Project Summary

Group Project - Penetration Testing Scenario

Purpose

|  |  |
| --- | --- |
| Goal / Outcome | * **Goal: - Provide a set of tools which can be used to create labs for students to practice pen-testing in a simulated scenario.** * **Create one or more challenging scenarios which can be used to test students’ pen-testing skills in a logical way.** |
| Main product | * **A pre-configured virtual environment or set of environments, which can be used to carry out one or more types of penetration test.** * **An E-commerce website which is designed for the purpose of simulating web-based attacks against.** * **Documentation which explains each step of every successful pen-test in a way that it can be easily recreated later for student labs.** |
| High-level Requirements | * **Research a variety of pen-testing methods which are used to exploit ‘known’ (or ‘unknown’?) vulnerabilities in a modern OS, Server, web app or software.** * **Documentation which shows these pen-testing methods being used to successfully exploit these vulnerabilities inside a virtual web or OS test scenario.** * **A set of pen-test tools inside a stable, virtual environment that students & demonstrators can use alongside the provided documentation to carry out penetration testing labs.** * **An E-commerce style website that should be used in conjunction with these tools to simulate web-based attacks such as ‘cross-site scripting’ and ‘SQL injections’.** |

Targets

|  |  |
| --- | --- |
| Duration | Quick and Clean |
| Budget | £0 and 0 Pence |

Major Risks

None, we are the champions.

Roles

TBC