Softwarica COLLEGE OF IT & E-COMMERCE | in collaboration with Coventry University

Student Assignment Brief

Contents

Assignment Information

Module Name:	Security
Module Code:	ST6005CEM
Assignment Title:	Coursework: Individual Report
Assignment Due:	1 August 2025 (11:55 PM)

Assignment Credit:	20 credits
Word Count:	2000 words
Assignment Type:	Coursework
Grading:	50% (Core Assessment)

Assessment Overview

You will be provided with an overall grade between 0% and 100%. You have one opportunity to pass the assignment at or above 40%.

Important Notice

The work you submit for this assignment must be your **own independent work**. More information is available in the 'Assignment Task' section of this assignment brief.

Assessed Module Learning Outcomes

The Learning Outcomes for this module align with the marking criteria which can be found at the end of this brief. Ensure you understand the marking criteria to ensure successful achievement of the assessment task.

1. Critically evaluate a range of encryption and authentication methods for a given set of requirements.
2. Critically evaluate the security of an IT ecosystem.

Assignment Task

Task and Mark distribution: Total Marks 100

In this coursework, you will be provided with a vulnerable Machine similar to real-world systems with multiple security flaws. Your task is to perform an intensive **security evaluation** and vulnerability testing on the provided Machine.

You can utilize various evaluation tools, methodologies, or frameworks, providing a detailed justification for each choice. Your goal is to identify as many vulnerabilities as possible, classify them by severity, and conduct an in-depth investigation on three vulnerabilities that you find most critical.

Introduction

1. **Evaluation Objectives and Scope:**
    - Clearly define the objective and scope of the security evaluation.
    - Provide an overview of the systems, applications, or components being tested.
2. **Evaluation Methodologies, Laws, and Compliance Framework:**
    - Mention the methodologies used for the security evaluation (e.g., PTES, WSTG).
    - Explain how the evaluation aligns with relevant laws, compliance regulations, and security standards.

Evaluation Process

3. **Methodology Selection and Justification:**
    - Explain the rationale behind choosing manual exploitation leading to automation as the evaluation method.
    - Justify why these methods are suitable for the evaluation.

Evaluation Results

4. **Summary of Findings:**
    - Summarize the key security risks identified during testing.
5. **Security Vulnerabilities Overview:**
    - Categorize and list the security vulnerabilities found, using a risk-rating system (e.g., CVSS scoring).
6. **Analysis of Three Critical Vulnerabilities:**
    - Select three critical vulnerabilities and provide:

- Introduction to the vulnerability.
- Severity Level (Severe, High, Medium, Low).
- Detailed description, including risks.
- Supporting evidence (screenshots, test results, code snippets).
- Recommendations to fix the identified vulnerability.

Conclusion

- Summarize key findings and implications of the security evaluation.

References

- List at least 15 sources, including books, research papers, security reports, and reputable websites.
- Use proper in-text citations.

Appendix

- Include additional supporting evidence, such as screenshots, payloads, or logs.

Video Demonstration

- Create a video demonstrating exploitation of the vulnerabilities found and exploited.
- The video should include a walkthrough of how the vulnerability was discovered with proper explanation around the Proof of Concept.

Note: For all assignments, submissions must follow strict documentation and presentation guidelines. Your **proof of concept (PoC) video must display your face** and have **clear audio**, explaining the vulnerability, why it exists, and how it could be exploited. The **Linux terminal in the screenshots or the video must be in the format Name@kali** instead of the default kali@kali or any generic system name. If demonstrating **XSS**, ensure that the **pop-up message includes your name in the alert section** as proof of execution. Additionally, **all screenshots must be clear, readable, and deterministic**, meaning they should consistently show verifiable results. To maintain the security and accessibility of sensitive security-related video content, please upload your submissions to a cloud storage service. Create a dedicated, publicly accessible, pre-shared folder, and provide the full access link. This approach avoids the potential for content removal or restriction that may occur on public video platforms like YouTube. Failure to adhere to these requirements may result in a deduction of marks or rejection of your submission.

Submission Instructions

Requirement	Details
File Naming	NAME_studentID
File Format	.docx/.pdf format
Submission Method	Campus 4.0 platform (submission link provided 2 weeks before deadline)

Marking and Feedback

How will my assignment be marked?

Your assignment will be marked by the Module Team using standardized criteria.

How will I receive grades and feedback?

