EVALUATION METHODOLOGIES PTES AND ISSAF OF PENETRATION TESTING FRAMEWORKS

THESIS

Submitted to Fulfill One of the Requirements in Obtaining a Master of Informatics (S2) Degree

ARDI PANJAITAN

20220130004

INFORMATION MASTER STUDY PROGRAM
NUSA PUTRA UNIVERSITY
SUKABUMI
2024

AUTHOR'S STATEMENT

TITLE	: ANALYSIS AND EVALUATION OF ISSAF AND PTES FRAMEWORKS FOR PENETRATIO NTESTING
NAME	: ARDI PANJAITAN
NIM	: 20220130004

I declare and take responsibility that this thesis is my own work except for excerpts and summaries, each of which I have explained the source of. If in the future another party claims that this thesis is his work, accompanied by sufficient evidence, then I am willing to have my Bachelor of Computer/Bachelor of Engineering degree canceled along with all the rights and obligations attached to that degree.

Thus, I have made this statement letter truthfully and without coercion from anyone.

Sukabumi, August 2024

ARDI PANJAITAN

THESIS APPROVAL

TITLE	: ANALYSIS AND EVALUATION OF ISSAF AND PTES FRAMEWORKS FOR PENETRATIO NTESTING
NAME	: ARDI PANJAITAN
NIM	: 20220130004

This thesis has been reviewed and approved

Head of Study Program,	Supervisors,
Prof. Ir. Teddy Mantoro, M.Sc., PhD.	Deshinta Arrova Dewi, S.Kom., M.Sc., PhD.
NIDN	NIDN

THESIS VALIDATION

TITLE	: ANALYSIS AND EVALUATION OF ISSAF AND PTES FRAMEWORKS FOR PENETRATIO NTESTING
NAME	: ARDI PANJAITAN
NIM	: 20220130004

This thesis has been tested and defended before the Board of Examiners at the Thesis Session on 04 August 2024. In our opinion, this thesis is adequate in terms of quality for the purpose of awarding the degree of Bachelor of Computers (S.Kom)/Bachelor of Engineering (ST)/Bachelor of Design (S. etc.).

Sukabumi, December 2024

Supervisor I	Examiner I
Deshinta Arrova Dewi, S.Kom., M.Sc., PhD	Prof. Ir. Teddy Mantoro., M.Sc., Ph.D
NIDN	NIDN
Supervisor II	Examiner II
Dini Oktarina Dwi Handayani., ST, M.Sc	Haris Al Qodri Maarif., M.Sc., PhD
NIDN	NIDN

DEDICATION

With all gratitude to God Almighty, love, and humility, I dedicate this work to:

1. Father and Mother

The pillars of my life, who have taught me the meaning of perseverance, sincerity, and unconditional love. Every prayer and drop of your sweat is the fuel for my spirit to keep moving forward. This thesis is proof that your love and prayers can turn dreams into reality.

2. My Supervisors and Lecturers

Who are like lanterns of knowledge, have patiently guided me through this academic labyrinth. Every word, advice, and direction from you is a solid foundation for every page I write. This work was born from your dedication to creating a better generation.

3. Friends and Comrades

A piece of the mosaic of this journey, who have shared laughter, tears, and hard work. Thank you for being irreplaceable traveling companions, who are always present in the most difficult and most beautiful moments.

4. Indadi Group

Thank you for supporting this journey both materially and immaterially. providing opportunities, trust and encouragement to continue moving forward to become invaluable inspiration.

Hopefully this contribution can provide a broad and sustainable positive impact for many parties.

5. My Beloved Alma Mater

a place where my little dreams were given wings to fly high. Thank you for being a second home full of inspiration, a place where my knowledge and character were forged to be stronger.

Hopefully this work will not only be a sheet of paper, but also a small legacy that can benefit many people. Thank you for all the support, prayers, and love that have made it possible.

FOREWORD

Praise be to the presence of God Almighty for all His mercy and grace so that the author can complete this thesis well. This thesis entitled "Evaluation Methodologies PTES And ISSAF Of Penetration Testing Frameworks" was prepared as one of the requirements for obtaining a Master's degree in the Informatics Study Program at Nusa Putra University. In the process of preparing this thesis, the author has received assistance, guidance and support from various parties. Therefore, the author would like to express his deep gratitude to:

1. Dr. Kurniawan, ST., M.Sc., MM as Chancellor of Nusa Putra University;
2. Prof. Ir. Teddy Mantoro, M.Sc., PhD as Head of School Computer Science Nusa Putra University;
3. Deshinta Arrova Dewi, S.Kom., M.Si., PhD and Dini Oktarina Dwi Handayani, ST, M.Sc as Supervisors;
4. All Master Of Computer Science Lecturers who have provided very usefull knowledge during lectures;
5. Parents and my family for their supports, patience, prayers and never getting tired of educating and giving, both material and non-material;
6. Fellow comrades in Master of Computer Science 2022 who always give encouragement and always accompany from the beginning of the lecture until now;
7. All parties who have assisted the author in writing this thesis;

The author would also like to express his thanks to family, friends, and all parties who cannot be mentioned one by one for their invaluable support and prayers. Finally, the author hopes that this thesis can provide positive benefits and contributions to the development of science, especially in the field of information system security.

