UDC 004.056 DOI https://doi.org/10.35546/kntu2078-4481.2024.3.28

V. M. KOZEL
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Computer Systems and Networks
Kherson National Technical University
ORCID: 0000-0002-2627-2499

IE. A. DROZDOVA
Senior Lecturer at the Department of Computer Systems and Networks
Kherson National Technical University
ORCID: 0000-0003-0276-6387

O. I. IVANCHUK
Postgraduate Student at the Department of Computer Systems and Networks
Kherson National Technical University
ORCID: 0000-0002-2058-4707

O. O. PRYKHODKO
Senior Lecturer at the Department of Specialized Translation
and Foreign Languages
Kherson National Technical University
ORCID: 0000-0002-8732-3659

RESEARCH OF PENETRATION TESTING METHODS

The article examines penetration testing methods as a vital tool for identifying vulnerabilities in modern information systems and networks. The attention is drawn to improving security in the face of a growing number of cyberattacks and analyzing ethical hacking to prevent intruders' threats. An overview of the main approaches to penetration testing, such as Black Box, White Box, and Gray Box, is provided. Each method assesses system security at different levels, depending on the information available about the network under test.

The classification of penetration testing by the tested aspects, such as testing of applications, networks, physical systems, and social engineering methods, is considered. The authors emphasize that web applications require special attention, as they are the main target of many attacks.

The article also presents a systematic approach to penetration testing, which includes six main stages: planning, information gathering, vulnerability detection, penetration attempt, analysis and reporting, and cleanup. The authors emphasize the importance of each stage for effectively protecting information resources and ensuring their resilience to attacks.

The article provides an overview of popular penetration testing tools, such as Kali Linux, Metasploit, Nmap, and Wireshark, and analyzes their application at different stages of the pentest. The international security standards used to develop a penetration testing methodology are discussed.

The conclusions emphasize the importance of penetration testing to identify and eliminate vulnerabilities in information systems. The authors note that effective penetration testing requires the professional skills of ethical hackers who can use the same methods as attackers but aim to strengthen system security.

Key words: *security, security testing tools, penetration testing, cybersecurity.*

В. М. КОЗЕЛ
кандидат технічних наук, доцент,
доцент кафедри комп'ютерних систем та мереж
Херсонський національний технічний університет
ORCID: 0000-0002-2627-2499

Є. А. ДРОЗДОВА
старший викладач кафедри комп'ютерних систем та мереж
Херсонський національний технічний університет
ORCID: 0000-0003-0276-6387

О. І. ІВАНЧУК
аспірант кафедри комп'ютерних систем та мереж
Херсонський національний технічний університет
ORCID: 0000-0002-2058-4707

О. О. ПРИХОДЬКО
старший викладач кафедри галузевого перекладу та іноземних мов
Херсонський національний технічний університет
ORCID: 0000-0002-8732-3659

ДОСЛІДЖЕННЯ МЕТОДІВ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

У статті детально досліджуються методи тестування на проникнення як ключового інструменту для виявлення вразливостей у сучасних інформаційних системах та мережах. Автори звертають увагу на важливість покращення безпеки в умовах зростаючої кількості кібератак та аналізують етичний хакінг як метод запобігання загрозам з боку зловмисників. У статті подано огляд основних підходів до тестування на проникнення, таких як Black Box (тестування «чорного ящика»), White Box (тестування «білого ящика») та Gray Box (тестування «сірого ящика»). Кожен із цих методів використовується для оцінки безпеки системи на різних рівнях, залежно від кількості доступної інформації про мережу, що тестується.

Розглянуто також класифікацію тестування на проникнення за аспектами, що перевіряються: тестування додатків, мереж, фізичних систем та методів соціальної інженерії. Автори підкреслюють, що особливої уваги потребують веб-додатки, оскільки вони є основною ціллю багатьох атак.

У статті також наведено системний підхід до тестування на проникнення, який включає шість основних етапів: планування, збір інформації, виявлення вразливостей, спроба проникнення, аналіз і звітність, а також очищення. Автори наголошують на важливості кожного з цих етапів для ефективного захисту інформаційних ресурсів та забезпечення їх стійкості до атак.

Стаття містить огляд популярних інструментів для проведення тестування на проникнення, таких як Kali Linux, Metasploit, Nmap та Wireshark, і аналізує їх застосування на різних етапах пентесту. Також розглянуто міжнародні стандарти безпеки, які можуть бути використані як основа для розробки методології тестування на проникнення.

