

Abstract

The purpose of the study is to find the best vulnerability scanner for Dyfed Powys Police to improve their IT security.

This will involve comparing different scanners. We will use assessment metrics devised and tested by researchers in previous studies of vulnerability scanners.

Aim and Objectives

Aim:

To carry out a comparative analysis of different vulnerability assessment tools to identify the best suitable vulnerability analysis tool to strengthen the IT security posture of Dyfed-Powys Police.

Objectives:

1. Research and identifying key metrics for assessing vulnerability scanners using key word searches e.g. vulnerability scanner metrics.
2. Setup a laboratory to compare and analyse vulnerability scanners.
3. Try to exploit the vulnerabilities identified. If they can be exploited, propose a mitigation strategy.

Research Overview

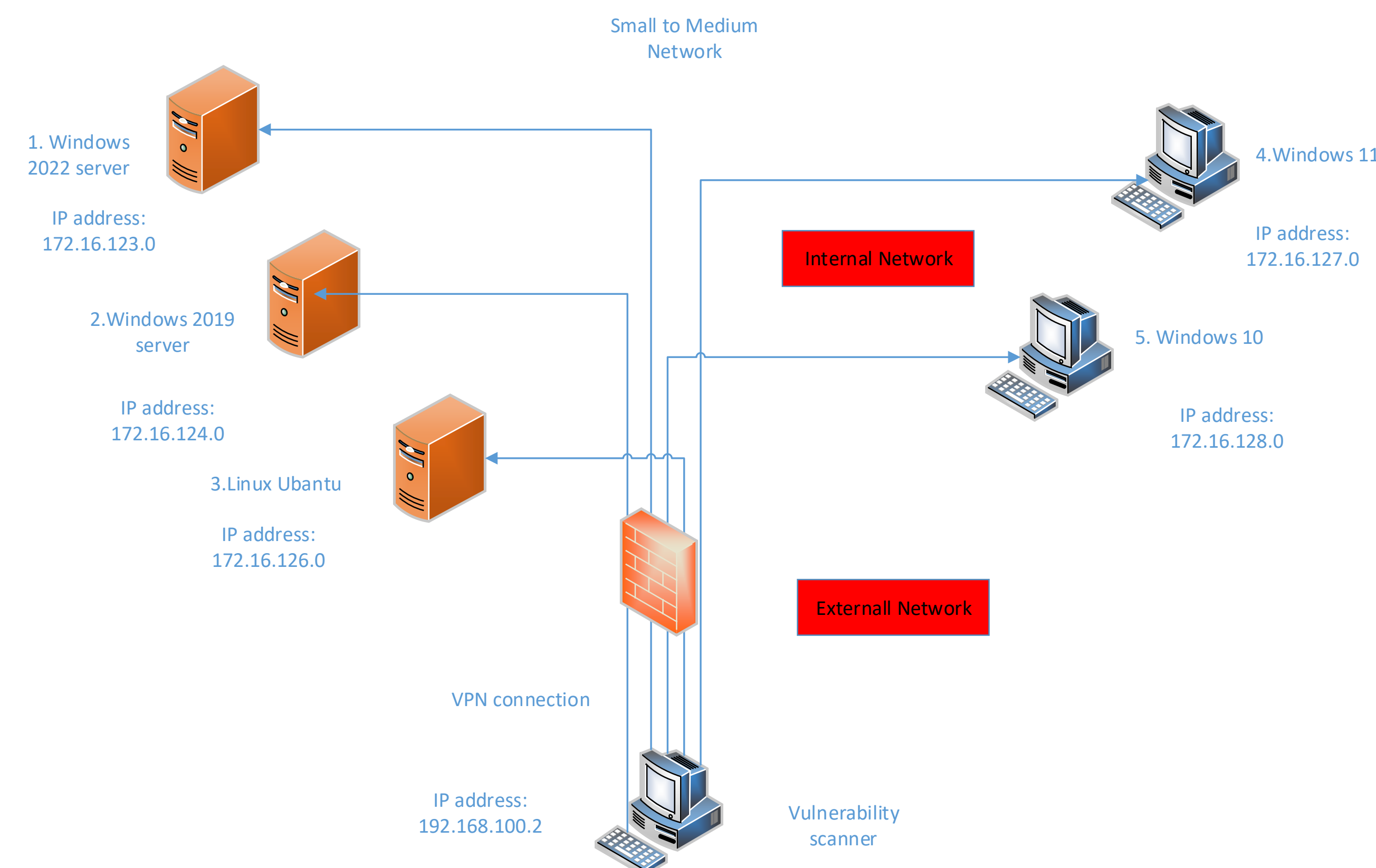
To compare and assess research vulnerability scanners, will use the following metrics identified in the literature review:

1. Detection Rates (Number of vulnerabilities identified) [1]
2. Usability (User-friendliness of the software) [2]
3. Reporting (customisation and report formats) [1][3]

Design and Implementation

Two vulnerability scanners, Open VAS and Nessus will be tested and analysed in a simulated network environment as shown in figure1.