LIST OF FIGURES

LIST OF TABLES

CONSENT SHEET

THESIS TITLE : ANALYSIS AND EVALUATION OF ISSAF AND PTES FRAMEWORKS FOR PENETRATIO NTESTING

NAME : ARDI PANJAITAN
NIM : 20220130004

THIS SCRIPT HAS BEEN CHECKED AND APPROVED

SUKABUMI, …….

Table of Contents

ABSTRACT

Currently, technological developments in the information sector have developed rapidly, so that cyber security is quickly becoming a strategic priority for both government and private organizations in facing various types of cyber attacks. Therefore, penetration testing plays a key role in assessing the security posture of information systems. Selection of the right penetration methodology is critical for effective testing. Penetration testing is one strategy used to mitigate the risk of cyber attacks. In this research analyzes and compares the methodology and framework provided by PTES and ISSAF. Methodology evaluations cover a variety of factors, including methodological depth, effectiveness, coverage, ease of use, and community support. Additionally, this research also explores practical applications, case studies, and real-world implementations of both methodologies to assess their capabilities in identifying and resolving security vulnerabilities. This research details the framework quality assessment of each method using Gab Analysis, Quality Metrics and Evaluation, and Framework Quality Evaluation. The findings from this research are expected to provide valuable insight into the strengths and weaknesses of PTES and ISSAF, assisting cybersecurity professionals and organizations in selecting the most appropriate methodology for their penetration testing needs. This research contributes to the ongoing discussion in the field of cybersecurity and aims to improve overall security practices by guiding in the selection of the most appropriate penetration testing methodology.

.

Keywords: PTES, ISSAF, Penetration Testing, website vulnerability, Reporting, ISO/IEC 25010:2013

.

BAB I
INTRODUCTION

1.1. Research Background

In an increasingly digital era, cyber attacks have become a very serious threat to countries, organizations and individuals. Cyberattacks can have a devastating impact on national security, corporate vulnerabilities, and even individual privacy.

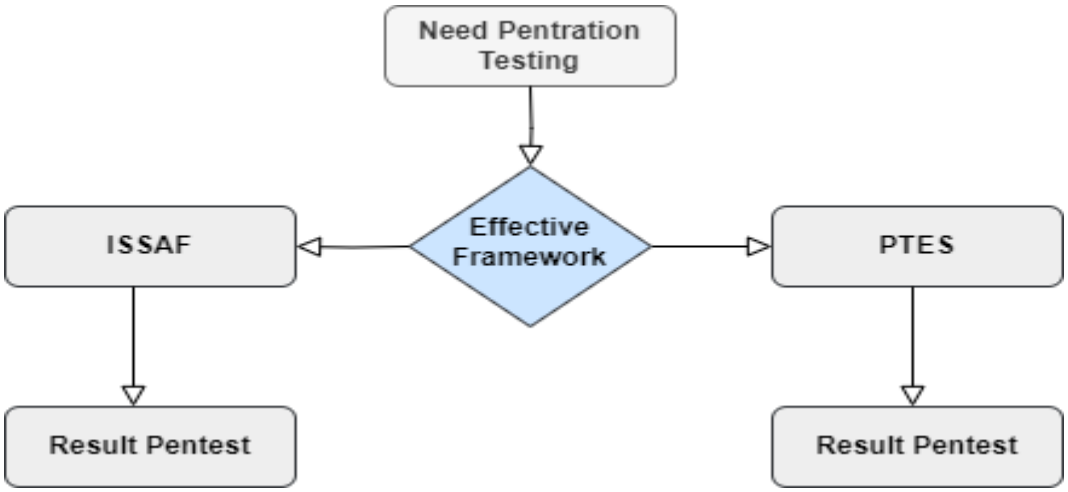
In the midst of this dynamic, the National Cyber and Crypto Agency (BSSN) as the institution responsible for cyber security in Indonesia has an important role in monitoring, reporting and dealing with cyber attacks. According to a report on the official website of the National Cyber and Crypto Agency (BSSN), in August 2023 there were 78,464,385 cases of traffic anomalies (Trojan Activity: 42,857,779, Malware: 15,595,053, Information Leak: 8,134,901, Exploit : 1,170,349, Advance Persistent Threat: 426,069, Web Application Attack: 410,573, Denial Of Service: 98,088 and Information Gathering: 23,665). In the same month, BSSN discovered 290,556 exposure data findings from 431 affected agencies and there were 19 cases of site hacking in August 2023, many of which were carried out on hidden pages and on weekdays from 18.00-06.00. The most frequent incident indications in the notifications sent were traffic anomalies and followed by Data Breach, Web Defacement, and Sensitive Data Exposure.

