Analysis of Network Penetration Testing Methods in Ensuring Network Security

Kengesbaev Salauat Kuanishbayevich

Associate Professor of the Department of Cybersecurity, Institute of Information and Communication Technologies and Military Communications

ABSTRACT

This article analyzes penetration testing methods that are important in ensuring security in modern information and communication networks. The study examines the processes of identifying vulnerabilities in network infrastructure, in particular, the penetration testing methodology in WLAN networks. The article provides a detailed analysis of the stages of information gathering (reconnaissance), network scanning, exploitation, and post-exploitation. In addition, security protocols used in Wi-Fi networks, methods for detecting open ports, and mechanisms for identifying possible attacks are also covered. The results of the study serve to improve the security of network infrastructure, identify vulnerabilities, and develop effective recommendations for eliminating them

Keywords: Network penetration testing, network security, WLAN, vulnerability scanning, exploitation, Kali Linux, port scanning, Wi-Fi security, cybersecurity

Introduction

Modern digital systems are increasingly penetrating all areas of society today, and information technology–based systems have become the main backbone of economic, governmental, and industrial processes. Therefore, cybersecurity issues are becoming significantly more relevant. According to international statistical data, global losses caused by cybercrime are projected to exceed 10 trillion US dollars by 2025 [1]. This demonstrates that cybersecurity is not only a technical issue but also a strategic and economic priority. In addition, IBM Security reports indicate that the average cost of a data breach exceeds 4 million US dollars, which poses a serious financial risk for organizations [2].

Threats to network infrastructure are increasing year by year, and their complexity is also growing. According to statistics, thousands of cyberattacks are carried out globally every day, and ransomware attacks alone have increased by more than 60 percent in recent years. A large portion of corporate networks remains vulnerable due to misconfiguration, outdated software, or weak authentication systems. At the same time, phishing, DDoS attacks, zero-day exploits, and insider threats are among the most common types of cyber risks. This situation further increases the necessity of continuous network security assessment and evaluation [3].

Penetration testing (pentest) is an important method in the field of information security used to identify the vulnerability of systems and networks to real attacks. Through the pentesting process, existing vulnerabilities in a system are identified, their exploitability is assessed, and the security level is practically tested. Research shows that organizations that regularly conduct pentesting experience significantly reduced losses from cyberattacks. Therefore, pentesting is considered an integral part of modern cybersecurity strategies.

The main purpose of this study is to analyze penetration testing methods in network

security assessment and to study their effectiveness. During the research, the theoretical foundations of pentesting, its stages, tools used, and methods for identifying and evaluating network vulnerabilities are examined. In addition, approaches to risk identification and prioritization are also analyzed. The scientific novelty of the study is related to the systematic analysis of the pentesting process and the integration of modern methods in network security assessment.

This article consists of an introduction, theoretical foundations, analysis of network penetration testing, evaluation of results, advantages and limitations of pentesting, and a conclusion. Each section is aimed at studying network security through a comprehensive approach.

Main part

Penetration testing (pentesting) is one of the modern and practical methods of information security assessment. It is considered a process aimed at identifying vulnerabilities in information systems and network infrastructures under conditions close to real attack scenarios. This approach enables organizations to evaluate their cybersecurity level through practical testing and plays an important role in identifying and reducing risks in advance.

Pentesting is closely related to the concept of ethical hacking, where ethical hacking is a broader concept that includes all security testing and attack simulations carried out on a legal basis to improve system security. Pentesting, in turn, is a specific and methodologically focused part of this process. Thus, ethical hacking is the general approach, while pentesting is its practical testing component.

Table 1. Main functions of pentesting

	**Protect your data** Organizations face various threats; therefore, protecting data is essential. Network penetration testing identifies vulnerabilities and improves system security. Vulnerability scanning provides only a general analysis and is usually used as a complementary tool to pentesting.
	**Understanding security controls** By conducting penetration testing, you can better understand which security controls are functioning effectively and which need to be strengthened. In addition, network pentesting allows an organization to analyze its overall security posture.
	**Preventing data leakage** Analyzing vulnerabilities in an organization's network in advance significantly reduces the likelihood of data leakage. Pentesting improves the overall security level of the system through general security assessment and cybersecurity audits.

