**NAPIER UNIVERSITY 2021  
Group Project  
Penetration Testing Scenario  
Final Report**

**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** - Executive Summary 2](#_Toc70435462)

[**Section 2** - Delivered Product 3](#_Toc70435463)

[**2.1** – Must-Have Deliverables 3](#_Toc70435464)

[**2.2** – Should-Have Deliverables 3](#_Toc70435465)

[**2.3** – Could-Have Deliverables 3](#_Toc70435466)

[**Section 3 -** Client Approval 4](#_Toc70435467)

[**Section 4 -** Closing Audit 5](#_Toc70435468)

[**4.1** – Team Satisfaction 5](#_Toc70435469)

[**4.2** – Client Satisfaction 5](#_Toc70435470)

[**Section 5 -** Lessons Learned 6](#_Toc70435471)

[**Appendices** 7](#_Toc70435472)

[**1.0 -** MoSCoW Prioritisation Scheme 7](#_Toc70435473)

# **Section 1** - Executive Summary

The team was tasked with creating a virtual cybersecurity platform for carrying out penetration testing. Our client wants to use this platform for teaching and to create labs for fourth-year students. The security-based scenario we were asked to create involves hosting an E-commerce style website inside of an unsecured server. This website was a minimum requirement set by the client; however, the team was given creative freedom to explore implementing other ideas for security exploits within this environment. Several main goals were set at the beginning of the project: -

* **Create a pre-configured virtual environment or set of environments, which can be used to carry out Cybersecurity penetration testing.**
* **Create** **an E-commerce style website within the virtualized environment, designed for simulating and testing web-based cyber-attacks.**
* **Create documentation that explains each step of all successful pen-tests in such a way that they can be easily recreated later for lab purposes.**

In addition to these main goals, the client also required that the platform makes use of modern Operating Systems, the vulnerabilities present could be exploited realistically by the students, and the exploitation of said vulnerabilities can be performed in a logical initiative manner that conveys the idea of privilege escalation. The client stated that they hope to use this work to improve upon the current standard of student labs within pen-testing by creating scenarios that closely resemble situations that are found within real-world business environments. Whilst these additional requirements are desirable, it was acknowledged both by the client and the team during the planning stages that these are potentially unachievable within the scope of the project and were given a lower MOSCOW priority. Some of the major challenges presented to the group during the development phase of this project were as follows: -

* **The scenario was developed by a group of security students who are not yet studying at the level that these labs are intended to eventually teach. This required that the team carry out extensive individual research into many areas that are relatively unfamiliar to their current studies.**
* **Cybersecurity & penetration testing are vast subject areas. The security team had to act quickly to decide which tests were most likely to yield positive results within our environment and avoid scope creep.**
* **Hosting an E-commerce website realistically, but also offline was a challenge due to the nature of online payment systems and their integration into modern websites. The team was not expected to be able to crack modern security systems or reveal any undiscovered vulnerabilities.**

Upon the project's closure, the team has successfully developed several pen-test exploits within the virtual environment and created extensive documentation to support each of these. The individual exploits are intended to be used as separate labs, but also have a logical exploit structure that allows students to move through each test hierarchically. In addition to these exploits, there are still several in progress such as the SQL injection, FTP server exploits, and development of rainbow tables. Future developments of this scenario, outside of the project timeframe, have been discussed with the client.

# **Section 2** - Delivered Product

This section of the report refers to the MOSCOW prioritization scheme, which is found in Section 1 of the Appendices. When comparing the delivered product to the original plan this scheme has been used to show which deliverables were successfully completed for the client. All documentation relating to these deliverables can be found in Section 2 of the Appendices.

## **2.1** – Must-Have Deliverables

* A Virtual-Network was **successfully created and delivered**.
* An unsecured, pre-configured server VM **was successfully deployed and delivered**.
* An E-Commerce style website designed to be intentionally vulnerable **was successfully implemented and delivered**.
* **AT LEAST** one penetration test which exploits vulnerabilities using user-configurations, hardware/software versions, or the website **was successfully created and delivered.**
* Documentation which clearly demonstrates to the reader in a step-by-step format how to recreate the pen-test in a student lab environment **was successfully created and delivered.**
* OVSM (VMWare) Virtual Machine files, a cloned copy of the final websites GitHub Repository and all relevant project documentation **were successfully created and delivered.**

