

**Web Application Security Testing: A NIDS-based Penetration Testing Approach**

**Review-1 Report**

|  |  |
| --- | --- |
| **NAME** | **ROLL NUMBER** |
| SHREYA MALSHETTY | 20211CCS0061 |
| JAYALAKSHMI D | 20211CCS0064 |
| CHAITHRA BANGER | 20211CCS0114 |
| SRUJANA MANJUNATH | 20211CCS0116 |

**COURSE NAME:**  CAPESTONE PROJECT

**COURSE CODE:**  PIP2001

**GROUP NUMBER:** CCS-G07

**CORSE INSTRUCTOR:**  Dr. Sharmasth Vali

**DATE & DAY:**  22-10-2024, TUESDAY

**SCHOOL:**  SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

**CONTENTS**

1.Aim

2.Objectives

3. Methodology

4. Architecture Diagram

5. Software Details

6. Future Work

7. Conclusion

8. References

**AIM:**

This report evaluates the effectiveness of using a Network Intrusion Detection System (NIDS) in conjunction with penetration testing for securing web applications. The approach aims to identify vulnerabilities, monitor network traffic, and enhance overall security posture.

**OBJECTIVES**:

1. Identify potential security threats and vulnerabilities in the web application.

2. Evaluate the effectiveness of NIDS in detecting and preventing attacks.

3. Assess the integration of NIDS with web application testing tools.

**METHODOLOGY:**

1. *Planning and Preparation:* Define the scope, including targets, objectives, and compliance requirements.

2. *Setup NIDS:* Install and configure a NIDS to monitor traffic to and from the web application.

3. *Traffic Analysis:* Monitor the traffic to identify potential threats and anomalies.

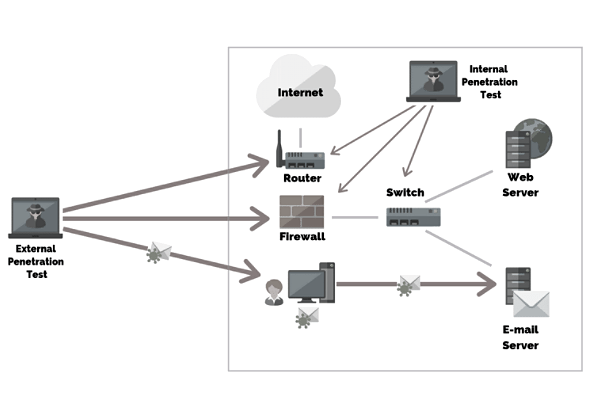
4. *Vulnerability Scanning:* Use tools like ZAP or Burp Suite to identify vulnerabilities in the web application.

5. *Exploitation:* Attempt to exploit identified vulnerabilities using Metasploit or similar tools.

6. *Post-Exploitation:* Analyse the impact of successful exploits and gather evidence.

7. *Reporting:* Compile findings, including identified vulnerabilities, risk levels, and remediation recommendations.

**ARCHITECTURE:**

****

**TOOLS:**

1. NIDS Tools

- Nmap

- Suricata

- Bro/Zeek

2. Web Application Testing Tools

- OWASP ZAP (Zed Attack Proxy)

- Burp Suite

- Nikto

3. Vulnerability Scanners

- Nessus

- Qualys

4. Penetration Testing Frameworks

- Metasploit

- Kali Linux

**FUTURE WORK:**

1. Conduct regular security testing and vulnerability assessments.

2. Implement a Web Application Firewall (WAF).

3. Develop a comprehensive security awareness program.

**CONCLUSION:**

The NIDS-based penetration testing approach offers a robust framework for enhancing web application security. By integrating continuous monitoring with proactive vulnerability testing, organizations can significantly reduce their risk exposure.

**REFERENCES:**

**[1] Alhamed M, Rahman MMH. A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. Applied Sciences. 2023; 13(12):6986.** [**https://doi.org/10.3390/app13126986**](https://doi.org/10.3390/app13126986)

**[2] Altulaihan EA, Alismail A, Frikha M. A Survey on Web Application Penetration Testing. Electronics. 2023; 12(5):1229.**

[**https://doi.org/10.3390/electronics12051229**](https://doi.org/10.3390/electronics12051229)

**[3] Vladimir Ciric, Marija Milosevic, Danijel Sokolovic, Ivan Milentijevic,**

**Modular deep learning-based network intrusion detection architecture for real-world cyber-attack simulation, Simulation Modelling Practice and Theory, Volume 133,2024,102916,ISSN 1569-190X,**

[**https://doi.org/10.1016/j.simpat.2024.102916**](https://doi.org/10.1016/j.simpat.2024.102916)

**[4] Saputra FA, Salman M, Hasim JAN, Nadhori IU, Ramli K. The Next-Generation NIDS Platform: Cloud-Based Snort NIDS Using Containers and Big Data. Big Data and Cognitive Computing. 2022; 6(1):19.** [**https://doi.org/10.3390/bdcc6010019**](https://doi.org/10.3390/bdcc6010019)

**[5] Alhamed M, Rahman MMH. A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. Applied Sciences. 2023; 13(12):6986.** [**https://doi.org/10.3390/app13126986**](https://doi.org/10.3390/app13126986)

**[6] Altulaihan EA, Alismail A, Frikha M. A Survey on Web Application Penetration Testing. Electronics. 2023; 12(5):1229.**

[**https://doi.org/10.3390/electronics12051229**](https://doi.org/10.3390/electronics12051229)

**[7] Vladimir Ciric, Marija Milosevic, Danijel Sokolovic, Ivan Milentijevic,**

**Modular deep learning-based network intrusion detection architecture for real-world cyber-attack simulation, Simulation Modelling Practice and Theory, Volume 133,2024,102916,ISSN 1569-190X,**

[**https://doi.org/10.1016/j.simpat.2024.102916**](https://doi.org/10.1016/j.simpat.2024.102916)

**[8] Saputra FA, Salman M, Hasim JAN, Nadhori IU, Ramli K. The Next-Generation NIDS Platform: Cloud-Based Snort NIDS Using Containers and Big Data. Big Data and Cognitive Computing. 2022; 6(1):19.** [**https://doi.org/10.3390/bdcc6010019**](https://doi.org/10.3390/bdcc6010019)

**[9] S. Kumar, S. Gupta and S. Arora, "Research Trends in Network-Based Intrusion Detection Systems: A Review," in IEEE Access, vol. 9, pp. 157761-157779, 2021.** [**https://doi:10.1109/ACCESS.2021.3129775**](https://doi:10.1109/ACCESS.2021.3129775)