Ocean Graham

Abstract

[Draw your reader in with an engaging abstract. It is typically a short summary of the document.   
When you’re ready to add your content, just click here and start typing.]

402IT – Information Security

Briefing Report



Table of Contents

[Table of Figures 1](#_Toc195538321)

[Introduction 2](#_Toc195538322)

[Current it environment 2](#_Toc195538323)

[findings 3](#_Toc195538324)

[recommendations 4](#_Toc195538325)

[cloud computing 5](#_Toc195538326)

[conclusion 5](#_Toc195538327)

[References 6](#_Toc195538328)

# Table of Figures

402IT – INFORMATion security

# Introduction

In this coursework the author will demonstrate a high degree of understanding of information security and the critical role in plays in guarding information from threats.

The second goal of this coursework is to identify the assets, faults/vulnerabilities and mitigation against these faults/vulnerabilities of the New England Hospital Case Study. Cloud Computing is also explored and elaborated as a strategy to migrate the New England Hospital database from a physical server room to cloud based storage of databases.

This Hospital is of high importance and value, being the first of its kind in Maidstone, Kent. This site currently is focused on COVID medical services, also providing 300 beds for rehabilitation.

Talk about standards?

# Current it environment

The New England Hospital has a large array of assets which allow regular function for the hospital, containing databases, services and other structures. The figure below categorises the identified assets into different categories.

|  |  |
| --- | --- |
| Category | Asset |
| Software | -Windows Server 2016  -Windows Server 2019  -Windows 8  - Windows 10  -Legacy Windows XP  - Linux based SQL database servers  -J2EE Glass Fish application servers  -Web Application Server  -Online Web Services via the Internet  -Building-wide Local Area Network (LAN) |
| Hardware | -Java Resource Adapter Architecture  -Workstations (Working on Windows 8 & 10)  -Removable Media (e.g. USB’s)  -Laptops and Mobile devices |
| Data | -Patients Databases  -Communication Databases  -Financial Databases  -Staff Databases  -Communications Databases  -Passwords & Logins |
| Structural | -Staff  -Facilities |

Figure 1 Asset table

# findings

With the assets found, vulnerabilities have been identified for a majority of the software assets using penetration testing and the Common Vulnerabilities and Exposures (CVE) site. This lists an array of publicly disclosed computer security flaws (<https://www.redhat.com/en/topics/security/what-is-cve>), allowing organisations to share and identify vulnerabilities that may be exposed within their systems.

The table below presents vulnerabilities (according to the CVE) for many of the software assets displayed.

|  |  |  |
| --- | --- | --- |
| Category | Asset | Vulnerability |
| Software | Windows Server 2016 | -End of Life (No more support)  -Remote desktop client allows attackers to execute code over a network. (**CVE-2025-26645**)  -External control of file names & paths via New Technology LAN Manager (NTLM) allowing spoofing (fraud via forgery) over network. (**CVE-2025-24996**)  - Windows Kernal memory info disclosure Vulnerability. (**CVE-2025-21323**) |
| Software | Windows Server 2019 | -End of Life (No more support)  -Remote desktop client allows attackers to execute code over a network. (**CVE-2025-26645**)  -External control of file names & paths via New Technology LAN Manager (NTLM) allowing spoofing (fraud via forgery) over network. (**CVE-2025-24996**)  -Windows Kernal memory info disclosure Vulnerability. (**CVE-2025-21323**) |
| Software | Windows Workstation 8  (Workstation working on Windows 8) | -End of Life (No more support)  -Microsoft Surface Security feature bypass vulnerability. (**CVE-2025-21194**)  **-**A kernel-mode driver in Windows 8 allows an Elevation of Privilege Vulnerability when it fails to properly handle objects in memory. (**CVE-2017-8552**) |
| Software | Windows Workstation 10  (Workstation working on Windows 10) | -Relative path traversal in Remote Desktop Client allows unauthorised attacker to execute code over network. (**CVE-2025-26645**)  **-**Heap-based buffer overflow in Windows Routing and Remote Access Service (RRAS) allows an unauthorised attacker to execute code over a network. (**CVE-2025-24051**) |
| Software | Legacy Windows XP | -End of Life (No more support)  -SQL injection in View User Profile in MicroWorld eScan Management Console allows remote attacker to dump entire database and gain windows XP command shell to perform code execution on database. (**CVE-2023-31702**) |
| Software | Linux based SQL database servers | -IBM Db2 for Linux is vulnerable to a Denial of Service (DoS), under specified non default configurations as the server may crash when using a specially crafted SQL statement by authenticated user.  (**CVE-2024-31882**) |
| Software | J2EE Glass Fish application servers | -SQL injection vulnerability in the UDDI Server allows remote attackers to execute Structured Query Language (SQL) commands. (**CVE-2016-2386**)  -Vulnerability in the Oracle Containers allows remote attackers to affect integrity. (**CVE-2010-0070**) |
| Software | Building-wide Local Area Network (LAN) | -Cross Site Scripting vulnerability allows a remote attacker to escalate privileges via the menu interface of the member center of the background administrator. (**CVE-2025-25960**) |
| Hardware | Java Resource Adapter Architecture | -JNDI injection into JDBC driver, leading to remote code execution. (**CVE-2024-54660**) |

Figure 2 Asset vulnerability table

Vulnerabilities found via penetration testing

* End of Life
* Spoofing
* DoS/DDoS
* SQL Injections
* Phishing
* Escalation of Privileges
* Outdated Hardware

# recommendations

Mitigation strategies

# cloud computing

3 cloud computing systems

SaaS, IaaS, PaaS

Risk and mitigations of cloud

# conclusion

# References