Provisional marks will be released once internally moderated. Feedback will be provided alongside grades release within 2 weeks (10 working days).

What will I be marked against?

Details of the marking criteria for this task can be found in the Assessment Marking Criteria section at the end of this brief.

Grade Requirements

You must achieve 40% or above to pass this assessment. Ensure you understand the marking criteria for successful completion.

Assignment Support and Academic Integrity

Getting Help

If you have any questions about this assignment, please meet your respective module leader or teacher for more information.

Language Standards

You are expected to use effective, accurate, and appropriate language within this assessment task.

Academic Integrity

The work you submit must be your own. All sources of information need to be acknowledged and attributed; therefore, you must provide references for all sources of information and acknowledge any tools used in the production of your work, **excluding Artificial Intelligence (AI)**.

We use detection software and make routine checks for evidence of academic misconduct. Definitions of academic misconduct, including plagiarism, self-plagiarism, and collusion can be found in Student handbook in Campus 4.0.

All cases of suspected academic misconduct are referred to for investigation, the outcomes of which can have profound consequences to your studies.

Support for Students with Disabilities

If you have a disability, long-term health condition, specific learning difference, mental health diagnosis or symptoms, contact the Student Support Office for assistance.

Unable to Submit on Time?

If events prevent you from submitting on time, guidance on extenuating circumstances is available in the Student Handbook or from the Student Support Office.

Administration of Assessment

Module Leader Name:	Arya Pokharel

Module Leader Email:	stw00105@softwarica.edu.np
Assignment Category:	Written
Attempt Type:	Standard
Component Code:	CW1

Marking Criteria

- **Reporting Document Formatting: 20**
- **Evaluation Methodology and Compliance Framework: 10**
- **Identified Vulnerabilities and Severity Classification: 15**
- **In-Depth Analysis and Understanding of Three Critical Vulnerabilities: 25**
- **Exploitation of Identified Vulnerabilities: 15**
- **Manual Exploitation: 15**

Assessment Criteria

0-39	40-49	50-59	60-69	70-100
The submission fails to adequately address the core penetration testing objectives. There is little to no identification of vulnerabilities, and the report reflects a poor understanding of the penetration testing process. Technical analysis is minimal, incorrect, or completely absent, showing no evidence of critical thinking or familiarity with penetration testing methodologies. Supporting artifacts such as code snippets, logs, or screenshots are either missing or used incorrectly, and referencing is poor or	The report addresses some basic penetration testing objectives but contains major omissions or errors. While some vulnerabilities are identified, the analysis lacks depth and is largely descriptive. There is limited evidence of technical coherence, and critical engagement with the testing methods is minimal. Supporting artifacts are sparsely used and may include errors in documentation or referencing. The analysis lacks depth, and the overall presentation is superficial. Conclusions	The report identifies several key vulnerabilities, but some important aspects may be overlooked. Critical analysis is present but tends to be superficial or inconsistently applied. Technical analysis may be overly descriptive in parts, though some basic understanding of penetration testing methodologies is demonstrated. Supporting artifacts such as screenshots, test results, and code snippets are included but may lack comprehensive	The report successfully addresses the penetration testing objectives. A good range of vulnerabilities identified and some evidence of critical review. Technical analysis is generally coherent, demonstrating a sound understanding of penetration testing methods, though it may lack the sophistication or originality of higher-scoring work. A good variety of artifacts is used to support the findings, with mostly accurate and appropriate referencing. Conclusions are solid and reflect a	The submission fully addresses all penetration testing objectives, identifying a comprehensive and well-justified range of vulnerabilities. The report demonstrates a deep understanding of the penetration testing process and exhibits strong critical thinking throughout. Technical analysis is clear, detailed, and insightful, showing mastery of penetration testing tools and methodologies. A wide range of well-integrated artifacts including code, screenshots, logs, and

not done at all. Conclusions are either missing or incorrect, with no attempt to discuss the real-world impact of the identified (or missed) vulnerabilities.	are weak, with limited reflection on the findings, and little understanding is shown regarding the practical implications of the vulnerabilities.	documentation or have referencing issues. The conclusions are present but not particularly deep, and practical implications are considered only at a surface level.	reasonable understanding of the impact of vulnerabilities, with practical implications acknowledged but not always fully explored.	test outputs are provided, all accurately referenced and professionally presented. The conclusions are outstanding, clearly summarizing key findings and offering well-developed reflections on the real-world impact and practical implications of the vulnerabilities discovered.