With the increasing number of data breaches and cyber attacks cyber security has become increasingly urgent. One of the key approaches in improving security is penetration testing, which is an important process for testing and identifying security vulnerabilities in a system. In the context of increasing cyber threats and the need to identify and address security vulnerabilities, organizations and cybersecurity professionals are faced with the challenge of selecting appropriate methodologies for penetration testing. There are two main methodologies that are often used, namely the Penetration Testing Execution Standard (PTES) and the Information Systems Security Assessment Framework (ISSAF), however, there has been no comprehensive evaluation that compares and evaluates these two methodologies. This research aims to investigate, compare, and

evaluate the PTES and ISSAF methodologies in the context of penetration testing. In the ever-changing and evolving world of cyber security, choosing the right methodology can have a major impact on the success of an organization's cyber security efforts.

By deeply understanding the characteristics, strengths, and weaknesses of each methodology, we can provide cybersecurity professionals and organizations with valuable insight into the best options for penetration testing to suit their needs. Through this comprehensive analysis, we can better understand how PTES and ISSAF methodologies can contribute to efforts to protect valuable information and reduce security risks in an increasingly complex cyber environment.

1.2. Problem Statement



Figures1: Penetration Testing Framework Problem

In an era of rapid development of information technology, cyber security has become a strategic priority for the government and the private sector. Increasingly sophisticated and diverse cyberattacks have become a serious threat that can damage information systems, organizations and individuals, resulting in significant losses. To deal with these threats, penetration testing has become a key approach in assessing the security posture of information systems. The two main methodologies often used in penetration testing are the Penetration Testing Execution Standard (PTES) and the Information Systems Security Assessment Framework (ISSAF). However, choosing the right methodology is a challenge for organizations, because

there has been no comprehensive evaluation comparing these two methodologies. Understanding the different characteristics, strengths, and weaknesses between PTES and ISSAF is a critical aspect to ensure effective and efficient security testing.

1.2.1 Problem Domains

a) PTES and ISSAF have different approaches to conducting information system security testing, which can lead to inconsistencies in test results between organizations.

b) These two frameworks do not fully accommodate the latest technological developments such as cloud computing, Internet of Things (IoT), and artificial intelligence in their testing methodology.

c) There is a gap between the specific needs of organizations and the scope of methodologies offered by PTES and ISSAF, especially in the face of evolving cyber threats.

1.2.2 Scientific Problems

a) There has been no comprehensive comparative study to analyze the effectiveness and efficiency of PTES and ISSAF in the context of continuously evolving cyber security threats.

b) Lack of integration between these two frameworks with current industry security standards such as the NIST Cybersecurity Framework or ISO 27001, which can hinder the adoption of best practices in security testing.

c) Limitations in measuring and comparing the impact of using PTES and ISSAF on improving the organization's overall security posture.

This research aims to investigate, compare, and evaluate the characteristics, advantages, and weaknesses of the PTES and ISSAF methodologies in the context of penetration testing. The analysis will cover the following aspects.

a). The structure and flexibility of each framework to accommodate various testing scenarios.

b). The depth and breadth of testing offered by both methodologies.

c). Ability to adapt to the latest technological developments and cyber threats.

d). Effectiveness in detecting and resolving vulnerabilities in various types of systems and infrastructure.

e). Suitability to the needs and resources of various types of organizations.

In addition, this research will explore the relevance of both frameworks in the context of current cyber threats, such as data leaks or frequent data breaches. The aspects that will be analyzed are as follows.

a). PTES and ISSAF's ability to test the security of systems that are vulnerable to data leaks, including platforms that process sensitive data such as personal or financial information.

b). The effectiveness of both frameworks in detecting vulnerabilities that could lead to data breaches, such as weaknesses in data encryption or user identity management.

c). The suitability of the methodology in addressing unique security challenges associated with data leaks, such as handling big data or mitigating risks associated with data storage and transfer.

d). The framework's ability to assess compliance with data protection regulations such as GDPR or local regulations specific to personal data management.

Through an in-depth understanding of these two methodologies, this research aims to provide better guidance to cybersecurity professionals and organizations in selecting the methodology that best suits their needs. It is hoped that the results of this research will provide valuable insights in efforts to improve cyber security practices, optimize the penetration testing process, and deal more effectively with growing cyber threats.

1.3. Research Objectives

1. Analyze and compare the PTES and ISSAF methodologies, identifying the strengths, weaknesses, and key differences between the two in the context of penetration testing with a focus on effectiveness in dealing with evolving cyber threats.

2. Assess the relevance of both frameworks to data leaks, evaluate the extent to which PTES and ISSAF can be used to identify, detect and address vulnerabilities that can cause data leaks, as well as compliance with data protection regulations such as GDPR.

.

1.4. Research Significance

In the ever-evolving digital era, cyber attacks have become a serious threat to countries, organizations and individuals. Based on a report from the National Cyber and Crypto Agency (BSSN) in August 2023, there were millions of cases of traffic anomalies, trojan activity, malware, information leaks, exploits and web application attacks. This research provides significant cybersecurity improvements by understanding and comparing PTES and ISSAF penetration testing methodologies. Through in-depth analysis, this research helps organizations select the most effective methodology to identify and address security vulnerabilities, ultimately improving their cybersecurity posture. Apart from that, this research also aims to reduce the risk of cyber attacks. By providing practical guidance in selecting an appropriate penetration testing methodology, organizations can reduce the risk of cyberattacks and the negative impacts they may have.