## **2.2** – Should-Have Deliverables

* **AT LEAST** three penetration tests, which demonstrate the exploitation of vulnerabilities across all the configured network elements (Server, Users, Website) **were successfully created and delivered.**
* Network should contain vulnerabilities but should not be left without security entirely (no firewall, no user security, outdated protocols/OS Versions) to maintain a realistic and challenging scenario for student labs. **This was partially delivered. Whilst some layers of security are in place, many of the current security standards had to be disregarded to allow most of our exploits to function appropriately**.
* Wherever possible, exploits should be shown to be utilising the project website. **Five out of the six completed exploits were shown to be exploiting or utilising the projects website.**

## **2.3** – Could-Have Deliverables

* **AT LEAST** five penetration tests, demonstrating multiple exploits of vulnerabilities across all configured network elements. **Six exploits were successfully delivered, with three more still currently in progress outside the scope of the project.**
* A realistic network which adheres to many of the modern security standards that are currently used in real business environments. Vulnerabilities on this network will be carefully tailored and well hidden, to simulate scenarios that could logically occur outside of a lab environment. **This was not delivered successfully. Whilst the group made efforts to maintain realism throughout the network, the final product still requires many unrealistic configuration changes for all exploits to properly function.**
* Self-directed tasks for students, such as locating hidden information within the network architecture. **This was partially delivered. The Cross-Site scripting exploit encourages students to explore online for various payloads upon completion of the step by step that was provided and the unfinished SQLi exploit provides similar opportunities.**

# **Section 3 -** Client Approval

This section is a confirmation of the client’s approval on the delivered product described in this report. The document shown below was signed by the client and has been copied then provided in the report as evidence of the work, completed and delivered, by our team.

Client sign-off

Penetration Testing Scenario

Materials checked against PMIS

* **A pre-configured virtual environment or set of environments, which can be used to carry out one or more types of penetration tests.**
* **An E-commerce style website within the virtualized environment, designed for simulating and testing web-based cyber-attacks.**
* **Documentation which explains each step of all *successful* pen-tests in such a way that they can be easily recreated later for lab purposes.**

I confirm that the results from the project have been completed and delivered as agreed.

Signed:

Date:

# **Section 4 -** Closing Audit

## **4.1** – Team Satisfaction

## **4.2** – Client Satisfaction

# **Section 5 -** Lessons Learned

# **Appendices**

## **1.0 -** MoSCoW Prioritisation Scheme

To allow flexibility in the scope, DSDM Atern uses the MoSCoW prioritization technique. This is a four-level scheme that is applied to the requirements that will be attempted during a timebox. The four priority levels are described in the table below.

**Label Interpretation**

**M** **-** Must-have items are essential for the product or for the business case of the project.

**S -** Should-have items are not essential but are nevertheless important for the quality of the finished product.

**C** **-** Could-have items are features that would be nice to have, but which would not compromise the overall quality if they were missing.

**W** **-** Won't-have items are not included in the current scope - this final category is more important than it first appears.

**M**

* A Virtual-Network
* An unsecured, pre-configured server VM.
* An E-Commerce style website designed to be intentionally vulnerable.
* **AT LEAST** one penetration test which exploits vulnerabilities using user-configurations, hardware/software versions, or the website.
* Documentation which clearly demonstrates to the reader in a step-by-step format how to recreate the pen-test in a student lab environment.
* Final Product hand should contain OVSM (VMWare) Virtual Machine files, a cloned copy of the final websites GitHub Repository and all relevant project documentation in PDF format.

**S**

* **AT LEAST** three penetration tests, which demonstrate the exploitation of vulnerabilities across all the configured network elements (Server, Users, Website).
* Network should contain vulnerabilities but should not be left without security entirely (no firewall, no user security, outdated protocols/OS Versions) to maintain a realistic and challenging scenario for student labs.
* The website should be of particular focus due to the time investment required for web development when designing and deploying an effective web strategy. Wherever possible, exploits should be shown to be utilising the project website.

**C**

* **AT LEAST** five penetration tests, which demonstrate multiple exploits of advanced vulnerabilities across all the configured network elements (Server, Users, Website).
* A realistic network which adheres to many of the modern security standards that are currently used in real business environments. Vulnerabilities on this network will be carefully tailored and well hidden, to simulate scenarios that could logically occur outside of a lab environment.
* Self-directed tasks for students, such as locating hidden information within the network architecture.

**W**

* Most up-to-date Server/Host OS for exploit targeting. The team cannot, reasonably, expect to uncover new exploits, given a modern OS’s high levels of security. This is the type of work currently being carried out by professional pen-testers and is well outside the scope of this university project. The team is focussing on OS models from 2016 onwards.
* A fully functioning payment system for the E-commerce website. Payment systems through banks and browsers are heavily regulated and attempting to break these systems without proper authorization to do so would most likely result in legal action against the individuals within the group or against the school of computing at Napier university.