MOSCOW Priotization REQUIREMENTS

Team 14 – Pen-Testing Scenario

**MoSCoW prioritisation**

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Network should contain vulnerabilities but should not be left without security entirely (no firewall, no user security, outdated protocols/OS Versions) to maintain a realistic and challenging scenario for student labs.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.