This research also makes a significant contribution to academic knowledge in the field of cybersecurity. By providing a comprehensive evaluation and comparison between two major penetration testing methodologies, PTES and ISSAF, this study adds to the existing literature and provides a basis for further research. It is hoped that the results of this research will provide valuable insights for cybersecurity professionals. In choosing the most appropriate methodology for penetration testing, these insights will help them improve their overall security practices, thereby providing better guidance in dealing with increasingly complex cybersecurity challenges.

This research not only provides practical benefits but also has broad implications in the field of cyber security. By understanding the differences and advantages of each methodology, organizations can make more informed and strategic decisions in protecting their digital assets. Support from this research is expected to advance cybersecurity practices and provide a strong foundation for the development of future penetration testing methodologies.

1.5. Problem Limitations and Research Assumptions

This research has several limitations and assumptions that need to be considered. First, the limited scope of the methodology. This research only discusses two main methodologies, namely PTES and ISSAF. There are many other

methodologies that may also be relevant but are not within the scope of this study. Second, assumptions about data and infrastructure. This research assumes that the data and infrastructure tested have characteristics that can be fairly compared between the two methodologies. Significant differences in system or network type may affect test results. Third, the limitations of the case study. Evaluation of the effectiveness of the methodology is carried out through specific case studies that may not cover all real-world scenarios. Therefore, the results of this study may not fully reflect the effectiveness of the methodology in different contexts. Fourth, limited time and resources. This research was conducted within a limited time frame and resources, which may have affected the depth of analysis and number of case studies that could be conducted. Fifth, community support and updates. This research assumes that the current level of community support and updates received by PTES and ISSAF remains constant. Changes in support or future methodology updates may affect the results of the study. These limitations and assumptions are important to consider so that the interpretation of research results can be carried out more precisely and objectively.

