

# Evaluate and model vulnerabilities discovered during an assessment of IT systems



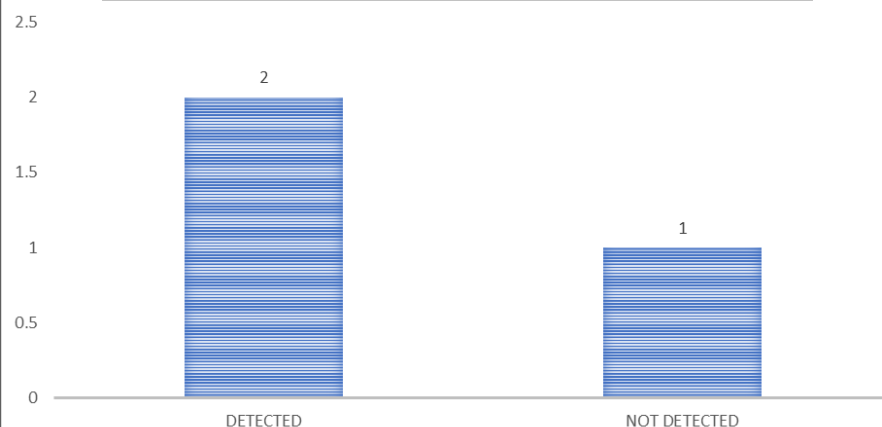
Prifysgol Cymru  
Y Drindod Dewi Sant  
University of Wales  
Trinity Saint David

Author: John M Williams (jmw5678@gmail.com) Supervisor: Munyaradzi Murira

## Conclusion

Threats from vulnerabilities can be determined using different modelling techniques. This project finds that by undertaking testing and modelling of three vulnerabilities, the threat ratings changed, and the vulnerability labelled as high under the CVSS model becomes critical. Microsoft Unquoted Service Path poses the greatest threat and should be remediated initially.

VULNERABILITIES DETECTED BY SERVER



## Introduction

Testing for vulnerabilities has become part of the routing maintenance needed to secure IT systems against current and future threats. The risks they pose to systems is determined using varying modelling techniques.

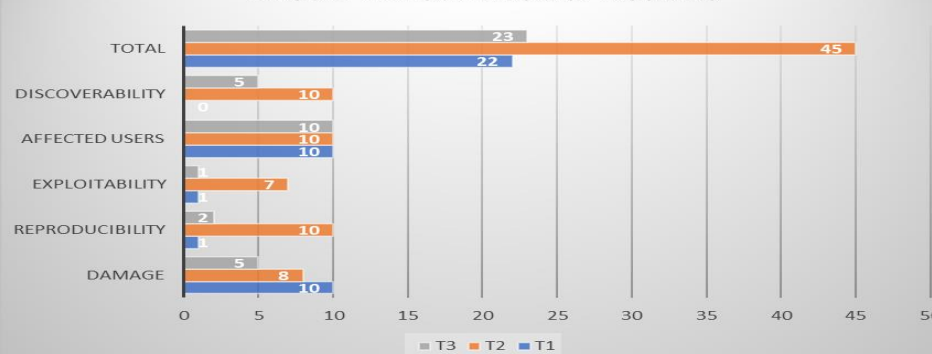
## Aim of Project

Analyse and understand three vulnerabilities, model the threat, and provide a conclusion and recommendations based on the modelling and testing, to improve the security posture of the systems under assessment.

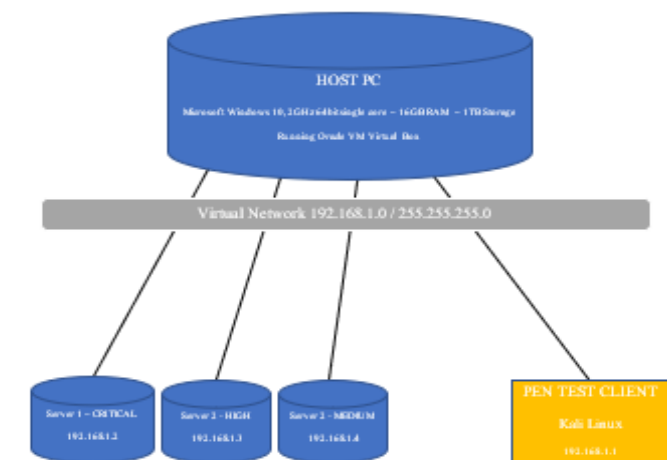
## Research Overview

1. What are vulnerability assessments and penetration tests?
2. In-depth review of the three selected vulnerabilities.
3. System requirements on how to undertake virtual lab testing
4. Risk modelling methodologies such as CVSS and DREAD

Dread Threat Model Results



## Virtual Lab Design



## Evaluations and Results

Two out of the three vulnerabilities were identified during the lab testing. DREAD modelling found differential threat classifications to be Critical, Medium and Medium.

## References

- [1] K. M. Henry, 'Penetration testing : protecting networks and systems', 2012.
- [2] P. S. Antón, R. H. Anderson, R. Mesic, and M. Scheiern, 'INTRODUCTION', in *Finding and Fixing Vulnerabilities in Information Systems*, 1st ed. in The Vulnerability Assessment and Mitigation Methodology. RAND Corporation, 2003, pp. 1-4. [Online]. Available: <http://www.jstor.org/stable/10.7249/mr1601darpa.9>