Several researchers have noted that penetration testing has three main approaches [4]. The most common approaches are black-box, white-box, and gray-box testing.

Black-box

In black-box testing, testers simulate an attack without having any information about the system infrastructure. In this approach, testers identify all vulnerabilities using their own methods and tools [4]. Real attack techniques

such as social engineering and remote access are used in this process. For example, testers start working with only the IP address of the network and do not have any additional information. After that, they simulate various attack techniques to identify all known and unknown vulnerabilities present in the network.

Table 2. The different penetration testing approaches.

Criteria	Black Box	White Box	Gray Box
Knowledge	Zero knowledge	Full knowledge	Some knowledge
Access level	Zero access testing as attacker.	Complete open access testing as developer.	Testing as user with access to part of the data.
Pros	It is more realistic.	More thorough, less likely to miss a vulnerability, and is faster. Intended for high-risk or sensitive data processing systems.	It is more efficient than a black box and saves both time and money.
Cons	It takes more time and increases the likelihood that a vulnerability will be missed.	More data must be delivered to the tester, which increases costs.	There are no significant disadvantages to this form of testing.

White Box

In white-box testing, testers simulate an attack with full knowledge of the system infrastructure, operating system details, IP addresses, and even certain passwords [4]. This approach allows testers to carry out attacks using their existing knowledge of the organization's system. For example, information such as an internal employee's personal data or system access rights can be used. This approach helps maintain the integrity of the organization's network infrastructure and reduces risks that may arise from internal attackers such as disgruntled employees (Table 2).

Gray Box

The gray-box approach is used as a combination of black-box and white-box methods. This approach allows both internal and external security aspects of the system to be analyzed together. In this case, testers have a limited amount of information about the network infrastructure. Using gray-box testing, internal and external security vulnerabilities in the system can be identified, and the likelihood of their exploitation by attackers is reduced [5].

The penetration testing process consists of systematic and sequential stages, and each stage contributes to a comprehensive security assessment (Figure 1).

1. Reconnaissance (Information Gathering). In this stage, initial information about the system or network is collected. For example, domain names, IP addresses, servers, and the technologies used are identified.
2. Scanning & Enumeration. In this stage, the network is scanned, and open ports, services, and potential vulnerabilities in the system are identified.
3. Exploitation. In this stage, the process of gaining access to or taking control of the system by using identified vulnerabilities is carried out.
4. Post-Exploitation. In this stage, additional capabilities within the system are explored, the level of access to data is examined, and the impact on the system is evaluated.
5. Reporting. In the final stage, a detailed report is prepared, including all identified vulnerabilities, attack methods, and recommendations for mitigation [6].