Nusa Putra
UNIVERSITY
2002
AMOR DEUS, PARENTIUM, CONCERVIS

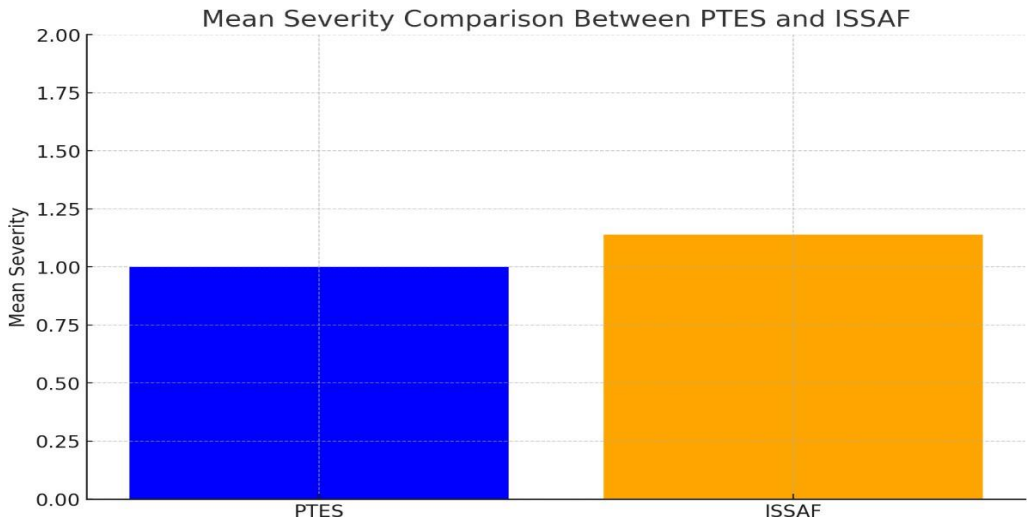
BAB V
CONCLUSIONS AND RECOMMENDATIONS

5.1. Conclusion

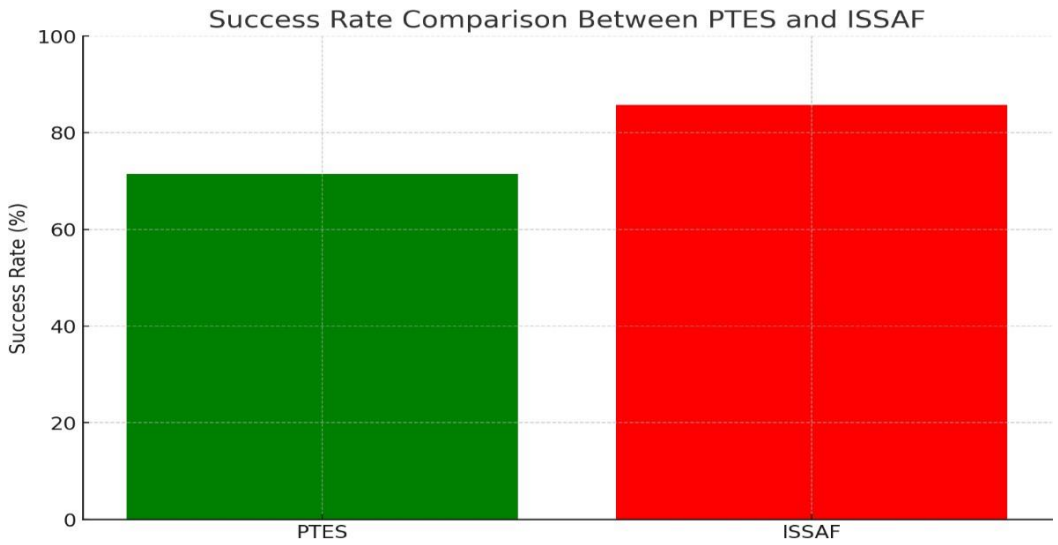
This conclusion provides a brief summary of the analyzes conducted in this document. Starting with a statistical analysis comparing the severity and efficacy of the PTES and ISSAF frameworks, it continues with a thematic analysis highlighting the important phases and tools used in security testing. Comparative analysis shows the difference in approach between PTES which is more aggressive in exploitation and ISSAF which is more focused on in-depth reporting and mitigation. In addition, this document also maps the application of the framework to the ISO/IEC 25010:2013 and ISO/IEC 25012 standards, and emphasizes the importance of data quality in security testing. The general conclusion confirms that both frameworks have their own strengths and weaknesses, with different focuses on dealing with security threats.

1. Data Analysis and Statistics

This document begins with a statistical analysis that includes calculations such as the mean severity level, success rate, as well as a comparison between the PTES and ISSAF frameworks. Mean Severity for PTES is around 1.0, while for ISSAF it is around 1.14. The PTES success rate was recorded at 71.43%, while ISSAF reached 85.71%. This data provides an overview of the effectiveness and severity of threats faced in testing with these two frameworks.



Figures24: Mean Severity Level



Figures25: Success Rate

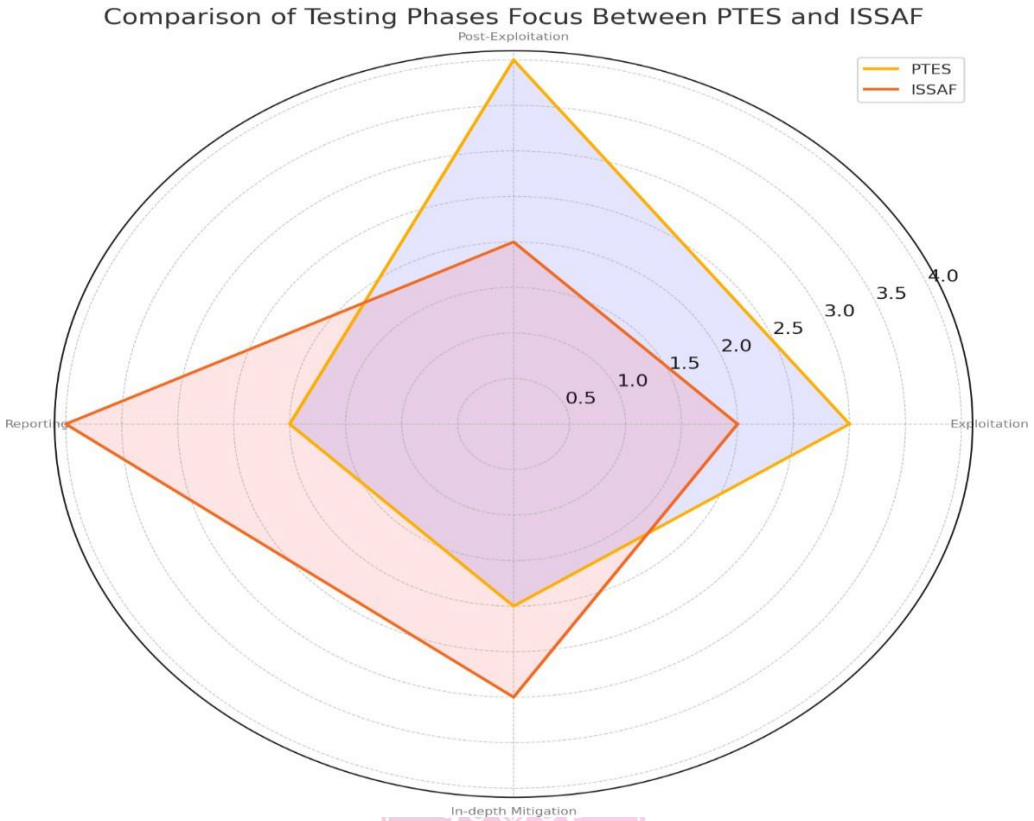
2. Thematic Analysis

The thematic analysis in this document identifies the main themes that emerged in the security testing process using PTES and ISSAF. Some important findings include. The second Testing phase of the framework highlights the importance of the Vulnerability Assessment phase in identifying critical vulnerabilities. Tools Used nmap and Metasploit are the primary tools used in both frameworks, reflecting industry standards in security testing. Frequently discovered vulnerabilities in default credentials and common configurations emphasize the importance of strong security policies. Recommended Mitigation Software updates and credential changes are the most commonly recommended mitigation actions.