Figure 1: Simulated network environment

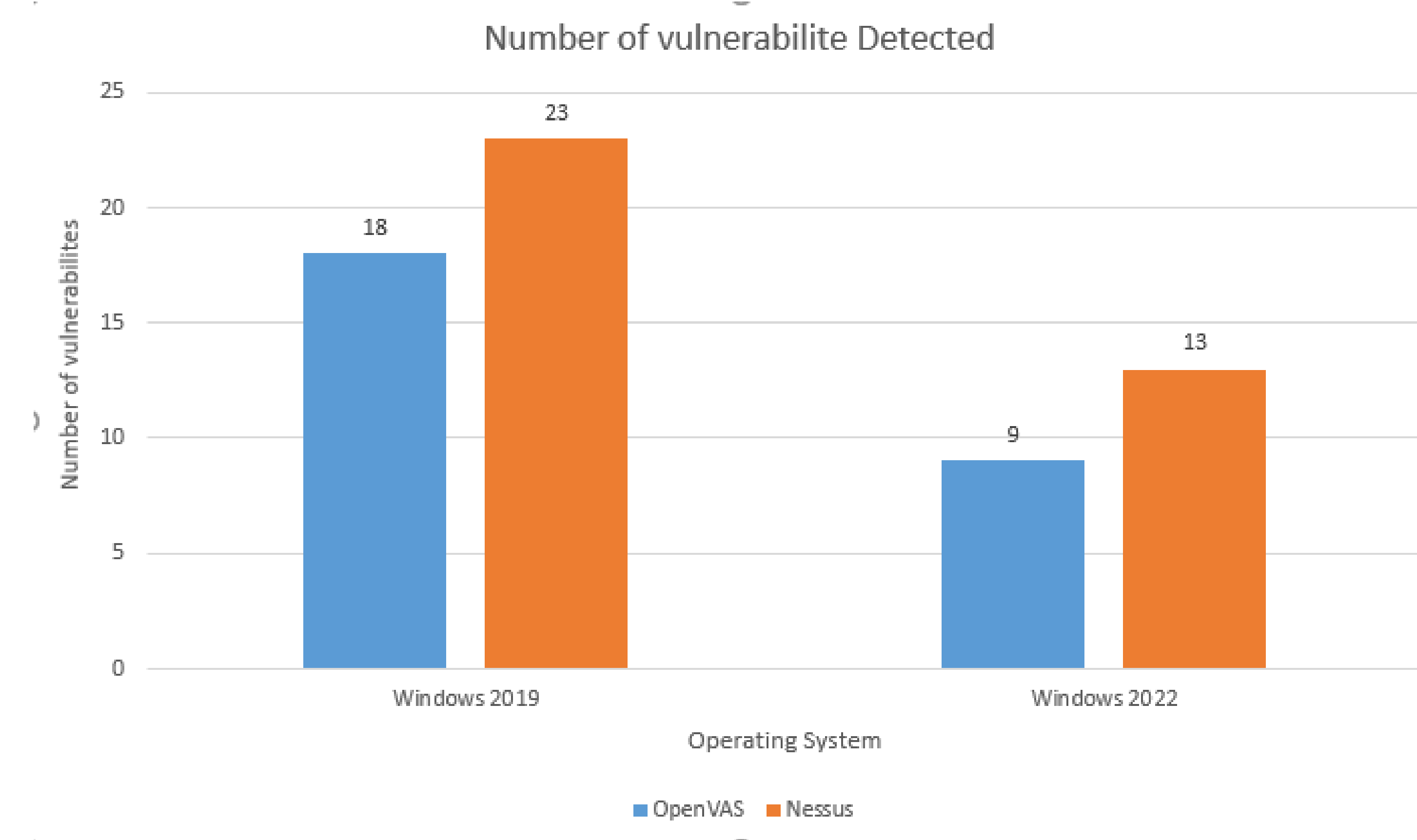


Analysis and Evaluation

The results of comparing and analysing Nessus and OpenVAS are below:

1. Detection Rates. Nessus identified a higher number of vulnerabilities than OpenVAS as shown in Figure 2
2. Usability was assessed on nine security objectives devised. The security objectives were based on the user being able to complete actions, such as starting and completing a vulnerability scan. Nessus completed seven out of the nine security objectives. OpenVAS only completed two out of nine security objectives.
3. Reporting was assessed on the user ability to customise reports and the different report formats that the report can be exported. OpenVAS offered the most flexibility when customising reports. Nessus was very limited. OpenVAS offered the five file formats to export reports e.g. PDF. Nessus only offered two report formats.

Figure 2: Number of vulnerabilities



Conclusion

Based on the results, it is recommend that Dyfed-Powys Police use Nessus and not OpenVAS because Nessus outperformed OpenVAS in two out of the three metrics to assess vulnerability scanners. Nessus detected a higher number of vulnerabilities compared to OpenVAS. Nessus outperformed OpenVAS in usability. OpenVAS did outperformed Nessus in reporting.

Reference

- [1] A. Kejiou and G. Bekaroo, "A Review and Comparative Analysis of Vulnerability Scanning Tools for Wireless LANs," in 2022 3rd International Conference on Next Generation Computing Applications (NextComp), Flic-en-Flac, 2022.
- [2] M. U. Aksu, K. Bicakci and E. Altuncu, "A First Look at the Usability of OpenVAS Vulnerability Scanner," in *Workshop on Usable Security (USEC)*, San Diego, 2019.
- [3] R. F. Khalil, *Why Johnny Still Can't Pentest: A Comparative Analysis of Open-source Black-box Web*, Ottawa: School of Electrical Engineering and Computer Science Faculty of Engineering University of Ottawa, 2018