

Department of Computer Science and Engineering - DISI
Second-cycle Degree in Digital Transformation Management
Class: LM-91

**Strengthening Cybersecurity
in the Digital Age
The Synergy of Penetration Testing
and ISO/IEC 27001**

Graduation thesis in
CYBERSECURITY

Supervisor
Gabriele D'Angelo

Candidate
Roberto Curcio

5th Session
Academic Year 2022-2023

Abstract

The thesis examines the inclusion of penetration testing in the regulatory framework of ISO/IEC 27001 and its impact on the cyber resilience of organizations during digital transformation. This scholarly investigation evaluates the effectiveness of penetration testing as a cybersecurity strategy by analyzing its compatibility with the ISO/IEC 27001 standard in a digital transformation context. The main objective is to clarify how this integration influences cybersecurity governance, risk management, and governance structures within organizations. The discussion also encompasses a comprehensive exploration of the ISO/IEC 27001 standard, its implementation, and the associated advantages and challenges in the digital era, emphasizing the importance of a proactive approach to information security. Through thorough analysis, the thesis emphasizes how the combination of penetration testing and ISO/IEC 27001 enhances organizational capabilities to effectively address cyber risks during digital shifts, fostering a culture of information security and strengthening overall resilience.

Dedication

*"Dicono che prima di entrare in mare
Il fiume tremi di paura.
A guardare indietro
tutto il cammino che ha percorso,
i vertici, le montagne,
il lungo e tortuoso cammino
che ha aperto attraverso giungle e villaggi.
E vede di fronte a sé un oceano così grande
che a entrare in lui può solo
sparire per sempre.
Ma non c'è altro modo.
Il fiume non può tornare indietro.
Nessuno può tornare indietro.
Il fiume deve accettare la sua natura
ed entrare nell'oceano.
Solo entrando nell'oceano
la paura diminuirà,
perché solo allora il fiume saprà
che non si tratta di scomparire nell'oceano
ma di **diventare oceano.**"*

Contents

Introduction	1
1 ISO/IEC 27001	5
1.1 History and development	5
1.2 Key components	8
1.2.1 From risk analysis to risk treatment	8
1.3 Implementation and certification process	11
1.4 Benefits and challenges in the digital era	16
1.4.1 Benefits	16
1.4.2 Challenges	17
1.4.3 Summaries	18
2 Vulnerability Scanning and Assessment	19
2.1 Definitions and importance	19
2.1.1 Definition of vulnerability	19
2.1.2 Definition of vulnerability scanning	22
2.1.3 Differences between Vulnerability Scanning and Vulnerability Assessment	22
2.1.4 Relationship with ISO/IEC 27001	23
2.2 Tools overview and process	24
2.2.1 The process	24
2.2.2 Results analysis and management	25
2.2.3 Most known tools for vulnerability scanning	26
2.3 Role in preparing penetration test	29
3 Penetration Testing	31
3.1 Definition, objectives, and importance	31
3.2 Types, Tools, and Techniques	33
3.3 Methodologies and Phases	36
3.3.1 Most common methodologies	36
3.3.2 Phases	38
3.4 Summary	42

- 4 Implementation 43**
- 4.1 Environment setup: Kali Linux and BWAPP 43
 - 4.1.1 Oracle VirtualBox and Kali Linux 43
 - 4.1.2 BWAPP (Buggy Web Application) 45
- 4.2 Vulnerability Scanning 46
 - 4.2.1 Nmap 47
 - 4.2.2 Nikto 49
 - 4.2.3 OWASP ZAP 51
- 4.3 Penetration testing 53
 - 4.3.1 Cross-Site Scripting (XSS) 54
 - 4.3.2 SQL Injection 55
- 4.4 Results Analysis 56

- 5 Conclusions 57**

Introduction

The digital transformation era indicates a turning point in the global landscape, denoting a period of profound and swift changes impacting the entire socio-economic context. This transformation, fueled by the emergence and widespread adoption of digital technologies, deeply influences business models and organizational processes. Digital transformation transcends the mere adoption of technological tools; it signifies a radical rethinking of how organizations create value, interact with their stakeholders, and competitively position themselves in the market.

In this scenario, businesses find themselves navigating an environment marked by unprecedented competitive intensity, compelled to reconsider their operational strategies and rethink their market approach. Digitalization presents new opportunities for product and process innovation, enabling companies to tap into new markets, optimize operational efficiency, and tailor their offerings to meet the demands of increasingly informed and connected customers.

Simultaneously, digital transformation poses significant challenges. The rapid evolution of digital technologies and consumer expectations demands from organizations an adaptability and continuous learning capability. Moreover, the shift towards digitalized business models necessitates a reevaluation of organizational structures, with a need to develop new competencies and foster a corporate culture oriented towards innovation and flexibility.

The ubiquity of digital transformation thus highlights a dual aspect: on one hand, it represents a powerful lever for growth and development for enterprises that can seize the opportunities provided by new technologies; on the other, it introduces elements of discontinuity and complexity that require a careful and proactive strategic approach. In this scenario, the ability to anticipate market trends, integrate advanced technological solutions, and reinvent business processes becomes a critical success factor, outlining the contours of a new competitive paradigm where digital agility emerges as a key element for the long-term sustainability of organizations.

Within this paradigm, cybersecurity gains unprecedented importance, becoming a fundamental pillar for the resilience and sustainability of organizations in the digital transformation era. The growing dependence on digital technologies

exposes companies to new risks and vulnerabilities, making the adoption of effective cybersecurity strategies essential to protect infrastructure, data, and business processes.

The integration of advanced computer systems and global interconnectivity amplifies potential security threats, from targeted cyber-attacks to data breaches, highlighting the need for a cybersecurity approach that is as dynamic as the technologies it aims to protect. In this context, organizations face complex challenges, ranging from identifying and managing vulnerabilities to preventing cyber threats, requiring specific skills and a constant commitment to training and updating human resources.

Cybersecurity, therefore, cannot be viewed merely as a technical aspect or a regulatory obligation to be fulfilled; it must be integrated into the overall corporate strategy, with a holistic approach that considers both technological, organizational, and human aspects. This implies the need to develop a security culture at all organizational levels, promoting awareness of risks and adopting responsible behaviors by all involved actors. Managing cybersecurity requires a balance between adopting innovative technologies and safeguarding the integrity, availability, and confidentiality of information. The challenge for organizations is to ensure that digitalization does not translate into greater exposure to cyber risks but is accompanied by the strengthening of cyber defenses through the definition of security policies, the creation of resilient infrastructures, and the implementation of cutting-edge cybersecurity practices.

Within this dynamic and challenging landscape, the ISO/IEC 27001 stands as a pivotal guide for organizations seeking to traverse the complex currents of digital transformation securely. Organizations are called upon to manage an increasing volume of data, often sensitive, while adopting emerging technologies that can introduce new vulnerabilities. This international standard for information security management serves as an indispensable reference point for the implementation, monitoring, and continuous improvement of cybersecurity practices, offering a structured and systematic framework for protecting corporate data. Its significance lies in its ability to provide a holistic approach to information security, encompassing all aspects from risk assessment to human resource management, from physical security to cybersecurity. By adopting this standard, organizations can ensure not only data protection but also the resilience of their information systems against increasingly sophisticated and varied threats. It also promotes a security culture that permeates the entire organization, raising awareness at every corporate level of the importance of adopting safe and responsible behaviors.

The following dissertation aims to explore a fundamental question:
"How does the integration of penetration testing within the ISO/IEC 27001 regulatory framework impact the cyber resilience of organizations undergoing digital

transformation, and what implications does it have for their cybersecurity governance?”

This research question intertwines the emphasis on digital transformation with the broader impact on cybersecurity governance, aiming to understand how penetration testing, aligned with ISO/IEC 27001, can enhance an organization’s ability to effectively manage cyber risks in periods of digital change.

The specific objectives of this study are varied and interconnected:

- Investigate the role and effectiveness of vulnerability assessment and penetration testing as part of the cybersecurity strategy in organizations undergoing digital transformation.
- Analyze the synergy between these practices and the ISO/IEC 27001 standard.
- Explore the broader implications of this integration on cybersecurity governance within organizations.

Following the enunciation of the research question and objectives, this introduction will proceed by introducing the content of the upcoming chapters. Each chapter is dedicated to exploring a distinct facet of the research, aiming to synthesize the findings and discern whether the new challenges in cybersecurity and governance frameworks, can be effectively integrated and tailored to meet the demands of digital transformation.

Thesis Structure Chapter 1 provides an exploration of the ISO/IEC 27001 standards, articulating its historical backdrop, core components, implementation, and certification processes, and ultimately, the associated benefits and challenges. This segment embarks on a broad analysis, offering an in-depth understanding of the standard from its inception—prompted by the necessity for a standardized approach to information security—through to its latest developments, which respond to technological advancements and user feedback. The discussion extends to the structure and significance of the fundamental elements of the Information Security Management System, underscoring their contribution to safeguarding the confidentiality, integrity, and availability of information. The chapter also examines the step-by-step process of implementation and certification, illustrating the pivotal role of corporate leadership in integrating the standard’s principles into organizational practices. Additionally, this part addresses the advantages of adopting the ISO/IEC 27001 standard, such as enhanced security risk management and global compliance, alongside the challenges, including integration with existing IT infrastructures and the continuous evolution of security threats.

Chapter 2 is devoted to the exploration of the concept of vulnerability assessment and vulnerability scanning, laying the groundwork for an in-depth understanding of vulnerability management provided by the standard. By conducting a methodical analysis, this chapter aims to unveil the mechanisms through which vulnerabilities in computer systems are identified, evaluated, and mitigated, highlighting the crucial importance of proactive strategies to prevent cyberattacks that could expose sensitive data and critical infrastructures. This examination aims to provide an overview of the dynamic and multifaceted process through which vulnerabilities emerge, are detected, and eventually resolved, emphasizing the significance of continuous monitoring and proactive management within the cybersecurity community.

Chapter 3 investigates the intricate concept of penetration testing, a process designed to uncover and exploit vulnerabilities within computer systems. This section offers an overview of penetration testing, including its definition, objectives, and the vital role it plays in the field. It discusses various testing methodologies, elucidating the differences in strategies and approaches to security. The chapter further explores the array of tools and techniques employed in conducting these tests, along with a discussion of the methodological phases that underpin the penetration testing activity. The chapter not only underscores the critical nature of penetration testing in identifying system vulnerabilities but also highlights its indispensable role in formulating a robust defense mechanism against the ever-changing landscape of cyber threats, thereby fostering a more secure and resilient digital environment.

Chapter 4 explores the practical experience gained through an internship at Brain Technologies in Torino, with a particular emphasis on the development of a virtual environment designed for vulnerability scanning and penetration testing. By leveraging well-known tools and specific platforms such as Kali Linux and BWAPP (Buggy Web Application), this chapter aims to provide an exhaustive overview of the methodologies, technical decisions, and practices adopted during the internship. The objective of this chapter is twofold. Firstly, it seeks to elucidate the setup of the testing environment, outlining the technical and strategic rationale behind selecting the tools for subsequent activities. Secondly, it aims to explore the operational phases of vulnerability scanning and penetration testing, demonstrating how these practices were integrated to assess and enhance the cyber resilience of an Information Security Management System.

Chapter 1

ISO/IEC 27001

1.1 History and development

The introduction of ISO/IEC 27001 was initially motivated by the need for a standardized approach to monitoring information security. The British Standard 7799 (BS 7799), published by the British Standards Institution in 1995, established the groundwork for the future global standard. BS 7799 was one of the pioneering frameworks to provide extensive guidance on information security management, risk assessment, and risk management, establishing the groundwork for what would later develop into ISO/IEC 27001. This evolution into the well-known Information Security Management Standard was profoundly shaped by the insights and methodologies outlined in BS 7799. As a trailblazer in its domain, BS 7799 was crucial for setting a precedent for systematic approaches to managing information security, assessing risks, and implementing risk management strategies. Its extensive standards and recommendations were pivotal in defining the core ideas and practices that would be refined and globally adopted in ISO/IEC 27001, marking a significant milestone in the progression of information security regulation and practices. Another significant precursor was the Code of Practice for Information Security Management, which later evolved into BS 7799-1. This code of conduct gained widespread recognition and was adopted by organizations, thereby establishing the foundation for systematic procedures in information security management. BS 7799-2, which focused on the standards for establishing, implementing, and documenting an Information Security Management System (ISMS), directly influenced the structure and content of the initial version of the standard. The principles and recommendations outlined in BS 7799-2 were integrated into ISO/IEC 27001, thereby bolstering its status as an internationally recognized standard.

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have developed global standards for

effective information security procedures. In collaboration, they worked to transform the principles of BS 7799 into a universally applicable framework, leading to the publication of ISO/IEC 17799 in 2000, which was later renumbered as ISO/IEC 27002. Officially introduced in October 2005, the first edition of ISO/IEC 27001 represented a significant advancement in information security. This edition is comprehensive in scope, tailored for diverse enterprises, and provides a structured framework for designing, overseeing, and enhancing an ISMS.

The history also reflects influences from various industry practices, evolving cybersecurity threats, and the growing need for a standardized approach to information security across different sectors. These factors have consistently influenced the development of the standard, ensuring its continued relevance and effectiveness in addressing modern challenges in information security.

The norm's development was a response to the global demand for a robust framework capable of effectively addressing diverse information security threats. It represented a significant advancement in standardizing information security procedures across international borders. The first edition established the framework for an ISMS, primarily focusing on safeguarding the confidentiality, integrity, and availability of information.

In 2013, the standard underwent significant modifications in response to technological advancements and user feedback. This modification emphasizes the objectives, performance monitoring, and ongoing improvement of the Security System. Additionally, it has incorporated the Annex SL format, thereby improving compatibility with existing ISO management standards. The reorganization of Annex A in the 2013 version led to a more streamlined and flexible set of controls, enabling greater adaptability in implementation. The upcoming update of ISO/IEC 27001, anticipated in 2022, is aligned with the ISO/IEC 27002:2022 standard. This updated version aims to address current concerns in cybersecurity, reflecting the latest trends and threats in information security. It serves as evidence of the standard's dedication to a proactive and adaptable approach to cybersecurity within a rapidly expanding digital ecosystem. Each edition of ISO/IEC 27001 emphasizes its continued relevance and effectiveness in a rapidly evolving technological landscape within emerging security threats, solidifying its reputation as a comprehensive framework for protecting information assets on a global scale.

