Assignment Specification
School of Computer and Engineering Sciences

Module Code CO7607	**Module Title** Penetration Testing and Active Defence	**Assessment No** 1 of 2	**Weighting** 70%
Title Penetration Testing Report		**In-Year Reassessment Offered** No	**Generative AI** Not Allowed
Summary This assignment requires students to complete a 3850-word Penetration Testing Report, consisting of a Technical Report and Executive Summary. The Technical Report should detail a simulated penetration test, covering methodology, tools, scans, exploits, vulnerabilities, and remediation advice. The Executive Summary should offer a non-technical overview for business stakeholders, highlighting key findings, risks, and recommendations. This task allows students to demonstrate technical skills and develop communication abilities for both technical and business audiences, preparing them for cybersecurity roles.		**Submission Date** 23/06/25 at 13:00 7-day Submission Window Allowed	**Feedback Due** 21/07/25 13:00

Scenario

You are working as a freelance penetration tester. A company known as Chester Research Ventures Ltd has requested a full penetration test of a computer system that plays a critical role in the organization's operations. The company is interested in determining the current security status of this virtual machine and identifying what needs to be done to protect the system from adversaries.

Resources Provided

To support this assessment, you have been provided with:

- A virtual machine image of the Chester Research Ventures Ltd system.
- A Kali Linux virtual machine to serve as the attacker's machine.

Both virtual machines have been provided as .ova files and both can be downloaded from Moodle. **You WILL need** to download and import both within VirtualBox to conduct your penetration test in that environment.

Assessment Overview

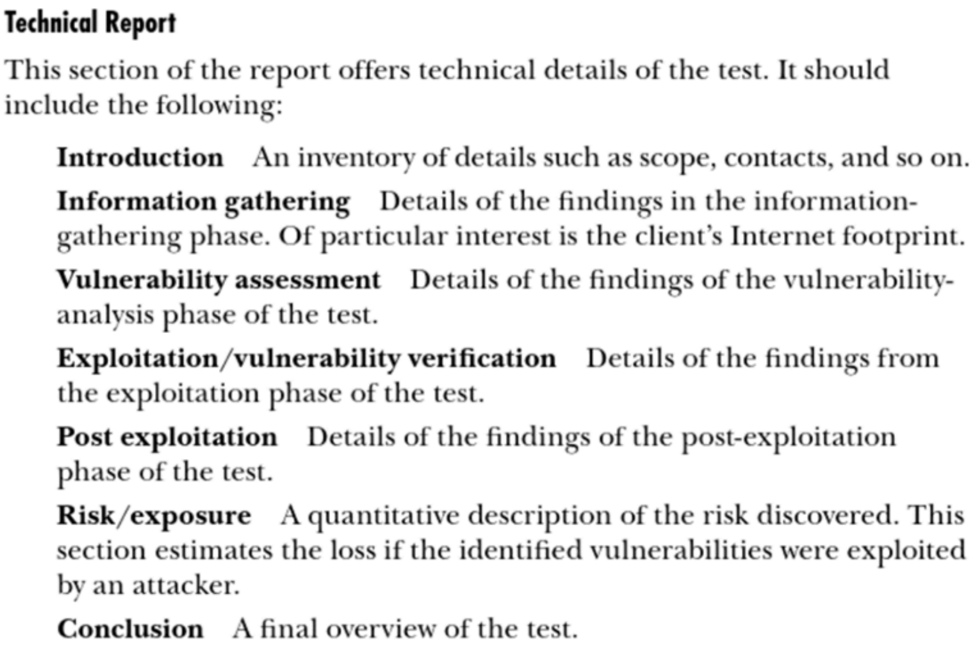
You are required to produce a Penetration Testing Report that consists of two parts:

Part 1: Technical Report (60%)

This section of the report, is a technical summary/overview of the penetration and should be tailored towards technical staff working at Chester Research Ventures Ltd should detail and include.

- An overview of your methodology, including tools and techniques used.
- Any scans or tests performed
- Overview of any vulnerabilities discovered and their severity.
- Any exploits attempted and/or performed.
- An overview of any suggested remediation techniques, informed by academic literature where appropriate.

It is required that you follow the below structure for a technical report as outlined in Weidman (2014);



Technical Report

This section of the report offers technical details of the test. It should include the following:

Introduction An inventory of details such as scope, contacts, and so on.

Information gathering Details of the findings in the information-gathering phase. Of particular interest is the client's Internet footprint.

Vulnerability assessment Details of the findings of the vulnerability-analysis phase of the test.

Exploitation/vulnerability verification Details of the findings from the exploitation phase of the test.

Post exploitation Details of the findings of the post-exploitation phase of the test.

Risk/exposure A quantitative description of the risk discovered. This section estimates the loss if the identified vulnerabilities were exploited by an attacker.

Conclusion A final overview of the test.

Note: The aim of this section of the report should contribute 60% of the overall report, 2310 words. **Please note that ALL terminal screenshots/figures** should clearly show your own individual assessment number i.e., J12345. **No marks can be awarded without your J number being clearly visible**. You may change this by using the below command on the Kali terminal.

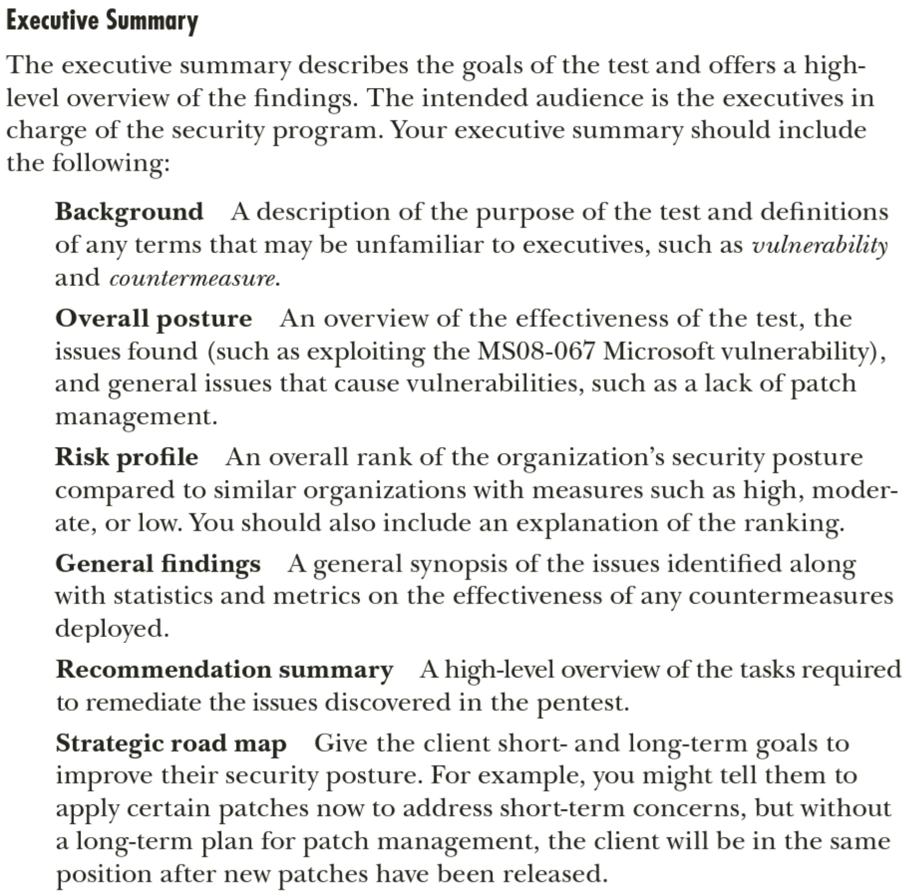
```
sudo nano /etc/hostname
```

Part 2: Executive Summary (40%)

This section of the report should be appropriately tailored towards a non-technical audience (shareholders and business executives) and show aim to;

- Summarise key findings in plain language.
- Describe potential business impacts.
- Highlight the most critical issues.
- Provide concise, actionable recommendations.

It is required that you follow the below structure for an executive summary as outlined in Weidman (2014);



Executive Summary

The executive summary describes the goals of the test and offers a high-level overview of the findings. The intended audience is the executives in charge of the security program. Your executive summary should include the following:

Background A description of the purpose of the test and definitions of any terms that may be unfamiliar to executives, such as *vulnerability* and *countermeasure*.

Overall posture An overview of the effectiveness of the test, the issues found (such as exploiting the MS08-067 Microsoft vulnerability), and general issues that cause vulnerabilities, such as a lack of patch management.

Risk profile An overall rank of the organization's security posture compared to similar organizations with measures such as high, moderate, or low. You should also include an explanation of the ranking.

General findings A general synopsis of the issues identified along with statistics and metrics on the effectiveness of any countermeasures deployed.

Recommendation summary A high-level overview of the tasks required to remediate the issues discovered in the pentest.

Strategic road map Give the client short- and long-term goals to improve their security posture. For example, you might tell them to apply certain patches now to address short-term concerns, but without a long-term plan for patch management, the client will be in the same position after new patches have been released.

