L. M. Kupershtein, Cand. Sc, Associate Professor; A. V. Prytula;
V. I. Malinovskyi, Cand. Sc. (Eng.), Associate Professor.

ANALYSIS OF THE TECHNOLOGIES OF WEB-APPLICATIONS PENETRATION TESTING

The paper analyzes the technology of penetration testing, used for detecting the vulnerabilities in web-applications. White box, grey box and black box methods are considered, each of these methods has its unique approaches and advantages in revealing the vulnerabilities . Standards OSSTMM, NIST, OWASP, PTES and ISAAF are considered in detailed, each of these standards provides its methodologies and recommendations for penetration test. For instance, OSSTMM, is international technology, which suggests the division into three main classes of safety and describes in details the procedures of preparation for testing. NIST is focused on planning, execution and post-operation, underlying the importance of collecting information at planning stage. OWASP stresses the need of the safety testing at each stage of the software development, PTES gives practical recommendations regarding each of seven stages of the penetration test. ISAAF suggests a three-phase approach, including planning, testing and formation of the report. Besides, the paper studies the frameworks Mitre ATT&CK, CIS Controls and Cyber Kill Chain, which help the organizations understand and counteract the cyberattacks. Mitre ATT&CK is known for its wide coverage of attacks and deep analysis of the tactics and methods of the attacks. CIS Controls is concentrated on specific security controls, which can be directly applied for systems protection, and Cyber Kill Chain provides structural approach to the analysis and prevention of cyber attacks. The paper also contains recommendations, regarding the implementation and usage of modern penetration testing techniques for the improvement of the information systems security. Results of the research can be useful for cybersecurity specialists and developers of web-applications, they will help understand better and implement the efficient methods of cybersecurity.

Key words: *web-application, penetration testing, penetration testing standards, frameworks of penetration testing.*

Introduction

Penetration testing is the process of cyberattack simulation on the information systems to detect vulnerabilities, which could be used by the intruders [1]. This is an important component of web-applications security, web-applications become more and more popular in all spheres of life and business. They are used to perform various functions, including processing of the confidential information, performing financial transactions for rendering on-line services. Penetration testing enables to identify and correct vulnerabilities, providing data security and reducing the risk of cyberattacks.

Modern web-applications can contain numerous components, which need security testing. These may be applications themselves, their web-interfaces (web-API), virtual containers, code repositories and other components. Each of these components may have their vulnerabilities, which are to be detected and corrected to provide complex security of the system.

Penetration testing of web-oriented information systems become more and more relevant as a result of wide usage of such systems and growing importance of web-technologies in all spheres of life. Nowadays there exist numerous risks, connected with the possible violation of confidentiality, integrity and accessibility of data [2]. Conclusions, made after performing penetration tests and further measures, aimed at security provision, help to avoid economic, financial and other kinds of damage. During penetration testing weak points of the system, caused by programming or technical errors, incorrect setting and other faults are revealed and verified. Besides, penetration testing enables to demonstrate the relevance of the revealed vulnerabilities and significance of the potential losses.

In modern society and business web-applications play an important role. Various technologies are used in the process of their development, they are constantly developing and improving.

However, application of web-applications is connected with risks, leading to violation of information security [3]. This can be explained by the fact that methods, used by the intruders, are constantly developing. The reason is vulnerability of the components of web-applications, internet since their development or may appear at different stages of the creation process and operation [4]. This results in non-sufficient level of web-application security against available threats.

Objective of the research is analysis of penetration testing technologies of the web-applications, generalization of the obtained data and development of the corresponding recommendations.

Main part

According to the terminology ND TPI 1.1-003-99, penetration testing – it is the test, the objective of which is the at temp to disconnect or overcome the security mechanisms [5]. As a rule, the script looks like this:

- penetration test planning;
- collection of the information , regarding target systems;
- search of vulnerabilities ;
- penetration in the system;
- report writing;
- cleaning the system from the consequences of the test.