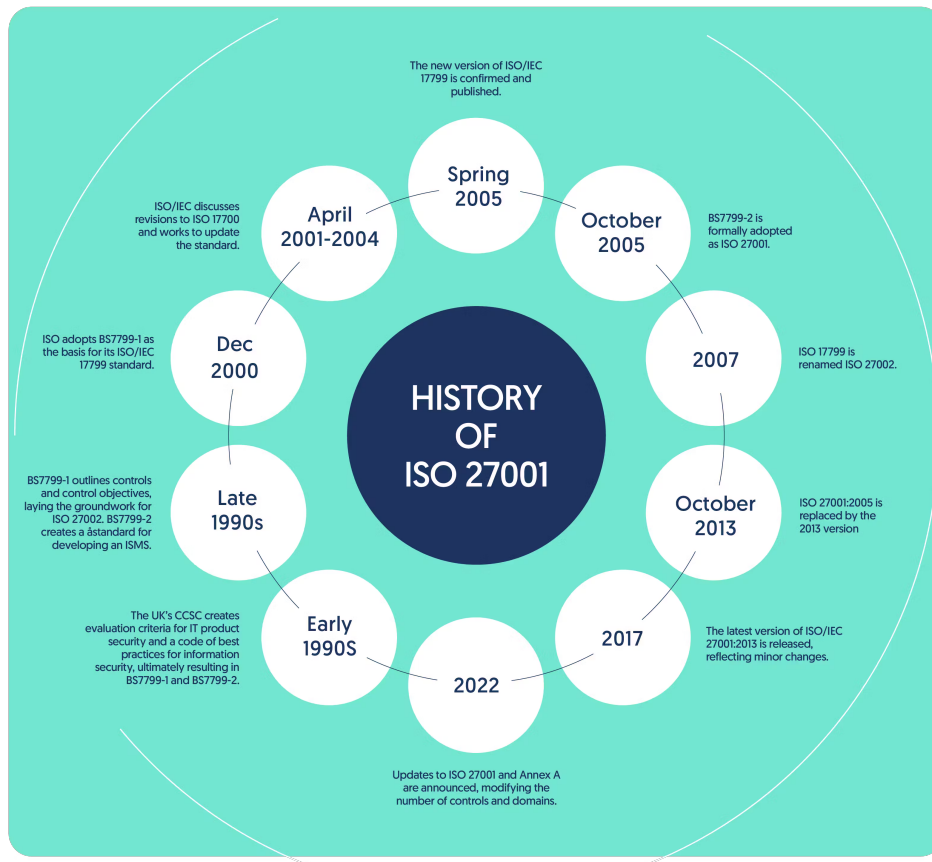


Figure 1.1: History of ISO/IEC 27001 (Source: own work)

The original scope of ISO/IEC 27001 was broad, making it applicable to businesses of all sizes, types, and industries. This universality constituted a pivotal element of the standard, enabling its use across different industries and sectors worldwide. The focus was placed on recognizing, evaluating, and controlling vulnerabilities to information security that are specific to the institution's circumstances. Furthermore, it included a set of controls specified in Annex A, offering a broad collection of best practices for information security. These controls encompassed various aspects of information security, including organizational, technical, and physical security measures. The objective of ISO/IEC 27001 was not limited to providing a list of requirements for an Information Security Management System; it also aimed to offer a systematic approach to information security that could be customized to address the unique risks and challenges encountered by individual enterprises. Its versatility and adaptability have established it as a fundamental tool for enterprises looking to enhance their information security posture progressively and consistently [13].

1.2 Key components

Acquiring a thorough understanding of the standard is essential for establishing and implementing strong measures to protect information security. This examination will specifically evaluate the ten fundamental elements that form the basis of this regulation. The analysis will not delve into intricate operational specifics but rather will present a comprehensive overview of the foundational elements delineated by ISO/IEC 27001. This involves evaluating the structural framework, risk management processes, and the roles of leadership and continuous improvement. This section aims to provide a comprehensive understanding of the basic concepts of the standard and their importance in the broader context of information security management.

1.2.1 From risk analysis to risk treatment

The Information Security Management System outlined in ISO/IEC 27001 represents a systematic and structured approach to the management and protection of an organization's information assets. The main objective of an ISMS is to ensure the confidentiality, integrity, and availability of information through the development of a full and consistent risk management system. This includes all guidelines, procedures, technological, and physical measures related to an organization's information risk management operations. A crucial aspect is its adaptability and suitability to a wide range of organizational circumstances. This adaptability enables organizations of various sizes, types, and sectors to develop an ISMS that is customized to their specific information security needs and risk profiles.

The process of developing and maintaining an ISMS according to ISO/IEC 27001 includes many major stages:

- **initial assessment and definition:** organizations start by defining the scope of the ISMS, which involves specifying the boundaries and applicability of the information security management system within the organization. This is crucial for determining the amount of implementation.
- **risk assessment and treatment:** undertaking a comprehensive risk assessment is a fundamental part of implementing an ISMS. This involves identifying potential security risks, vulnerabilities, and their impact on the organization's information assets. Based on this assessment, the organization then decides on appropriate risk treatment steps, which may include implementing specific controls outlined in Annex A of the standard or adopting other risk reduction strategies.

- **internal audits:** the organization implements the chosen controls to mitigate the identified risks. These controls are selected based on their effectiveness in minimizing specific risks and their alignment with the organization's broader objectives and operational context.
- **monitoring and review:** an ISMS is not static; it requires regular monitoring and revision. This ensures that the system remains successful in the presence of changing internal and external variables, such as heightened threats, technological advancements, and organizational changes.
- **continual improvement:** a key principle is the focus on continuous improvement, which, although traditionally associated with the Plan-Do-Check-Act (PDCA) model, has adapted to allow for a more adaptable approach. Organizations are encouraged to implement a suitable and effective continuous improvement strategy, which may include but is not limited to, the PDCA cycle. This involves regularly assessing and monitoring their systems to identify areas for improvement, ensuring their ongoing suitability, adequacy, and effectiveness in line with evolving business and security objectives. By doing so, companies can continuously modify and adapt to changes in technology, risks, and business objectives over time.

Following the creation of an ISMS, a crucial element is the risk management process. This method is not a one-time effort but a constant and vital part of maintaining an efficient secure system. It is designed to be dynamic, adapting to the evolving landscape of information security threats and organizational changes.

The standard stipulates that the risk management process begins with *risk identification*. This requires a diligent effort to identify potential risks to the organization's information assets. These risks may include a wide range of threats, from cyberattacks and data breaches to physical disasters and human errors. It is also crucial for organizations to identify vulnerabilities within their systems that could be exploited by these threats. The identification phase plays a crucial role in developing an understanding of the potential threats that could compromise the confidentiality, integrity, and availability of information. Once risks have been identified, the next stage is *risk analysis*. This stage assesses the probability of specific hazards occurring and their potential impact on the organization. Risk analysis helps prioritize risks according to their severity and probability, providing a clear view of which issues need immediate attention and resources. This prioritization is essential to ensure that the most critical threats are addressed promptly, thereby minimizing the likelihood of significant information security disasters. After the analysis, *risk management* includes *risk evaluation*. This stage assesses the risks within the framework of the organization's overall risk tolerance and security objectives. At this point, decisions are made about which risks to accept, avoid,

transfer, or mitigate. This evaluation is a strategic exercise that aligns the risk management approach with the organization's overarching objectives and risk tolerance. The final phase of the risk management process involves *risk treatment*. This involves selecting appropriate security measures or controls to effectively manage the identified threats. The organization may choose to use specific controls outlined in Annex A or alternative methods for mitigating risks. The selection of controls is based on their effectiveness in reducing recognized hazards to a level that is deemed acceptable. During this step, the organization also develops a risk treatment plan that outlines how the selected controls will be implemented, specifies who will be responsible, and sets the timeframe for execution.

Throughout the process of risk management, it is essential to participate in regular monitoring and evaluation. The constantly changing hazard landscape and the dynamic nature of organizational environments require ongoing surveillance. This practice ensures the effective identification and mitigation of new and emerging threats. Moreover, it provides an opportunity to analyze the effectiveness of current controls and make any necessary adjustments. Constructing and maintaining an Information Security Management System in accordance with the norm is a strategic decision that helps organizations systematically manage their information security risks.

Expanding on the foundational Information Security Management System and its inherent risk management procedure as mandated by the regulation, the subsequent crucial component involves understanding and implementing the control objectives stipulated within the standard. These objectives form the structural foundation of the ISMS, enabling a systematic approach to mitigate identified threats to the security of the organization's information. Control objectives in ISO/IEC 27001 essentially represent the goals or outcomes that enterprises aim to achieve in order to ensure the effective management of specific information security risks. Each control target covers a specific area of information security and is designed to address particular vulnerabilities identified during the risk assessment process. The purpose of these objectives is to encourage organizations to develop strong policies that protect their information assets from potential risks and vulnerabilities. The control objectives cover a wide range of areas within information security, including organizational policies, physical security, human resource security, access control, cryptography, and operational security. These objectives are not meant to be prescriptive, but rather to provide a framework for organizations to develop controls that are customized to their specific risk landscape and operational needs. The implementation of control objectives requires businesses to fully understand their relevance to specific security concerns and operational circumstances. This analysis leads to the selection of applicable controls, working as practical solutions to accomplish these objectives efficiently.

The role of the system's architecture is greatly influenced by the presence of Annex A in the document. Annex A consists of a overall compilation of control sets, which are further classified into 14 categories and encompass a total of 114 controls. Each control is identified by a unique alphanumeric code consisting of four characters. These controls address a wide range of security concerns and are extremely important for organizations to customize their security measures to align with their specific risks and objectives. Annex A serves as a valuable reference guide, helping companies ensure global coverage of critical security procedures. This guidance entails carefully aligning the organization's selected security measures with those recommended in Annex A, as A. Calder highlighted in his book [4]. This alignment is crucial for creating the Statement of Applicability (SoA), a fundamental document that outlines the relevance and implementation status of each control selected from Annex A. The Statement of Applicability (SoA) not only documents the controls that have been implemented but also provides justifications for including or excluding specific measures from Annex A. This ensures that the organization adopts an individualized and efficient approach to information security management. In addition to serving as a checklist, Annex A, in conjunction with ISO 27002, provides best practice guidelines for implementing and operating these controls.

However, it is important to note that companies may need to exceed the standards set by ISO 27002 in certain areas, depending on their unique operational environment and evolving security requirements. This dynamic strategy ensures that enterprises maintain a robust and adaptable security posture, aligning with the constantly evolving landscape of information security threats. The selection and execution of controls based on an organization's risk assessment and specific demands are critical. Organizations need to evaluate factors such as their size, the nature of their operations, the regulatory environment in which they operate, and their risk tolerance. Subsequently, these controls are integrated into the organization's operational procedures to ensure their successful implementation and monitoring as part of the overall requirements of the standard.

1.3 Implementation and certification process

The implementation of ISO/IEC 27001 is not solely a procedural action carried out by a corporation, but rather a strategic decision that necessitates a profound commitment from the top management. This commitment is of utmost importance as it not only establishes the direction but also allocates the necessary resources for the successful execution of the endeavor. The process commences with the assimilation of the principles delineated in the standard into the organizational framework, thereby demonstrating a comprehensive understanding of the significance of

safeguarding information. The guidance demonstrated by top management’s leadership is pivotal in steering the organization towards a mindset that prioritizes security, ensuring that the implementation aligns harmoniously with the overarching objectives and risk management policies of the organization. This alignment is critical to guarantee that the Information Security Management System effectively safeguards the informational assets of the organization and encourages its strategic aims. The integration of information security into the fundamental business processes is preferable to treating it as a distinct entity.



Figure 1.2: ISO/IEC 27001 Certification Process (Source: kolide.com)

The first step involves conducting a thorough *gap analysis*. This crucial step involves conducting a detailed assessment of the organization’s current information security procedures and practices and comparing them to the rigorous requirements set by the regulation. The gap analysis serves a dual purpose: firstly, it reveals the areas where the organization’s current practices do not meet the standards, highlighting specific vulnerabilities and flaws in the current security framework; secondly, it provides a clear roadmap for the required improvements, making it easier to allocate resources efficiently. This analysis is an ongoing process rather than a one-time effort, ensuring that the organization consistently adapts and improves its security procedures to align with the constantly evolving nature of information security threats. By clearly identifying weaknesses, organizations can develop targeted initiatives for improvement, thereby establishing a strong foundation for the development of a resilient Information Security Management System.

Following the gap analysis, the organization proceeds to a crucial phase in the

implementation process, the risk assessment and risk treatment strategy. This stage involves a methodical and systematic analysis of the organization's information security landscape to identify potential threats and vulnerabilities. The *risk assessment* process aims to identify the likelihood and impact of various security hazards, providing a framework for prioritizing them based on their potential impact on the business. This assessment is crucial for making informed decisions about how to address each risk, whether through mitigation, transfer, avoidance, or acceptance. Once the risks are recognized and prioritized, the next stage is risk treatment. This entails choosing suitable controls from Annex A to manage and reduce the identified risks to a satisfactory level. The *risk treatment strategy* is tailored to the organization's unique risk profile and operational requirements. It is a dynamic document that reflects changes in the threat environment or the organization's internal context, such as new procedures, systems, or changes in the external environment. This strategy not only specifies the precise controls to be implemented but also includes timelines, responsibilities, and resource allocation for executing these controls. By thoroughly analyzing and addressing risks, the company ensures that its ISMS is strong, resilient, and capable of protecting its information assets from current and future threats.

After formulating a risk treatment plan, the organization proceeds with selecting and implementing the necessary *controls* outlined in Annex A. The Annex offers a comprehensive compilation of security control objectives and measures. The organization selects relevant measures from this set to minimize the identified risks. The process of selecting controls is strategic and requires a delicate balance between risk level, the potential impact of the controls, and the cost and complexity of implementation. The implementation of these controls involves integrating them into the organization's procedures and systems. This integration is of extreme importance to ensure that the controls effectively mitigate risks to an acceptable degree. Controls can encompass a range of technical solutions, such as encryption and access controls, as well as management and operational procedures, including staff training and incident management policies. Additionally, the organization must ensure that these controls are consistently applied across all relevant areas as defined by the scope of the ISMS. The effectiveness of these controls depends not only on their implementation but also on continuous monitoring and evaluation to ensure their ongoing efficacy and relevance. This constant scrutiny is a crucial aspect of the organization's unwavering commitment to maintaining a secure Information Security Management System, addressing evolving risks, and complying with emerging legal and regulatory obligations. Through careful selection and application of necessary policies, the company increases its defense against information security risks, making its ISMS a strategic resource for protecting its important information assets.

Documentation and record-keeping are essential components for effective compliance with the standard. The compilation and maintenance of detailed documentation is essential for demonstrating the compliance of the system with the established standard. This involves the development and updating of rules, processes, responsibilities, and duties that align with the objectives of the ISMS. Critical documents include the policy, risk assessment, and treatment reports, as well as records of training, internal audits, and management reviews. These documents serve as a reference for managing the ISMS and provide evidence of compliance during both internal and external audits. Proper documentation ensures the accurate description, understanding, and consistent utilization of all aspects of the ISMS throughout the organization. In addition to documentation, the organization must also establish effective channels for staff training and awareness. *Training* and awareness programs are essential to ensure that all employees, regardless of their role, understand the importance of information security and their specific responsibilities within the ISMS. These programs should encompass the organization's information security regulations, the repercussions of non-compliance, and the proper procedures for reporting security incidents. Regular training sessions, workshops, and communication campaigns contribute to fostering a strong security culture within the organization. By ensuring that staff members are well-informed and alert, the organization strengthens its initial defense against information security threats. Insufficient training and awareness initiatives, along with inadequate documentation and record-keeping, not only impede the operation of the ISMS but also have minimal impact on the audit process for certification.

The *internal audit* plays a crucial role within the framework, providing an impartial assessment of the effectiveness of the ISMS. This procedure involves a thorough evaluation of the system to ensure that policies and procedures not only comply with the standard but are also being effectively implemented and maintained throughout the organization. Internal audits facilitate the identification of non-compliance areas and potential areas for improvement, providing valuable insights into the operational efficiency of the organization's security systems. These audits should be conducted at scheduled intervals by qualified professionals who are unbiased and independent from the area being audited, to guarantee objectivity and impartiality. Following internal audits, *management reviews* form another critical component of the process. These reviews, conducted by top management, are crucial for evaluating the overall functionality. Management reviews analyze the findings of internal audits, employee feedback, the status of risk mitigation measures, and the results of any external audits or compliance checks. This evaluation process ensures that the ISMS is aligned with the strategic objectives of the organization and effectively addresses current and emerging information security risks. Both internal audits and management reviews are crucial for ensuring the

ongoing existence and continuous improvement of the systems. They facilitate the identification of areas where the organization's system may need improvement or fine-tuning, ensuring that the system adapts to changes in the organization's internal and external environment.

