

1. Introduction

As digital infrastructure becomes more integral to daily life, the security of home and office networks is increasingly critical. Cyber threats such as malware, unauthorized access, and data breaches now affect not only businesses but also individuals, especially with the rise of IoT devices and remote work. [1].

Penetration testing is a proactive method used to identify and fix vulnerabilities before they can be exploited. This project focuses on applying penetration testing tools—like Nmap, Nessus, Wireshark, and Burp Suite—to assess the security of home networks. These tools simulate real-world attacks to uncover weaknesses in configurations, software, and user behavior.

The study emphasizes the growing importance of securing home networks, which often lack formal assessments despite their complexity. It also highlights the educational and preventative value of penetration testing, especially as personal and professional networks increasingly overlap.

3. Sources

Undertaking a Literature review to build your research on existing knowledge is argued by [2] to be the starting point for all research activity and should be a priority for the researcher. The literature review for this project will focus on identifying existing research and theories of Penetration testing, with a particular focus on White Box Penetration Testing to ensure any findings can support or contradict previous studies undertaken. Literature delves into fundamental concepts, techniques, and approaches such as vulnerability assessment, ethical hacking, and exploit development [3],[4]. It identifies research gaps and demonstrates the importance of this effort in solving current cybersecurity concerns. This will act as a foundation for building knowledge and applying theory to practice [2].

5. Implementation

The primary objective in the implementation stage is to simulate real-world cybersecurity scenarios using virtual machines (VM) to assess vulnerabilities on a home PC setup.

A Windows 11 VM was deployed to represent the target system (Home PC), while a Linux Ubuntu VM was used to conduct testing procedures such as network scanning and vulnerability detection as shown in fig. 3 and 4. Nessus, chosen due its popularity based on the control it provides [5] was installed on the (Home PC) to identify security flaws, and connectivity between the two systems was established using IP-based communication.

This implementation lays the groundwork for further testing and evaluation, providing a secure and functional environment to execute penetration testing tasks in line with the project's objectives.

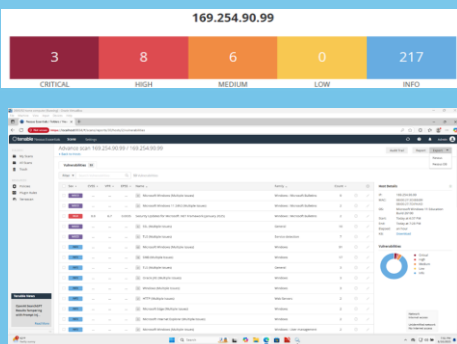


Fig 3: Nessus Report before Mitigation

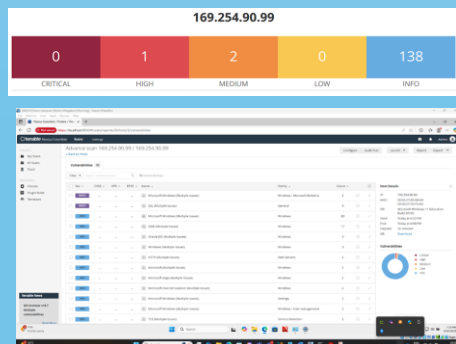


Fig 4: Nessus Report after Mitigation

6. Conclusion

This research highlights the effectiveness of white box penetration testing in improving home computer security. Drawing on a strong theoretical foundation, the study used a qualitative approach and simulated real-world attacks using Nessus and Nmap to identify vulnerabilities such as outdated software and insecure configurations. Findings confirmed the presence of critical issues, many of which were successfully mitigated, validating the approach. Despite some limitations-particularly with SSL/TLS and registry vulnerabilities-the research demonstrates that white box testing provides valuable insights and is a vital tool for proactive cybersecurity [6], both for individuals and broader applications.

2. Aims and Objectives

Aim

The main aim of this project is to assess the security posture of a typical home network by conducting a structured penetration test, namely White Box Penetration Testing. The outcome of the penetration test goal is to identify potential vulnerabilities and to undertake mitigation to address these security risks to assess its effectiveness.

Objectives

- To conduct a comprehensive literature review to identify the main theories and related work.
- To outline the research methodology that will be used.
- To detect and identify vulnerabilities in network services and configurations using White Penetration Testing tools.
- To test and evaluate the effectiveness of White Penetration Testing to eliminate vulnerabilities in a home computer system.
- To provide a written report about the effectiveness of White Penetration testing and propose improvements/recommendations, considering any need to further to mitigate any risks associated with the vulnerabilities identified.