Considering this, there exists several approaches to perform penetration tests [6]:

- white box – simulation of the intruders` actions, aimed at system breach, the intruders have access to the system and complete information about the system structure;
- grey box – simulation of the intruders` actions, aimed at system breach, the intruders have partial information about the system (ranges of IP-addresses, identifiers of the wireless networks, access to the system with low privileges level, etc.);
- black box – simulation of the intruders` actions, they have only the name of the company and practically zero information about the system.

To perform penetration testing of web-applications nowadays there exist several most frequency used techniques:

- Open Source Security Testing Methodology Manual (OSSTMM);
- National Institute of Standards and Technology (NIST);
- Open Web Application Security Project (OWASP);
- Penetration Test Execution Standard (PTES);
- Information System Security Assessment Framework (ISSAF).

OSSTMM is international methodology for the assessment of the information security, developed by ISECOM (Institute for Security and Open Methodologies) [7]. Objective of this methodology is to provide basic principles of the assessment of the security, including the division into three main classes of security: COMSEC (communication security channel), PHYSSEC (physical security channel) and SPECSES (spectrum security channel). These classes are divided into five interaction channels with the organization assets, which must be verified by the tester, including physical security, wireless and information-telecommunication networks, data transfer networks and human factor via using the methods of social engineering. Main advantages of this methodology are detail description of the procedures of preparation to testing, methods and approaches to security assessment and the detail explication of the key terms and notions in the sphere of information security. However, this methodology does not comprise the description of the tools, used for tests execution, although gives a set of rules and procedures, which help to understand the degree of web-applications protection against various types of attacks.

Methodology NIST Special Publication 800-115 distributes the process of the information security assessment into three basic phases: planning, execution and post-operation [8]. Planning phase, according to the authors of the methodology is a decisive factor for the successful assessment

of the security, it is used for the collection of information, needed for the execution of the assessment, for instance, about the assets to be assessed, threats which are of interest, regarding the assets and means of the security control, which will be used for threat mitigation and for the development of the approach to the assessment. Security assessment should be considered as any other project with the plan of project management for solving goals and tasks, volume, requirements, roles and obligations of the team, limitations, factors of success, assumptions, resources, time boundaries and results. Main objectives at the stage of execution are to reveal vulnerabilities and their verification, if necessary. This phase should concern the activity, connected with the planned method and technique of assessment. Although specific actions for this stage differ, depending on the type of assessment, after the completion of this stage the evaluators detect weak points of the system, network, and organization process. The last phase includes the analysis of the obtained data, revealing of the causes of vulnerabilities, development of recommendations, aimed at their elimination and report preparation. This document contains general review of the methods of verification of computer systems security, including web-applications with short description. For instance, check of the network for misuse, analysis of the journals, verification of the system configuration, verification of the files integrity, scanning of vulnerabilities, and wireless networks, etc. Moreover, the document contains references to program products, necessary for carrying out the tests and to other normative papers and methodologies. However, it should be noted that this document was elaborated in 2008 and nowadays it does not correspond to modern level of the information technologies and penetration methods in web-applications.

Authors of OWASP Testing Guide technique underline the need to implement testing of web-applications security at each of the stages of the software development [9]. According to OWASP Testing Guide technique testing is performed in the following order:

- collection of the information;
- testing of the configuration;
- testing of the mechanisms of the identification control;
- testing of the authentification process;
- testing of the authorization process;
- testing of the mechanisms of sessions control;
- testing of the processing of the input data from the user;
- errors processing;
- testing of the mechanisms, realizing cryptographic functions;
- testing of the business-logic of the application;
- testing of the client part.

At each of the stages the information to be collected during testing, how to process the obtained information, what components of the application should be checked and programming tools, by means of which testing could be performed at each stage with the examples of their usage, is described in details. At the end of each stage the links are given, they contain additional useful information regarding the characteristic features of testing. The best application is security testing of web-applications with the stress on the most spread vulnerabilities and threats.