The certification audit marks the endpoint of the ISO/IEC 27001 implementation process. This crucial stage involves an *external audit* carried out by a reputable authority to assess the compliance of the ISMS with the standard. The certification process usually involves two stages: an initial assessment to evaluate the readiness of the ISMS, followed by a more detailed official examination. The formal evaluation thoroughly examines the effectiveness of the Information Security Management System, including the adequacy of the chosen controls, the effectiveness of the risk management process, and the overall compliance with the standard. The successful completion of this external audit results in the issuance of the ISO/IEC 27001 certification, confirming the organization's commitment to the protection of their information's security.

However, obtaining certification does not imply the end of the effort. The preservation and ongoing improvement of the ISMS is a crucial element within the framework. After obtaining certification, the organization enters a phase characterized by *continuous vigilance and progress*. This phase involves regularly monitoring, evaluating, and updating the organization's system to ensure its ongoing effectiveness and adaptability to changes in information security risks, technological advancements, and business processes. The maintenance of the systems involves regularly conducting of internal audits, management reviews, and implementing action plans based on the findings of these assessments. These activities aim to continuously strengthen the system. Furthermore, organizations must also plan for regular surveillance audits conducted by the certification entities. These audits, which typically occur on an annual basis, ensure continuous adherence to the established standard and scrutinize the effectiveness of the system within its operational context. The surveillance audits focus on confirming that the organization not only maintains its ISMS but also remains committed to continuous improvement. Moreover, there is a requirement for recertification, typically occurring every three years. The recertification audit involves a thorough assessment of the entire ISMS to ensure its ongoing compliance and effectiveness. This evaluation also examines any significant modifications or enhancements made to the ISMS since the previous certification audit. The importance of this recertification process cannot be understated, as it ensures that the organization's ISMS remains strong, relevant, and aligned with the most current best practices in information security management.

1.4 Benefits and challenges in the digital era

1.4.1 Benefits

One of the primary benefits of ISO/IEC 27001 in the digital environment is its holistic approach to cybersecurity. As organizations increasingly rely on digital technologies for their operations, they become more vulnerable to cyber threats. The standard provides a robust framework for effectively managing these risks, implementing an Information Security Management System in accordance with regulations enables organizations to effectively manage cybersecurity risks by systematically identifying and evaluating these risks. This regulation provides significant benefits in the digital realm by aligning with global data privacy regulations. The rigorous controls and exemplary practices provide a structured framework that assists companies in complying with these procedures. Compliant organizations not only protect sensitive data but also demonstrate their commitment to data privacy, which is increasingly crucial to customers and stakeholders.

This standard is essential for integrating security considerations into the core of digital transformation activities, ensuring that the risk of security breaches is minimized from the outset of such programs. It not only enhances the organization's reputation but also strengthens client confidence, which is crucial in today's digital market.

Moreover, the standard's focus on continuous development aligns seamlessly with the dynamic nature of the digital world, where technological advancements and security concerns escalate rapidly. This inherent flexibility mechanism enables businesses to update their ISMS over time, ensuring resilience against the constantly evolving threat landscape.

Furthermore, empirical evidence has established a clear and undeniable correlation between the adoption of ISO/IEC 27001 and the improvement of organizational performance. As demonstrated by Podrecca et al. [14], companies that are ISO/IEC 27001 accredited experience significant improvements in their profitability, labor productivity, and sales performance. This positive correlation emphasizes the importance of adhering to this standard, as it not only enhances information security but also promotes organizational value and provides a competitive advantage in the marketplace, demonstrating how adherence to the standard is a strategic investment that enhances the financial well-being and operational efficacy of enterprises.

1.4.2 Challenges

The adoption of this international standard for information security management systems offers significant advantages in the digital landscape. However, enterprises face numerous challenges when it comes to adopting and integrating this standard. These challenges stem from the rapid advancement of technology, diverse organizational structures, and the continuously expanding cybersecurity threat landscape. The incorporation of the standard into current IT infrastructures poses a significant challenge, especially in environments that include a mix of outdated and less secure technologies. Achieving a precise implementation of the controls outlined in the Information Security Standard within a vast technological environment requires a deep understanding of both the existing IT architecture and the criteria set forth by the standard. This complexity becomes even more pronounced as organizations pursue digital transformation, integrating new technologies such as cloud solutions, Internet of Things (IoT) devices, and AI-driven systems.

Moreover, effectively staying ahead of and defending against evolving cybersecurity threats is a challenging task. The cybersecurity landscape is constantly evolving, with new vulnerabilities and attack strategies emerging frequently. The implementation of the standard goes beyond addressing current security risks; it also involves anticipating and preparing for future threats. This requires a proactive and forward-thinking approach to cybersecurity that is resource-intensive and demands ongoing vigilance. The implementation is hindered by organizational constraints: Securing acceptance and commitment from all levels of the organization, especially from top management, is essential for a successful implementation. This can be challenging in situations where information security is not considered a strategic priority. Fostering an understanding of the importance of information security among employees and ensuring compliance with the criteria set by the regulation involves a significant shift towards integrating security practices into regular operations.

Maintaining adherence to the standard against rapid technological and business changes presents another set of challenges. The standard requires not only initial compliance but also ongoing conformity, which necessitates regular updates, audits, and evaluations of the ISMS. This can be especially challenging for all organizations, particularly smaller ones with limited cybersecurity capabilities. The financial and resource costs associated with establishing and maintaining an ISMS that aligns with the norm can be overwhelming. The costs associated with setting up, deploying, auditing, and continuously improving an ISMS are significant. While the long-term benefits of a robust information security system outweigh these costs, they can still pose barriers, especially for smaller organizations and those operating in marginally profitable sectors.

1.4.3 Summaries

The commitment of ISO/IEC 27001 to continuous development is crucial for navigating the expanding realm of digital threats. It is essential for organizations to continuously improve their Information Security Management Systems to keep pace with the growing cyber threats, technological advancements, and changes in business operations. This proactive approach ensures that the ISMS remains effective over time, adapting to new cybersecurity challenges as they arise.

As the digital landscape expands, this framework plays a significant role in ensuring regulatory compliance. In fact, compliance with the standard demonstrates the firm's commitment to safeguarding personal and sensitive information, fulfilling legal obligations, and building trust among its stakeholders. The regulatory authorities tasked with overseeing the standard must consistently assess and update its rules, regulations, and best practices in light of technological advancements and emerging threats.

In conclusion, ISO/IEC 27001 can be seen as a milestone, that helps enterprises in managing the complex and dynamic digital ecosystem. Its well-structured but flexible framework empowers organizations to proactively address future digital trends and security issues. By embracing a forward-thinking approach and adapting to technological advancements, this recognized international standard is essential for enterprises aiming to protect their digital future.

Chapter 2

Vulnerability Scanning and Assessment

2.1 Definitions and importance

Vulnerability management is a fundamental aspect in the safeguarding of organizations' cybersecurity. This methodical approach is devoted to the identification, evaluation, and mitigation of flaws within computer systems, networks, and applications. The main goal is to prevent cyber attacks that have the potential to compromise sensitive data and critical infrastructures. The adoption of proactive strategies, in conjunction with the utilization of advanced scanning and evaluation tools, is imperative for maintaining strong cybersecurity measures in a constantly evolving technological environment.

2.1.1 Definition of vulnerability

In cybersecurity, a vulnerability refers to a flaw in information technology products that could compromise security policies or adversely affect the security and resilience of the system [5]. Despite minor discrepancies, the various definitions of vulnerability share a common essence. This approach emphasizes the subjective nature of vulnerabilities, which can be interpreted in various ways depending on one's perspective. What users or developers see as a problem, attackers may view as a potential opportunity. The development and enhancement of software, which are essential for technological progress, often lead to new vulnerabilities. These vulnerabilities create what is commonly referred to as "exposure windows" [1], which indicate periods when systems are especially susceptible to security risks until a comprehensive solution is implemented on all devices running the compromised software.

In the exploration of cybersecurity vulnerabilities, a procedural approach unveils a complex lifecycle, characterized by distinct stages from inception to resolution. These stages represent a simple way to understand and manage cybersecurity risks:

- **Creation:** This initial stage involves the unintentional introduction of a vulnerability during the software development process. It underscores the challenges inherent in creating complex software systems and the inevitability of oversights despite rigorous testing protocols. Factors contributing to vulnerability creation include coding errors, inadequate security design, and the use of insecure third-party components. The emphasis on early detection and secure coding practices is vital in mitigating the risks at this foundational level.
- **Discovery:** At this juncture, vulnerabilities come to light through various means. The discovery might be the result of internal audits, user reports, or external entities, including security researchers and, unfortunately, malicious actors. The serendipitous nature of these discoveries, often occurring without a structured search for flaws, highlights the unpredictable landscape of cybersecurity. This phase raises ethical and strategic questions about disclosure practices and the responsibility of finding parties, balancing between alerting the community and preventing information from aiding potential attackers.
- **Disclosure:** marks the transition of a vulnerability from an unknown issue to a recognized threat. This phase can unfold through formal channels, such as responsible disclosure programs, or through direct communication with the developers. The process of disclosure is fraught with challenges, including timing, the method of communication, and the potential for premature exposure that could escalate the risk before remediation is possible. Strategies for effective disclosure involve coordinated efforts among developers, researchers, and regulatory bodies to ensure timely and secure communication.
- **Correction:** the actionable response to a disclosed vulnerability, where developers and security teams collaborate to devise and deploy a fix. This often takes the form of software patches or system updates designed to rectify the vulnerability. The complexity of this stage lies in the need for rapid development without compromising the quality of the fix, ensuring compatibility, and facilitating widespread adoption among users to close the exposure window efficiently.

- **Proliferation:** the vulnerability may enter a proliferation phase if details become widely disseminated before widespread patch application. This stage is characterized by increased awareness and, potentially, exploitation attempts as the information reaches both benign and malicious parties. The challenge here is to manage the dissemination of information to minimize harm and encourage prompt protective measures among the user base.
- **Scripting:** development of automated tools or scripts that exploit the vulnerability, lowering the barrier to entry for attackers and increasing the potential for widespread system compromise. This automation represents a significant escalation in the threat level, as it allows individuals with limited technical expertise to execute sophisticated attacks. Efforts to combat this phase include the development of intrusion detection systems, enhanced security measures, and public awareness campaigns.
- **Extinction:** The final stage, extinction, is achieved when the vulnerability no longer poses a significant threat, either because affected systems have been patched or updated, or because the vulnerable technology has become obsolete. Achieving extinction is an ideal outcome, reflecting the collective effort of the cybersecurity community to address and neutralize threats. This phase embodies the goal of resilient and adaptive security postures that evolve in response to emerging challenges.

Throughout these stages, the utmost significance of persistent monitoring, forward-thinking administration, and synergistic endeavors across the cybersecurity community is underscored. By comprehending and maneuvering through these phases proficiently, stakeholders can alleviate the hazards linked to cybersecurity vulnerabilities, safeguarding both individual systems and the wider digital ecosystem.

The conceptual model of the vulnerability lifecycle, while providing a simplified overview, fails to fully encompass the intricate dynamics of vulnerability development in the field. Intentionally creating vulnerabilities leads to the merging of the emergence and detection phases. The disclosure of a vulnerability can indicate both its discovery and publication simultaneously. The resolution phase, which is of great importance to users, may be delayed or remain unachieved due to developers' reluctance to issue patches, the impracticality of resolving certain issues, or administrators' failure to update systems. As a result, it is necessary to reevaluate the vulnerability lifecycle model to more accurately reflect the complexities involved in managing vulnerabilities.

2.1.2 Definition of vulnerability scanning

Many programs are transitioning to online platforms, raising concerns about the security implications they present for end users. It is crucial to prioritize the protection of these users, which necessitates conducting a thorough examination of any vulnerabilities in the software application that could potentially expose users to significant security risks [18].

Different categories of scanners are:

- **Port Scanners:** used to scan the ports to determine the open and closed ports, operating systems, and services offered.
- **Application Scanners:** used to assess a specific application on the network to track its weaknesses that can be further used to cause risk to the system.
- **Vulnerability Scanners:** used to find out the vulnerabilities in the system which if accessed by a malicious user or hacker can put the whole network system at risk [7].

Vulnerability scanning is a crucial operation in the field of cybersecurity, proving to be a complex and multi-layered process aimed at systematically identifying weaknesses and gaps in computer systems, networks, and applications. Through the use of advanced scanning technologies and complex analytical procedures, this process conducts a comprehensive analysis of IT infrastructures to identify every potential vulnerability that could be exploited by malicious actors. These actions not only uncover security holes but also categorize them based on their severity, providing businesses with crucial data to prioritize mitigation activities. This practice is crucial for safeguarding the integrity of computer systems and preventing attacks that could expose sensitive data or disrupt critical activities. Therefore, vulnerability scanning is one of the fundamental pillars of an organization's cybersecurity strategy, representing a proactive step toward creating a secure and resilient digital environment.

2.1.3 Differences between Vulnerability Scanning and Vulnerability Assessment

The comparison of vulnerability scanning and vulnerability assessment, despite sharing objectives in cybersecurity, reveals significant differences in their methodologies, approaches, and depth of analysis. Vulnerability scanning focuses on automatically identifying common weaknesses in systems and networks using tools that conduct tests to detect specific vulnerabilities. This procedure is generally faster and provides an overview of security vulnerabilities that require attention.

In contrast, a vulnerability assessment takes a more comprehensive and detailed approach, not only identifying vulnerabilities through scanning but also categorizing them, evaluating their associated risks and establishing priorities for mitigation based on their potential impact on the organization. This process involves using automated testing tools followed by manual analysis to interpret the results of the scan, leading to a deeper understanding of security risks and more effective strategies for mitigation [2].

2.1.4 Relationship with ISO/IEC 27001

Vulnerability scanning is an essential component within the framework of Annex A of ISO/IEC 27001, especially in relation to vulnerability management. This intricate process plays a significant role in helping organizations comply with the stringent standards established by the industry, which require the identification, assessment, and mitigation of risks to information security. By integrating vulnerability scanning into their security protocols, institutions can take a proactive approach to identifying and addressing vulnerabilities, thus strengthening their digital defenses against potential attackers.

The regular implementation of vulnerability scanning not only fulfills a technical requirement but also demonstrates an organization's dedication to maintaining the highest standards of information security. Such rigorous practices are crucial for demonstrating compliance with the comprehensive security measures outlined by ISO/IEC 27001, which is a prerequisite for obtaining certification within this globally recognized framework. The certification process highlights an organization's commitment to maintaining a strong ISMS, demonstrating its ability to effectively protect sensitive data from unauthorized access and breaches.

Furthermore, the implementation of vulnerability screening goes beyond simply achieving certification. It involves establishing a well-structured vulnerability management program that strictly adheres to industry-recommended security practices. This alignment is crucial for cultivating a culture of ongoing improvement within the organization, where security measures are regularly examined and updated to address evolving risks. Such an innovative approach to vulnerability management not only significantly reduces the likelihood of security incidents but also enhances the organization's resilience against cyber threats.

Engaging in regular vulnerability scanning instills businesses with a heightened awareness of the prevailing threat landscape. This enhanced awareness is critical for formulating and implementing targeted preventive measures that are precisely tailored to mitigate specific risks. By doing so, enterprises can ensure that their security measures are both efficacious and adaptable, capable of addressing the intricacies of a rapidly expanding digital ecosystem.