4. Design

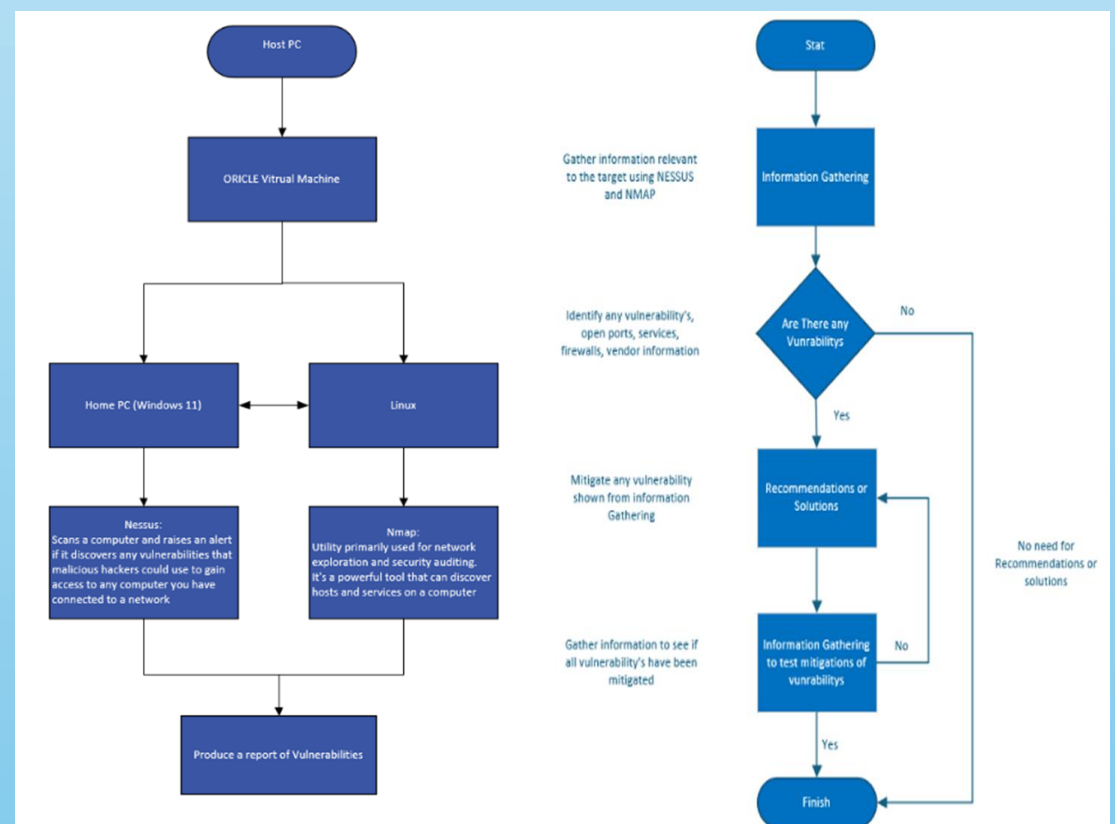


Fig 1: Experiment Design Flow chart

Fig 2: Penetration Testing Life Cycle

The experiment showing the flowchart and penetration testing lifecycle shown in Fig.1 and 2 was conducted using a virtualised environment on a host PC, where two virtual machines (VMs) were deployed: one running Windows (Home PC) and the other Linux. Nessus was installed on the Home PC to perform in-depth vulnerability scans, identifying issues like misconfigurations, missing patches, and exploitable weaknesses. Nmap, running on the Linux VM, was used to map the network, identify active hosts, and detect open ports.

7. Reference

- [1] S. Singh, Y.-S. Jeong, and J. park, "A Survey on Cloud Computing Security: Issues, Threats, and Solutions," vol. 75, Sep. 2016, doi: 10.1016/j.jnca.2016.09.002. Available: https://www.researchgate.net/publication/308012933_A_Survey_on_Cloud_Computing_Security_Issues_Threats_and_Solutions. [Accessed: Apr. 10, 2025]
- [2] H. Snyder, "Literature review as a research methodology: An overview and guidelines," Journal of Business Research, vol. 104, no. 1, pp. 333–339, Nov. 2019, doi: <https://doi.org/10.1016/j.jbusres.2019.07.039>.
- [3] S. Karen and M. Peter, "Guide to Intrusion Detection and Prevention Systems (IDPS)ed", Available: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf>. [Accessed: Apr. 11, 2025]
- [4] J. Erickson, Hacking: The Art of Exploitation, 1st ed. San Francisco: No Starch Press, Incorporated, 2003 [Accessed: Apr. 25, 2025]
- [5] H. M. Z. A. Shebli and B. D. Beheshti, "A study on penetration testing process and tools," May 2018, pp. 1–7. doi: 10.1109/LISAT.2018.8378035. Available: <https://ieeexplore.ieee.org/abstract/document/8378035>. [Accessed: Apr. 21, 2025]
- [6] M. E. Whitman and H. J. Mattord, Principles of information security. Thomson Course Technology Boston, MA, 2009.