3. Comparative Analysis

The comparative analysis compares PTES and ISSAF based on various aspects, such as testing phases, tools used, vulnerabilities identified, and mitigation strategies. PTES places more emphasis on exploitation and post-exploitation, while ISSAF focuses more on in-depth reporting and mitigation. PTES uses Greenbone for additional vulnerability assessment, while ISSAF is more flexible in exploitation using Metasploit. This difference suggests a more aggressive approach

from PTES in exploiting vulnerabilities, while ISSAF prioritizes long-term compliance and mitigation.



Figures26: Comparison of Testing PTES and ISSAF

Radar graph depicting a comparison of the focus on the testing phase between two security frameworks, namely PTES and ISSAF. The following is an explanation of each aspect compared in the graph:

a. Exploitation

PTES has a greater focus on the exploitation phase. This suggests that PTES is more likely to aggressively exploit vulnerabilities discovered during testing. On the other hand, ISSAF also covers exploitation, but with a slightly lower focus compared to PTES, indicating a more balanced or perhaps more conservative approach in this aspect.

b. Post-Exploitation

PTES focuses significant efforts on the post-exploitation phase, which includes steps after successful exploitation to understand the broader impact of the exploited

vulnerability. ISSAF, on the other hand, shows a relatively balanced focus in this phase, still highlighting its importance but not as intensively as PTES.

c. Reporting

ISSAF shows a higher focus on reporting compared to PTES. This shows that ISSAF emphasizes the importance of in-depth and detailed documentation in reporting test results. PTES may be more practical and direct in its approach, with a greater focus on action rather than reporting.

d. In-depth Mitigation

ISSAF is placing greater emphasis on in-depth mitigation, involving not only quick fixes but also long-term strategic steps to strengthen security. PTES may provide mitigation recommendations, but its primary focus remains on exploitation and direct understanding of the vulnerability. Overall, this graph shows that PTES tends to focus more on direct action and exploitation, whereas ISSAF places greater attention on in-depth reporting and mitigation. This approach reflects the philosophical differences between the two frameworks in handling security testing, where PTES is more oriented towards technical exploitation, while ISSAF emphasizes compliance and long-term protection.

4. Quality In Use ISO/IEC 25010

Based on an in-depth evaluation using the "Quality in Use" dimension from ISO/IEC 25010, we can draw several important conclusions regarding two penetration methodologies, namely PTES (Penetration Testing Execution Standard) and ISSAF (Information Systems Security Assessment Framework). Each methodology has strengths and weaknesses that can impact the effectiveness and efficiency of security testing.

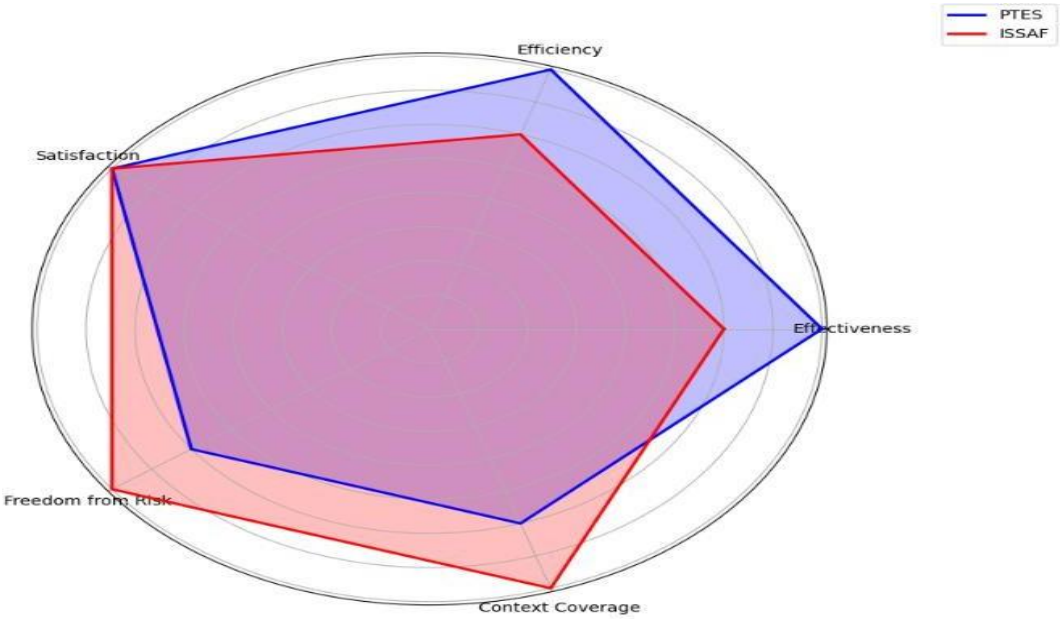
Effectiveness shows that PTES is superior in terms of speed of vulnerability identification, which is especially important in scenarios where rapid action is required. However, the weakness of PTES lies in the lack of depth of analysis, which can cause some vulnerabilities to not be fully detected. In contrast, ISSAF is more in-depth in its approach, although slower, allowing for more comprehensive identification of vulnerabilities. However, this slower approach can be a drawback in situations where speed is a key factor.