2.2 Tools overview and process

2.2.1 The process

As mentioned earlier, a vulnerability scanner is a sophisticated software tool meticulously designed to autonomously detect security vulnerabilities within computer systems and networks. This tool meticulously examines systems to uncover known vulnerabilities, including improperly configured settings, gaps in security updates, and flaws within software applications. The primary goal of these instruments is to proactively identify vulnerabilities, thus enabling their prompt mitigation. This proactive discovery plays a crucial role in significantly enhancing an organization's security position, making it an indispensable asset in the field of cybersecurity.

The complex process of choosing the most appropriate vulnerability scanner requires a thorough analysis of several crucial factors. Initially, it is crucial to identify the specific objectives of the scan, including the desired scope of coverage—such as networks, web applications, and operating systems—and the level of detail required to be uncovered. Subsequently, the compatibility of the scanner with the existing IT infrastructure must be thoroughly evaluated to ensure it supports the platforms and systems currently in use. Another crucial consideration is the usability aspect, including how easily the scanner's findings can be interpreted and its ability to seamlessly integrate with other security tools or risk management frameworks. Ultimately, a cost-benefit analysis should guide the decision-making process, balancing the available budget with the need to conduct a thorough and effective scan.

The process of using a vulnerability scanner begins with its configuration, during which scan parameters are defined based on specific security objectives. This involves identifying target systems and customizing the scanner's settings to improve the effectiveness and accuracy of the scan. The next phase involves the actual execution of the scan, during which the tool examines designated systems and compares detected details against a database of known vulnerabilities. This stage is crucial for identifying vulnerabilities that could potentially be exploited. Notably, the selection of sources for vulnerability information varies in terms of reliability and currency. More recent sources may use fewer formal approaches, which can impact their reliability. It is crucial to recognize that relying solely on scan results could be misleading, as the investigation may be limited or superficial, and the source could overlook certain vulnerabilities in the analyzed software [2].

This accurate approach underscores the importance of vulnerability scanners in the cybersecurity ecosystem, emphasizing the need for careful selection and utilization to ensure the integrity and security of an organization's digital assets.

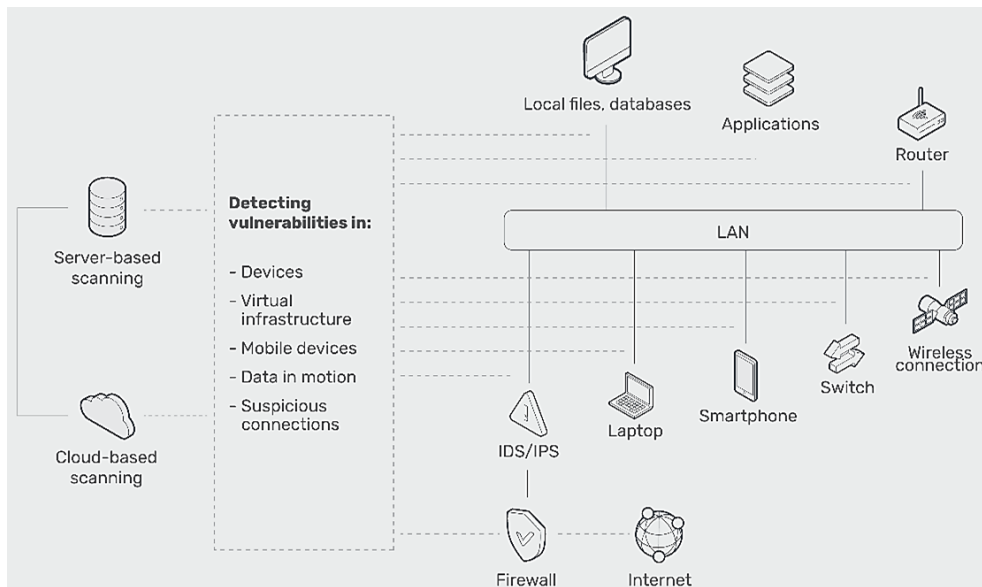


Figure 2.1: How a vulnerability scanner works (Source: getapp.com)

2.2.2 Results analysis and management

The analysis of vulnerability scan results is a complex and crucial task that requires a thorough examination of the collected data to identify and prioritize security risks according to their severity. During this critical phase, a comprehensive evaluation of the identified vulnerabilities is conducted, carefully scrutinizing them based on their severity, the potential harm they may cause to the organization, and the ease with which malicious actors can exploit them. Such an evaluation is of utmost importance because it facilitates the identification of the most critical security weaknesses that require immediate attention. Consequently, businesses can efficiently allocate their resources to address these vulnerabilities. The ultimate result of this approach is to combine research findings to produce comprehensive reports. These reports play a crucial role in the field of cybersecurity by providing customized recommendations for addressing vulnerabilities, and helping organizations take the essential steps to strengthen their cybersecurity defenses. The importance of these reports cannot be overstated. They are essential tools for IT security managers, providing them with well-informed perspectives necessary to make strategic decisions about resource allocation for addressing the most critical vulnerabilities.

The integration of the gathered data into the organization's ISMS is essential for managing the outcomes of vulnerability analysis, especially in line with the criteria established by the ISO/IEC 27001 standard. This integration requires the implementation of corrective measures based on the established priorities identified

in the analysis, following the risk treatment principle outlined in the standard. The comprehensive process involves updating risk registries, designing and implementing mitigation measures, and assessing the effectiveness of these actions through future testing and evaluations. Such a comprehensive approach ensures that the organization not only addresses current weaknesses but also strengthens its resilience against future security threats. This ongoing process of improvement is essential for upholding a strong security posture that complies with the rigorous standards of ISO/IEC 27001, thus protecting the organization's information assets from constantly changing cybersecurity threats. This methodology emphasizes the need for a proactive and dynamic approach to information security management, ensuring that companies remain vigilant and adaptable in the face of new vulnerabilities and security challenges.

2.2.3 Most known tools for vulnerability scanning

Automated vulnerability scanning tools are essential for organizations' cybersecurity defenses. These advanced systems carefully analyze networks, systems, and applications to identify security vulnerabilities, incorrect configurations, and potential security threats, using databases that are continuously updated. This process enables organizations to proactively identify and address weaknesses before they can be exploited by malicious actors, thereby enhancing the protection of critical data and infrastructure. Furthermore, some advanced tools have the ability to autonomously correct identified vulnerabilities, which significantly reduces the workload for cybersecurity professionals and developers. This autonomous correction feature not only speeds up the remediation process but also ensures that vulnerabilities are addressed promptly, strengthening the organization's defense mechanisms against potential cyber threats. By incorporating these tools into their cybersecurity strategy, organizations can attain a higher level of security preparedness, making it significantly more difficult for attackers to breach their defenses.

Following, there will be an overview of some of the most effective and widely used vulnerability scanning tools in the field. These tools represent the cutting edge in the fight against cyber threats, empowering organizations to proactively identify, analyze, and mitigate vulnerabilities within their digital infrastructures. The following description aims to explore the unique characteristics, operational advantages, and technical specifications of each tool, providing a clear and comprehensive understanding of their functionalities and the added value they bring to the field of cybersecurity defense. Selecting the right vulnerability scanning tool requires careful consideration of several factors, such as compatibility with the current infrastructure, ease of integration, the scope of vulnerability coverage, and effectiveness in detecting and resolving vulnerabilities. Thus, the following

analysis aims to assist organizations in choosing the solution that best fits their specific security needs

By providing a comprehensive exploration of these tools, the literature helps organizations better understand how to leverage these tools to enhance their security posture, ensuring a more resilient defense against the increasing threats in the digital landscape. The process of choosing an appropriate vulnerability scanning tool involves evaluating the tool's ability to seamlessly integrate into existing systems, its effectiveness in identifying and addressing vulnerabilities, and its overall impact on the organization's cybersecurity framework. The aim is to empower organizations with the knowledge to make informed decisions that align with their security objectives and operational needs.

Herein is provided an overview of the major vulnerability scanning tools analyzed in this research:

- **Nexpose:** sophisticated software vulnerability assessment tool developed by Rapid7, stands out for its comprehensive approach to identifying and mitigating risks associated with software vulnerabilities. This tool is adept at scanning a wide array of components, including web applications, databases, networks, and operating systems, to detect potential threats, assess their risk level, and develop remediation plans to swiftly address these vulnerabilities. It facilitates a proactive vulnerability management strategy for security professionals, aiming to preemptively seal security loopholes within network infrastructures, thereby preventing unauthorized access and the compromise of sensitive information. A significant advantage of NeXpose is its integration with Metasploit products, enhancing its capability to identify vulnerabilities across diverse platforms and prioritize them based on the likelihood of exploitation. This prioritization helps in focusing remediation efforts on the most critical vulnerabilities, thereby optimizing the allocation of resources and reducing operational costs. The reports generated by NeXpose guide administrators in targeting interventions effectively, minimizing the risk of exposure [16].
- **Nmap:** also known as Network Mapper, is an open-source tool designed for network exploration and security auditing. It efficiently scans large networks but can also target individual hosts. Nmap utilizes raw IP packets in various ways to identify available hosts on a network, their offered services (including application names and versions), operating systems and their versions, firewall and packet filter types, among other features. One of its most notable capabilities is remotely determining the operating system of a device through TCP/IP stack fingerprinting. Nmap sends TCP and UDP packets to a remote host and analyzes the responses to identify the operating system's characteristics, including the vendor, the operating system, version,

and device type. This tool is available across multiple platforms, in fact it supports most operating systems and is widely used for security audits. However, network administrators and system managers also find it valuable for routine tasks such as network inventory management, scheduled service updates, and monitoring hosts or uptime. Nmap's output includes a scan of targeted entities, providing additional information based on the selected options. A key component is the port table, listing port numbers, protocols, service names, and their current statuses, such as "open" for ports actively accepting connections. Open ports are crucial for security and operational scans alike, as they indicate available network services. Detailed information on software versions and supported IP protocols can also be provided, enhancing utility for security and network management. The tool offers its own Graphical User Interface (GUI), available for Linux, Windows, Mac OS X, and BSD, that aims to simplify its use for beginners while retaining advanced features for experienced users [16].

- **Nikto:** recognized as an open-source tool dedicated to web server evaluation, designed with the capability to uncover not only configurations and software on web servers but also insecure default files. It incorporates a database with more than 6,400 files deemed potentially dangerous and performs checks for outdated server versions across more than 1,000 servers, in addition to identifying version-specific issues on over 270 servers. Nikto's analytical prowess extends to detecting a range of potential issues and security vulnerabilities, such as server and software misconfigurations, pre-installed default files and programs, unprotected files and applications, and obsolete servers and software. Built on LibWhisker2, it is versatile enough to operate on any platform that supports a Perl environment, making it compatible with Windows, Mac OSX, and various Linux distributions. Furthermore, Nikto supports SSL, proxies, and host authentication, among other features, and can be updated automatically through command-line instructions [3].
- **Uniscan:** an open-source tool designed for web application security analysis, targeting vulnerabilities like Remote File Inclusion (RFI), Local File Inclusion (LFI), and Remote Command Execution (RCE). It excels in detecting critical security issues, including cross-site scripting, SQL injection, and more. Uniscan's advanced features include server fingerprinting, automated searches via Google and Bing, and a detailed vulnerability scanning process. Its integration of functionalities such as web crawling, SSL and proxy support, and modular architecture enhances its capability to identify, analyze, and mitigate web application vulnerabilities effectively, making it a sophisticated tool in cybersecurity efforts [3].

The revised overview highlights Nikto and Uniscan’s specialized roles in web application security, focusing on their unique capabilities without redundant details from the comprehensive tool summary. Nikto excels in identifying a broad range of web server vulnerabilities, while Uniscan targets specific threats like RFI, LFI, and RCE, crucial for mitigating severe security risks. Nmap, distinct for network mapping and service enumeration, offers extensive insights into network infrastructures. Nexpose, recognized for its vulnerability management lifecycle coverage, benefits from Metasploit integration for practical vulnerability testing. This diversity underscores the necessity for varied tools in cybersecurity strategies, each tailored to specific challenges.

FEATURE	NEXPOSE	NMAP	NIKTO	UNISCAN
USE CASE	Extensive Vulnerability Management	Network discovery and auditing	Web server vulnerability scanning	Web application vulnerability scanning
KEY CAPABILITIES	Deep network scans, risk categorization	Host discovery, port/service scanning	Over 6,700 checks for web server issues	Focuses on RFI, LFI, RCE
INTEGRATION	With Metasploit for enhanced management	Versatile, adaptable to many environments	SSL/HTTP proxy support	Advanced server fingerprinting
FOCUS	Risk assessment, actionable insights	Network topology, service identification	Exhaustive web server checks	Critical web app vulnerabilities
REPORTS	Detailed with prioritization	Granular network details	Various detailed formats	Straightforward text files

Figure 2.2: Vulnerability Scanner comparison (Source: own work)

2.3 Role in preparing penetration test

In summarizing the key insights presented in this chapter, it underlined the crucial significance of vulnerability scanning and assessment as fundamental components of a robust cybersecurity framework. These procedures are essential for detecting, evaluating, and prioritizing vulnerabilities, closely aligning with the requirements specified by the ISO/IEC 27001 standard for ISMS. This highlights their pivotal role in reinforcing defenses against security threats. The effective incorporation of vulnerability scanning and assessment of organizational security practices not only meets the requirements mandated by regulations but also lays the foundation for proactive cyber risk management, emphasizing the significance of an approach centered on continuous improvement within the ISO/IEC 27001 compliance framework.

Vulnerability scanning and assessment are fundamental initial steps that contribute to a more comprehensive analysis offered by penetration testing. Identifying and prioritizing vulnerabilities are essential activities for planning effective

penetration tests. These tests can verify the effectiveness of security measures against realistic attack scenarios. Vulnerability scanning enables organizations to gain a clear understanding of the weaknesses in the security of their information systems, identifying areas that require immediate attention. Conversely, penetration tests use this information to simulate targeted attacks and assess the ability of digital assets to withstand sophisticated intrusion attempts. Therefore, vulnerability scanning and assessment emerge as indispensable tools in fortifying cyber defense, serving as the basis for a thorough and compliant analysis of cybersecurity.

The importance of vulnerability scanning and assessment procedures in relation to compliance with ISO/IEC 27001 standards is crucial for the establishment of an effective ISMS. Through a systematic process of identifying, evaluating, and prioritizing vulnerabilities, organizations can proactively align their security practices with the strict requirements outlined by the regulation. This course of action not only identifies areas of risk within the IT infrastructure but also lays a strong foundation for implementing specific corrective measures, thereby strengthening information security.

Integrating these processes into the ISMS framework facilitates a cycle of continuous improvement, which is a fundamental pillar of the ISO/IEC 27001 standard. This dynamic approach to security management empowers organizations to quickly adapt to emerging threats and technological advancements, ensuring the ongoing effectiveness of protective measures. The ability to show unwavering commitment to improving information security not only strengthens the organization's resilience but also helps maintain stakeholder confidence and fulfill compliance responsibilities.

In concluding this section, it is imperative to lay the groundwork for the subsequent extensive discussion on the practice of penetration testing. The upcoming discussion will highlight the importance of penetration testing as a crucial supplement to vulnerability scanning and assessment. It provides a more thorough validation of the effectiveness of implemented security measures against realistic attack scenarios. The following section aims to explore the operational alignment between cybersecurity practices and the strategic framework outlined in the ISO/IEC 27001 standard. It illustrates how integrating these processes significantly strengthens information security management within organizations. This transition emphasizes the importance of a comprehensive understanding of security methodologies, including both theoretical concepts and practical applications, to ensure a secure digital environment that meets international standards.

