CITS3006 Project 2025

Version:	0.1
Date:	18 September 2025

In this project, you will work in a team to create a vulnerable box for use in penetration testing, and exercise penetration testing techniques.

Project admin

- This project comprises 40% of your final grade, and 40 marks are awarded for it – 20 marks for task 1, and 20 marks for task 2.
- Students will be allocated to a group of 4–5 students for the project.
- After final submission, group members will be asked to evaluate the contributions made by each team member, including themselves, using the Feedback Fruits tool on the Blackboard LMS.
  - A Contribution Factor (ranging from 0.0 to 1.2) is calculated based on these assessments and is used to adjust the final project grade accordingly (with a maximum possible final grade of 100%).
  - It is highly recommended that students keep a spreadsheet (updated weekly) tracking each member's allocated tasks and contributions, and/or use a private GitHub repository to track version control. While these records are not submitted with the project, teaching staff may request to see them if any discrepancies arise during the grading process.
  - Completing these peer evaluations *is* a threshold requirement for receiving marks for the project, but is not itself an assessment. No mark is awarded for it.
- The standard University late penalties apply to ALL members if you defer your group deliverables.

Project timeline

- Weeks 9-10: Team formation and box building
- Week 11: Pen-testing peer boxes
- Week 12: live presentation of pen-testing
- After week 12: Peer evaluation of group members.

Task 0: Team Forming (week 9)

- Teams of 4-5 students have been created and are available in spreadsheet form on Moodle and in MS Teams (here).
- You should get in touch with the other students in your group, and plan how you will tackle the project.
- Appoint one student to be the point of contact (PoC) for teaching staff. Once you've nominated a person, email cits3006-pmc@uwa.edu.au to let staff know who they are.

Task 1: Configure a vulnerable box (weeks 9-10; 20 marks)

Your team of cybersecurity experts is conducting a security exercise for your pen testers. This is done by building a vulnerable web/app/etc. server (you can use any kind of theme you like). Later on, the pen testers will be tasked with finding the vulnerabilities you have "hidden" in the vulnerable web server.

You should use the standard Ubuntu base image provided in Moodle as a starting point.

You can reuse e.g. web app software produced as part of open source projects, but should document in your report what you used, where you got it from, and what changes you made.

Vulnerability requirements

The server should contain vulnerabilities as follows:

- 3 **web vulnerabilities** (e.g. SQLi, XSS, CSRF, file upload)
- 3 **privilege escalation vulnerabilities**

Total: ~**6 vulnerabilities**.

Out of the privilege escalation vulnerabilities, there must be at least 2 ways to gain root access.

Ideally, you want the vulnerabilities to be exploitable, but not so easy to find that they can be automatically found just by running e.g. Metasploit.

What to submit (Friday 11:59 pm, week 10)

You will submit a report, a vulnerable box, and a recorded video demo. (Recorded demos avoid unexpected glitches that can happen during live presentations, and require less scheduling.) Your marker may also get in teach with your point of contact (PoC) to arrange an MS Teams or face-to-face meeting for your group to respond to queries and clarify any issues arising out of the demo or report. (You can have additional people present, but it's recommended to keep it to 2–3 max.)

1. **Report (via Moodle):**
    - Your report should be clear and concise. As long as it contains the necessary sections, the structure is up to you.
    - It should contain a "vulnerabilities" section. List the vulnerabilities you have created, the software they relate to, and provide descriptions of how they can be exploited.
    - It should contain a "vulnerable image" section. Include a link to the VM image shared under deliverable 2, below. If there are any setup instructions, provide them (but ideally, your VM should start any necessary services or software when it is booted).
    - It should contain a "demo" section. Include a link to the uploaded video demo shared under deliverable 3, below.
    - It should contain a "challenges" section. Discuss any challenges you encountered, and how you addressed them.
2. **VM image (.ova, via OneDrive + Teams):**
    - Your point of contact (PoC) should upload the vulnerable image in .ova format to OneDrive, and make it shareable with the MS Teams group `WRK-cits3006 files`.
    - The vulnerable box should be able to be run in VirtualBox 7 on an x86-64 host (Windows or Linux).

3. **Recorded demo video (via OneDrive + Teams):**
    - Submit a **recorded video** showcasing your vulnerable box. The video should be uploaded to OneDrive, and made shareable with the MS Teams group `WRK-cits3006 files`.
    - In your video (20 minutes maximum), you should briefly identify the vulnerabilities, and demonstrate key vulnerabilities being exploited. You don't need to demonstrate all the vulnerabilities.

Hints

- DON'T do everything yourself! High marks aware awarded to groups that demonstrate good penetration testing skills, and who focus on quality over quantity. In the context of this project, "quality" means that you are able to not only demonstrate skills you have learned in the unit, but can also research and apply more advanced skills derived from further research into the topic.
- In the marking, we value *clarity* and *concision*. Think about what someone reading your report and encountering your box for the first time would want to know, if organising training for pen testers. Have you provided tables of contents? Is your PDF easily searchable? Have you provided executive summaries for the busy reader, and presented material using lists or tables where appropriate?

