



Author: Matthew James (1809299) Supervisor: Nitheesh Kaliyamurthy

Introduction

Thousands of NHS Wales staff utilise DHCW technology services every day for Welsh patients. While NHS Wales supports millions of clinicians messaging, connecting and joining-up care allowing doctors, nurses, and health staff to have each patient's information's to hand where and when it is required. [1] DHCW are required to protect Personal identifiable information (P.I.I) [2] by various laws such as General Data Protection Act (GDPR) [3]. Information of various nature will be traversing networks within the NHS Wales internal networks and the wider internet to provide information where required. Certain security requirements scrutinised internally must be met to ensure the security of this information.

Figure 1

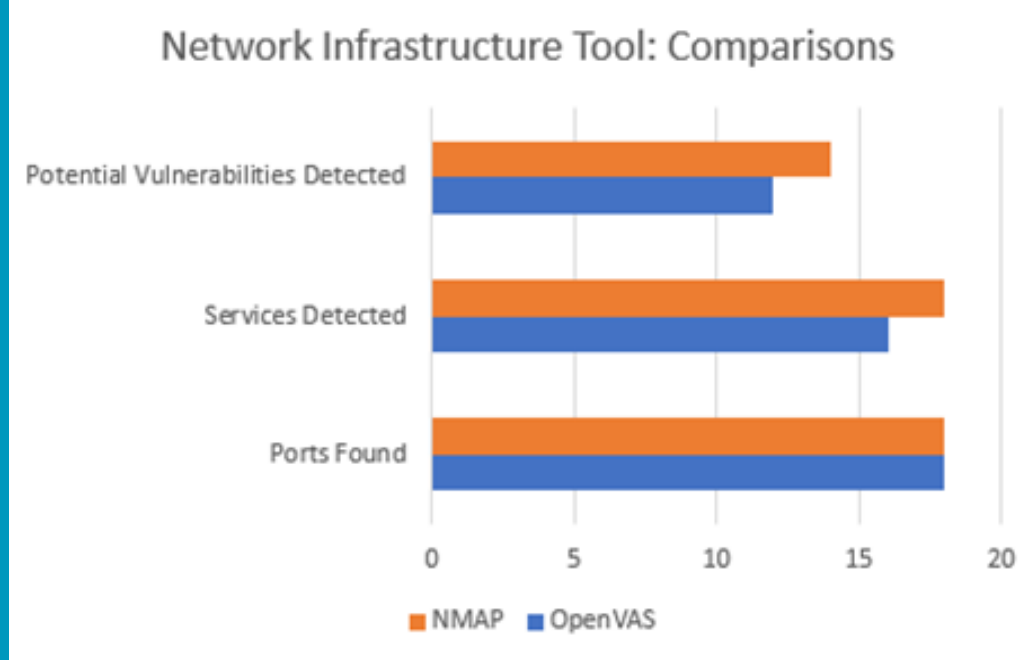


Figure 2

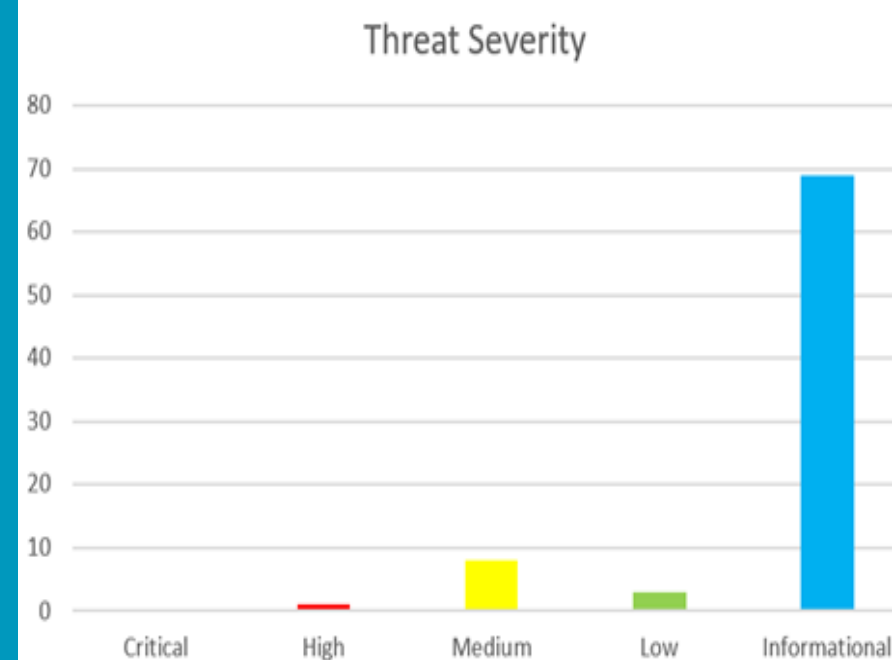


Figure 3

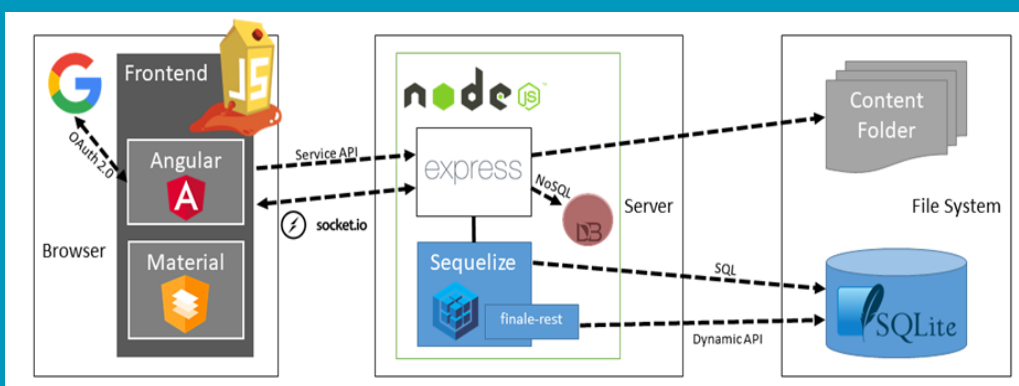
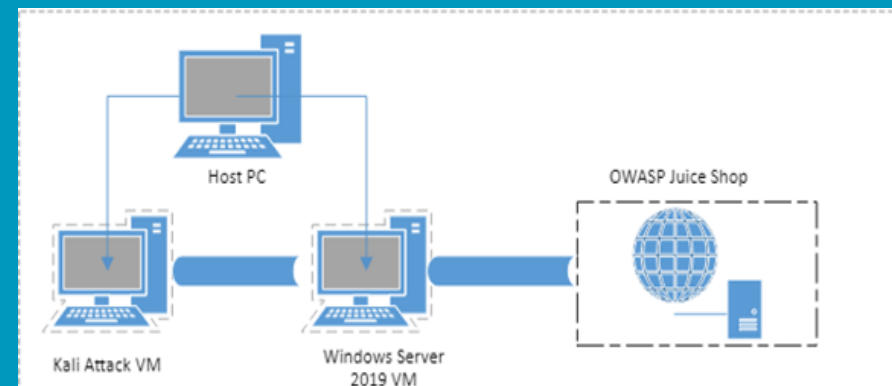


Figure 4



Results & Analysis

The results from the project can be found within the full report.

In figure 1 you can see a snippet of the OpenVAS & NMAP Comparison where NMAP stays slightly ahead in all most areas. Figure 2 highlights the Severity rating of OpenVAS scan results showing a large amount of informational. Figure 3 you can see Burp suites Scan of OWASP Juice shop, Burp Suite was unable to identify all of the known issues with the Web application and provided an absurd amount of Informational data. See full report for full comparison / results.

Aims and Objectives

Aim:

Compare different identified Pen Testing tools and analysis their effectiveness / efficiency in testing various web and network infrastructures in a simulated lab environment.

The Project aims to follow the structure approach as shown below:

- Create criteria for research
- Conduct initial literature review on infrastructure & web app testing tools
- Select tools for both infrastructure & web app testing based on the criteria
- Conduct various vulnerability assessments within a simulated environment
- Analyse and compare tools
- Recommend network penetration testing tool based on analyse
- Recommend web penetration testing tool based on analyse

Design & Implementation

A simulated virtual environment was designed and built to produce results for analysis. The implementation contains the following elements:

Windows Server 2019
Kali Linux (Debian)
OWASP Juice Shop—Figure 4
Tenable.SC — unavailable
Net sparker — unavailable

Burp Suite
Metasploit
Nmap/Zenmap
Tenable.IO — unavailable
Acunetix — unavailable

Research

Top Threats for Web applications:

- Broken Access Control
- Cryptographic-Failures
- Injection
- Insecure Design
- Security Misconfigurations

Top Threats for Network Infrastructure:

- Open Ports
- Security Misconfigurations
- Insecure Design
- Unencrypted-Communications
- Privilege Escalation