Висновки підкреслюють важливість використання тестування на проникнення для виявлення та усунення вразливостей у інформаційних системах. Автори зазначають, що ефективне тестування на проникнення потребує професійних навичок етичних хакерів, які здатні використовувати ті ж самі методи, що й зловмисники, проте з метою зміцнення безпеки систем.

Ключові слова: *безпека, засоби тестування безпеки, тестування на проникнення, кібербезпека.*

Problem statement

Today, Internet security requires significant improvement. Breaking into a system, or hacking, is an activity in which an attacker exploits the weakness in a system for personal benefit or pleasure. Those who engage in hacking are called hackers, crackers, or intruders. Their goals can range from entertainment and profit to disrupting the activities of others and gaining recognition. However, they all have a common goal: to find and exploit vulnerabilities in a system. As public and private organizations move more and more of their critical functions, such as e-commerce, marketing, and database access to the Internet, attackers have more opportunities to obtain confidential information through web applications. Therefore, protecting systems from hacker attacks is becoming critical.

Ethical hacking aims to identify and eliminate system weaknesses and vulnerabilities. It is a moral process aimed at improving network security.

Research publications

Although few studies have been devoted to security testing tools, researchers focus on testing and analyzing potential software vulnerabilities. The research [1] analyzed several technical articles published from 2005 to 2020 on web application security testing. Paper [2] identifies the problems faced by developers and users of web applications. Studies [3, 4] compare the results of automated and manual testing, emphasizing the importance of manual testing to identify specific vulnerabilities that can only be detected with the help of specialist experience. The analysis confirmed the importance of finding practical tools to minimize the risks and vulnerabilities of websites.

Research objective

This study aims to investigate possible vulnerabilities and threats currently the most common in the field of information security, as well as to develop methods of protection against them.

The relevance of this study is related to the need to ensure the security and resilience to vulnerabilities of modern computing systems and the Internet in various areas of organizations' activities. Whether it is a business organization, government agency, educational institution, or even a medical facility, it is essential to be confident in their information security.

The main material

Penetration testing is a systematic process of checking hardware and software that forms a complex data storage and transmission network. It allows you to assess network security by simulating actual attacks and exploits. This method makes it possible to investigate the weaknesses of any organization's security system in detail [5].

Penetration testing is a simulation of an attack on a system, network, equipment, or other object to assess its vulnerability to actual attacks. This process is performed by an ethical hacker who acts with the system owner's permission. Simply put, it is a procedural security audit of a network or application.

Ethical hackers and attackers are different and play different roles in the security sphere. Ethical hackers use the same tools and techniques as attackers but do not damage systems or steal information. Instead, they assess the level of security, notify owners of the identified vulnerabilities, and give recommendations on how to eliminate them. Thus, penetration testing can be classified into three categories depending on the hacker's "hat color."

"White" hackers are authorized professionals who work for a company with good intentions and high moral standards.

"Black" hackers, on the other hand, aim to harm computer systems and networks. They act solely in their interests and for profit. They are also called "crackers," "malicious hackers," or "intruders."

"Gray" hackers combine the features of both white and black hackers. They may act for ethical reasons.

Penetration testing can be classified into three types according to the approach used [8]:

1) Black Box.

2) White Box.

3) Gray Box.