Chapter 3

Penetration Testing

3.1 Definition, objectives, and importance

The activity known as penetration testing is a crucial process designed to uncover and identify vulnerabilities within a specific system. This analysis can be conducted internally or externally to the system, allowing for the identification of vulnerabilities within the area under review and the exploitation of its weaknesses. This evaluation includes all components of the IT infrastructure, such as applications, network devices, and physical security measures. Penetration testing can also involve adopting the mindset of a hacker and employing techniques that a malicious individual might use, simulating their actions. The word “hacker”, in the common terminology, refers to individuals who access an IT infrastructure without authorization in order to fulfill malicious actions. This distinction highlights the fundamental difference between a penetration tester (also known as a pentester) and a hacker. Both use similar methodologies and techniques to intervene in a system, but pentesters are authorized individuals who are not permitted to destroy their client’s infrastructure. Another significant difference between pentesters and hackers is that the former are tasked by a specific organization on identifying all vulnerabilities within a system, not just those that provide privileged access.

Penetration testing has emerged as an essential tool in cybersecurity. It is aimed at proactively identifying and addressing system vulnerabilities before they can be exploited by unauthorized entities. By systematically probing these components, penetration testing uncovers vulnerabilities that could threaten the integrity, confidentiality, and availability of information assets.

Adopting a hacker’s perspective during penetration testing provides invaluable insights into the security status of a system. By emulating the tactics, techniques, and procedures (TTP) of potential adversaries, penetration testers can better anticipate and thwart attack vectors. This approach emphasizes the ethical boundary

that distinguishes penetration testers from their malicious counterparts.

One of the main goals of penetration testing is to evaluate the security of a system, which is becoming more closely linked to technological advancements in today's era, and therefore more vulnerable to potential intrusions and attacks. It is important to remember, however, that the purpose of penetration testing is not to attack or breach an organization's IT system, but rather to provide insights and recommendations for the issues discovered. Considering penetration testing as a cyclical operation, it should be repeated over a specified period due to the continuous updates and evolution of systems. This iterative process is essential for maintaining a strong defense against a constantly evolving threat landscape. Based on these assertions, penetration testing can be seen not just as a one-time audit, but a continuous cycle of evaluation, recommendation, and improvement aimed at achieving and maintaining an optimal level of security. In addition, pen-testing primarily provides an initial step toward understanding an organization's current security posture by identifying its flaws, prioritizing the identified risks and assessing their impact. Once risks are identified, the penetration test provides a security framework that enables the mitigation of financial losses and reduces the infrastructure to its minimum level of risk [21].

As organizations become more integrated with technological advancements, the range of vulnerabilities and the potential for unauthorized access also expand accordingly. Penetration testing has emerged as a vital tool in the cybersecurity arsenal, serving not only as a defensive mechanism against external threats but also as a proactive measure to fortify the security infrastructure. By meticulously identifying and evaluating system vulnerabilities, penetration testing facilitates a structured approach to risk management.

The importance of penetration testing in the context of cybersecurity, particularly within the ISO/IEC 27001 standard, is crucial for ensuring the computer resilience of organizations. This standard specifies the requirements for an ISMS, with a particular focus on identifying, assessing, and treating security risks. The Annex A includes a set of security controls, where vulnerability assessment and penetration testing can be identified as crucial components for verifying the effectiveness of implemented security measures. Through these processes, organizations can not only meet the standard's requirements but also take a proactive approach to risk management, thereby strengthening their defenses against constantly evolving cyber threats.

This strategy empowers organizations to actively counter cyber threats, safeguarding data and infrastructure. By identifying vulnerabilities early, it promotes a culture of ongoing security enhancement and ensures compliance with current standards, reducing legal and reputational risks. This proactive perspective not only strengthens defenses but also embeds a culture of vigilant risk management,

ensuring adaptability in the face of the dynamic cyber threat landscape.

3.2 Types, Tools, and Techniques

Within the context of penetration testing, there exist two foundational methodologies that guide the approach to this activity: black-box testing and white-box testing. The core distinction between these two methodologies lies in the extent of information available to the penetration tester concerning the systems under examination [20].

Black-box testing represents a method where an attack is simulated from an external perspective, hence it is frequently referred to as "external testing." In this scenario, the tester operates without detailed knowledge of the infrastructure, effectively emulating the actions a potential attacker might undertake by exploiting detected vulnerabilities. This process aims to ascertain whether unauthorized access to the system is feasible and, if so, the extent of data that could potentially be compromised. The essence of black-box testing lies in its simulation of real-world attacks, mirroring the limited information an external attacker would possess, thereby evaluating the system's defense mechanisms against unforeseen threats.

Conversely, white-box testing, also known as "internal testing," involves a scenario where the tester conducts a simulated attack with comprehensive knowledge of the infrastructure in question. This approach enables testers, in collaboration with system owners, to focus on specific targets, thereby assessing the integrity and robustness of the organization's security measures. White-box testing provides an in-depth evaluation of internal security, revealing vulnerabilities that may not be detectable through external methods.

Merging the principles of these two testing strategies leads to the development of greybox testing. This hybrid approach equips testers with partial knowledge of the system, bridging the gap between black-box and white-box testing. By providing some information, grey-box testing optimizes the testing process, allowing for a more efficient identification of vulnerabilities by eliminating the need for testers to spend time uncovering publicly available information.

In addition to the classification between white-box and black-box, penetration tests also differ depending on the type of test [6]:

- **Web application penetration testing:** Web applications often comprise the majority of the vulnerable attack surface on the internet. These applications operate on web servers, so it is essential to assess the server's security against both internal and external attacks. Given that web servers operate on port 80/TCP (Transmission Control Protocol), it is imperative to exercise extreme caution and implement multiple safeguards for the server. An

exploit refers to a specific vulnerability that allows the execution of malicious code by using a particular script. In this specific context, it is crucial to pay special attention to inadequate authentication mechanisms, logical flaws, unintended content disclosure, and, most importantly, to ensure that the web server remains up to date. The two most critical vulnerabilities for web applications are SQL (Structured Query Language) injection and Cross-site Scripting (XSS). SQL injection is a technique that involves sending malicious code to exploit the lack of control over the input data received by a web application that uses an SQL database. This type of vulnerability, for example, allows unauthorized access to restricted areas of a website, enabling authentication at the highest levels without the necessary access credentials. It also permits viewing or modifying sensitive data. To exploit SQL injection, it is necessary to first identify the injection point and then create a payload that disrupts a dynamically constructed query. Identifying the injection point involves testing each user input utilized by the web application. If the webpage behaves differently during this test, the application is considered vulnerable to SQL injections. Once the injection point is identified, the payload can be utilized. Cross-site scripting, instead, is a type of vulnerability attack that allows an attacker to manipulate the content of a web application. XSS occurs when data from untrusted sources is included in a web page without being properly sanitized or sufficiently encoded beforehand. To identify an XSS vulnerability, it is essential to scrutinize all user inputs to ascertain whether they are reflected in any form in the application's output (reflection point). After identifying the reflection point, it is crucial to determine whether it is possible to inject HTML code and observe if it appears in the output. This allows for gaining control of the output page. Cookies present a significant vulnerability in web applications, with exploits such as XSS allowing hackers to steal cookies, that can be used to impersonate a legitimate registered user. The majority of web applications are assessed through black box analysis, where the pentester evaluates the application from the perspective of a hacker, attempting to compromise it using a variety of existing tools for web application penetration testing. This methodological approach emphasizes the importance of a comprehensive security strategy that includes vigilant monitoring, timely updates, and the implementation of advanced security measures to protect against the constantly changing landscape of web-based threats.

- **Network penetration testing:** The primary aim of a network penetration test is to reveal vulnerabilities within the most crucial areas of a company's infrastructure that are vital for its operations. This type of assessment plays a pivotal role in evaluating the entire network, including essential compo-

nents like firewalls, database servers, and web servers. By conducting network penetration testing, organizations can enhance their security measures by employing specific tools and methodologies that meticulously identify and analyze network issues and breaches. These tools and processes are highly skilled at identifying all potential vulnerabilities that could be exploited by potential attackers. In this context, the vulnerabilities and weaknesses identified may involve compromised or altered data or systems due to exploits, viruses, Trojans, Denial of Service attacks, and similar threats. However, it is also crucial to consider other types of vulnerabilities that may arise from patches and updates or errors in servers, routers, and firewalls. The network penetration testing process involves a comprehensive and iterative approach to identifying and exploiting vulnerabilities within an organization's network infrastructure. Initially, a detailed examination is carried out to discover vulnerabilities in the most critical systems. Following this, the identified vulnerabilities are exploited to assess the depth of potential breaches. Subsequent steps include an in-depth review of internal systems to identify further vulnerabilities, enhancing the understanding of the network's security posture. This cycle of identification, exploitation, and review is performed repeatedly to ensure a thorough fortification of the network against potential cyber threats. By meticulously identifying and exploiting vulnerabilities, network penetration testing provides valuable insights into the security weaknesses of an organization's network infrastructure. Consequently, this allows for the strategic strengthening of defenses against potential cyber threats, safeguarding critical business assets and data. The iterative nature of the process ensures a continuous improvement cycle, where each iteration aims to uncover and address previously undetected vulnerabilities, ultimately enhancing the overall security framework of the organization.

- **Software penetration testing:** regarded as particularly challenging to manage due to potential issues that may arise both at the implementation and design levels. Within this domain, it is possible to distinguish between two main types of tests: functional tests and security tests. Functional tests are designed to verify that a given functionality correctly performs a specified task, ensuring that the software operates as intended for its primary use cases. These tests are critical in validating the operational effectiveness of software systems, focusing on the accurate execution of specific functions. On the other hand, security tests are tasked with probing deeply and directly into the security risks to ascertain how the system behaves under attack. Such tests aim to uncover vulnerabilities that could potentially be exploited by malicious entities, thereby posing a significantly higher challenge compared to functional tests. The reason for this increased difficulty

is that security tests are conducted to identify if and how the system can fail. Unlike functional tests that verify correct operations, security tests deliberately push the system to its limits to induce failure modes. These tests are meticulously planned with the objective of forcing the system to manifest errors, thereby revealing the conditions under which these errors occur. While functional tests assess the system's ability to perform intended tasks under normal conditions, security tests evaluate the resilience and robustness of the system against malicious attacks. The latter requires a profound understanding of potential security threats and the sophisticated techniques that attackers might employ.

3.3 Methodologies and Phases

3.3.1 Most common methodologies

Many different models have been adopted for penetration testing. The best-known and most used are known as flaw hypothesis and attack tree.

The flaw hypothesis methodology consists of 5 phases [8]:

1. **Information Gathering:** penetration testers initiate the process by acquiring comprehensive information pertaining to the target system. This enables them to comprehend the system's architecture, operational dynamics, and applications, with the objective of delineating the system's design to identify potential vulnerabilities.
2. **Flaw Hypothesis:** drawing from gathered data and known vulnerabilities in comparable systems, the evaluators hypothesize potential flaws within the system under review. The examination encompasses the system's management and maintenance policies and procedures, pinpointing vulnerabilities not only in its technical components but also in its execution and operational management. This phase leverages expertise and insights from previous assessments to uncover new vulnerabilities or reaffirm those already identified.
3. **Flaw Testing:** the testers then proceed to validate the hypotheses of defects. In this phase, vulnerabilities are categorized according to their significance and the predefined objectives. The prioritization in classification fluctuates based on whether the testing goal is to identify design flaws, implementation errors, or vulnerabilities that are particularly exploitable in external attacks.
4. **Flaw Generalization:** following the successful exploitation of a defect, the examination process evolves as testers seek to extrapolate from the initial discovery. This involves identifying defects of a similar nature within the

system, with the objective of broadening their investigative framework to uncover associated vulnerabilities

5. **Flaw Elimination:** in the final stage, testers recommend strategies to mitigate or eliminate identified flaws, although direct involvement in fixing these issues is beyond their scope of duties. Penetration testers provide comprehensive explanations regarding the vulnerabilities uncovered, their potential impact, and the manner in which malicious actors could exploit them. This is aimed at aiding the adoption of effective security measures.

The Attack Tree methodology stands as an advanced approach to the penetration testing field, proving particularly effective in scenarios where preliminary information about the target system is insufficient. This model simulates a cyber attack, reflecting the actions of an external aggressor facing an unfamiliar system. By employing a hierarchical structure that encompasses a root node, intermediate (parent) nodes, and terminal (child or leaf) nodes, the Attack Tree aims to depict the primary objective of the attack (root node) and the various pathways (child nodes) that could lead to such an outcome.

In this framework, child nodes signify conditions or preliminary actions required to activate their directly connected parent node. Achieving the root objective signifies a successful attack. The intermediate goals, outlined by the internal nodes, illustrate the diverse strategies and combinations of actions necessary to perpetrate the attack, while the leaves of the tree detail the specific techniques utilized. Although Attack Trees provide a general overview applicable to a broad range of systems, their practical utility in detecting specific vulnerabilities is constrained without concrete details about the system under examination. To enhance the effectiveness of the process, it is recommended to develop a secondary, more nuanced attack tree. This second tree addresses the system's vulnerabilities in a more specific and detailed manner, transforming each generic attack (leaf of the first tree) into a set of targeted actions, considering the peculiarities of the system being studied. Thus, the subgroups of the second tree offer a precise mapping of the conditions under which the attack objective can be realized, significantly enriching the effectiveness of penetration testing [22].

the system's integrity is not inadvertently compromised. This phase also encompasses administrative duties, such as the aggregation of pertinent documents and the management of specialized equipment. This authorization, frequently termed as the "rules of engagement" (ROE), is expected to enumerate IP addresses or ranges for testing, stipulate any host-specific restrictions, and outline an array of permissible techniques, including but not limited to DoS attacks, password cracking, and network sniffing, as sanctioned by the organization.