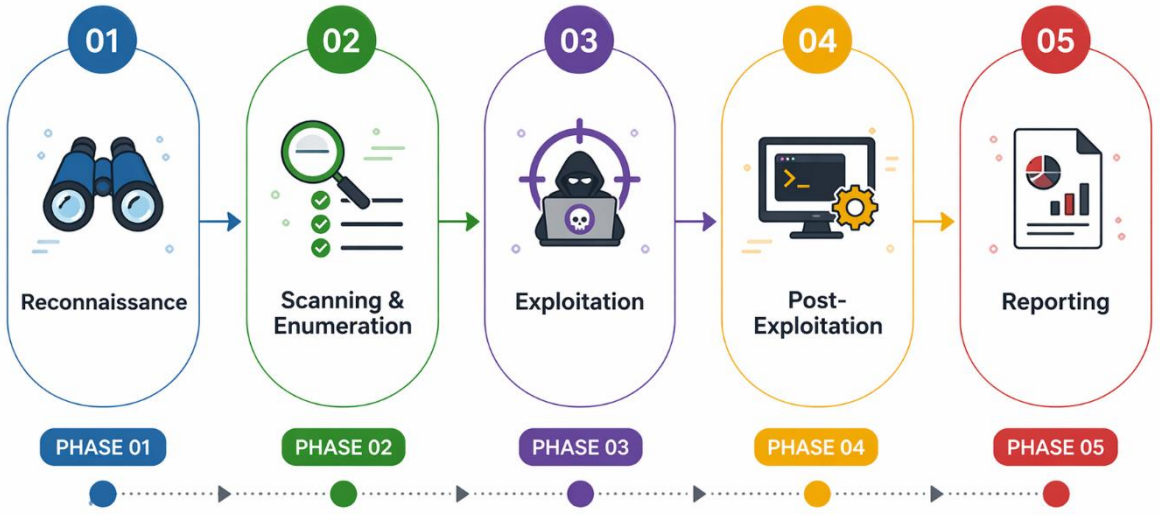

Fig. 1. Main stages of the penetration testing process

Penetration testing is one of the important methods used to identify security vulnerabilities in information systems and infrastructures. In practice, penetration testing is divided into several main types [7].

Network penetration testing is aimed at identifying vulnerabilities in network infrastructure, and it analyzes the security configuration of servers, routers, and other network devices.

Web application penetration testing examines the security of web applications and is used to identify vulnerabilities in authentication, data input forms, and interaction with the server.

Wireless penetration testing evaluates the security level of wireless networks and is focused on identifying unauthorized access or encryption weaknesses in Wi-Fi networks.

Mobile platform security testing analyzes the security mechanisms of mobile applications and mobile operating systems.

Cloud infrastructure penetration testing is used to assess the security level of services and virtual infrastructure in cloud computing environments.

Network penetration testing

Network penetration testing is one of the important cybersecurity methods aimed at assessing the security level of network infrastructure and identifying existing vulnerabilities within it. Through this process, the effectiveness of protection mechanisms in an organization's networks is evaluated, and potential attack points are identified [8].

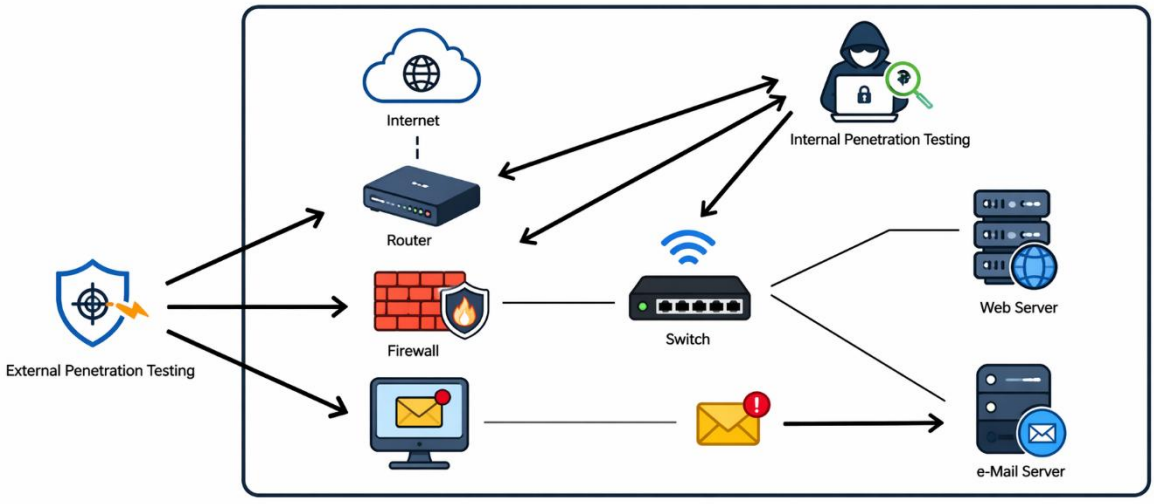

Fig. 2. Network penetration testing process

Network penetration testing is generally divided into internal and external tests. Internal tests simulate attacks that could be carried out by a user or employee with access to the organization's internal network. External tests, on the other hand, examine attempts to gain unauthorized access to the organization's network via the internet [9].