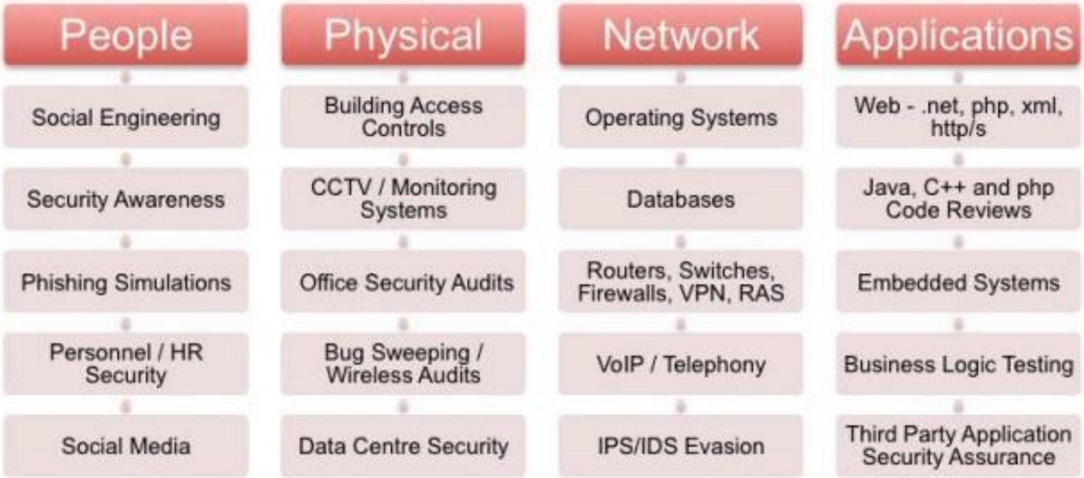
Black Box is the most practical attack performed by the pentester without any prior information about the target system. It is the most effective way to evaluate a security system because it simulates attacks. The pentester does not have access to any information about the network, including its structure, hardware types, or applications used. He must learn the target system from scratch to achieve the desired result. This type of testing aims to simulate an actual cyber attack fully.

White Box is a formalized testing approach where the pentester has basic information about the target infrastructure, including network structure, IP addresses, and other essential details. With basic knowledge of the target network, the pentester can work more focused on identifying and fixing vulnerabilities. This type of testing is usually done in close collaboration with the organization, and its goal is to help create a robust security system.

Gray Box is a combination of black box and white box approaches. The pentester has limited information about the target system, such as the server's IP address or the application's source code. This method is less popular but allows you to test the system partially inside and outside. The pentester can simulate an attacker's actions to check the system's reliability with available information.

Types of penetration testing.

Penetration testing types can be divided into four categories depending on which security aspects they assess, as shown in Figure 1 [9, 10, 11].



People	Physical	Network	Applications
Social Engineering	Building Access Controls	Operating Systems	Web - .net, php, xml, http/s
Security Awareness	CCTV / Monitoring Systems	Databases	Java, C++ and php Code Reviews
Phishing Simulations	Office Security Audits	Routers, Switches, Firewalls, VPN, RAS	Embedded Systems
Personnel / HR Security	Bug Sweeping / Wireless Audits	VoIP / Telephony	Business Logic Testing
Social Media	Data Centre Security	IPS/IDS Evasion	Third Party Application Security Assurance

Fig. 1. Classification of penetration testing

1) Application penetration testing focuses on identifying application vulnerabilities related to data monitoring and firewall security issues. Web applications, especially those based on a client-server architecture and transmitting information

over a network, can have critical vulnerabilities that are dangerous to the target system. Many modern web applications have vulnerabilities that have yet to be addressed. This testing covers all these aspects to ensure network security.

2) Network penetration testing is one of the key elements in conducting a pentest in an organization. Depending on the organization's size, the physical network may have security gaps that often go unnoticed during setup. To ensure a secure network, penetration testing is performed on devices such as routers, switches, modems, and hubs to identify possible vulnerabilities. It is a process in which a pentester ethically attacks an organization's network to find weaknesses and eliminate them using exploits.

3) Penetration testing of physical systems focuses on checking physical security. Vulnerabilities in this category relate to unauthorized physical access to target machines in the organization. Authentication and restricted access are thoroughly inspected during physical testing. This method is essential because it allows you to gather information about the target system directly through physical presence on the network. It aims to improve the effectiveness of physical systems' authentication, authorization, and access control.

4) Social engineering penetration testing aims to assess vulnerabilities related to the human factor. The basic information for such attacks can be obtained through search engines such as Google or social networks such as Facebook and X (Twitter), where a large amount of personal information is shared. In addition, public meetings and communication with people are significant weaknesses attackers can exploit. This penetration testing type helps assess the risk of unauthorized access to confidential information.

