care and protection

of data in organizations (SMEs, SMEs, and large companies) to detect vulnerabilities to technical or systematic problems allowing efficient results against unwanted intruders ([1] [2] [3] [4]).

In addition, [5] mentioned that computer security ensures the absence of risks in any of the elements of a system such as hardware, software, computer human resources, networks, users, data and procedures, interrupting that any user or unauthorized personnel can have access to the information contained in the system and avoiding to modify, damage, alter, eliminate and/or give it any treatment that is not authorized [5]-[1]. In summary, computer data security is essential for the detection of threats and anomalies that violate data security, in order to identify the causes of a vulnerability to prevent, reduce and prevent access to an asset of the company among others [5]-[1].

Likewise, in the study of [6] they carried out an implementation of an experimental computer security system that contains the services of a virtual private network, a firewall and an intrusion detection system for the system to mitigate possible attacks that seek to penetrate and breach the security systems of the company, based on this process it was possible to neutralize the denial of service attacks and brute force attacks in an expected way improving the security of a small local network in a satisfactory manner. However, computer media users technology should have a critical sense about the activities they perform on their computers, especially those connected through the Internet, despite this, there are still many users who seem to isolate computer security to the background of interest [7].

Therefore, computer security ensures the integrity and privacy of the information of a computer system and its users, executing good security measures that prevent damage that can be caused by intruders [8]. On the other hand, the characteristics of computer security of information (data) is to ensure compliance with certain qualities that data must meet, such as reliability, integrity, availability and confidentiality [9]. In short, information security is part of the structure of any company, so it ensures confidential information and access to it [10].

Techniques and methods

The objective of this research is the comparison of information security methodologies to counter cyber attacks with the following discernment: year of inception, country of development, definition, characteristics, method, phases, benefits. These criteria were fundamental to compare the information of each development methodology presented to evaluate their functions and classify which one is more efficient to avoid some anomalies in an entity. On the other hand, this study is of a descriptive qualitative level since it will validate the differences and similarities of the methodologies to see which one is more adaptable for an environment and feasible for the network technician. Therefore, a table is detailed based on the three most relevant methodologies at present in order to see the advantages and differences through qualities and methodical processes of implementation of the methodologies to improve security and counteract different cyber attacks.

Table 1: *Computer security methodologies to counter cyber attacks.*

Indicators	Comparative study of computer security methodologies for countering cyber attacks		
	Methodology de ISSAF	Methodology de OSSTMM	Methodology de OWASP
Year Of Initiation	------	It was created in 2000 by ISECOM [11].	2001 [12]
Development Country	------	EEUU [11]	EEUU [13]
Definition	It is a methodology that is based on a framework developed to evaluate the security of information systems, thus having a structure of security analysis in several domains, and the specificities of the tests are called Criteria [14].	It is a methodology developed where it allows to have the evaluation through the security having the levels of risk assessment and the steps in which a penetration test is taken [15].	The OWASP methodology is a method that centralizes its functionalities to web applications and the guarantees they provide to protect their integrity, the task proposed by this analysis method is to help organizations to make decisions, demonstrating vulnerabilities and possible risks [16].
Characteristics	ISSAF offers a high value proposition for infrastructure security by assessing existing security controls against critical vulnerabilities. Therefore, it addresses different characteristic points such as: (a) risk assessment, (b) enterprise structure and management, (c) controls assessment, (d) commitment management, (e) security policy development, and (f) general best practices [17].	Practicing the OSSTMM methodology helps to reduce the important points for which it is shaped by its characterization: (i) reduce false positive and false positive cases of reproducible security measurements, (ii) allows to have a frame of reference of types of security tests in penetration testing and white box auditing and (iii) evaluate collected results that are consistent, quantifiable and confidence that is held in the methodology [18].	In the OWASP methodology it allows to have the following features such as: the scope of testing, start of testing, description of testing techniques, general clarification about the OWASP testing framework [19].

Indicators	Comparative study of computer security methodologies for countering cyber attacks		
	Methodology de ISSAF	Methodology de OSSTMM	Methodology de OWASP
Year Of Initiation	------	It was created in 2000 by ISECOM [11].	2001 [12]
Development Country	------	EEUU [11]	EEUU [13]
Method	In the ISSAF methodology, characterization is allowed in the following: (a) perform testing and security analysis, (b) establish the requirements, (c) define the methodology for the processes that are explored in testing, and (d) define the scope in different areas [20].	OSSTMM is a methodology that is based on improving security performance for the protection of computer equipment, the present methodology is divided into: (i) channels, (ii) modules, (iii) environments and (iv) security testing phases [21].	The OWASP methodology includes a report that is used within organizations to report on various threats and risks that are interpreted by different organizations as vulnerable sites [22].
Phases	The methodology takes three types of phases that help to strengthen the quality control and evaluation test, which are: (a) Planning and Preparation, (b) Evaluation Reporting and (c) Object Cleaning and Destruction [14].	The OSSTMM methodology, standardized and ordered different verifications and evaluation tests that can be performed for a computer audit so it is applied in this case study as is the: Induction Phase, Interaction Phase, Investigation Phase and Intervention Phase [23].	OWASP has identified a list of the top ten web application security risks that can be used for vulnerability mapping, including: (1) Injection, (2) Broken authentication, (3) Exposure to sensitive data, (4) XML external entities, (5) Broken access control, (6) Incorrect security configurations, (7) Cross-site scripting, (8) Insecure deserialization, (9) Use of components with known vulnerabilities, and (10) Insufficient logging and monitoring [24].