Penetration testing standard PTES describes seven main stages of penetration testing [10]:

- preliminary interaction between sides;
- collection of information;
- modeling of threats;
- analysis of vulnerabilities;
- operation of vulnerabilities;
- post-operation period and assessment of possible losses as a result of the attacks;
- reports formation.

Separate part of PTES standard is the section of technical recommendations, where necessary software and additional information for practical realization of penetration is described. It is worth

using for practical orientation approach, which provides detailed technical recommendations regarding penetration testing.

Technique ISAAF is developed by the Open Information Systems Security Group (OSSIG). According to ISAAF technique penetration testing consists of three phases [11]:

– planning and preparation for testing (signing of the agreement between the customer and performer for penetration test realization, coordination of the testing technique and set of the programs for penetration testing realization);

– penetration test realization (collection of the information, drawing up a network diagram to be tested, identification of the vulnerabilities, measures, aimed at penetration in the system, obtaining the access to the resources, compromising remote users / sites concealment of traces);

– formation of the report about carried out penetration test (list of the programs and techniques, used during testing, data and time of testing, list of found vulnerabilities, recommendations for security improvement).

Technique ISAAF allows to carry out:

- assessment of the passwords security;
- assessment of network devices security;
- assessment of firewalls security;
- assessment of the network intrusion detection system security;
- assessment of web-applications security;
- assessment of operation systems security;
- audit of the program code;
- analysis of data bases security.

Generalized results of the analysis of the above-mentioned techniques of penetration testing by various criteria are presented in Table 1, where the following symbols are used:

- «+» – is in full;
- «±» – is in brief or mentioned;
- «–» – this material is missing or presented in such a way that it has no value.

Table 1

Results of the comparative analysis of penetration test techniques

Criterion	OSSTMM	NIST	OWASP	PTES	ISSAF
1	2	3	4	5	6
Recommendations regarding the discussions with the customer objectives and tasks of testing	+	±	+	+	+
Recommendations regarding preparation of the testing agreement	+	±	–	±	+
Legal aspects of testing	±	+	–	–	+
Recommendations regarding the collection of information about the object to be tested	+	+	+	+	+
Detail recommendations regarding the analysis and assessment of vulnerabilities	±	±	+	+	+
Recommendations regarding the stages of testing and their content	+	+	+	+	+
Separate recommendations regarding testing of telecommunication networks	+	+	±	+	+
Separate recommendations regarding testing of the wireless networks	+	+	–	+	+
Separate recommendations regarding web-applications testing	±	–	+	+	±
Separate recommendations regarding testing of physical infrastructure security	+	–	–	+	+
Separate recommendations regarding verification of the passwords security	–	+	±	+	+
Separate recommendations regarding verification of data bases security	–	–	±	–	+
Separate recommendations regarding verification of output code security	–	–	±	–	+
Recommendations regarding specific software, used for testing	–	–	±	+	+
Recommendations regarding formation of the testing report	+	–	+	+	+
Analysis and recommendations regarding the elimination of the determined vulnerabilities	–	+	–	–	+

As it is seen from Table 1 the most proven technique of penetration testing both in theoretical and practical plan is ISSAF technique. Techniques OSSTMM and NIST are of theoretical character. Technique PTES is practice-oriented and contains wide set of technical recommendations and specific vulnerabilities which are to be verified during penetration testing.

As each penetration testing technique contains numerous rules and recommendations to follow in the course of their realization, there appears the need to write a specialized software, which will help to automate the analysis and implementation of the above-mentioned techniques. In this content there emerges a need to consider and use the programming frameworks, which help to identify the potential threats and implement efficient counteractions. One of the most popular frameworks for this purpose is Mitre ATT&CK [12], it analyses tactics and methods of attacks, enabling the organizations to understand how the intruders can use faults in the system. Another widely used framework – CIS Controls [13], is focused on specific security controls, which can be used for risks minimization by all organizations. To understand their efficiency and usefulness for specific needs a detailed comparison should be carried out, taking into account various aspects, such as attacks coverage, difficulty of use, practicality of use and support of the community. Besides, it is important to consider Cyber Kill Chain [14], which provides the information for analysis and protection against cyber attacks, describing the stages of cyber attack, helps to understand how the

intruders can penetrate into the system. Generalized results of the analysis of the popular frameworks by different criteria are presented in Table 2.