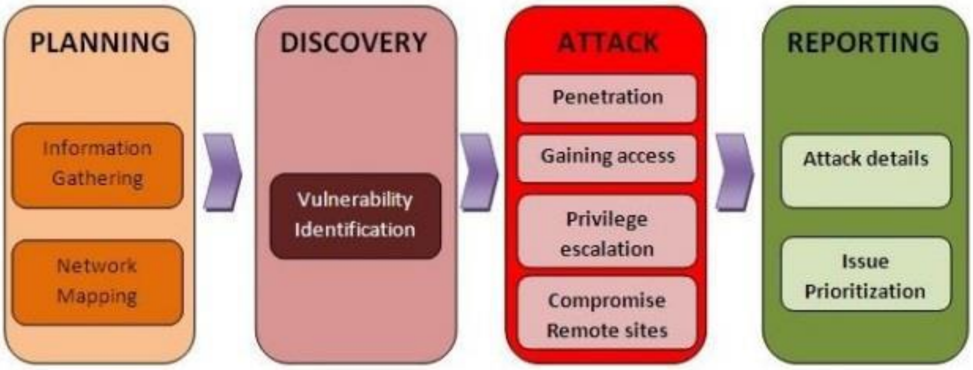


Fig. 2. The main steps of penetration testing

Use of a systematic approach.

The systematic approach to penetration testing consists of six stages (Figure 2) that ensure efficiency and a comprehensive system security assessment. These stages integrate a step-by-step methodology that every penetration tester must follow.

1) Planning and preparation.

This stage is the starting point for any penetration testing. It includes planning, preparation, and agreement between the organization's owners and testers on the objectives of the test, the methods used, and the expected results. The penetration tester familiarizes himself with the target system, determines a strategy to maximize the exploitation of vulnerabilities, and provides recommendations for their elimination. Privacy policies, timeframes, and schedules are also discussed.

2) Collection and analysis of information.

In this stage, known as "reconnaissance," information about the target system is gathered. The tester sets up a platform to collect information about the organization's network and applications using online sources such as websites, social networks, or special Linux-based tools. This stage is divided into two types:

– Passive information gathering: involves searching for information on the Internet without directly interacting with the target organization.

– Active information gathering: involves direct interaction with the system, such as receiving banners that may reveal more information.

Tools like Google Hacking or Shodan can help gather information about target systems.

3) Identification of vulnerabilities.

This stage, known as scanning, involves using various tools to find vulnerabilities based on the information collected. The pentester analyzes operating systems, applications, and network components to identify possible attack points. Scanning is divided into three categories:

– Network scan: aims to detect all hosts on the network, obtaining information about their IP addresses, operating systems, and servers.

– Port scanning: helps to identify open ports on specific hosts that can be used for an attack.

– Vulnerability scanning: Scans for possible operating system, applications, or network services vulnerabilities.

4) Penetration attempt.

At this stage, the pentester uses the collected data and prepared exploits to test the vulnerabilities found during the scan. It sends exploits accompanied by payloads, which allows you to exploit the vulnerability of the target system successfully. It will enable you to assess the organization's security level and show how well the system can withstand an attack.

5) Analysis and reporting.

This stage involves the preparation of detailed documentation of the work performed. The report should describe all the methods and procedures used for testing, including an assessment of the system's security level. It helps the organization understand where the vulnerabilities are and how to eliminate them. The report is also a reference for future audits and can be used at the information-gathering stage.

6) Cleaning.

After the test, the pentester removes all traces of its presence on the system to ensure the network is clean and secure. It includes undoing all settings and changes made during the test so that the organization can ensure no vulnerabilities or settings are left active. Properly executing this step is essential to ensure system security and prevent possible attacks.

This methodology allows for deep and comprehensive penetration testing, ensuring maximum efficiency in identifying and eliminating system vulnerabilities.

Many tools are on the market to help pentesters and system administrators test and build a secure network to protect against attacks. Most of these tools are free and open source, designed for ethical hacking. Depending on the penetration testing stage, scanners, test platforms, vulnerability detection tools, etc., can be used [12, 13, 15]. Some popular tools are listed in Table 1.

Table 1

Penetration testing tools

№	Instrument	Type
1	Brutus	Password selecting tool
2	Dradis	Scanning report program
3	Dnstuff	Network Utility
4	Hydra	Password guessing tool
5	Hping	Network Utility
6	John the Ripper	Password recovery tool
7	Kali Linux	Linux OS
8	Metasploitable	Virtual machine for penetration testing
9	Metasploit	Exploit testing tool
10	Maltego	Network visualizer
11	Nmap	Network scanner
12	Netcraft	Website scanner
13	Nessus	Vulnerability scanner
14	Netcat	Network Utility
15	Python	Programming language
16	Scapy	Network Utility
17	Ubuntu	Linux OS
18	Wireshark	Traffic analyzer

In addition to tools, there are various standards that pentesters rely on to assess system security. Some of the most commonly used standards are shown in Table 2.