Indicators	Comparative study of computer security methodologies for countering cyber attacks		
	Methodology de ISSAF	Methodology de OSSTMM	Methodology de OWASP
Year Of Initiation	------	It was created in 2000 by ISECOM [11].	2001 [12]
Development Country	------	EEUU [11]	EEUU [13]
Benefit	The ISSAF methodology verifies the security of a network, system or application. The framework can explicitly focus on a specific target technology which may include routers, switches, firewalls, intrusion detection and prevention systems, storage networks, virtual private networks, various computer systems, operation, web application servers, databases, etc [25].	Based on the methodology it is promoted to have the very important points for this development plan, such as: move the content and create a barrier between it and other users, replace the threat from a harmless state and decrease the threat [23].	The OWASP methodology is a good quality tool that allows to create a strategy, both in web applications and in any other development project. It is often considered the side of conveying the importance of security to users and/or people who have no knowledge about security, such as: executives, developers or designers [13].

Results and Discussion

The different methods proposed on the basis of the methodologies that are being developed in the different fields are as follows: (a) ISSAF Methodology, (b) OSSTMM Methodology and (c) OWASP Methodology these mentioned methodologies are to have correct information security. [14] mentioned that ISSAF methodology is a study framework that is based on evaluating the information system in security analysis which is determined in various domains so it is evaluated by each specified evaluation criteria. In addition, the OSSTMM method is similar to the ISSAF method where it is argumentative in performing the evaluations by having quantitative security at the time of having risk by detailing the steps before, during and after a penetration assessment that is obtained through the methodology indicates [15]. However, the OWASP method allows having the difference in its theory because it has the functionality of focusing on computer security functions based on web applications that are safeguarded in the integrity of that methodology so it presents the analyses of assistance in decision making avoiding the vulnerability and risks that can assist in the time of cyber attacks that is obtained day after day [16].

On the other hand, [17] mentioned that the ISSAF methodology offers you a proposal to evaluate the controls so it is characterized in offering a high level of assurance in the vulnerabilities of critical risk in a computer security system, since, it is founded in its evaluation characterization the following important points such as: (a) risk assessment, (b) business

structure and management, (c) controls assessment, (d) commitment management, (e) security policy development, and (f) general best practices. This study is different from the OSSTMM methodology since it is characterized under the assessment point as: (i) reducing false-positive and false positive cases of reproducible security measurements, (ii) allowing to have a frame of reference of types of security tests in penetration testing and white box auditing and (iii) evaluating collected results that are consistent, quantifiable and confidence in the methodology [18]. Otherwise, the OWASP methodology is characterized based on the points where it is considered: the scope of testing, the start of testing, description of testing techniques, general clarification about the OWASP testing framework [18].

Accordingly, [20] described that the ISSAF methodology allows identifying the most important points in the analysis of information security thus having to (a) perform security testing and analysis, (b) establish the requirements, (c) define the methodology for the processes that are explained in testing, and (d) define the scope in different areas. Thus having the methodology, in the points raised we have an identification of risks, analyze, evaluate, and establish the reduction in its impact of measures. In addition, under the OSSTMM methodology for the elaboration of a methodology it is possible to have the difference under another method of computer security thus having the appropriate structure for the following elaboration, such as: (i) channels, (ii) modules, (iii) environments and (iv) security testing phases [21]. Therefore, the OWASP methodology is similar to the studies, since, it allows to have the proper relationship at the time of detecting an incident or risk threat regarding the web pages by the subject of different entities that is had through many hacking vulnerabilities that penetrate the violation of information security system [22].