These tests are particularly important in corporate networks and are widely used to ensure security in banking systems, telecommunication infrastructures, and large-scale information systems.

Wireless Local Area Network Penetration Testing

In the current era of digital transformation, wired and wireless networks are widely used for data exchange and communication between devices. Network technologies play an important role in public and private organizations in fields such as education, healthcare, trade, and manufacturing. They are also widely used in everyday life, for example in the use of social networks.

However, along with the widespread use of networks, security issues are also increasing. Cyberattacks carried out by attackers can cause significant damage to network infrastructure, interrupt organizational operations, and lead to major financial losses.

Wireless networks (WLAN) are among the most widely used networks today. They are widely adopted due to their convenience, but this very convenience also makes them an easy target for attackers. Authentication and encryption protocols have been developed to protect wireless networks. The most common encryption technologies are WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) [10].

Nevertheless, vulnerabilities also exist in the modern Wi-Fi security protocol WPA2. According to research, attackers can decrypt data considered encrypted through a KRACK (Key Reinstallation Attack). Through this, sensitive information such as credit card data, passwords, messages, and emails can be stolen [11].

To reduce such threats, penetration testing plays an important role in network infrastructure. Penetration testing helps improve security by identifying and eliminating vulnerabilities in the network. Therefore, pentesters should think like attackers and test the system accordingly.

In some studies, various tools have been used to examine Wi-Fi security protocols. For example, using tools such as Wi-Fi adapters, Raspberry Pi, Kali Linux, Aircrack-ng, Airodump-ng, and Airplay-ng, methods for cracking WEP keys, analyzing WPA2 handshake processes, and performing KRACK attacks have been studied.

In addition, a system called CheckShake was developed to detect anomalies in the handshake process of Wi-Fi protocols. It was found to operate with 93.39% accuracy and a 5.08% false alarm rate in detecting KRACK attacks [12].

Researchers have proposed various architectural environments for penetration testing of wireless local area networks (Figure 3).