Table 2

Standards for security assessment

Abbreviation	Name
WASC	Web Application Security Consortium
OSSTMM	Open Source Security Testing Methodology Manual
OWASP	Open Web Application Security Project
ISSAF	Information Systems Security Assessment Framework
NIST	National Institute of Standards and Technology

The most common vulnerabilities described in these standards:

– SQL injection;

– Hidden backdoors;
– Cross-Site Scripting;
– Cross-Site Request Forgery;
– Command Injection;
– Bypassing Authentication.

Many network security companies hire pentesters based on their ability to exploit these vulnerabilities.

Conclusions

Penetration testing is a versatile tool for finding weaknesses in a system because it uses the same methods as real attackers. Identifying these weaknesses is insufficient; the next step is appropriately hardening the system. An essential part of the process is to have the system tested by a professional and experienced ethical hacker.

The debate between ethical (white) and malicious (black) hackers is a long-running war with no end. White hackers help companies understand their security needs, while black hackers illegally intrude and harm organizations for personal gain.

A wealth of information and software is available for penetration testing, some of which are presented in this article. Penetration testing is a comprehensive component of information technology. Vulnerabilities can be in any system part: software, hardware, code, or system architecture. Therefore, when it comes to security, modern security methods, including ethical hacking, must be addressed.

Considering this, many professionals believe that familiarizing yourself with the basics of penetration testing is highly beneficial in terms of technological knowledge and general awareness.

Bibliography

1. Aydos, M., Aldan, Ç., Coşkun, E., Soydan, A. Security testing of web applications: A systematic mapping of the literature. *Journal of King Saud University – Computer and Information Sciences*. 2022. № 34(9), Pp. 6775-6792. DOI: 10.1016/j.jksuci.2021.09.018.

2. Mubshra, Q., Shahid, F., Mohd, H., Nizam, B., Md, N., Atif, A. A Rigorous Approach to Prioritizing Challenges of Web-Based Application Systems. *Malaysian Journal of Computer Science*. № 34. 2021 DOI: 10.22452/mjcs.vol34no2.1.

3. Dukes, L., Yuan, X., Akowuah, F. A case study on web application security testing with tools and manual testing. *Proceedings of IEEE Southeastcon-2013*. 2013. Pp. 1-6. DOI: 10.1109/SECON.2013.6567420.

4. Shahid, J., Hameed, M., Javed, I., Qureshi, K., Ali, M., Crespi, N. (). A Comparative Study of Web Application Security Parameters: Current Trends and Future Directions. *Applied Sciences*. 2022 № 12. P. 4077. DOI: 10.3390/app12084077.

5. Тест на проникнення – Wikipedia 2024. URL: https://uk.wikipedia.org/wiki/%D0%A2%D0%B5%D1%81%D1%82_%D0%BD%D0%B0_%D0%BF%D1%80%D0%BE%D0%BD%D0%B8%D0%BA%D0%BD%D0%B5%D0%BD%D0%BD%D1%8F

6. Ric Messier. Penetration Testing Basics: A Quick-Start Guide to Breaking into Systems : Apress. 2016. 115 p.

7. ДСТУ ISO/IEC TS 27008:2019 (ISO/IEC TS 27008:2019, IDT) Інформаційні технології. Методи захисту.

8. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах № 26 від 2005 р." URL: https://zakon.rada.gov.ua/laws/show/2594-15.

9. Top 5 Penetration Testing Methodologies and Standards URL: https://www.getastra.com/blog/security-audit/penetration-testing-methodology/#.

10. Oriyano Sean-Philip. Penetration Testing Essentials. Sybex, a Wiley brand. 2017. 363 p.

11. Baloch Rafay. Ethical hacking and penetration testing guide. Auerbach Publications. 2017. 523 p.

12. Wilhelm, Thomas. Professional penetration testing: Creating and learning in a hacking lab. Newnes. 2013. 525 p.

13. BSI – Study A Penetration Testing Model. Federal Office for Information Security, 111 p. URL:
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.html

14. Gilberto Najera-Gutierrez, Juned Ahmed Ansari. Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux. Packt Publishing Ltd. 2018.