- **Discovery phase:** this phase can be divided into two main activities:
 - Reconnaissance and target discovery: The foremost objective of this investigative phase is the comprehensive acquisition of data pertaining to the system under analysis, covering both technical and non-technical dimensions. It encompasses the identification of the operating system, potential vulnerabilities, and pertinent organizational information. The process of reconnaissance splits into passive endeavors—such as network searches and analyses of connected systems—and active ones, where preliminary data is corroborated through direct techniques. The prevalent methodologies are Social Engineering, which employs psychological manipulation for the extraction of information from employees; Garbage Picking, the inspection of disposed documents for sensitive data revelation; and Internet Footprinting, a legitimate and secure strategy for target identification employing browsers, search engines, and databases to amass corporate data, execute network enumeration, and pinpoint active computers and services via utilities like ping and traceroute.
 - Scanning and Enumeration: The scanning phase enables the identification of systems within the target network. It allows for the examination of which ports are open and which are filtered, the services operating on these ports, operating system details, network pathways, and more. Understanding these specifics facilitates the detection of vulnerabilities within the system. From this point forward, it is imperative for the tester to proceed with caution to avoid overwhelming the system or network with excessive traffic. This approach not only ensures a thorough analysis but also maintains the integrity of the network infrastructure under examination.
- **Assessment phase:** At this critical stage, the identification and analysis of vulnerabilities is of vital importance, serving as an essential link to the previous phase of discovery. The elements identified during the discovery phase provide vital inputs for the in-depth assessment of the securities and vulnerabilities of the system:

- **Vulnerability identification:** during this stage, security professionals embark on a comprehensive examination of systems or networks that extends beyond the preliminary assessment conducted in the discovery phase. Leveraging gathered data, such as details on operating systems, IP addresses, and the services under inquiry, the process actively identifies potential vulnerabilities and threats. Significant vulnerabilities include software flaws, improper system configurations, susceptible accounts, and unnecessary services. Many different vulnerability databases are available, providing up-to-date information on vulnerabilities and associated risks, thereby facilitating a more informed and effective security analysis. This stage is crucial for the thorough identification and understanding of security weaknesses that could be exploited.
- **Vulnerability Analysis:** the vulnerabilities identified undergo a meticulous analysis. Pentesters are tasked with assessing the security level of systems or networks, differentiating between genuine vulnerabilities and false positives. This process may utilize automated tools, equipped with internal databases for the identification of both recent and older vulnerabilities, or manual checks for a more specific and contextualized analysis of the environment under examination. In conducting this assessment, pentesters must navigate through the complexities of security systems, employing a blend of technological resources and expert judgement to accurately identify potential security flaws. This thorough evaluation ensures that only legitimate vulnerabilities are addressed, thereby enhancing the overall security posture of the system or network in question.
- **Exploration phase:** the penetration testing attack phase is recognized as the most challenging segment of the process. It is at this juncture that practitioners, utilizing tools and information garnered in preceding stages, aim to achieve comprehensive control over the system under review. This phase involves a meticulous identification and analysis of vulnerabilities within selected targets, facilitating the execution of an attack, the confirmation of identified vulnerabilities, and, upon success, the pursuit of obtaining higher privileges within the system. The exploitation of vulnerabilities is conducted with utmost caution, considering potential impacts and testing exploits in controlled environments to mitigate risks associated with the deployment of critical techniques, such as buffer overflow exploits. Exploit frameworks play a pivotal role in this phase, enhancing penetration efficiency. The focus then shifts to privilege escalation, where penetration testers devise strategies to elevate their access level, aiming for root privilege or, in the context of

networks, analyzing traffic to intercept sensitive data. The use of rootkits or backdoors may aid in securing elevated privileges, which is crucial for gaining complete control over the system or network. This stage demands a methodical and precise approach, highlighting the significance of a thorough evaluation and cautious implementation of exploits to optimize the attack's effectiveness while preserving the integrity of the system under examination.

- **Reporting phase:** at this stage, the role of the tester assumes vital importance as they possess a comprehensive understanding regarding the various weaknesses inherent within the system or network under examination. This specific phase gives upon the tester the capability to provide in-depth insights pertaining to the vulnerabilities identified during the evaluation process. It is the responsibility of the reports generated within this specific context to incorporate a comprehensive evaluation of the vulnerabilities, encompassing a thorough analysis of the potential risks associated with these weaknesses as well as the development of feasible solutions aimed at mitigating or eliminating them. The primary objective of the final report is to offer the organization a lucid comprehension of their present security position concerning their systems or network infrastructure. This document serves as a tool in enabling the company to assess the efficacy of their current security measures and identify areas that necessitate improvement.



Figure 3.2: Penetration testing phases (Author: Colecchia S.)

3.4 Summary

The above analysis recognizes penetration testing as an essential component within the framework of the ISO/IEC 27001 standard, serving as a proactive instrument for organizations to identify and mitigate system vulnerabilities. This practice encompasses a systematic procedure that replicates both external and internal attacks, thus enhancing the resilience of information technology systems. The implementation of this approach not only aids in conforming to current security standards but also fosters a culture of proactive security, which is indispensable in the rapidly evolving digital era. The cyclical nature of penetration testing, in conjunction with the requirements established by the standard, emphasizes the significance of an ongoing commitment to enhancing cybersecurity measures. This process also plays a critical role in the strategic management of risks and in fortifying defenses against increasingly sophisticated threats. Through the adoption of penetration testing, organizations are equipped with a robust methodology to strengthen their cybersecurity posture, preserving the safeguarding of informational assets against potential breaches, thereby ensuring the sustained protection and security of critical data.

Chapter 4

Implementation

4.1 Environment setup: Kali Linux and BWAPP

This chapter endeavors to thoroughly explore the experiential knowledge acquired during an internship at Brain Technologies in Torino, with a particular emphasis on establishing a virtual setting for vulnerability assessment and penetration testing. By leveraging specific tools like Nmap, Nikto, and OWASP ZAP inside a simulation environment made with Kali Linux and BWAPP (Buggy Web Application), the chapter attempts to present a broad overview of the methodologies, technical decisions, and practices implemented throughout the project experience.

The primary aim of this chapter is dual: firstly, to clarify the configuration of the testing environment, outlining the technical rationales behind the selection of Kali Linux and BWAPP as the main basing instruments for the following activities; and secondly, to examine the operational phases of vulnerability scanning and penetration testing.

4.1.1 Oracle VirtualBox and Kali Linux

Following a meticulous assessment of the available options, Kali Linux was chosen as the primary environment for conducting testing activities. The selection of Kali Linux was predicated on both technical and strategic criteria, with the ultimate goal of leveraging advanced tools for penetration testing and vulnerability scanning.

Kali Linux, developed by Offensive Security, is recognized as a leading Linux distribution within the cybersecurity domain. It is equipped with an extensive collection of tools for penetration testing, forensic analysis, and ethical hacking, pre-installed to facilitate immediate operational readiness. The selection of Kali Linux for this thesis was based on its open-source access and its extensive toolset, which eliminates the need for additional software installations, allowing for the

direct initiation of testing activities. Its architecture supports modularity, enhancing its capability to integrate a wide range of specific security testing tools, thus demonstrating its versatility in addressing diverse cybersecurity challenges effectively. The distribution also features customized workspaces and the capability for automated scripting, which streamlines the integration of specific methodologies into the project workflow. The decision to employ Kali Linux is further justified by its global community, comprising both users and developers, who contribute to regular updates, security enhancements, and provided technical support.

Opting to deploy Kali Linux within a virtualized environment facilitates the creation of a distinct, safeguarded operating system dedicated to executing security evaluations in a compartmentalized setting, thereby diminishing potential threats to the primary system. The process of integrating a new virtual machine via Oracle VirtualBox commenced with the acquisition of Kali's ISO image directly from its official website, followed by the adjustment of technical parameters, such as the selection of the Linux operating system, specifically the 64-bit Debian variant, alongside the calibration of RAM and disk space allocations. Such calibrations were aimed at enhancing system performance while simultaneously preventing undue strain on the host's resources. The installation's finalization was achieved through the utilization of Kali Linux's graphical setup interface, which addressed various configuration needs such as disk segmentation, network setup, and the determination of necessary software components.



Figure 4.1: Kali Linux Desktop

After successfully setting up the testing environment, the following step was then the selection of a suitable infrastructure, intended to replicate the conditions of a real-world organization.

4.1.2 BWAPP (Buggy Web Application)

After a thorough analysis of various alternatives, bWAPP, an acronym for Buggy Web Application was chosen for being among the most well-known and utilized vulnerable web applications in the field of cybersecurity for educational and training purposes [10]. bWAPP provides a safe and controlled environment to explore and experiment with a wide range of web vulnerabilities, covering over a hundred bugs found in real applications, including all the common security risks identified by the Open Web Application Security Project (OWASP).

Before the installation of bWAPP, setting up an Apache server and a MySQL database was essential to establish a suitable environment where the application could be executed efficiently. This setup was essential because bWAPP relies on a functioning web server and database to simulate web application vulnerabilities effectively.

The initial step involved installing the Apache web server on the Kali Linux operating system. The installation process was straightforward, through the execution of the command `sudo apt-get install apache2` in the terminal. After installation, Apache's active status and listening on port 80 were confirmed using the command `sudo systemctl status apache2`. Following this, the web server's root directory was configured to host the bWAPP files, ensuring that security settings and file permissions were adequately adjusted to thwart unauthorized access.

The subsequent phase focused on installing and setting up the MySQL database management system. MySQL was chosen for its compatibility with bWAPP and its reliability as a database management system. Installation was carried out using the command `sudo apt-get install mysql-server`, followed by the initialization of a new database instance through the command `sudo systemctl mysql start`. Through MySQL's command-line interface, a new database was created with the command and a user with specific privileges for that database, ensuring that the bWAPP application had the necessary permissions to perform database operations without compromising system security. Once the Apache server and MySQL database were configured, the installation of bWAPP started. Firstly, the bWAPP zip folder was downloaded from the official website and positioned in `/var/www/html`, serving as the root directory where bWAPP would reside for access through the Apache web server. Regarding the configuration of the database, a MySQL user was configured with the necessary privileges for accessing and amending this database. This procedure ensured that bWAPP was capable of interfacing seamlessly with its database for both retrieval and storage tasks. The `settings.php` file, located within the admin directory of bWAPP, was then modified to incorporate the connection specifics to the MySQL database, encapsulating details such as the name of the database, user credentials, and password. In the matter of configuring file permissions, appropriate permissions were assigned to

various directories encapsulated within the bWAPP environment, encompassing documents, images, passwords, and logs. This allocation was imperative, guaranteeing that the application possessed the requisite permissions for its optimal functionality. During the concluding phase of installation and access, the bWAPP installation interface was accessed via a web browser by directing it to `127.0.0.1/bWAPP/install.php`, culminating in the completion of the installation process.

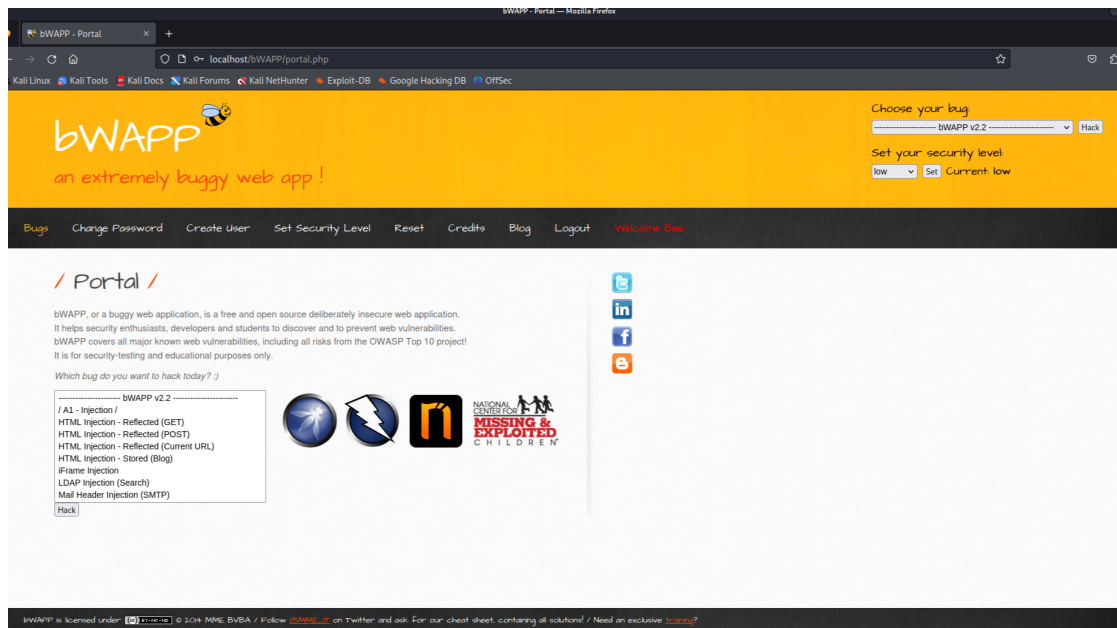


Figure 4.2: bWAPP home page

4.2 Vulnerability Scanning

Upon completing the installation and configuration of bWAPP, the next step in the process involved selecting the most suitable tools for performing vulnerability scanning on the specifically prepared infrastructure. Given the wide array of tools available on Kali Linux, this choice necessitated a careful examination of the characteristics, functionalities, and specific application areas of each tool in order to identify those best aligned with the research objectives.

Following a careful analysis in the literature and on the web, the primary candidates identified were Nmap, Nikto, OWASP ZAP, Metasploit, and Burp Suite. Each tool presents a different set of capabilities for identifying vulnerabilities and assessing the security of web applications. However, considering the particular needs of the project and the infrastructure represented by bWAPP, the final choice

fell on the following tools for the reasons listed below:

- **Nmap** was chosen for its technical proficiency in detecting hosts and services, efficiently mapping the network infrastructure, and identifying active ports and available services. This selection is underscored by Nmap's suitability for initial penetration testing phases, where it offers a detailed examination of the network's vulnerability landscape [3].
- **Nikto**, a specialized web vulnerability scanner, conducts tests on web servers to identify more than 6,700 potential vulnerabilities and security issues. It facilitates host authentication, subdomain prediction, enumeration of usernames via Apache and CGIwrap, and employs mutation techniques for identifying phishing vulnerabilities within web servers. It was also chosen because of its ease of use and the ability to generate detailed reports of its scans, which are useful for better analyzing the results for academic purposes [16].
- **OWASP ZAP** was chosen for its function as an effective attack proxy to analyze, test, and detect web application vulnerabilities during the development and testing phases. The main reason for the choice lies in its graphical interface and HTTP/HTTPS traffic manipulation capabilities, making it a comprehensive tool for security testing. As an open-source, Java-based tool developed by the OWASP project, ZAP offers extensive features, including web crawling, vulnerability identification, fuzzing analysis, and automated scans [10].

The decision to focus on these three tools was driven by the goal of understanding the widest possible range of potential vulnerabilities, from network mapping, to service discovery, to detailed analysis of web applications. The choice also lies in their similarities, for exhaustive confirmation of the results, and their differences, for operational adaptability and differences in use through different user interfaces.

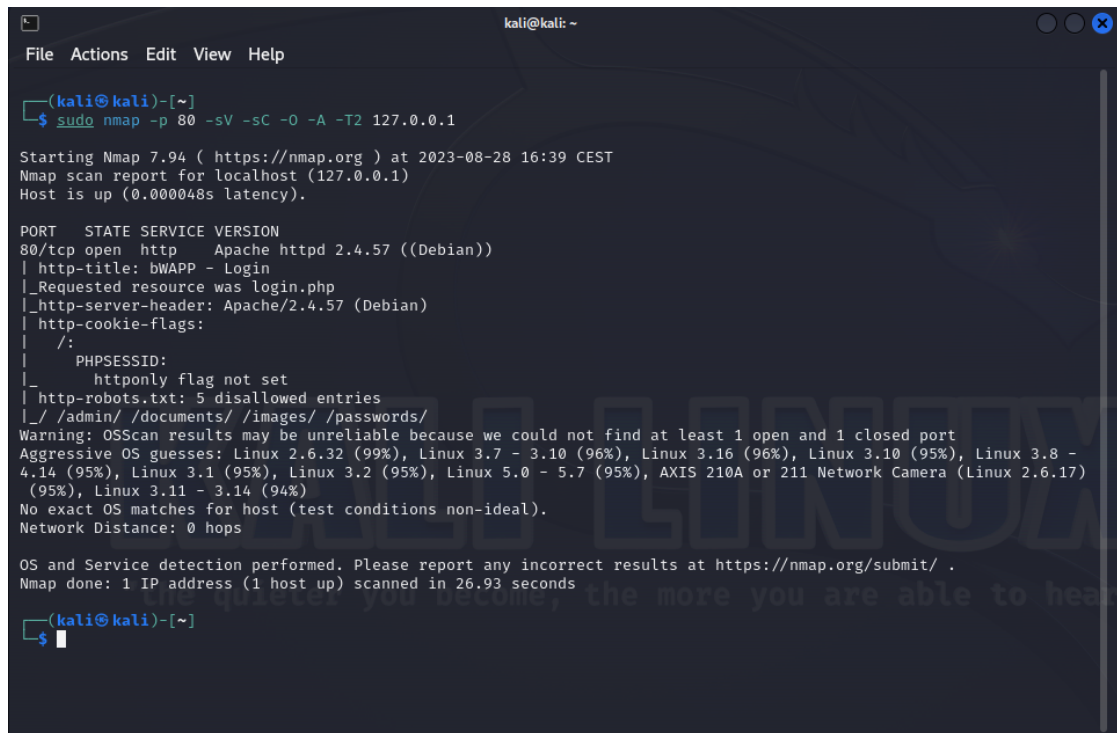
4.2.1 Nmap

The deployment of Nmap as the initial tool in the vulnerability scanning process provided a complete and detailed overview of the bWAPP network environment. The execution of the command line

```
sudo nmap -p 80 -sV -sC -O -A -T2 127.0.0.1
```

facilitated an in-depth analysis, specifically targeting port 80, which is predominantly utilized for HTTP traffic. The chosen parameters enabled the identification of the service version (`-sV`), the implementation of standard scanning scripts to arise additional information (`-sC`), the determination of the operating system (`-O`), an advanced scan (`-A`), and a timing template that moderates the scanning

speed to enhance accuracy and stealth (-T2). This strategic approach not only underscores the importance of preliminary scanning in understanding the security landscape but also exemplifies the meticulous configuration of Nmap to maximize the efficacy of the vulnerability assessment.



```

kali@kali: ~
└─(kali@kali)-[~]
└─$ sudo nmap -p 80 -sV -sC -O -A -T2 127.0.0.1

Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-28 16:39 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000048s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.57 ((Debian))
|_ http-title: bWAPP - Login
|_ Requested resource was login.php
|_ http-server-header: Apache/2.4.57 (Debian)
|_ http-cookie-flags:
|   /:
|   PHPSESSID:
|   httponly flag not set
|_ http-robots.txt: 5 disallowed entries
|_/admin/ /documents/ /images/ /passwords/
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 2.6.32 (99%), Linux 3.7 - 3.10 (96%), Linux 3.16 (96%), Linux 3.10 (95%), Linux 3.8 -
4.14 (95%), Linux 3.1 (95%), Linux 3.2 (95%), Linux 5.0 - 5.7 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17)
(95%), Linux 3.11 - 3.14 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.93 seconds

└─(kali@kali)-[~]
└─$

```

Figure 4.3: Nmap script and output

The findings from the scan have unveiled essential details regarding the underlying infrastructure of bWAPP. The listening service on port 80 has been identified as "http," operated by Apache httpd version 2.4.57 on a Debian system. This piece of information is important as each version of the web server may harbor specific known vulnerabilities that could be exploited in subsequent stages of penetration testing. Moreover, the analysis of the HTTP server header has corroborated the Apache version, providing an added layer of detail concerning the running software.

Additionally, the detection of a robots.txt file configured to disallow certain paths, such as /admin/, /documents/, /images/, and /passwords/, signals areas of the application that the developers aim to conceal from search engines. While this configuration was purposeful for testing objectives, in a real-world scenario, it could unveil insightful information on potential sensitive areas within the application. The discovery of the *bWAPP - Login* page through the resource

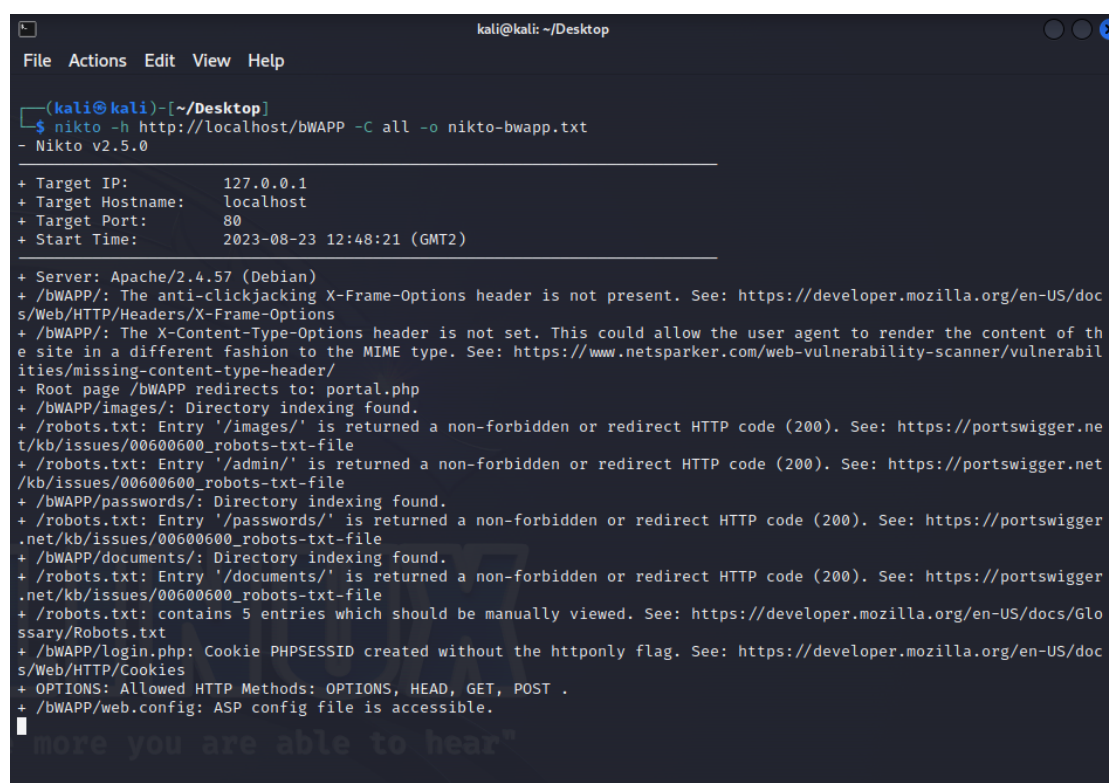
request `/login.php` is a critical piece of information for planning penetration testing attacks. This is because login pages frequently serve as targets for brute force attempts, SQL injection, and other exploitation techniques. Understanding the application's workflow and identifying areas that may be vulnerable is vital for conducting focused security testing. This knowledge allows testers to devise strategies that can effectively identify and address potential security weaknesses within the system.

4.2.2 Nikto

The utilization of Nikto followed the execution of Nmap scan, concentrating on a more intricate examination of specific vulnerabilities within the tested web application. By employing the command line instruction

```
nikto -h http://localhost/bWAPP -C all -o nikto-bwapp.txt
```

the process generated an extensive analysis, offering insightful findings into the security vulnerabilities of the application.



```
kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali)-[~/Desktop]
└─$ nikto -h http://localhost/bWAPP -C all -o nikto-bwapp.txt
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 80
+ Start Time: 2023-08-23 12:48:21 (GMT2)

+ Server: Apache/2.4.57 (Debian)
+ /bWAPP/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /bWAPP/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page /bWAPP redirects to: portal.php
+ /bWAPP/images/: Directory indexing found.
+ /robots.txt: Entry '/images/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/admin/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /bWAPP/passwords/: Directory indexing found.
+ /robots.txt: Entry '/passwords/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /bWAPP/documents/: Directory indexing found.
+ /robots.txt: Entry '/documents/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 5 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /bWAPP/Login.php: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
+ /bWAPP/web.config: ASP config file is accessible.
```

Figure 4.4: Nikto script and output

The generated report highlighted several critical issues that necessitate particular attention:

- **Absence of Security Headers:** the HTTP response headers X-Frame-Options and X-Content-Type-Options are missing, making the application susceptible to clickjacking attacks, where users might be tricked into clicking on something different than expected, and Multipurpose Internet Mail Extensions (MIME) sniffing attacks, which elevate the risk of executing malicious content in unintended contexts.
- **PHPSESSID Cookie Without HttpOnly Attribute:** this omission renders cookies susceptible to XSS (Cross-Site Scripting) attacks, as it enables clientside scripts to access the cookies.
- **Permitted HTTP Methods:** HTTP methods that may not be necessary are allowed, broadening the attack surface available to an adversary.
- **Directory Indexing:** the indexing of directories such as `/admin/`, `/documents/`, `/images/`, and `/passwords/`, has been discovered, potentially exposing files or sensitive information not meant for public access.
- **Access to Configuration Files and Sensitive Data:** files like `web.config`, `phpinfo.php`, and `config.inc` are accessible, disclosing sensitive information about server configuration, software versions, and credentials.
- **Vulnerability to Cross-Site Scripting (XSS):** an XSS vulnerability has been identified in the file `test.php`, indicating that the application does not adequately sanitize user input.
- **Accessible Administration and Login Pages:** the existence of login pages and administrative sections (`/admin/`, `/login.php`) marked as of interest suggests potential entry points for targeted attacks.

4.2.3 OWASP ZAP

OWASP ZAP (Zed Attack Proxy) leverages a graphical user interface (GUI) alongside proxy capabilities to intercept and modify HTTP/HTTPS traffic between the browser and the web application. This strategy enabled the execution of a simplified and dynamic interactive scan, facilitating the analysis of requests and responses generated through standard application usage.

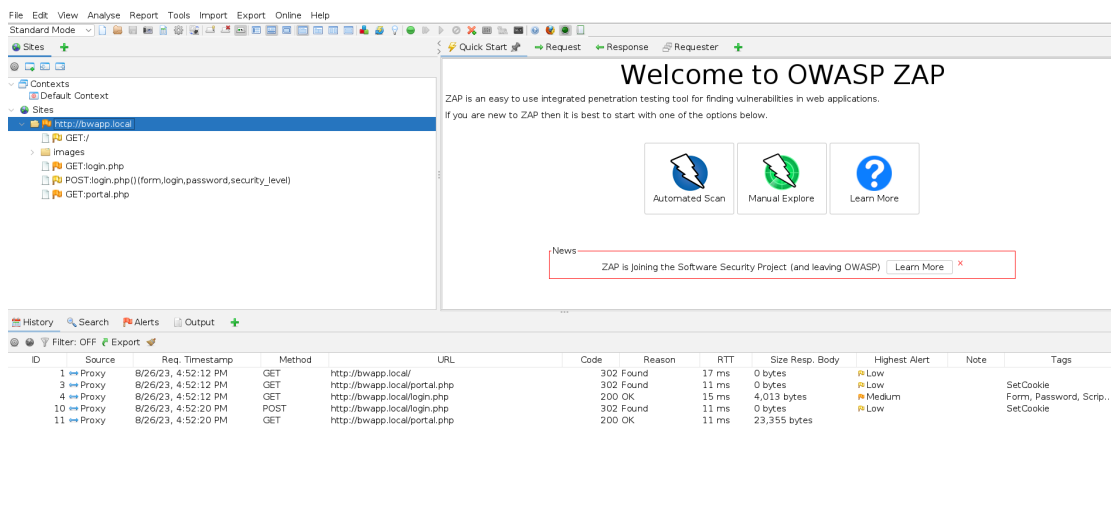


Figure 4.5: OWASP ZAP home page

Thanks to its proxy settings, that redirected the network traffic into the tool, the scanner was able to automatically recognize the web application and its paths. This instrument contains a wide array of diagnostic and offensive capabilities aimed at assisting in the detection, examination, and exploitation of vulnerabilities:

- **Active Scanner:** builds on preliminary outcomes from automated examinations by assertively employing recognized methods of attack to pinpoint more subtle security weaknesses.
- **Passive Scanner:** observes the data exchange to and from the web-based application for signs of security lapses, without actively dispatching harmful requests. This approach helps to reduce the possibility of interfering with the application's operations.
- **Forced Scanner:** tries to navigate to restricted sections of the application without the requisite permissions, revealing resources that are not adequately secured.
- **Fuzzer:** dispatches a broad spectrum of inputs to the application to identify abnormal responses that may signify security vulnerabilities.

Among these functionalities, the most versatile and adaptable tool is automated scanning, adept at performing comprehensive assessments with minimal setup. It utilizes a spider tool to scrape applications, mapping out the structure and identifying points of entry for potential attacks. The scanner then probes these points with a variety of payloads to detect common vulnerabilities such as SQL injection, cross-site scripting (XSS), and insecure server configurations.

The output generated from the automated scanning is an HTML report, which categorized identified vulnerabilities according to a risk-confidence matrix. This approach facilitates the process of prioritizing vulnerabilities based on their severity and exploitability likelihood, simplifying the pinpointing of areas that necessitate immediate corrective measures.

		Confidence				Total
		User Confirmed	High	Medium	Low	
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	2 (12.5%)	3 (18.8%)	1 (6.2%)	6 (37.5%)
	Low	0 (0.0%)	1 (6.2%)	3 (18.8%)	1 (6.2%)	5 (31.2%)
	Informational	0 (0.0%)	0 (0.0%)	2 (12.5%)	3 (18.8%)	5 (31.2%)
	Total	0 (0.0%)	3 (18.8%)	8 (50.0%)	5 (31.2%)	16 (100%)

Figure 4.6: Risk-Confidence Matrix (Source: OWASP ZAP Scanning Report)

Key Points from the OWASP ZAP Analysis:

- Medium-Level Risks with High Confidence:** the absence of a "Content Security Policy (CSP)" header elevates the potential for attacks such as script injection, underscoring the criticality of instituting CSP directives to alleviate these vulnerabilities. This highlights the essential role that implementing comprehensive Content Security Policies plays in mitigating the risk associated with script injection attacks and similar exploits. The detection of a hidden file (`/server-status`) could unveil crucial details regarding server configuration, thereby potentially laying bare the infrastructure to security risks. The presence of such hidden files is indicative of potential

oversights in server security management, which could inadvertently expose critical system configurations to malicious entities.

- **Medium-Level Risks with Moderate Confidence:** identified vulnerabilities include directory browsing and the absence of the "X-Frame-Options" header on `/portal.php`, which may divulge sensitive information and facilitate clickjacking attacks. These vulnerabilities, about directory browsing and inadequate framing policies present a tangible threat by potentially exposing sensitive data and enabling unauthorized interactions.
- **Low-Level Risks:** server version information and the lack of security measures in cookies have been flagged as minor vulnerabilities, yet they contribute to the overall risk view. These lesser concerns, though minor, collectively contribute to an enhanced risk profile by potentially facilitating more targeted exploits.

The methodology employed by OWASP ZAP is based on the systematic analysis and dynamic evaluation of web applications. These applications are particularly susceptible to a range of vulnerabilities, arising from the intricate interactions between client-side and server-side components. This tool has proven very effective in identifying problems related to content security policies, cookie management, and server configurations.

By classifying vulnerabilities according to their levels of risk and certainty, it provides valuable information necessary for developing strategies aimed at vulnerability mitigation and efficient allocation of security resources.

4.3 Penetration testing

Upon the completion of the vulnerability scanning phase, utilizing tools such as Nmap, Nikto, and OWASP ZAP, the process progressed towards a more targeted stage of penetration testing. This particular stage aimed to address vulnerabilities associated with Cross-Site Scripting (XSS) attacks and SQL Injection, which are widely recognized as common and high-risk threats to web applications [19]. These vulnerabilities were also identified as potentially critical during the scanning phase.

Cross-Site Scripting attacks exploit the failure of a web application to adequately sanitize input, thereby allowing malicious scripts to be injected into web pages accessed by other users. Such attacks can result in session theft, unauthorized modification of web content, and further malicious activities against users of the site.

SQL Injection, on the other hand, represents a different type of attack that takes advantage of weaknesses in the handling of SQL queries. This enables at-

tackers to execute unauthorized SQL commands, gain access to sensitive data, and potentially compromise the entire database.