Table 2

Results of the comparative analysis of the popular frameworks

Comparison criterion	Mitre ATT&CK	CIS Controls	Cyber Kill Chain
1	2	3	4
Coverage of attacks	Wide, describes various tactics and methods of attacks	Less wide, is focused on specific controls	Describes the stages of cyber attack
Complexity of usage	High, requires experience and understanding	Low, simple and understandable recommendations	Depends on the level of the user`s expertise
Practicality of use	High, provides specific actions for protection	High, direct connection with the system security	Provides the data for the analysis and cyber attacks security
Community support	Yes, active community of experts and updating	Yes, community of experts with practical recommendations	Data accessable for analysis but less activity of the community
Need for updating	Yes, updates taking into account new threats	Yes, but updating is less frequent	Yes, taking into account the development of cyber threats

By the results of the comparative analysis of Mitre ATT&CK and CIS Controls several important conclusions could be made. Both frameworks are useful tools to provide the security of web-applications and information systems in general. Mitre ATT&CK is characterized by wide coverage of the attacks and deep analysis of the tactics and methods of attacks, that makes it valuable resource for the investigation of threats and determination of the security strategy. On the other hand CIS Controls concentrate of specific security controls, which can be applied directly to provide system security.

Regarding practical application, CIS Controls are characterized by simplicity and direct connection with the security practice, this makes them efficient for practical application. At the same time, Mitre ATT&CK needs more expertise and research work for its usage.

Both frameworks have active experts communities which give support and updating. However, it is important to take into account that Mitre ATT&CK requires more frequent updating, taking into account changing cyber threats.

In general, the choice between these two frameworks depends on the specific needs and context of the organization, but they both may be useful tools to improve the security level and information system protection.

Regarding Cyber Kill Chain, it enables to provide information for the analysis and security against cyber attacks, describing stages of cyber attack and help to understand how the intruders can enter the system. This framework can supplement the analysis of Mitre ATT&CK and CIS Controls, providing more complete picture of the threats and means of their revealing and avoiding.

With the growth of the complexity and spreading of the digital platforms, problems of their reliability and security become very important. Study and implementation of machine learning for support and improvement of penetration testing becomes critically important task. For instance, in the study [15] for the solution of the problem of attacks tree analysis the authors used the method of machine learning. Q-learning was taken as a basis for attacks path searching. However, small space of action and selection space reduced the practical value of the given development. In authors opinion [15] useful improvement in the problems of attacks tree analysis for penetration testing became the technology of reinforcement deep leaning.

Technologies of artificial intelligence, such as reinforcement learning are more and more frequently used for penetration testing. There exist a number of frameworks which use these

technologies this helps enhance the efficiency and accuracy of testing. For instance, PentestGPT [16] is one of such frameworks, that integrated technologies of artificial intelligence for detection and analysis of the vulnerabilities in web-applications. In future, these approaches may become standard in the field of cyber security, providing more reliable protection of the information systems. Application of the machine learning methods enables to automate testing process, reduce human factor and improve the process of revealing new and unknown vulnerabilities [17].

Conclusions

Security of web-applications against the attacks of the intruders depends on the technologies and components, used for the construction of web-applications as well as on the possible vulnerabilities in these components. Analysis of penetration testing technologies was carried out. Wide choice of means enables to perform the search of vulnerabilities, however, the efficiency of their usage depends on the algorithm of actions, according to which the search is performed. According to the research, there exist international standards, regarding the processing of information about vulnerability, data bases of vulnerability and tools for their searching. Separate organizations deal with the development of penetration testing techniques. However, greater part of the techniques embraces wide range of cyber security problems, then there appears the need of additional time expenses for the analysis of the vulnerabilities according to available techniques and selection of those components, which are suitable for web-applications testing.