Efficiency measures how quickly and resource-efficient the methodology is in achieving goals. PTES excels in efficiency, using tools such as Nmap and Metasploit that enable fast detection. However, this efficiency sometimes comes at the expense of test coverage. ISSAF, although more systematic, tends to be less efficient in the use of resources and time, which may not be ideal in conditions that demand rapid results.

Satisfaction or user satisfaction also plays an important role in determining a more appropriate methodology. PTES provides fast results that are satisfying for users who need fast testing, but its lack of depth of analysis can reduce satisfaction for those who need more detailed reports. On the other hand, ISSAF provides more comprehensive reports that tend to satisfy users who require in-depth analysis, although it takes longer.

Freedom from Risk assesses a methodology's ability to minimize risk. PTES is effective in quickly reducing immediate risks, but focusing on quick exploits can lead to hidden vulnerabilities that go undetected, increasing long-term risks. ISSAF, with its more in-depth approach, is better at reducing long-term risks, although it can be slower to detect immediate threats.

Context Coverage or context coverage is an assessment of how well a methodology can function in various operational conditions. PTES is designed to function in a variety of test scenarios with good flexibility, but its limited scope may not cover all different operational contexts. ISSAF offers broader and more detailed coverage, which can be an advantage in more complex tests, although it requires more time and resources. Overall, the choice between PTES and ISSAF depends on the specific testing needs. PTES is better suited to situations where speed and efficiency are critical, while ISSAF is better suited to scenarios where depth of analysis and more comprehensive coverage are required. In some cases, a combination of these two methodologies may provide optimal results, with PTES used for initial rapid testing and ISSAF used for subsequent in-depth analysis.



Figures27: Quality In Use ISO/IEC 25010

5. Data Quality Characteristics

In the context of data quality, this document emphasizes the importance of various characteristics, such as accuracy, completeness, consistency and credibility. PTES and ISSAF ensure that the data used in testing and safety assessments is accurate, complete and reliable, and complies with applicable standards.

6. General Conclusion

Overall, this document provides a comprehensive overview of how PTES and ISSAF are used to identify and address security threats in information systems. Both frameworks have their strengths and weaknesses, with PTES focusing more on aggressive exploitation and ISSAF placing more emphasis on long-term mitigation and compliance. A deep understanding of data characteristics and product quality is also an important aspect in ensuring the success of testing and the security of the system being tested.

5.2. Recommendations

These recommendations will highlight the importance of a security strategy that is integrated and tailored to an organization's needs. In the face of increasingly complex security threats, organizations need to combine the advantages of various approaches to create more effective and resilient protection systems. The following

recommendations offer concrete steps to leverage the strengths of PTES and ISSAF, adapt security strategies based on organizational context, and build a proactive and sustainable security culture.

1. Combine PTES' Aggressive Exploitation Approach with ISSAF's Deep Mitigation.

The aggressive exploitation approach promoted by PTES offers the advantage of detecting and deeply understanding the potential impact of each discovered vulnerability. By exploiting technical system weaknesses, PTES allows organizations to see the extent to which vulnerabilities can be exploited by attackers in real-world scenarios. However, without proper mitigation and in-depth reporting, these exploits may not provide long-term benefits to system security. On the other hand, ISSAF is known for its strong focus on comprehensive reporting and in-depth mitigation strategies. This framework helps organizations to not only fix existing vulnerabilities, but also strengthen overall security through the implementation of more stringent and ongoing security policies and procedures. By combining the aggressive approach of PTES and the mitigation strategy and in-depth reporting of ISSAF, organizations can ensure that any vulnerabilities discovered are not only effectively exploited, but also followed up with robust mitigation measures. This integration will create a balance between technical detection and long-term protection, providing a more solid layer of security that is resilient to evolving threats.

2. Adjust Security Strategy Based on Organizational Needs and Context.

Every organization has unique security needs that are influenced by factors such as industry, size, regulations, and the level of threats they face. Therefore, it is important to adapt the implementation of the security framework based on the identified advantages and disadvantages of PTES and ISSAF. Organizations in high-risk industries such as finance or healthcare may prioritize in-depth mitigation and structured reporting to ensure compliance with strict regulatory standards. In this case, ISSAF with its focus on long-term audit and mitigation may be the primary choice, with the exploitation element of PTES used to ensure the most critical vulnerabilities are also prioritized. In contrast, for organizations operating in a more dynamic environment and focused on rapid response to threats, the

aggressive exploitation approach of PTES may be preferred. However, this must be balanced with ISSAF's mitigation strategies to ensure that any exploits are followed by remedial actions that not only address the problem temporarily but also prevent similar attacks in the future. By adapting strategies based on operational context, organizations can ensure that they not only react to threats, but also proactively protect their information assets through the approach that best suits their needs.