On the other hand, [14] mentioned that the phases of the ISSAF methodology are taken in three very important points to carry out the control and evaluation tests: (a) Planning and Preparation, (b) Evaluation Reporting. and (c) Object Cleanup and Destruction. This study differs from the OSSTMM methodology having the paragraph that provides the information of phases to develop where it consists of having an appropriate structure such as: (i) Induction Phase, (ii) Interaction Phase, (iii) Investigation Phase, and (iv) Intervention Phase [23]. Moreover, in the methodology of this study OWASP is different because it has several stages that describes the structuring such as (1) Injection, (2) Broken authentication, (3) Exposure to sensitive data, (4) XML external entities, (5) Broken access control, (6) Incorrect security configurations, (7) Cross-site scripting, (8) Insecure deserialization, (9) Use of components with known vulnerabilities, and (10) Insufficient logging and monitoring [24].

Finally, [25] mentioned that the ISSAF methodology examines the structure of computer network security thus allowing to focus on a transparent framework in technology based on virtual private networks that are taken in web application and database servers. This study differs from the OSSTMM methodology that is had the elaboration of the benefits of as a structure for its development as it is had that: move the content and creates a barrier between it and other users, replace the threat of a harmless state and decrease the threat [23]. Therefore, the type of OWASP method is to have good tools and create strategies, thus contemplating web applications as any development project. Often this methodology bases on conveying the importance of computer security to people who do not contemplate huge knowledge such as executives, developers, or designers [13].

Conclusions

The following conclusions are: regarding the definition criterion, it can be determined that the OWASP methodology is the most appropriate because it foresees the possible future

difficulties that may arise due to inadequate decision making, focusing on protecting organizations through their web pages so that the probity of the organization is not questioned.

In addition, in relation to characteristics, the methodology of OSSTMM is convincing since, it assures to offer the most precise information in measure of security discarding to plenitude the possible errors thanks to the diverse security tests that possess which, will allow making an investigation to depth clarifying doubt and with trustworthy results. For that reason, this methodology was taken as one of the most outstanding in all the computer security parts that helps to prevent risks and always contemplates to give evaluations of tests.

On the other hand, about the criterion of methodical processes the ISSAF methodology is visualized with the most efficient one since, it is possible to carry out the suitable security tests to the organization defining its areas of scope in order to specify the risks, in addition, to estimate the decrease of the measures to its effect.

On the other hand, regarding the phases, the OSSTMM methodology is appropriate in view of the fact that it offers total security for the company to which it provides the service by the adequate configuration and verification for a good audit report, which is associated with ethical hacking.

Finally, in relation to the benefit of the OWASP methodology, given that it provides the securitization strategy in all types of projects for the company in which it will be carried out, however, it does not supplant the people who are experts in security; on the contrary, it facilitates the understanding to people who do not have a broad knowledge of it, such as executives or any person who are in charge of the operation of the company.

Recommendations

The recommendations are the following: this study was conducted under the qualitative approach, because of this in the future it can be elaborated in a quantitative one allowing to evaluate the performances of each methodology and to be able to base the objectives to obtain results for each criterion. On the other hand, it can be synthesized in a study of evaluation of different methods or types to develop methodologies based on information security, thus having the differences and similarities focused on large companies and seeing the effectiveness against the implemented methodology. In addition, this investigation can increase since this study can be elaborated in a mixed margin, since, it possesses in the qualitative method as quantitative to obtain more efficient results and quality of presentation in the article. In synthesis, the different indicators should be raised to develop more comparative methodologies and thus to have more studies in the different parts of the world to develop for each category of security. Finally, it is proposed to continue developing this research in different variables based on computer security methodologies that help to encourage students to elaborate scientific articles based on computer security, information security, and others.

References

V. Gauthier, R. Méndez, J. Cano, J. Ramió and L. Sánchez. Computer security. (2020)
A. Paredes, I. Quevedo, L. Chalacán. Computer security in SMEs in the city of Quevedo. Journal of business and entrepreneurial studies. 4, 2 (2020)
J. Cartuche, D. Hernández, R. Morocho and C. Radicelli. Security iot: main threats in an asset taxonomy. Hamut'ay. 7, 3 (2021)