For achieving optimal results, independently on the methods of penetration test used, it is important that the tester adheres to certain methodology. The most widely used methodologies are OSSTMM, NIST, OWASP, PTES and ISAAF.

OSSTMM is an expert methodology for execution of tests and security metrics, this methodology was reviewed. Speaking about its practical application it is suitable for all-round security testing, that requires deep analysis of the organization security in the spheres of communication security, physical security and spectra security, it is perfect for the organizations, seeking to assess in details its security infrastructure, especially when communication and physical security are important.

NIST provides specific recommendations, regarding penetration testing for improvement of tests accuracy. Its best application is for creation of serial procedures of security testing which correspond to Federal Regulations of the USA and standards. NIST is suitable for the organizations, which must observe American government security standards or use widely recognized framework, that is integrated with the available requirements regarding compliance.

OWASP is developed by the community, that takes into account the latest threats and logic errors of the processes, except software vulnerabilities. The best application — testing of web-applications security with the stress on the most widely spread vulnerabilities and threats. Especially suitable for the developers teams during the life—cycle of the software development (SDLC) to integrate security testing in the development process, in particular, at early stages to reveal vulnerabilities in time.

PTES is directed on creation of modern standard for penetration testing and improvement of the business knowledge concerning the expectations from such testing. It is worth applying PTES for practically-oriented approach, which provides detailed technical recommendations concerning penetration testing carrying out. PTES is useful for security services providers and internal security teams which regularly carry out penetration tests and need structural methodology with clear instructions for each phase of testing.

ISAAF provides detailed technique of penetration testing and allows to evaluate the security of various components of the information systems, including web-applications. It is suitable for the detail operational testing of various components of information systems, including networking devices, firewalls and web-applications. ISAAF is ideally suitable for large organizations and IT-departments, which need reliable framework for carrying out security assessment and penetration tests which cover many aspects of their IT-infrastructure.

Program frameworks help to detect threats and secure systems. Having in view various needs and peculiarities of organizations, the analysis, carried out, demonstrates that Mitre ATT&CK and CIS Controls may be useful tools. Mitre ATT&CK is known for its wide coverage of the attacks and deep analysis, whereas CIS Controls is directed on the specific security controls. Additional comparative analysis shows that the choice between these frameworks depends on such factors as complexity of usage, practical application and frequency of updating. Both frameworks have active experts communities, they render assistance and updating, but Mitre ATT&CK needs larger expertise and more frequent updating. Regarding the analysis of Cyber Kill Chain, it supplement understanding of threats and helps reveal protection strategies against cyber attacks. This framework, in combination with other methodologies and frameworks, can provide more complete picture of cyber security for web-applications and other information systems.

Mitre ATT&CK and Cyber Kill Chain are useful for the organizations which are concentrated on understanding and smoothening of the threats as a result of stable and long attacks. These frameworks are more suitable for security teams, dealing with the analysis of the tactics, techniques of the threats and prepare security strategies, correspondingly, whereas CIS Controls provides the set of efficient controls and is more suitable for the organizations, requiring direct, understandable recommendations, which directly influence the systems security from general threats.

Thus, the choice of the methodology and testing methods, their further realization are key elements for providing high level of security of any information system.

In the process of penetration testing standard or framework selection, it is important to take into account specific needs of the specific organization, importance of the systems, taking part, qualification of the security team as well as any regulation requirements to be complied. Combining of the elements from different methodologies and frameworks may be efficient for the creation of the individual strategy of the security assessment, that involves all the necessary aspects.

REFERENCES

1. An overview of penetration testing [Electronic resource] / Aileen G. Bacudio, 1Xiaohong Yuan, 2Bei-Tseng Bill Chu [et al.] // International journal of network security & its applications (IJNSA). – 2011. – Vol. 3, № 6. – P. 19 – 38. – Access mode: https://doi.org/10.5121/ijnsa.2011.3602.