15. Johansen, Gerard. Kali Linux 2–Assuring Security by Penetration Testing : Packt Publishing Ltd. 2016.

16. Cameron Buchanan, Vivek Ramachandran. Kali Linux Wireless Penetration Testing Beginner's Guide: Master wireless testing techniques to survey and attack wireless networks with Kali Linux, including the KRACK attack : Packt Publishing Ltd. 2017.

17. Matthew Denis, Carlos Zena, Thaier Hayajneh. Penetration testing: Concepts, attack methods, and defense strategies. *IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. IEEE. 2016.

18. Georgia Weidman Penetration Testing – A hand on introduction to hacking. San Francisco. 2014

19. Ge Chu, Alexei Lisitsa. Penetration Testing for Internet of Things and Its Automation. *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. IEEE, 2018.

References

1. Aydos, M., Aldan, Ç., Coşkun, E., Soydan, A. (2022). Security testing of web applications: A systematic mapping of the literature. Journal of King Saud University – Computer and Information Sciences, 34(9), 6775-6792, https://doi.org/10.1016/j.jksuci.2021.09.018.

2. Mubshra, Q., Shahid, F., Mohd, H., Nizam, B., Md, N., Atif, A. (2021). A Rigorous Approach to Prioritizing Challenges of Web-Based Application Systems. Malaysian Journal of Computer Science, 34, https://doi.org/10.22452/mjcs.vol34no2.1.

3. Dukes, L., Yuan, X., Akowuah, F. (2013). A case study on web application security testing with tools and manual testing. Proceedings of IEEE Southeastcon-2013, 1-6. https://doi.org/10.1109/SECON.2013.6567420.

4. Shahid, J., Hameed, M., Javed, I., Qureshi, K., Ali, M., Crespi, N. (2022). A Comparative Study of Web Application Security Parameters: Current Trends and Future Directions. Applied Sciences, 12, 4077, https://doi.org/10.3390/app12084077.

5. Wikipedia (2024). Retrieved from https://uk.wikipedia.org/wiki/%D0%A2%D0%B5%D1%81%D1%82_%D0%BD%D0%B0_%D0%BF%D1%80%D0%BE%D0%BD%D0%B8%D0%BA%D0%BD%D0%B5%D0%BD%D0%BD%D1%8F1

6. Ric Messier. Penetration Testing Basics: A Quick-Start Guide to Breaking into Systems / Apress, 2016. 115 p.

7. DSTU ISO/IEC TS 27008:2019 (ISO/IEC TS 27008:2019, IDT) Information technologies. Security methods. [in Ukrainian].

8. Zakon Ukrainy «Pro zakhust informatsii v informatsiino-telekomunikatsiinykh systemakh» [The Law of Ukraine «On the protection of information in information and telecommunication systems» from 2005, № 26]. (n.d.). zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/2594-15. [in Ukrainian].

9. Top 5 Penetration Testing Methodologies and Standards – Retrieved from https://www.getastra.com/blog/security-audit/penetration-testing-methodology/.

10. Oriyano Sean-Philip. Penetration Testing Essentials. Sybex, a Wiley brand, 2017, 363 p.

11. Baloch Rafay. (2017). Ethical hacking and penetration testing guide. Auerbach Publications, 523 p.

12. Wilhelm, Thomas. (2013). Professional penetration testing: Creating and learning in a hacking lab. Newnes, 525 p.

13. BSI – Study A Penetration Testing Model. Federal Office for Information Security, 111 p. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.html

14. Najera-Gutierrez, Gilberto, and Juned Ahmed Ansari. (2018). Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux. Packt Publishing Ltd.

15. Johansen, Gerard, et al. (2016). Kali Linux 2–Assuring Security by Penetration Testing. Packt Publishing Ltd.

16. Buchanan, Cameron, and Vivek Ramachandran. (2017). Kali Linux Wireless Penetration Testing Beginner's Guide: Master wireless testing techniques to survey and attack wireless networks with Kali Linux, including the KRACK attack. Packt Publishing Ltd.

17. Denis, Matthew, Carlos Zena, and Thaier Hayajneh. (2016). «Penetration testing: Concepts, attack methods, and defense strategies.» IEEE Long Island Systems, Applications and Technology Conference (LISAT).

18. Penetration Testing- A hand on introduction to hacking, Georgia Weidman, no starch press, San Francisco, 2014.

19. Chu, Ge, and Alexei Lisitsa. (2018). «Penetration Testing for Internet of Things and Its Automation.» IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS).