INTERNATIONAL JOURNAL OF DIGITAL RESEARCH
Research Article

International Journal of Digital Research
www.ijdr.net
E-ISSN: 3033-179X
Volume 2; Issue 3; 2026, P.p. 59-71

The Role of Penetration Testing in Identifying Cybersecurity Vulnerabilities

Iqra Bibi

Centre of Excellence in Education, Innovation & Research, Pakistan
ORCID: 0009-0002-3865-8951
Email: iqrabibiiqrabibi75@gmail.com

https://doi.org/10.63711/ijdr.net20260305

ABSTRACT

The rapid development of digital technologies has increased both the efficiency of information systems and the complexity of cybersecurity threats. As organizations increasingly depend on digital infrastructures, identifying vulnerabilities before they can be exploited has become an essential part of cybersecurity management. This study examines the role of penetration testing in identifying security weaknesses and evaluates several commonly used penetration-testing approaches, frameworks, and techniques. The paper combines a review of established approaches, including OSSTMM, OWASP, PTES, and NIST, with a practical penetration-testing demonstration using Nmap. The experimental scan identified several accessible network services, including Telnet (port 23), DNS (port 53), and HTTP (port 80), while FTP (port 21) and SSH (port 22) were found to be filtered. The scan also provided information about the target device and its operating environment.

These findings demonstrate how penetration testing can reveal potentially exposed services and provide useful information for assessing security risks and improving system protection. The study concludes that regular, authorized penetration testing can support vulnerability identification, risk assessment, and the implementation of appropriate remediation measures. However, the practical demonstration is limited to a single target environment and should therefore be interpreted as an illustrative case rather than a comprehensive security assessment.

Keywords: *Cybersecurity, Penetration Testing, Vulnerability Assessment, Ethical Hacking, Nmap, Network Security, Reconnaissance.*

INTRODUCTION

In today's world, digital technologies are advancing rapidly, providing numerous benefits to individuals, businesses, and organizations. At the same time, the increasing dependence on digital systems has created new cybersecurity challenges. Organizations may face significant risks when sensitive information is inadequately protected or when security weaknesses remain unidentified. Common cybersecurity threats include phishing, malware, social engineering, unauthorized access, and the exploitation of vulnerable systems.

Penetration testing plays an important role in addressing these challenges. It is a controlled security assessment in which authorized testing techniques are used to identify and evaluate vulnerabilities before they can be exploited by malicious actors. Penetration testing can help organizations assess the security, stability, and resilience of their systems, networks, and applications and determine whether existing security controls provide adequate protection for sensitive information.

Vulnerability assessment is closely related to penetration testing and focuses on identifying weaknesses and potential security gaps within a system. Security tools and structured methodologies can be used to detect vulnerabilities and evaluate their potential impact. Penetration testing extends this process by examining how identified weaknesses may affect the security of a system under controlled conditions. Together, vulnerability assessment and penetration testing can support organizations in strengthening their security frameworks and reducing exposure to cyber threats.

Real-world penetration-testing case studies demonstrate the practical value of this approach. For example, security assessments may identify weak passwords, exposed services, open ports, insufficient access controls, or system misconfigurations that could potentially provide unauthorized access to organizational resources. Identifying such weaknesses allows organizations to implement appropriate remediation measures before they are exploited.

Figure 1 illustrates the key elements and interactions involved in a penetration-testing assessment, including the target, testing scope, objectives, models, and security analysis.

Figure 1. Key Elements and Interactions in Penetration Testing

The aim of this study is to examine the role of penetration testing in identifying cybersecurity vulnerabilities by combining an overview of established penetration-testing approaches and frameworks with a practical Nmap-based demonstration. The study focuses on the identification of accessible and filtered network services and the interpretation of these findings from a cybersecurity perspective. In this way, the paper illustrates how practical penetration testing can contribute to vulnerability identification, risk assessment, and the improvement of system security.

LITERATURE REVIEW

The early development of penetration testing can be associated with the work of James P. Anderson, who contributed to the development of systematic approaches to computer security and the identification of security vulnerabilities. His work examined methods through which computer systems could be evaluated for potential security weaknesses and unauthorized access. These early contributions subsequently influenced the development of security monitoring, intrusion detection, and penetration-testing practices (Anderson, 1972, 1980).

Studies conducted between 2019 and 2021 increasingly presented penetration testing as a modern approach to addressing cybersecurity problems. During this period, organizations and research laboratories adopted various security measures aimed at identifying vulnerabilities at an early stage and improving network security. Security assessment tools, including Nmap and other Linux-based security tools, have been used to evaluate system defences and identify potential security gaps. These approaches allow organizations to detect vulnerabilities and strengthen their overall cybersecurity posture (Kumar & Tlhagadikgora, 2019; Alhamed & Rahman, 2023).

The widespread adoption of both wired and wireless network infrastructures has significantly transformed modern organizational operations. Wireless local area networks (WLANs), in particular, have become widely used because of their flexibility, accessibility, and relatively low implementation costs. Despite these advantages, WLANs remain vulnerable to various security threats, including unauthorized access, eavesdropping, packet sniffing, and denial-of-service (DoS) attacks. The characteristics of wireless communication may expose networks to a broader attack surface and therefore make the identification and mitigation of WLAN vulnerabilities an important area of cybersecurity research.

A penetration-testing case study conducted by Dionach highlights the importance of proactive security assessments in identifying system security weaknesses. In this case study, both external and internal penetration-testing approaches were applied to evaluate system security. The assessment revealed several weaknesses, including weak user passwords, insufficient access-control mechanisms, and misconfigured system components. These vulnerabilities represented potential entry points through which unauthorized users could gain access to sensitive organizational systems. The findings demonstrate that even relatively minor security weaknesses can increase exposure to cyberattacks if they are not properly addressed. Following the assessment, remediation strategies were recommended to improve system protection and reduce identified risks (Dionach, 2022).

Another critical aspect of information management is information security, which focuses on protecting data against unauthorized access, misuse, modification, disclosure, and other potential threats. Since organizational information frequently contains sensitive or critical data, ensuring its confidentiality, integrity, and availability is essential. Organizations therefore implement different security mechanisms and technologies to protect information systems against emerging threats and vulnerabilities. Penetration testing and vulnerability assessment can contribute to this process by

identifying security weaknesses before they are exploited (Sadlek et al., 2022; Alhamed & Rahman, 2023).

Figure 2 illustrates a typical wireless-network security scenario in which network traffic may be monitored or captured through the wireless communication medium.

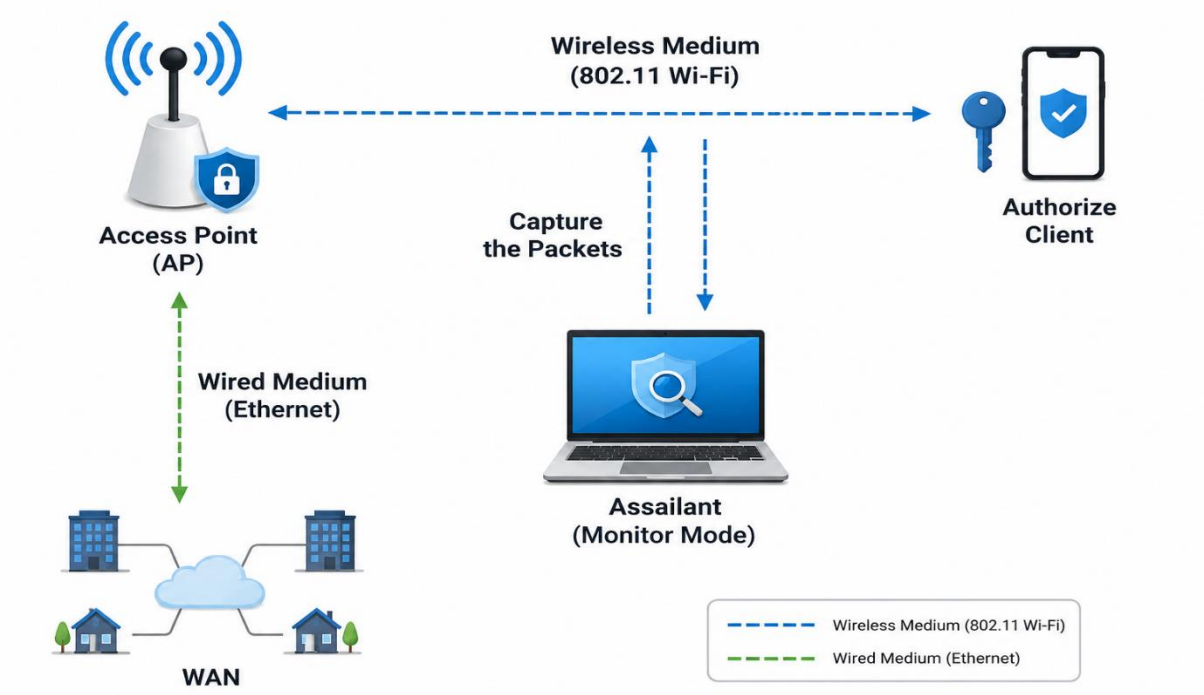

Figure 2. Wireless Network Security and Packet-Capture Scenario

Penetration-testing techniques can also be applied to publicly accessible applications and information resources, including search engines. An important contribution in this area is Google Hacking for Penetration Testers by Johnny Long, which presents advanced search-engine techniques commonly referred to as “Google hacking.” These techniques can be used to identify unintentionally exposed sensitive information and potential security weaknesses in publicly accessible web resources (Long, 2005).

Rather than involving the direct transfer of data within a network, Google hacking and related reconnaissance methodologies focus on discovering and analyzing information that has been unintentionally made publicly accessible, such as email addresses, misconfigured files, system information, and improperly protected credentials. By using advanced search queries and reconnaissance techniques, security professionals can identify information exposure and potential security weaknesses before they are exploited by malicious actors (Long, 2005).

METHODOLOGY

Ethical hacking and penetration testing are closely related cybersecurity practices aimed at identifying and mitigating security weaknesses. Ethical hacking represents a broad cybersecurity discipline that focuses on evaluating different security aspects of information systems, whereas penetration testing is a more structured and systematic approach used to identify vulnerabilities and

potential attack vectors in computer systems, networks, and applications. With the increasing frequency and sophistication of cyberattacks, organizations face significant financial and operational risks. Consequently, strengthening cybersecurity measures has become essential for protecting sensitive information and critical assets (Alhamed & Rahman, 2023; Parveen & Shaik, 2023).

In this research, different case-study approaches to penetration testing are also considered. Depending on the type of application, network, or information system being assessed, researchers and security professionals may design and apply different models for conducting penetration tests. One or more case studies may be applied depending on the specific objectives of the security assessment and the vulnerabilities expected to be present.

In some situations, a focused case-study model involving a specific testing environment and a single tester may provide a more efficient approach by reducing the time required for the assessment and allowing greater attention to a defined security target. This study investigates suitable approaches that can help enhance organizational security through an analysis of established security assessment frameworks, including OSSTMM, OWASP, PTES, ISSAF, and NIST (Al-Ahmad et al., 2023; Alhamed & Rahman, 2023). Furthermore, the research examines penetration-testing methods and considers their effectiveness, advantages, and limitations in different security-assessment scenarios. The study also explores structured stages of penetration testing, including planning and scoping, active scanning, open-port assessment, reporting, and remediation (Alhamed & Rahman, 2023; Parveen & Shaik, 2023). In addition, various penetration-testing tools and techniques are considered in order to determine their effectiveness in identifying security weaknesses and enhancing the overall security framework of modern information systems (Kumar & Tlhagadikgora, 2019; Sadlek et al., 2022).

Classification of Penetration Testing

Penetration testing can be classified into different approaches depending on the location of the tester, the amount of information provided before the assessment, and the level of awareness within the target organization (Alhamed & Rahman, 2023; Al-Ahmad et al., 2023).

1) Internal Penetration Testing

In internal penetration testing, the security assessment is conducted from within an organization's network environment. An authorized penetration tester is provided with the necessary access and guidelines to evaluate internal security controls and identify potential vulnerabilities, such as exposed services, open ports, weak passwords, or system misconfigurations.

Planning: First, the scope, objectives, and target of the penetration test are defined.

Scanning: In the second phase, the tester examines the target environment to identify potential vulnerabilities, such as open ports, exposed services, weak passwords, or insecure configurations.

Exploitation: In the third phase, identified vulnerabilities may be tested under controlled and authorized conditions in order to determine their potential security impact.

Reporting: In the final phase, a report is prepared describing the findings and identified weaknesses. The results can then be used for further security analysis and the implementation of appropriate remediation measures.

2) External Penetration Testing

External penetration testing is conducted from outside the organization's internal network and focuses on externally accessible systems and services. In this approach, the penetration tester may

have limited prior information about the target environment. Publicly available information, IP addresses, websites, exposed services, and open ports can be examined in order to identify potential security weaknesses.

3) Blind Penetration Testing

In blind penetration testing, the tester is provided with only limited information about the target organization, such as its name. The tester then independently collects the information necessary to identify potential entry points and vulnerabilities. This approach can help evaluate how much information and access a potential external threat actor could obtain with minimal prior knowledge of the organization.

4) Double-Blind Penetration Testing

In a double-blind penetration test, the tester receives little or no prior information about the target environment. At the same time, the organization's employees or security personnel are not informed in advance about the specific timing or methods of the security assessment.

The purpose of this approach is to evaluate whether an organization is prepared to detect and respond to a realistic security incident. It can also help assess the effectiveness of existing security measures and determine how employees and security personnel respond under controlled testing conditions.

Penetration-Testing Frameworks

A) Open Source Security Testing Methodology Manual (OSSTMM)

The Open Source Security Testing Methodology Manual (OSSTMM) provides a structured methodology for conducting security assessments and identifying security weaknesses. It guides penetration testers and security professionals in systematically evaluating different aspects of operational security and includes areas such as operational security testing, channel testing, security metrics, and trust analysis (Al-Ahmad et al., 2023).

B) Open Worldwide Application Security Project (OWASP)

The Open Worldwide Application Security Project (OWASP) is a globally recognized initiative focused on improving the security of software and web applications. It provides freely accessible resources, methodologies, tools, and best-practice guidelines that can help organizations and security professionals identify, assess, and mitigate security vulnerabilities in applications and related environments (OWASP Foundation, n.d.).

C) Penetration Testing Execution Standard (PTES)

The Penetration Testing Execution Standard (PTES) provides a structured approach to conducting penetration tests. It defines a series of standardized phases that assist security professionals in planning security assessments, identifying vulnerabilities, evaluating potential security risks, conducting controlled testing, and reporting the results of penetration tests (Penetration Testing Execution Standard, n.d.; Al-Ahmad et al., 2023).

D) National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) provides standardized guidelines and recommendations relevant to information-security testing and assessment. These guidelines assist organizations in conducting security assessments in a systematic and consistent manner. By following NIST guidance, organizations can apply established security-testing practices, identify vulnerabilities,

assess potential risks, and improve their overall cybersecurity posture through a structured and standardized testing approach (Scarfone et al., 2008).

E) Information Systems Security Assessment Framework (ISSAF)

The Information Systems Security Assessment Framework (ISSAF) provides a structured approach to conducting information-system security assessments and penetration testing. It covers different stages of the security-assessment process and can assist security professionals in identifying vulnerabilities, evaluating security controls, and documenting the results of security testing (Al-Ahmad et al., 2023).

Figure 3 summarizes several major penetration-testing frameworks and illustrates how different methodologies can contribute to a more comprehensive security-assessment process.

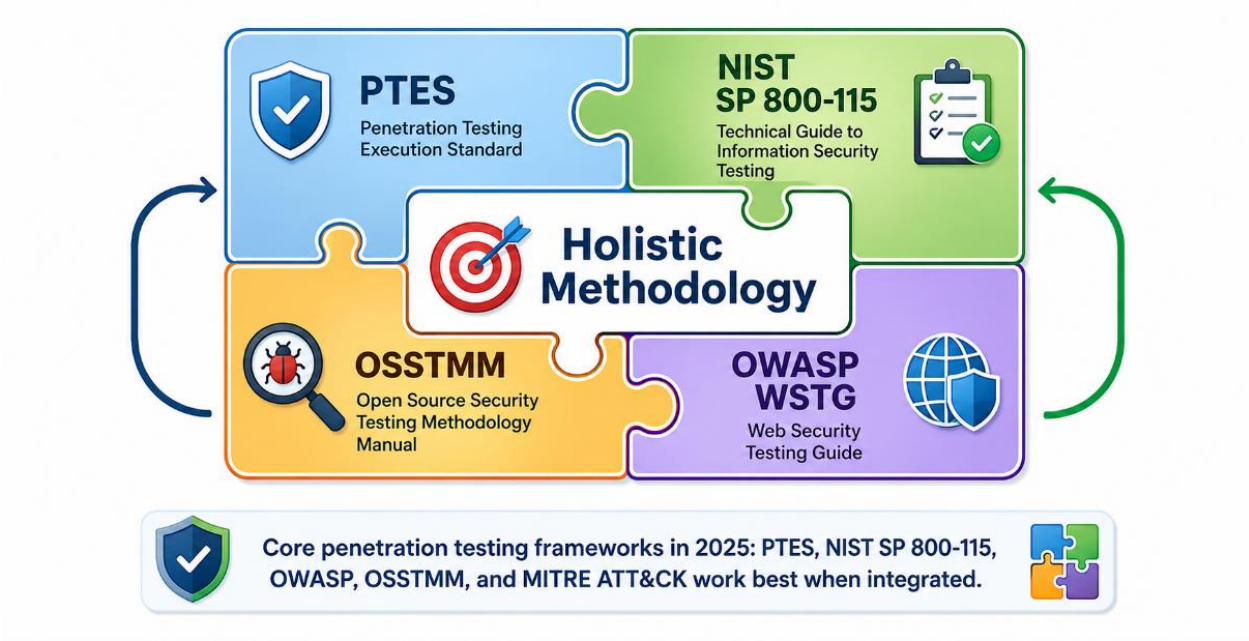

Figure 3. Integrated Penetration-Testing Frameworks and Methodologies

PHASES

The penetration-testing process can be divided into several key phases, each serving a specific purpose in identifying, assessing, and understanding potential security vulnerabilities.

1. Reconnaissance

Reconnaissance is the first phase of penetration testing. During this phase, information about the target is gathered before potential vulnerabilities are identified. Various methods and techniques are used to collect relevant information through either active or passive approaches. The purpose of this phase is to obtain sufficient knowledge about the target environment, which helps identify potential vulnerabilities and plan the subsequent stages of the assessment effectively.

2. Scanning and Enumeration

The second phase is scanning and enumeration. During this stage, different strategies and tools are used to detect potential weaknesses within the selected target system. The purpose of this phase is to gather technical information and identify vulnerabilities that may pose security risks.

3. Exploitation

The third phase is exploitation. During this stage, identified vulnerabilities are tested to determine whether they can be used to gain access to the target system. Such vulnerabilities may include weaknesses in web applications, weak passwords, insecure services, or system misconfigurations. Under controlled and authorized conditions, the penetration tester attempts to exploit these vulnerabilities in order to evaluate their potential impact and determine the level of access that could be obtained.

4. Post-Exploitation

The final phase is post-exploitation. At this stage, access to the target system has already been achieved through identified vulnerabilities, open ports, or other entry points. The penetration tester evaluates the level of access obtained, the resources and data that may be accessible, and the potential impact of the identified vulnerabilities. These activities are performed within the authorized scope of the penetration test.

Figure 4 provides a visual overview of the main phases of the penetration-testing process, from planning and information gathering to vulnerability assessment, testing, impact evaluation, and remediation.

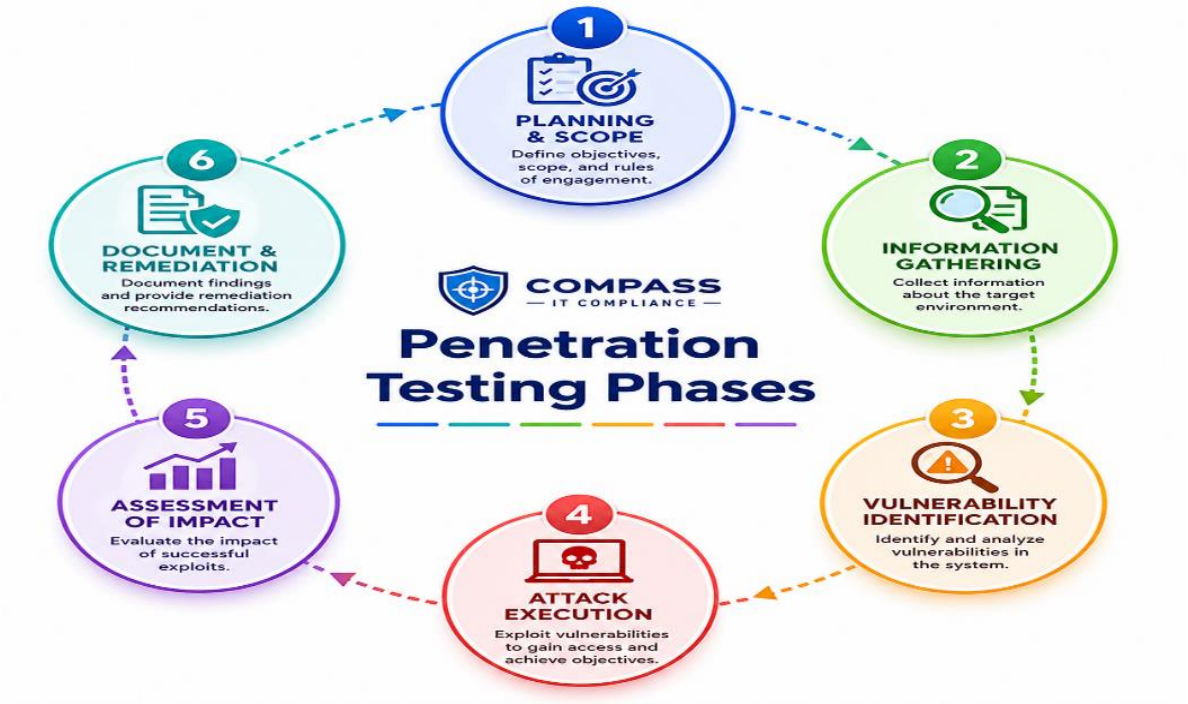

Figure 4. Main Phases of the Penetration-Testing Process

EXPERIMENTS & ANALYSIS

Penetration testing is one of the most useful techniques for identifying security weaknesses and improving the overall security of information systems. Previous large-scale data breaches demonstrate the potential consequences of vulnerabilities and insufficient security measures. For example, Adobe experienced a major security breach affecting approximately 153 million user records, while Google has also faced security incidents affecting a significant number of users (VikingCloud, 2025). Such

incidents demonstrate the importance of continuous security assessment, vulnerability identification, and the implementation of appropriate measures to protect organizational systems and sensitive data.

In response to increasing cybersecurity risks, organizations have strengthened their security practices by employing specialized security professionals and conducting regular security assessments. Effective penetration testing requires appropriate planning, the definition of clear testing objectives, and the identification of the target environment before the assessment is performed.

For the practical assessment presented in this study, Nmap was used to examine the target system. Nmap is a network scanning tool commonly used in vulnerability assessment and penetration testing to identify hosts, accessible ports, services, and other information relevant to the security of a target system.

The target address was scanned using Nmap, and the resulting information was analysed to identify accessible network services and potential security weaknesses. The scan identified a number of open ports, while the relevant results were subsequently examined for further security analysis, as presented in Figure 5.

Figure 5. Nmap scan results showing identified network ports and services.

The Nmap scan identified several open ports on the target system, including Telnet (port 23), DNS (port 53), and HTTP (port 80). The presence of these open ports indicates that the corresponding network services are accessible and should therefore be considered when evaluating the security of the target system.

Telnet (port 23) represents a potential security concern because the protocol transmits information, including authentication credentials, without encryption. If Telnet is enabled and accessible, sensitive information may therefore be exposed during communication. The use of more secure encrypted alternatives should be considered where appropriate.

The scan also identified DNS (port 53) as an accessible service. The presence of an open DNS port indicates that the target system provides or communicates through a DNS-related service. Its configuration and accessibility should be evaluated as part of the overall security assessment.

In addition, HTTP (port 80) was identified as open, indicating the availability of a web-based service or management interface. Since HTTP communication is not encrypted by default, the

configuration and purpose of the exposed service should be examined to determine whether additional security measures are required.

The identified open ports and corresponding services provide useful information about the target system's network exposure and help determine which services may require further security assessment. Figure 6 presents the Operating System Detection.

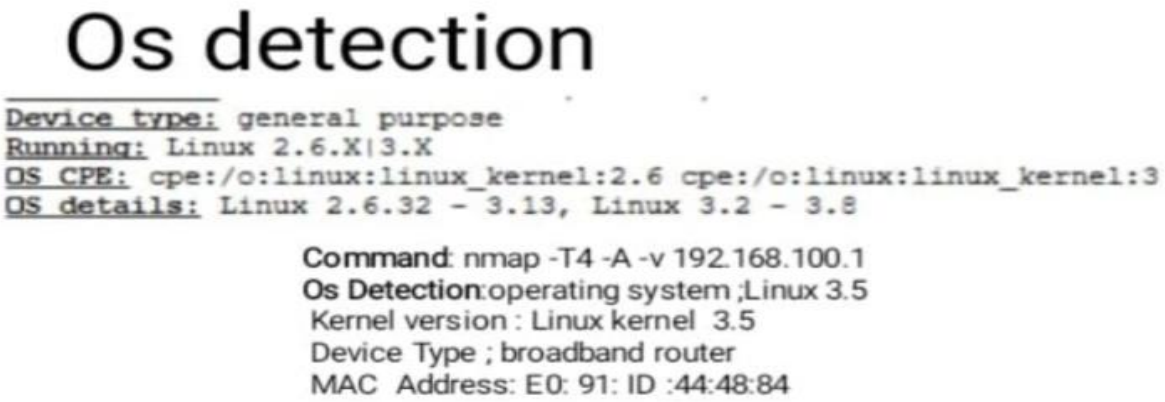

Figure 6. Nmap Operating System Detection Results for the Target Device

The operating system detection scan provided additional information about the target device. Based on the Nmap scan results, the target was identified as a router running Linux Kernel 3.5. Operating system detection can provide useful information during penetration testing because the identified operating environment may help the tester evaluate system characteristics and identify areas that may require further security assessment.

Figure 7. Nmap Firewall Detection Results Showing Filtered FTP and SSH Ports

In this case, the identification of the target as a Linux-based router complements the port-scanning results and provides additional information about the system environment. These findings contribute to a more complete understanding of the target and its potential security exposure, as

presented in Figure 6. Figure 7 presents the firewall-detection results, showing that FTP (port 21) and SSH (port 22) were identified as filtered by the Nmap scan.

The firewall analysis showed that FTP (port 21) and SSH (port 22) were in a filtered state. In Nmap scanning, a filtered port indicates that network filtering mechanisms prevent the scanner from determining whether the port is open or closed. This result suggests that firewall rules or other access-control mechanisms may be restricting communication with these services.

Filtering access to ports such as FTP and SSH can reduce their direct exposure to unauthorized connections and therefore contribute to the protection of the target system. However, a filtered state should not by itself be interpreted as evidence that the corresponding service is completely secure. Instead, it indicates that a filtering mechanism is controlling or restricting access to the port.

The results of the practical assessment demonstrate how penetration testing and network scanning can provide information about accessible services, filtered ports, and the operating environment of a target system. In this case, the Nmap scan identified several open services, including Telnet (port 23), DNS (port 53), and HTTP (port 80), while FTP (port 21) and SSH (port 22) were filtered. The operating system detection results additionally identified the target as a router running Linux Kernel 3.5. Together, these findings illustrate how penetration-testing tools can support the identification and assessment of potential areas of security exposure.

CONCLUSION

This study examined the role of penetration testing in identifying cybersecurity vulnerabilities and discussed various approaches, techniques, and frameworks used in security assessment. Penetration testing provides a structured method for gathering information about a target environment, identifying potential security weaknesses, and evaluating how these weaknesses may affect the overall security of information systems.

The practical assessment conducted in this study demonstrated the application of Nmap for identifying accessible network services and obtaining information about the target environment. The scan identified several open ports, including Telnet (port 23), DNS (port 53), and HTTP (port 80), while FTP (port 21) and SSH (port 22) were identified as filtered. The operating system detection results also indicated that the target device was a router running Linux Kernel 3.5. These findings demonstrate how network scanning can provide useful information for identifying areas that may require further security assessment.

The study also discussed different penetration-testing approaches and established security frameworks that can support organizations in conducting systematic security assessments. Regular and authorized penetration testing can help organizations identify vulnerabilities before they are exploited, evaluate existing security controls, and implement appropriate remediation measures to strengthen the protection of systems and sensitive data.

While modern technologies provide significant advantages to individuals and organizations, they also introduce new cybersecurity challenges and risks. Therefore, organizations should continuously evaluate their security measures and adopt appropriate technologies, methodologies, and security practices to protect their systems against evolving threats. The practical demonstration presented in this study is limited to a single target environment and a specific network scan; consequently, the findings should be interpreted as an illustrative case rather than a comprehensive assessment of penetration-testing effectiveness.

Declaration by Authors
Ethical Approval: Approved
Acknowledgement: None
Source of Funding: None
Conflict of Interest: The authors declare no conflict of interests.

REFERENCES

Al-Ahmad, A. S., Kahtan, H., & Alzoubi, Y. I. (2023). Overview on case study penetration testing models evaluation. *Emerging Science Journal, 7*(3), 1019–1036. https://doi.org/10.28991/ESJ-2023-07-03-025

Alhamed, M., & Rahman, M. M. H. (2023). A systematic literature review on penetration testing in networks: Future research directions. *Applied Sciences, 13*(12), 6986. https://doi.org/10.3390/app13126986

Anderson, J. P. (1972). *Computer security technology planning study* (Technical Report ESD-TR-73-51). Electronic Systems Division, Air Force Systems Command.

Anderson, J. P. (1980). *Computer security threat monitoring and surveillance*. James P. Anderson Co.

Apiiro. (n.d.). *Web application penetration testing*. https://apiiro.com/glossary/web-application-penetration-testing/

Dai, W., Zhou, J., Ye, C., & Xu, G. (2026). Automated penetration testing system based on PTES and ATT&CK. In M. Kadoch, M. Cheriet, & X. Qiu (Eds.), *Information processing and network provisioning* (Communications in Computer and Information Science, Vol. 2594, pp. 433–444). Springer. https://doi.org/10.1007/978-981-95-1340-6_35

Dionach. (2022). *Penetration testing case study: Why an internal penetration test delivers results*. https://dionach.com/wp-content/uploads/2022/12/DIONACH_PENTEST_CASE_STUDY.pdf

IBM. (n.d.). *Penetration testing methodologies and standards*. IBM Think. https://www.ibm.com/think/insights/pen-testing-methodology

Imperva. (n.d.). *Penetration testing*. https://www.imperva.com/learn/application-security/penetration-testing/

Infosec Institute. (2019, July 7). *The history of penetration testing*. https://www.infosecinstitute.com/resources/penetration-testing/the-history-of-penetration-testing/

Kumar, R., & Tlhagadikgora, K. (2019). Internal network penetration testing using free/open-source tools: Network and system administration approach. In A. K. Luhach, D. Singh, D. H. K. Hawari, M. Lingras, & P. S. Yu (Eds.), *Advanced informatics for computing research* (Communications in Computer and Information Science, Vol. 956, pp. 257–269). Springer. https://doi.org/10.1007/978-981-13-3143-5_22

Long, J. (2005). *Google hacking for penetration testers*. Syngress. https://doi.org/10.1016/B978-1-931836-36-4.X5000-3

OWASP Foundation. (n.d.). *OWASP Web Security Testing Guide (WSTG), version 4.2*. https://wstg.owasp.org/v4.2/

Parveen, M., & Shaik, M. A. (2023). Review on penetration testing techniques in cyber security. In *2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)* (pp. 1265–1270). IEEE. https://doi.org/10.1109/ICAISS58487.2023.10250659

Penetration Testing Execution Standard. (n.d.). *PTES technical guidelines*. https://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

PurpleSec LLC. (2020, January 1). *Pentest report: Example Institute*. https://purplesec.us/wp-content/uploads/2019/12/Sample-Penetration-Test-Report-PurpleSec.pdf

Sadlek, L., Čeleda, P., & Tovarňák, D. (2022). Current challenges of cyber threat and vulnerability identification using public enumerations. In *Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES 2022)* (Article 10). ACM. https://doi.org/10.1145/3538969.3544458

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). *Technical guide to information security testing and assessment* (NIST Special Publication 800-115). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-115

Shinde, P. S., & Ardhapurkar, S. B. (2016). Cyber security analysis using vulnerability assessment and penetration testing. In *2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)* (pp. 1–5). IEEE. https://doi.org/10.1109/STARTUP.2016.7583912

VikingCloud. (2025, March 31). *Penetration testing examples: Real-world scenarios & insights*. https://www.vikingcloud.com/blog/penetration-testing-examples

How to cite this article:

Bibi, I. (2026). The Role of Penetration Testing in Identifying Cybersecurity Vulnerabilities. *International Journal of Digital Research*, *2*(3), 59–71. https://doi.org/10.63711/ijdr.net20260305

*****