Figure 5

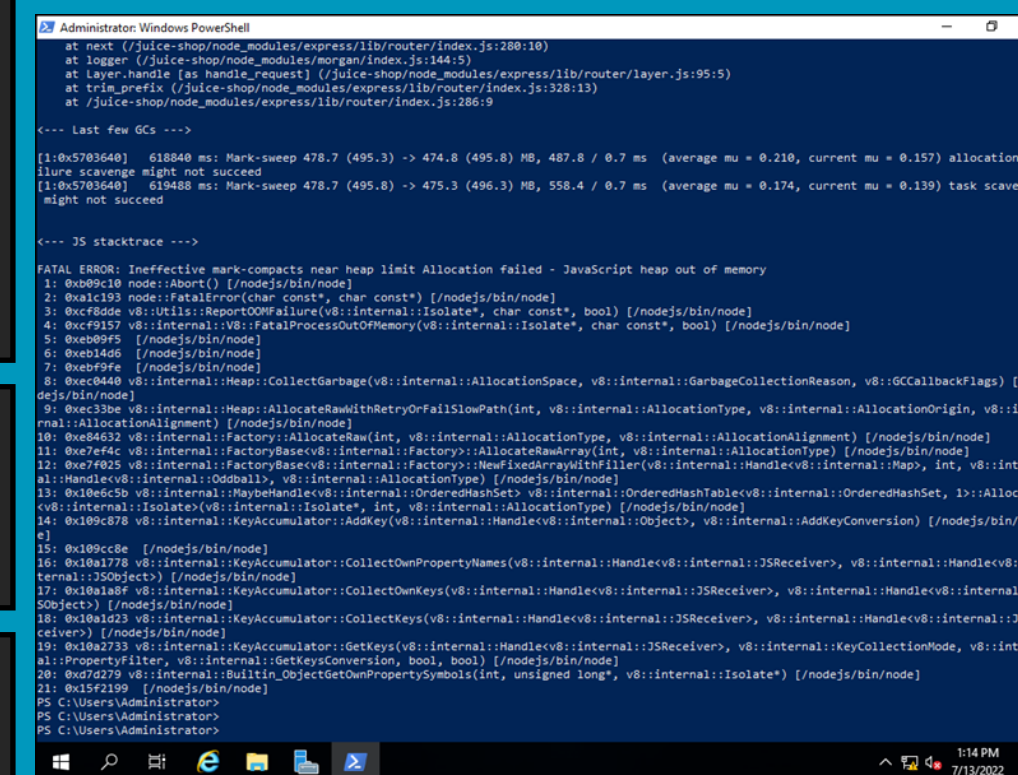
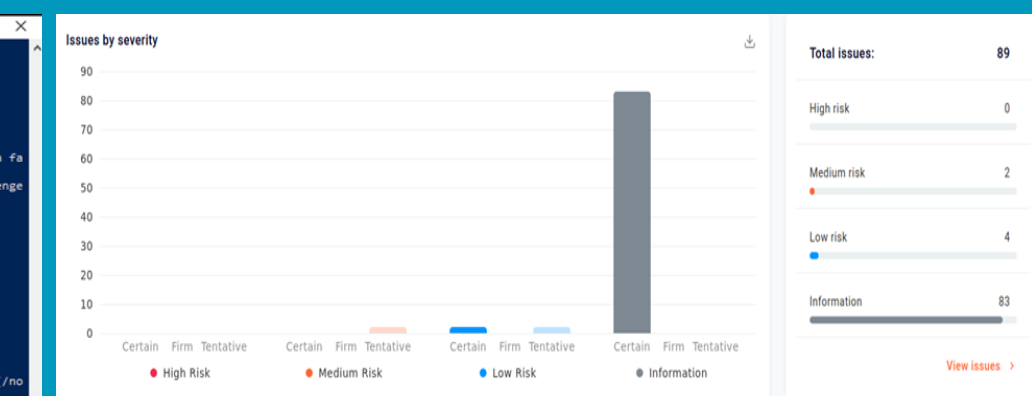


Figure 6



References

1. <https://dhcw.nhs.wales/about-us/>
2. <https://www.imperva.com/learn/data-security/personally-identifiable-information-pii/>
3. Cabinet Office, Government Security, 2018

Table of Figures

1. NMAP Vs OpenVAS
2. OpenVAS Risk Severity
3. OWASP Juice Shop Architecture
4. Simulated Virtual Environment
5. Metasploit Crashing Web Application
6. Burp Suite Scan of OWASP Juice shop

Conclusions & Recommendation

The project was to investigate the various web application and network infrastructure tools, this has provided the author with a greater understanding of the tools and technologies used within the project and allowed them to evaluate each tool again the criteria. The aim of this project was to provide DHCW with a recommendation on Web application and network infrastructure testing tools. Unfortunately, the author has decided to not provide a recommendation at this time but has highlighted additional future workings.