M. Huerta, J. Ferreira, L. Rodriguez, R. Clotet, R. Gonzales and D. Rivas. Design of a building security system in a university campus using RFID technology. (2017)
E. Carvajal. Technologies, computer security and human rights. IUS ET SCIENTIA. 4, 1 (2018)
J. Marín, A. Patiño and J. Acevedo. Implementation of a computer perimeter security system using VPN, firewall and IDS. Universidad Católica de Oriente Journal. 31, 45 (2020)
R. Roque and C. Juarez. Awareness and training to increase computer security in university students. PAAKAT: journal of technology and society. 8, 14 (2018)
M. De martini and M. Rios. The impact generated by computer security in Mendoza's SMEs. (2019)
W. Madrigal. Computer security. (2019)
R. Zambrano. Study on the knowledge and applicability of computer security in companies. (2018)
J. Allaica. Computer security audit following the Open Source Security Testing Methodology Manual (OSSTMM) for the company MEGAPROFER SA. (2020)
M. Gallegos. Implementation of controls to a web application using owasp methodology for security assurance. (2019)
V. Chavarria. Study of attacks against website. OWASP. (2020)
E. Silva and M. Ducuara. Procedural Design for the Protection of SQL Injection Attacks SQL and NOSQL Databases. (2017)
L. Chappell and G. Combs. Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide. Reno: Chappell University. (2016)
J. Delgado. Análisis de seguridad mediante metodología OWASP a redes inalámbricas en universidad laica Eloy Alfaro de manabi extensión en el Carmen. (2020)
H. Paltan. Development of a computer security mitigation plan to a wireless data communication network for a private institution, through the application of ethical hacking to identify threats, risks and vulnerabilities. (2019)
Y. Cruz. OSSTMM methodology for the detection of security bugs and vulnerability in 64-bit operating systems at the end-user level. (2016)
B. Lindao and K. Pilco. Development of a security model for wordpress based on Owasp. (2020)
M. Hurtado and L. Mendaño. Implementation of ethical hacking techniques for the discovery and evaluation of vulnerabilities of the network of a state portfolio. (2016)
Y. Cruz and C. Martinez. OSSTMM methodology for the detection of security bugs and vulnerability in 64-bit operating systems at the end-user level. Scientific journal Dominion of Sciences. (2017)
R. Rault, L. Schalkwijk, M. Agé, N. Crocfer, R. Crocfer, D. Dumas and ... S. Lasson Seguridad informatica - Hacking Ético. Barcelona: Ediciones ENI. (2015)
D. Gordón and R. Pacheco. Análisis de Estrategias de Gestión de Seguridad Informática con Base en la Metodología Open Source Security Testing Methodology Manual (OSSTMM) para la Intranetde una Institución de Educación Superior. Computational Computing. 1 (2018)
D. Kellezi, C. Boegelund, and W. Meng. Securing open banking with Model-View-Controller architecture and OWASP. Wireless communications and mobile computing. (2021)
E. Diaz. Analysis of penetration testing methodologies using Ethical Hacking. (2018)

Author

Francisco Manuel Hilario Falcón

Professor and researcher with experience in various studies and several publications in indexed journals. He is a systems engineer, master in systems engineering, doctor in systems engineering. Member of the College of Engineers of Peru with Reg. CIP No. 99835. Professional experience as Information Technology and Telecommunications Manager, Statistics and Informatics Manager, Information Technology Consultant, IT Project Manager, Virtual Classroom Administrator, Systems Analyst, Information Technology Specialist. International certifications: Scrum Master Certified (SMC) ID: 712972. Scrum Fundamentals Certified (SFC) ID: 715526. Cybersecurity Management Certification - ISO-27032 N° 200600094-19050005. Information Security Management and Administration Certification - ISO-27001 N° 200700052-19050007. Digital Transformation Certification N° GS3 HHP QYP.

Author

Milner David Liendo Arévalo

Work experience of more than 23 years in Information Technology and Business Management. Experience as Project Manager and Project Leader guided by the PMI model. Experience in Implementation of IT Best Practices ITIL V04, ISO20000. Experience in Processes and Procedures Implementation with BPM. Experience in Strategic Planning consulting and Business Intelligence management. Expert in IT consulting and support. Experience as University Professor in Undergraduate and Postgraduate and belonging to the scientific community of CONCYTEC. Experience in Smart Cities and Digital Transformation Projects.

Author

Giancarlo Sanchez Atuncar

Systems Engineer graduated from the Universidad César Vallejo, has a Master's Degree in Systems Engineering with mention in Information Technology, has a Diploma in Didactics and Graduate Research, has a second specialty in Information Technology and Communication, at the University Esan. He is currently a PhD Candidate in Systems Engineering at the Universidad Nacional Federico Villarreal, is a Senior Professor at the Universidad Cesar Vallejo, and is a member of the College of Engineers of Peru with recognition for more than 8 years of experience as a Systems Engineer.

Author

Ivan Crispin Sanchez

Systems Engineer graduated from the Universidad Nacional Federico Villarreal, has a Masters Degree in University Teaching from the Universidad Cesar Vallejo, has a Diploma in Graduate University Teaching, and a second Masters Degree with mention in "Senior Management". and a second Masters degree with mention in "Senior Management". Professional experience as Head of Information Technology and Telecommunications, Information Technology Consultant, IT Project Manager, Systems Analyst, IT Professional Specialist. He is currently a PhD candidate in Systems Engineering at the Universidad Nacional Federico Villarreal, He is a university

professor with more than 15 years in several universities, and is a member of the Peruvian College of Engineers with Reg. CIP N° 58591 with recognition for more than 20 years of experience as a Systems Engineer.