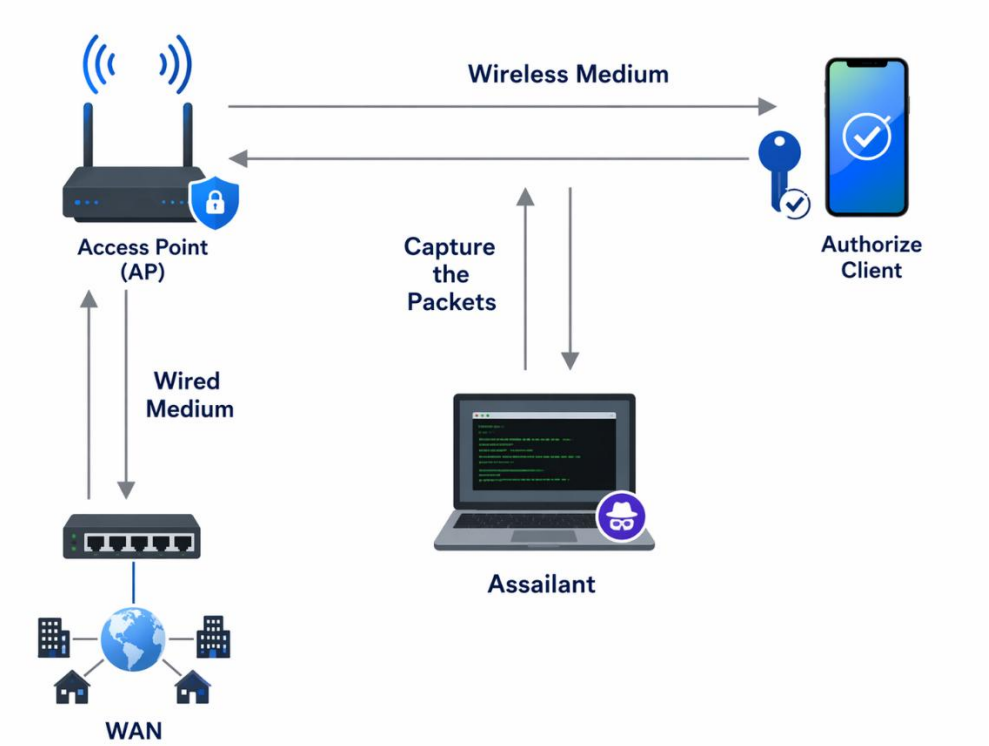

Fig. 3. WLAN penetration testing architecture

Before starting WLAN penetration testing, it is important to properly configure the environment. The environment used for penetration testing mainly consists of hardware and software components.

Hardware components include routers, attacker devices (such as laptops), WLAN network cards, and authorized client devices (such as mobile devices).

In addition, software tools such as “airodump-ng” and “aircrack-ng” can be used for eavesdropping on WLAN traffic, packet sniffing, and capturing data.

Also, utilities such as “mac-changer” and “aireplay-ng” can be used to spoof MAC addresses of Access Points (AP) and authorized client devices.

The laptop used for performing the attack has the Kali Linux operating system installed, which is a system specifically designed for penetration testing. All necessary software tools are downloaded and installed on this system.

The client device (mobile device) has all the required information about the target network. This device has a certain operating system installed and connects to the internet via the Access Point (AP) [13].

There are various standard methodologies for performing network penetration testing. During WLAN penetration testing, researchers have described the steps of security assessment in a wireless network environment as follows (Figure 4).

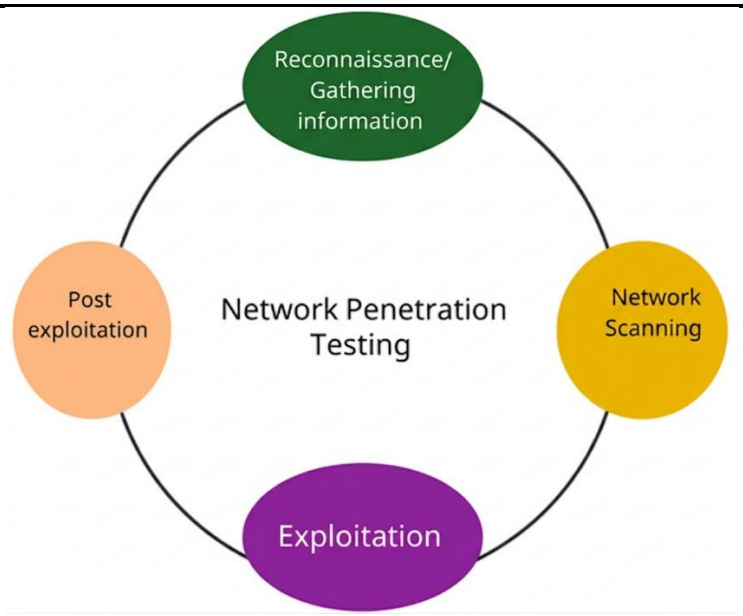

Fig. 4. Network penetration testing

1. Reconnaissance (Information Gathering)
In this stage, testers collect information about the network and its connections. Information about the target object is searched, and initial traces (footprints) of the network are created without being detected. In addition, existing protection mechanisms in the system are identified, and information about DHCP, DNS, and subnet IP addresses is obtained [14].
2. Network Scanning
In this stage, security vulnerabilities in remote networks or local hosts are identified. IP addresses of active hosts are collected, and Layer 2 devices are identified. Then, open ports are scanned using tools such as Nmap and Nessus. As a result, a table containing IP addresses, MAC addresses, and open ports is created.
3. Exploitation
In this stage, various attacks are carried out by using identified vulnerabilities. Methods such as password cracking to access WLAN networks, DoS attacks, and identifying router passwords are used.
4.Post-Exploitation
In this stage, recommendations for network protection are provided. Testers identify and document sensitive data in the network, configuration settings, communication channels, and connections with other devices.
During the scanning phase of the penetration testing process, many identified ports may contain known vulnerabilities, and if they are open, they can be used to carry out attacks.