4.3.1 Cross-Site Scripting (XSS)

The examination of the Cross-Site Scripting (XSS) vulnerability within the bWAPP application was conducted by embedding a straightforward script into the input field of one of the website's pages:

```
<script>alert('test XSS script')</script>
```

This particular script was crafted to assess the susceptibility of the application to XSS attacks, aimed to exploit distinct areas where the user's input is echoed back directly onto the web page without undergoing proper cleaning processes. The successful execution of this attack highlighted a critical shortfall in the application's defensive mechanisms against XSS threats. Specifically, it underscored bWAPP's failure to implement adequate input filter measures, thereby permitting the arbitrary execution of scripts within the user's browser context. The emergence of the JavaScript alert confirmed of the application's vulnerability to XSS attacks. This vulnerability not only compromises the integrity of user sessions but also significantly escalates the risk of severe security breaches, including but not limited to, the theft of cookies, manipulation of user sessions, and the perpetration of phishing schemes.

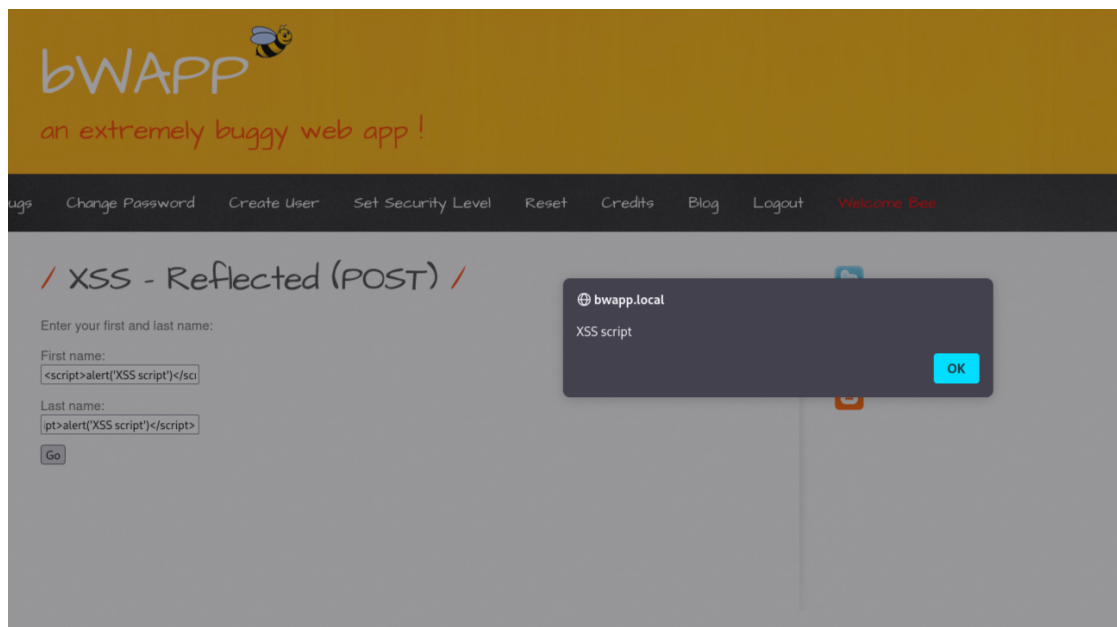


Figure 4.7: Successful Cross-site scripting

4.3.2 SQL Injection

The employment of SQL Injection, a prevalent attack technique targeting web applications, is aimed at exploiting vulnerabilities present in the SQL query management to manipulate or compromise the underlying database. The essence of SQL Injection attacks lies in their ability to gain unauthorized access to data, alter or destroy information, or potentially take control of the system hosting the application. This form of attack becomes feasible when user input, accepted by the web application, is directly incorporated into an SQL query without undergoing proper validation. Consequently, attackers can inject malicious SQL commands through user interface's input to carry out unauthorized operations on the database.

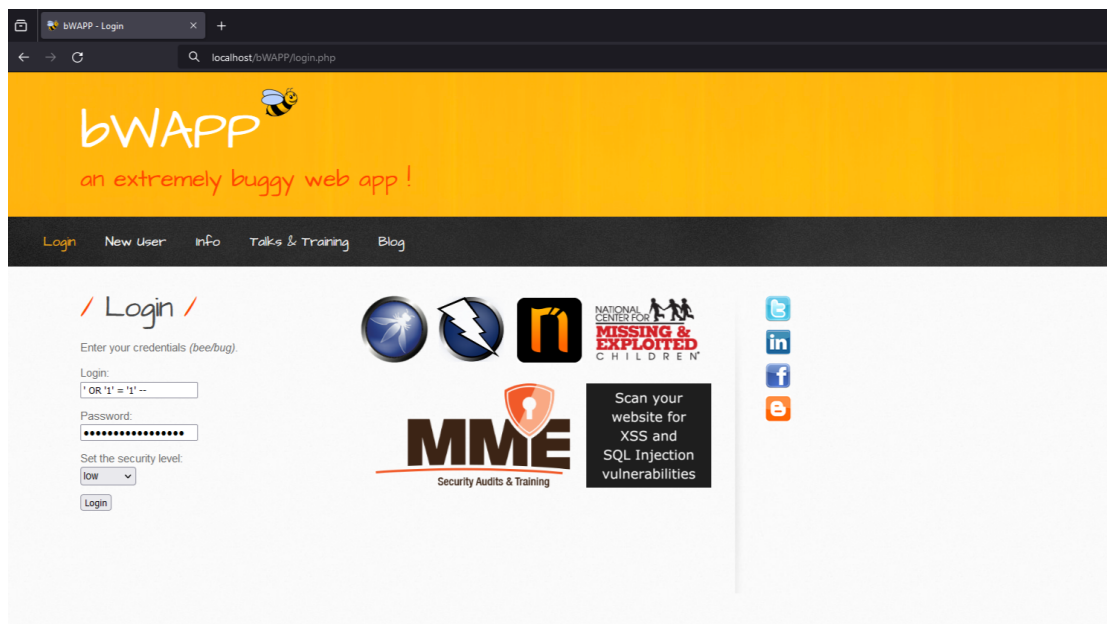


Figure 4.8: SQL Injection on bWAPP login page

Within the testing context, which is intentionally designed with vulnerabilities, the utilization of the SQL Injection script

```
' OR '1'='1' --
```

in the login page serves as a concrete illustration of how SQL Injection attacks can be executed and the preventive measures that may be employed. This specific command, when inserted into fields meant for user login credentials — typically the password or username field — exemplifies an SQL Injection vulnerability.

The above command modifies the original logic of the SQL query employed by the application for verifying login credentials [10]. The `OR` operator allows for the specification of alternative conditions in a `WHERE` clause, and `'1'='1'` represents a condition that is invariably true. The double dash `--` signifies the introduction of a comment in SQL, effectively disregarding the remainder of the application's original query, thus facilitating the success of the attack irrespective of the application's conditions. This command instructs the database to return all rows where the altered condition holds true, invariably resulting in the attack's success. As a result, the application may interpret the response as a successful login verification, granting access to the attacker without the need for valid credentials. The successful execution of this script on bWAPP's login page underscores the application's vulnerability to SQL Injection attacks, enabling unauthorized access to the application's restricted areas.

4.4 Results Analysis

The research executed employing tools such as Nmap, Nikto, and OWASP ZAP has disclosed that a systematic methodology towards vulnerability scanning and penetration testing constitutes an essential component for evaluating the security of web applications. These instruments have demonstrated considerable efficacy in detecting a wide array of vulnerabilities, ranging from those that are commonly recognized, like XSS (Cross-Site Scripting) and SQL Injection, to those that are less evident, pertaining to server configuration or user session management. The accuracy of the analysis assists in identifying critical vulnerabilities, thus enabling system administrators and information security professionals to apply precise remedial actions.

The association between the identified vulnerabilities and the security measures prescribed by the ISO/IEC 27001 standard is identified as a key element of the analysis. Aligning specific vulnerabilities with the respective measures of the standard highlights the importance of a cohesive security management strategy, integrating penetration testing with a stringent regulatory framework. This amalgamation aims to augment an organization's security posture, guaranteeing compliance with international norms and effective defense against cyber threats.

The implementation of these methodologies, through the utilization of sophisticated tools and adherence to a systematic and organized approach, facilitates the effective identification and mitigation of vulnerabilities, thus enhancing the cyber resilience of organizations. The incorporation of these practices into security management protocols, conforming to the ISO/IEC 27001 standard's guidelines, is crucial for developing a resilient and adaptable ISMS.

Chapter 5

Conclusions

The main goal of this thesis was to investigate the effectiveness of the existing regulatory framework represented by the international standard ISO/IEC 27001 in facilitating businesses' adaptation to digital transformation, specifically examining the role and added value of penetration testing practices in this process. Through a methodical analysis, it aimed to determine whether such practices could be considered not only as tools for cybersecurity defense but also as enhancers for corporate governance in the face of challenges posed by digitalization. Therefore, it sought to understand how the integration of penetration testing within cybersecurity strategies could actually strengthen organizations' resilience, improving their ability to protect critical data and infrastructure. This study intended to provide a significant contribution to the debate on how businesses can effectively adopt regulations and best security practices to successfully navigate the evolving digital landscape, evaluating the long-term impacts on the structure and culture of organizational security.

Throughout the dissertation, the ISO/IEC 27001 regulatory framework is explored, describing its history, development, and key components, the benefits of adopting such a standard for information security management, as well as the challenges related to its implementation. Subsequently, the research focuses on the methodologies, tools, and techniques of penetration testing, outlining how these practices are essential for identifying and mitigating vulnerabilities within corporate information systems. The methodological approach to vulnerability assessment is analyzed, providing details on the most commonly used software tools in this area. Moreover, a practical case study is presented, illustrating what the process of vulnerability scanning and penetration testing execution within a system might look like. Through the use of specialized platforms and software, it is demonstrated how penetration testing techniques significantly contribute to strengthening the cyber resilience of organizations. Finally, the thesis concludes with a summary of the results, aiming to provide significant insights for industry professionals, pol-

icymakers, and stakeholders interested in developing more effective and resilient cybersecurity strategies.

It has been demonstrated that penetration testing and other vulnerability management practices are fundamental pillars in the cyber risk management of organizations. A strategic collaboration between these tools and the current regulatory framework would not only improve cyber resilience through a proactive approach to risk management but would also enrich governance structures by implementing more effective and targeted cybersecurity practices. The integration of these practices amplifies an organization's ability to anticipate, identify, and mitigate cyber risks more effectively. These techniques, functioning as a dynamic audit, allow for the simulation of targeted cyber attacks, thus providing a holistic view of potential vulnerabilities. This process, if aligned with the rigorous standards of regulation, ensures that security measures are not only compliant with international best practices but are also continuously updated in response to emerging threats. Moreover, this would promote an organizational environment where information security is perceived as a shared responsibility, fostering the development of stronger cybersecurity policies, strategic planning, and a more anticipatory approach to risk management. In this context, the business approach is not limited to mere compliance with a standard but evolves into a dynamic process of continuous improvement, aimed at protecting digital assets and ensuring operational continuity, while also ensuring greater transparency and accountability within organizations. In this way, organizations can demonstrate to internal and external stakeholders their commitment to data protection and cyber risk management. This is particularly relevant in an era where digital trust plays a crucial role in the reputation and success of companies.

In conclusion, the commitment to continuously improve and adapt to the changing dynamics of the digital landscape will be essential to maintaining and enhancing information security in organizations. The ability to anticipate and effectively respond to cyber threats, integrating innovative strategies such as penetration testing with established regulatory frameworks, could certainly represent a key factor for the success of organizations' cybersecurity governance in the era of digital transformation.

Bibliography

- [1] Full disclosure and the window of exposure, 2001.
- [2] Vulnerability assessment (vulnerability analysis), 2006.
- [3] University computer network vulnerability management using nmap and nexpose. *International Journal of Advanced Trends in Computer Science and Engineering*, 10(6):3084–3090, 2021.
- [4] S. Watkins A. Calder. IT governance: An international guide to data security and ISO27001/ISO27002. Kogan Page, 2015.
- [5] W. A. Arbaugh, W. L. Fithen, and J. McHugh. Windows of vulnerability: a case study analysis. *Computer*, 33(12):52–59, 2000.
- [6] A. Bacudio, X. Yuan, B. Chu, and M. Jones. An overview of penetration testing. *International Journal of Network Security & Its Applications*, 3(6):19–38, 2011.
- [7] Sheetal Bairwa, Bhawna Mewara, and Jyoti Gajrani. Vulnerability scanners-a proactive approach to assess web application security. *International Journal on Computational Science & Applications*, 4, 2014.
- [8] M. Bishop. *Introduction to computer security*. Addison-Wesley, 2008. Chapter 20: Vulnerability Analysis.
- [9] A. Busleiman, C. Martorella, D. Sarrazyn, H.M. Racciatti, and K. Asgarally. Information systems security assessment framework (issaf) – penetration testing framework. Open Information Systems Security Group, 2005.
- [10] Voo Teck En and Vinesha Selvarajah. Cross-site scripting (xss), 2022.
- [11] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). ISO/IEC 27001: Information technology — security techniques — information security management systems — requirements. 2013.

- [12] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). ISO/IEC 27001: Information technology — security techniques — information security management systems — requirements. 2022.
- [13] M. Podrecca M. Sartor G. Culot, G. Nassimbeni. The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. In *The TQM Journal*, volume 33, pages 76–105, 2021.
- [14] M. Podrecca M. Sartor G. Culot, G. Nassimbeni. Information security and value creation: The performance implications of ISO/IEC 27001. volume 142, page 103744, 2022.
- [15] British Standards Institution. ISO/IEC 27001:2022 journey guide. 2022.
- [16] N. Karangle, A. K. Mishra, and D. A. Khan. Comparison of nikto and uniscan for measuring url vulnerability. In *10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2019.
- [17] P. Lachkov, L. Tawalbeh, and S. Bhatt. Vulnerability assessment for applications security through penetration simulation and testing. *Journal of Web Engineering*, 21(07):2187–2208, 2022.
- [18] J. Nilsson. Vulnerability scanners. Master of science thesis at department of computer and system sciences, Royal Institute of Technology, Kista, Sweden, 2006.
- [19] S. V. N. Parasram, A. Samm, D. Boodoo, G. Johansen, L. Allen, T. Heriyanto, and S. Ali. *Kali Linux 2018: Assuring Security by Penetration Testing: Unleash the full potential of Kali Linux*. Packt Publishing, 4 edition, 2018.
- [20] I.P.A.E. Pratama and A.M. Rhusuli. Penetration testing on web application using insecure direct object references (idor) method. In *2022 International Conference on ICT for Smart Society (ICISS)*, pages 01–07, 2022.
- [21] U. Ravindran and R.V. Potukuchi. A review on web application vulnerability assessment and penetration testing. *Review of Computer Engineering Studies*, 9(1):1–22, 2022.
- [22] V. Saini and Q. Duan. Attack tree-based security analysis for myproxy online credential repository.

List of Figures

1.1	History of ISO/IEC 27001 (Source: own work)	7
1.2	ISO/IEC 27001 Certification Process (Source: kolide.com)	12
2.1	How a vulnerability scanner works (Source: getapp.com)	25
2.2	Vulnerability Scanner comparison (Source: own work)	29
3.1	Example of an Attack Tree (Author: De Biase G.)	38
3.2	Penetration testing phases (Author: Colecchia S.)	41
4.1	Kali Linux Desktop	44
4.2	bWAPP home page	46
4.3	Nmap script and output	48
4.4	Nikto script and output	49
4.5	OWASP ZAP home page	51
4.6	Risk-Confidence Matrix (Source: OWASP ZAP Scanning Report)	52
4.7	Successful Cross-site scripting	54
4.8	SQL Injection on bWAPP login page	55