**NAPIER UNIVERSITY   
Group ProjecT 2021  
kENNETH BROWN - 40090523  
SELF EVAULATION**

**Team 14 – Penetration Testing Scenario  
  
Project Manager: Kenneth Brown  
PM Support/ Server Administrator: Davide Pisanu  
Security Team Manager: Tom Neil  
Security Team: Luis Loaysa  
Web Team Manager/ Back-End Developer: Connor Grattan  
Web Team / Front-End Developer: Jake Salt**

**Project Client: Robert Ludwiniak**

**Project Sponsor: Andrew Partridge**

Contents

[**Section 1** - Introduction 2](#_Toc71041951)

[**Section 2** - Teamwork 3](#_Toc71041952)

[**Section 3 –** Project Management 4](#_Toc71041953)

[**Section 4 –** Drive for Results 5](#_Toc71041954)

[**Section 5 -** Conclusion 6](#_Toc71041955)

[**Appendix** 7](#_Toc71041956)

[**1.0 -** 7](#_Toc71041957)

[**2.0** - 7](#_Toc71041958)

[**3.0** - 7](#_Toc71041959)

# **Section 1** - Introduction

This report is for the purpose of self-evaluation and critical reflection on my recently completed Group Project. The team consisted of six members whose names and roles can be found on the cover page to this document. My own role within the team was as the project manager and our client was Robert Ludwiniak. Our projects goal was to create a virtual penetration testing scenatio which is to be used later to develop student labs for fourth year Cybersecurity students. Inside the scenario Robert asked us to include a server and an E-commerce website which was vulnerable to web-based malicious attacks such as SQL injections and Cross-Site Scripting. He also asked that we limit ourselves to using modern OS hardware so that he could attempt to maintain a sense of realism within the scenario and to make improvements on some of the current labs, which still often demonstrate modern pen-testing techniques on relatively outdated operating systems.

# **Section 2** - Teamwork

# **Section 3 –** Project Management

# **Section 4 –** Drive for Results

# **Section 5 -** Conclusion

# **Appendix**

## **1.0 -**

## **2.0** -

## **3.0** -