2. ND TPI 3.6-004-21. Normative document of the system of technical security of the information. – Valid from 2008-01-01. – Official edition. – Kyiv : [б. в.], 2021. – 23 p. (Ukr).

3. Web-applications security: Why is it important? [Electronic resource] //Company ITBIZ. – Access mode : https://itbiz.ua/statti-ta-obzori/zaxist-veb-dodatkiv-chomu-ce-vazhlivo/. (Ukr).

4. Analysis of the problems of web-applications security [Electronic resource] / A. Prytula, L. Kupershtain // Materials of All-Ukrainian scientific-practical Internet conference «Youth in science: research, problems, prospects» : International scientific conference, Vinnytsia, May 20, 2024. – Vinnytsia, 2024. – Access mode: https://conferences.vntu.edu.ua/index.php/mn/mn2024/paper/viewFile/19523/16190. (Ukr).

5. ND TPI 1.1-003-99. Normative document of the system of technical security of the information. – Valid from 1999-04-28. – Off edition. – Kyiv : [б. в.], 1999. – 22 p. (Ukr).

6. Types of penetration testing | black box vs white box vs grey box [Electronic resource] / Mark Nicholls // Redscan. – Acces mode : https://www.redscan.com/news/types-of-pen-testing-white-box-black-box-and-everything-in-between/.

7. OSSTMM 3 | the open source security testing methodology manual contemporary security testing and analysis [Electronic resource] / P. Herzog // ISECOM. – Access mode : https://www.isecom.org/OSSTMM.3.pdf.

8. Technical guide to information security testing and assessment. recommendations of the national institute of standards and technology [Electronic resource] / Karen Scarfone, Murugiah Souppaya, Amanda Cody [et al.] // NIST Technical Series Publications. – Access mode : https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf.

9. OWASP testing guide [Electronic resource] // OWASP. – Access mode : https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf.

10. The penetration testing execution standard [Electronic resource] // PTES. – Access mode : http://www.pentest-standard.org/index.php/Main_Page.

11. Information systems security assessment framework (ISSAF) draft 0,2.1 [Electronic resource] // Untrusted Network. – Access mode : https://untrustednetwork.net/files/issaf0.2.1.pdf.

12. Mitre att&ck [Electronic resource] // MITRE ATT&CK. – Access mode : https://attack.mitre.org/.

13. CIS controls [Electronic resource] // CIS. – Access mode : https://www.cisecurity.org/controls.

14. Cyber kill chain [Electronic resource] // Lockheed Martin. – Access mode : https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

15. Tvoroshenko I. Research of regression and modular testing of web applications [Electronic resource] / Irina Tvoroshenko, Heorhii Maksimenko // Science, theory and practice : Interational scientific conference, Tokyo, 12–15 October 2021. – London, 2021. – P. 406 – 411. – Access mode : https://openarchive.nure.ua/handle/document/17929.

16. Pentest Gpt: evaluating and harnessing large language models for automated penetration testing [Electronic resource] / Gelei Deng [et al.]. – Access mode : https://arxiv.org/pdf/2308.06782.

17. Prytula A. Application of artificial intelligence for penetration testing / A. Prytula, L. Kupershtain // Materials of LIII scientific-technical conference of the divisions of Vinnytsia National Technical University (STC VNTU-2024) : All-Ukrainian scientific conference, Vinnytsia, March 20–22, 2024. – Vinnytsia, 2024. – P. 345 – 349. (Ukr).

Editorial office received the paper 22.06.2024.
The paper was reviewed 26.06.2024.

Kupershtain Leonid – Cand. Sc. (Eng.), Associate Professor with the Department of Information Security.
Vinnytsia National Agrarian University.

Prytula Andriy – Post Graduate with the Department of Information Security, e-mail: andrik.pritula@gmail.com.

Malinovskyi Vadym – Cand. Sc. (Eng.), Associate Professor with the Department of Information Security, e-mail: vad.malinovsky@gmail.com.
Vinnytsia National Technical University.