Note: The aim of this section of the report should contribute 40% of the overall report, 1540 words.

Additional Information

Learning Outcomes Assessed

- LO1: Critically analyse and evaluate networked systems for vulnerabilities and weaknesses
- LO2: Demonstrate an understanding of access, attack and defence methods
- LO3: Demonstrate the use of some complex penetration testing and active defence tools
- LO4: Carry out a complete and detailed penetration test
- LO5: Demonstrate the ability to report on and advise on networked system security

Assessment Support

Students can get support on this module by speaking to the module leader (Ashley Wood) in sessions, by reaching out via email (ashley.wood@chester.ac.uk) or by booking a 1-2-1 meeting online on the booking page here

Submission Window, Exceptional Circumstances, and Assessment Regulations

You are expected to submit work by the submission date specified at the start of the assignment specification. Some assignments may support a 7-day window in which students can submit work late without penalty and this will be specified below the submission date at the start of this brief. Any work submitted outside of the submission date (or submission window where allowed) will be given a mark of zero.

You can find details about what you need to do if you are unable to submit the assessment on time on the Registry Services Exceptional Circumstances Portal page. Any deferral request must be submitted online within 7-days of the final submission date (or submission window where allowed). In all cases, evidence will be required to support the deferral.

You can find out more about University regulations related to assessment on the Registry Services Assessment Regulations page.

Academic Conduct

The material you submit must be your own work. You must not collude with your peers on your work unless the brief explicitly allows this (such as in the case of group work). The penalties for breaching the academic conduct policy are severe. The minimum penalty is usually zero for that piece of work. Further information is available below:

- Academic Conduct
- Excess Word Count Penalties
- Cite Them Right Online guidance

Generative AI

The use of generative AI tools where not permitted will be treated as a breach of the academic c**onduct** policy.

This assignment **does not** permit the use of any generative AI tools, including but not limited to ChatGPT, Gemini, Copilot, Midjourney, and others.

Submission Information

- The final submission shall be 3850 words (with ± 10% flexibility), submitted as a Word or PDF document to Moodle via a submission link on the CO7607 Moodle page.
- An excess work count penalty of -5 marks per 1000 words excess will apply, e.g., if a 1000-word assignment, 5 marks deducted for 1101-2100 words).
- Permissible word count excludes the student's name, title of module and assignment, references to sources, bibliography, graphs, tables, maps, diagrams, captions and appendices.
- Please note, any work which is submitted elsewhere, other than via the turn-it-in link on the CO7607 Moodle page, will receive a mark of Zero and shall not be marked.
- The use of generative AI tools IS NOT PERMITTED and will be treated as a breach of the academic integrity policy.
- **Work submitted more than 7 calendar days late will NOT be marked and will receive a mark of zero.**

Assessment Criteria Postgraduate

Assignment Task (LOs Covered)	**Fail** (<50%)	**Pass** (50-59%)	**Merit** (60-69%)	**Distinction** (>=70%)
Part 1: Technical Report (60%) (LO1, LO2, LO3, LO4, LO5)	• Incomplete or poorly structured report • Major errors or omissions in methodology or testing • Few or no vulnerabilities identified or discussed • Poor or absent use of tools and techniques • Screenshots/figures missing or otherwise lacking evidence • Limited understanding of security concepts	• Basic structure with some relevant content • Some methodology and tools presented • Vulnerabilities partially identified and described • Limited exploitation or testing evidence • Screenshots included but with minor issues • Demonstrates basic understanding of penetration testing	• Clear methodology and structured approach • Good use of appropriate tools and techniques • Vulnerabilities identified with discussion of severity • Evidence of exploitation supported by screenshots • Good remediation advice with some academic support and referencing in APA7 format.	• Comprehensive and professional structure • Advanced and well-documented use of tools • Deep vulnerability analysis with risk prioritisation • Sophisticated exploitation techniques demonstrated • Excellent use of screenshots with clear identification • Remediation advice supported by academic literature in APA7 format.
Part 2: Executive Summary (40%) (LO1, LO2, LO3, LO4, LO5)	• Unclear or overly technical language • Key findings poorly summarised or omitted • No clear recommendations or business impact analysis • Inappropriate for non-technical audience	• Basic summary of findings using mostly plain language • Some attempt at identifying business impact • Limited or vague recommendations • Partially suitable for intended audience	• Well-written summary with clear findings • Clear explanation of business impacts • Relevant and actionable recommendations • Appropriately tailored to a non-technical audience	• Exceptionally clear, concise, and persuasive summary • Strong understanding of business relevance and impacts • Highly actionable and prioritised recommendations • Excellent communication tailored for executives