3. Building a Proactive Security Culture with a Combined Approach.

The combined approach of PTES and ISSAF not only provides technical advantages, but can also help in building a more proactive security culture within the organization. By involving multiple teams in the exploitation and mitigation process, from technical to managerial, organizations can increase awareness and commitment to the importance of information security at all levels. An aggressive exploitation approach can improve a security team's technical skills, while in-depth reporting and mitigation can provide greater insight into business impact and regulatory compliance. This will create an environment where the team not only focuses on identifying problems, but also on solving and preventing them in the future.

4 Invest in Training and Team Capacity Building.

Combining these two frameworks also requires investment in training and capacity building of security teams. PTES requires strong technical skills in exploitation, while ISSAF requires deep analytical capabilities in reporting and mitigation. Proper training will ensure that the team is able to execute both aspects effectively and add value to the overall security of the organization.

With this longer and more accurate approach, organizations can build a security strategy that is not only reactive but also proactive, able to respond to existing threats while preparing for future challenges.

REFERENCES

Sanjaya, I. G. A. S., Sasmita, G. M. A., & Sri Arsa, D. M. (2020). Information technology risk management using ISO 31000 based on issaf framework penetration testing (Case study: Election commission of x city). International Journal of Computer Network and Information Security, 12(4), 30–40.

Alhamed, M., & Rahman, M. M. H. (2023). A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. In Applied Sciences (Switzerland) (Vol. 13, Issue 12). MDPI.

Nabila, M. A., Mas'udia, P. E., & Saptono, R. (2023). Analysis and Implementation of the ISSAF Framework on OSSTMM on Website Security Vulnerabilities Testing in Polinema. Journal of Telecommunication Network, 13(1).

PManuel, F., Falcón, H., David, M., Arévalo, L., Sanchez Atuncar, G., & Crispin Sanchez, I. (n.d.). Comparative Study of Computer Security Methodologies for Countering Cyber Attacks (Vol. 13).

Sarker, K. U., Yunus, F., & Deraman, A. (2023). Penetration Taxonomy: A Systematic Review on the Penetration Process, Framework, Standards, Tools, and Scoring Methods. Sustainability, 15(13), 10471

Mardianto, I., Sediyono, A., & Hafzan, A. (2015). Analisa Kerentanan Sis.trisakti.ac.id Menggunakan Teknik Vulnerability Scan. JETri, 13(1), 90-100. ISSN 1412-0372.

Rafeli, A. I., Seta, H. B., & Widi, I. W. (2022). Pengujian Celah Keamanan Menggunakan Metode OWASP Web Security Testing Guide (WSTG) pada Website XYZ. Jurnal Informatik, 18(2), 97-103. ISSN 2655-139X (ONLINE), ISSN 0216-4221.

Goel, J. N., & Mehtre, B. M. (2015). Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. Procedia Computer Science, 57, 710–715. https://doi.org/10.1016/j.procs.2015.07.458.

Mushlih, M., Fitri, R., & Wardiah, I. (2019). Penetration Testing Tool untuk Menguji Kerentanan SQL Injection Secara Otomatis Berbasis Web. Prosiding SNRT (Seminar Nasional Riset Terapan) Politeknik Negeri Banjarmasin, 7 November 2019, 1-5.

Ardita, I. K. A. O., Dwidasmara, I. B. G., & Widiartha, I. M. (2023). Analisis Kerentanan Sistem Informasi Berbasis Website Menggunakan Metode Penetration Testing. Jurnal Pengabdian Informatika, 1(4), 1043–1046.

Prastika, D. P., Triyono, J., & Lestari, U. (2019). Audit dan Implementasi CIS Benchmark pada Sistem Operasi Linux Debian Server (Studi Kasus: Server Laboratorium Jaringan dan Komputer 6, Institut Sains & Teknologi AKPRIND Yogyakarta). Jurnal JARKOM, 6(1), 1-6. E-ISSN: 2338-6304.

Nugroho, A. H. S. (2023). Vulnerability Assessment Web Proposal Tugas Akhir Mahasiswa Menggunakan Acunetix dan NMAP. e-Proceeding of Engineering, 10(2), 1615-1621.

Ashar, R. (2022). Analisis Keamanan Open Website Menggunakan Metode OWASP dan ISSAF. Jurnal Informasi dan Teknologi, 4(4), 211-218.

Nelsa, P., Ramadhani, L., & Rahmad, B. (2022). Evaluasi Kualitas Layanan Sistem Informasi Nota Dinas Elektronik (NDE) PT Telkom Indonesia Tbk Menggunakan Standar ISO/IEC 25010:2022 Dimensi Quality In Use Karakteristik (Effectiveness, Freedom From Risk, Dan Context Coverage). Fakultas Rekayasa Industri, Universitas Telkom.