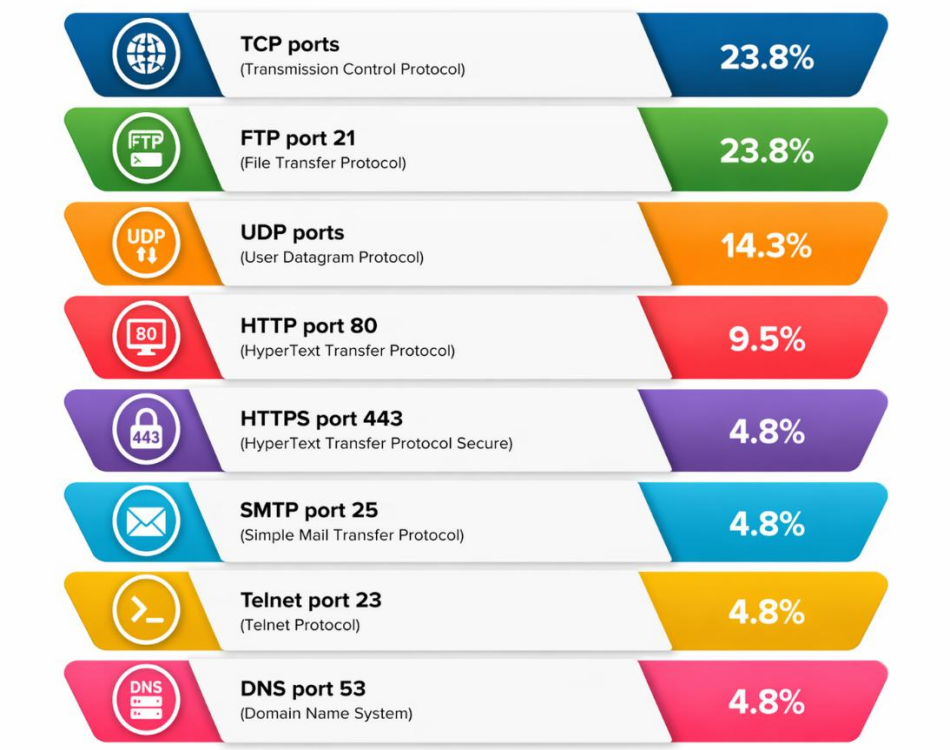

Fig. 5. Techniques for protecting open ports

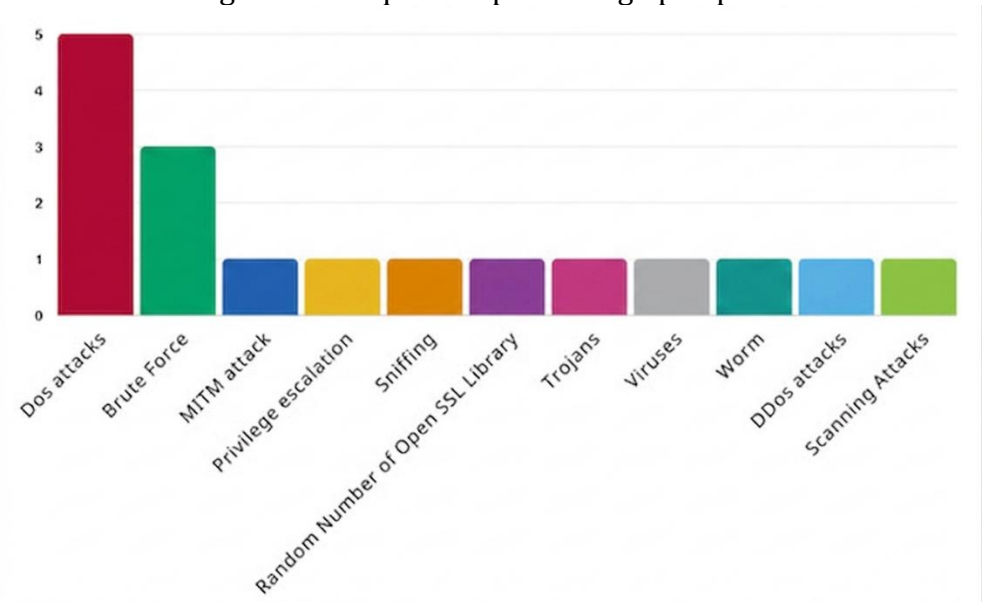

Fig. 6. Types of attacks targeting the use of open ports

It is recommended to conduct additional research on improving network penetration testing using machine learning with deep reinforcement learning to enhance testing based on the specific topology of WLAN networks.

Conclusion

This study analyzed the importance of penetration testing methods in evaluating network security. According to the analysis results, penetration testing is an important tool for identifying and eliminating vulnerabilities in network infrastructure. Through penetration testing processes carried out in WLAN networks, open ports, misconfigurations, and weaknesses in authentication mechanisms can be identified. In addition, modern testing tools provide the possibility of a comprehensive assessment of network security. The results of the study show that the regular application of penetration testing methods ensures the stable

operation of network systems and increases the level of protection against cyberattacks.

References

1. Cybersecurity Ventures. (2024). *Official Cybercrime Report 2024–2025*. https://cybersecurityventures.com
2. IBM Security. (2024). *Cost of a Data Breach Report 2024*. https://www.ibm.com/security/data-breach
3. ENISA. (2024). *Threat Landscape Report 2024*. https://www.enisa.europa.eu
4. Jayasuryapal, G.; Meher Pranay, P.; Kaur, H. A Survey on Network Penetration Testing. In Proceedings of the IEEE 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), London, UK, 28–30 April 2021.
5. Packetlabs. Black-Box vs. Grey-Box vs. White-Box Penetration Testing. 19 April 2022. Available online: https://www.packetlabs.net/posts/types-of-penetration-testing (accessed on 6 May 2023).
6. Scarfone K., Souppaya M., Cody A., Orebaugh A. *Technical Guide to Information Security Testing and Assessment*. NIST Special Publication 800-115, National Institute of Standards and Technology, 2008.
7. Georgia Weidman. *Penetration Testing: A Hands-On Introduction to Hacking*. No Starch Press, 2014.
8. Ali Dehghantanha, Kim-Kwang Raymond Choo. A survey of penetration testing techniques and tools. *Computers & Security*, 2019.
9. Sven Dietrich, Neil Long. Penetration testing: A framework for network security evaluation. *IEEE Security & Privacy*, 2018.
10. Singh; Rajawat, G.; Sharma, J. Wireless Cyberspace. *J. Anal. Comput. (JAC).* **2022**, *16*, 1–4.
11. Jain, S.; Pruthi, S.; Yadav, V. Ethical Hacking of IEEE 802.11 Encryption Protocols. *J. Xi'an Shiyou Univ. Nat. Sci. Ed.* **2009**, *18*, 108–112.
12. Agrawal, A.; Chatterjee, U.; Maiti, R.R. CheckShake: Passively detecting anomaly in Wi-Fi security handshake using gradient boosting based ensemble learning. *IEEE Trans. Dependable Secur. Comput.* **2023**, 1–13.
13. Alsahlany, A.M.; Alfatlawy, Z.H.; Almusawy, A.R. Experimental Evaluation of Different Penetration Security Levels in Wireless Local Area Network. *J. Commun.* **2018**, *13*, 723–729.
14. Syed, S.; Khuhawar, F.; Arain, K.; Kaimkhani, T.; Syed, Z.; Sheikh, H.; Khan, S. *Case Study: Intranet Penetration Testing of MUET*; Mehran University of Engineering and Technology: Jamshoro, Pakistan, 2020; pp. 17–19.