Task 2: Pen-testing Exercise (weeks 11-12, 20 marks)

At the start of week 11, the submitted boxes will be made available via OneDrive + MS Teams.

During week 11, your team will attempt to analyse and exploit other teams' boxes. The emphasis is on reproducible exploitation of a small number of boxes rather than trying to exploit as many boxes as possible.

Aim to identify a small number of boxes where you can exploit at least one as thoroughly as you can, and 1–3 others where you can write up an assessment of their difficulty level to exploit. You should document how you identified these boxes.

Requirements

- Fully exploit **one** peer box and produce a clear, reproducible discussion of that exploitation. Include proof of compromise where possible (screenshots, log excerpts, recorded terminal sessions, or timestamps in the submitted video).
- Provide difficulty assessments for **1–3 additional boxes**. For each additional box you attempted, give a difficulty rating on a 1–10 scale (1 = very easy, 10 = very hard), and a brief justification (a few sentences) explaining the factors that influenced your score (e.g. complexity of the exploit chain, tooling required, time to discovery, need for manual analysis vs. automation).

What to submit (Friday 11:59 pm, week 11)

You should submit a **report (via Moodle)**: a single PDF that includes:

- An executive summary.
- For the fully exploited box: step-by-step description of discovery and exploitation, the commands and tools used, evidence (screenshots, log snippets, video timestamps).
- For each assessed box (1–3): the 1–10 difficulty rating and brief justification.

- Any caveats or limitations (for example, if some parts of an exploit could not be executed due to time or environment constraints).
- You can include screenshots within the PDF or provide clearly labelled links to OneDrive resources such as log files or other attachments (make sure link permissions are correct and shared with the MS Teams group `WRK-cits3006 files`).

Task 2 live presentation (week 12)

- Your team will give a **live presentation** demonstrating some exploits from Task 2.
- A booking sheet will be available in week 11.
- All members are expected to attend the scheduled session, and be able to demonstrate any contributions.
- Demo time: max 20 minutes.

Appendices

Task 1 indicative marks

A submission (consisting of a report, recorded demo and vulnerable box) is classified into one of the following categories:

Not yet satisfactory (0–9 marks / 0–45%) The submitted box fails to implement the types of vulnerability required; the demo fails to demonstrate the vulnerabilities; the report is not aligned with the demo; or responses to marker queries are poor, with a lack of technical details.

Satisfactory (10–13 marks / 50–65%) Submissions in this category should show the following attributes

- The types of vulnerability required are all implemented.
- The demo demonstrates the implemented vulnerabilities.
- The report generally aligns with the demo.
- Q&A answers are reasonable and demonstrate some understanding of the technical details.

Proficient (14–20 marks / 70–100%) Submissions in this category should show the following attributes

- The types of vulnerability required are all implemented, and are of high quality.
- The demo demonstrates the implemented vulnerabilities.
- The report aligns well with the demo, is well-structured, and explains the vulnerabilities clearly.
- Q&A questions are clearly answered and demonstrate a strong understanding of the technical details.
- 1–4 bonus marks (though not taking the marks beyond 100%) may be awarded for demonstration of advanced techniques beyond the taught material.

Task 2 indicative marks

Task 2 (pen-testing exercise and live presentation) is worth 20 marks. Submissions will be classified into categories and awarded marks according to the criteria below.

Not yet satisfactory (0–9 marks / 0–45%) Submissions in this category will be ones that show the following attributes

- The submitted report and demo do not clearly demonstrate a full exploit of any peer box.
- Evidence for claimed exploits is missing, incomplete, or not reproducible.
- Difficulty ratings for other boxes are absent, inconsistent, or unsupported by rationale.
- The live presentation/demo fails to demonstrate technical understanding or is not runnable during the scheduled slot.
- Responses to marker queries are incomplete or show misunderstanding of basic technical details.

Satisfactory (10–13 marks / 50–65%) Submissions in this category will be ones that show the following attributes

- A full exploit of one peer box is documented and demonstrated; evidence (screenshots, logs, video timestamps, commands used) is provided.
- Difficulty ratings for 1–3 other boxes are provided, with short justifications for each rating.
- The report is generally clear, and the demo demonstrates the key exploit steps; the live presentation addresses the main technical points.
- Q&A answers show reasonable technical understanding.

Proficient (14–20 marks / 70–100%) Submissions in this category will be ones that show the following attributes

- A thorough, reproducible exploit of one peer box is documented and demonstrated. The submission includes clearly labelled evidence (e.g. step-by-step commands, output, screenshots, video timestamps) that enables a technical reader to understand and reproduce the exploit.
- Difficulty ratings for 1–3 other boxes are present and justified with concise reasoning (e.g. time required, tooling needed, complexity of exploitation path).
- The written report is well structured and concise, explaining discovery methodology, exploitation technique, and remediation advice for the exploited box.
- The live presentation clearly demonstrates the exploit(s), highlights lessons learned, and the team responds competently to technical questions.
- 1–4 bonus marks (though not taking the marks beyond 100%) may be awarded for: high quality evidence, write-ups that include remediation suggestions, and demonstration of advanced techniques beyond the taught material.