Student Assignment Brief

This document is intended for Coventry University Group students for their own use in completing their assessed work for this module. It must not be passed to third parties or posted on any website. If you require this document in an alternative format, please contact your Module Leader.

Contents:

The work you submit for this assignment must be your own independent work, or in the case of a group assignment your own groups' work. More information is available in the 'Assignment Task' section of this assignment brief.

Assignment Information

Module Name: Ethical Hacking

Module Code: 7024CEM

Assignment Title: Resit Coursework

Assignment Due: 6pm Monday 11th August 2025

Assignment Credit: 15 credits

Word Count (or equivalent): 2000 words +/- 10%

Assignment Type: Coursework

Percentage Grade (Applied Core Assessment). You will be provided with an overall grade between 0% and 100%. You have one opportunity to pass the assignment at or above 40%.

Assignment Task

You will be given a number of Virtual Machines representing a small office of an SME. You are required to perform a Professional Penetration Testing examination and write a report about your findings and recommendations to improve the security of the system.

The report should have the following (or equivalent) structure:

1. Reconnaissance and target analysis
2. Exploitation (describing in detail the steps you have taken, tools you used)
3. Post-exploitation
4. Recommendations (how to make the target machines secure - this should address all vulnerabilities which you have identified in your assessment, not just the ones you have exploited
5. Conclusions (this should contain evaluation of your work and also describe some alternative approaches you could have taken)

You do not need to provide an Executive Summary. Sections 1-3 of report should contain appropriate screen-shots and sample sessions from your work and any references supporting your findings/decisions. As a guide, your report should be about 2000 words

Submission Instructions:

Submit the coursework by the due date using the link on Aula.

Your assignment should be submitted as a single document (i.e., Word, PDF or Markdown).

If you make use of additional materials (such as GitHub, or supporting videos) you should include a clear link to the supporting material in your report.

Important: In the case of GitHub repositories, they should be set to **private, with** the relevant **teaching staff added as collaborators.** Having a publicly available repository could lead to an academic misconduct case being raised against you, as people have been known to steal work from other student's repos.

Late submissions will be awarded 0 marks. If you have a genuine reason for needing to submit late, you can request an extension from faculty registry.

Marking and Feedback

How will my assignment be marked?

Your assignment will be marked by the course team.

How will I receive my grades and feedback?

Provisional marks will be released via Aula

Feedback will be provided by the module team alongside grades release

You will access the feedback via Aula on the Turnitin platform.

Your provisional marks and feedback should be available within 2 Weeks

What will I be marked against?

Details of the marking criteria for this task can be found at the bottom of this assignment brief.

Assessed Module Learning Outcomes

The Learning Outcomes for this module align to 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. The following module learning outcomes are assessed in this task:

1. Critically discuss the legality and scope of ethical hacking and critically evaluate the technical, legal and ethical issues relating to its application in different environment.
2. Interpret and evaluate penetration testing methodologies and security assessment tools based on the scope, requirements and technologies of the system.
3. Evaluate the security of a system via penetration tests, using an appropriate methodology, analyse potential vulnerabilities related to organisational, policy or technical issues.
4. Evaluate and report the outcomes of a penetration test to a professional standard, recommending and specifying suitable countermeasures.

Assignment Support and Academic Integrity

If you have any questions about this assignment, please see the Student Guidance on Coursework for more information.

Spelling, Punctuation, and Grammar:

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

Academic Integrity:

The work you submit must be your own, or in the case of groupwork, that of your group. 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, including 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 on the Student Portal. All cases of suspected academic misconduct are referred for

investigation, the outcomes of which can have profound consequences to your studies. For more information on academic integrity please visit the Academic and Research Integrity section of the Student Portal.

Support for Students with Disabilities or Additional Needs:

If you have a disability, long-term health condition, specific learning difference, mental health diagnosis or symptoms and have discussed your support needs with health and wellbeing you may be able to access support that will help with your studies.

If you feel you may benefit from additional support, but have not disclosed a disability to the University, or have disclosed but are yet to discuss your support needs it is important to let us know so we can provide the right support for your circumstances. Visit the Student Portal to find out more.

Unable to Submit on Time?

The University wants you to do your best. However, we know that sometimes events happen which mean that you cannot submit your assessment by the deadline or sit a scheduled exam. If you think this might be the case, guidance on understanding what counts as an extenuating circumstance, and how to apply is available on the Student Portal.

Administration of Assessment

Module Leader Name: Antal Goldschmidt

Module Leader Email: **ab2216@coventry.ac.uk**

Assignment Category: Coursework

Attempt Type: MainSit

Component Code: CW

Assessment Marking Criteria

	Reconnaissance **Weighting (10%)**	**Desktop** **Weighting (20%)**	**Server** **Weighting (30%)**	**Recommendations and Discussion** **Weighting 30%**	**Report Structure** Doesn't align to MLO's but it's important. Weighting: 10%
80 to 100%	As 70% with exceptional, discussion and analysis.	As 70% with Exceptional Discussion and Analysis	As 70% with Exceptional Discussion and Analysis	As 70% with exceptional discussion and analysis	As 70+ with exceptional presentation and analysis, good use of references to support arguments.
70 to 79%	Detailed and comprehensive scanning process. One or more tools used to identify structure of the network and services running on it. Scanning process also includes vulnerability identification Comprehensive discussion and analysis of the results of the scanning process. Clear analysis of how the scanning process has led to discovering vulnerabilities	Relevant vulnerabilities identified and used to exploit the system Comprehensive post exploitation tasks are completed, multiple tasks completed. Good discussion and analysis of the process	Initial access to server gained through multiple vulnerabilities. Comprehensive post exploitation tasks are completed, Root access to server gained Persistent connection created etc. Good discussion and analysis of the process	Excellent discussion of security issues found. Issues are classified and discussed using a well-known risk rating system (i.e., OWASP) Clear Suggestions for mitigating flaws are given, Suggestions are relevant to the issues detected. Analysis of how vulnerabilities are related, or fit into the wider security context is given	Clear report structure, headings match the marking criteria. Introduction / Conclusions provide context to the report, giving relevant background to topic, and providing a clear summary of results. Good use of references to support arguments made.

60 to 69%	Detailed scanning phase. One or more tools are used to identify network services. Some use of tools for vulnerability identification. Some discussion of the scanning phase, with analysis of issues found. Discussion goes beyond re-iterating the output of the scanning tools used.	Relevant vulnerabilities identified and used to exploit the system Multiple post exploitation tasks are completed, for example dumping password hashes, and creating a persistent backdoor.	Initial access to server gained through multiple vulnerabilities. Comprehensive post exploitation tasks are completed, Root access to server gained or Persistent connection created etc.	Good discussion of security issues found. Issues are classified and discussed using a well-known risk rating system (i.e., OWASP) Suggestions for mitigating flaws are given, Suggestions are relevant to the issues detected	Clear report structure and presentation. Appropriate introduction and conclusions, summarising reports contents, wider context of the report discussed. Good analysis of reports contents, with use of references to support arguments.
50 to 59%	Appropriate tools used to discover structure of network, and services running on it. Some analysis of the scanning phase, describing how items discovered during scanning can lead to compromise. Although this is limited to re-iterating the tools output. Limited analysis from the student,	Success in comprising desktop Relevant vulnerabilities identified and used to exploit the system Some limited post exploitation tasks are completed, for example dumping password hashes, or creating a persistent backdoor.	Initial access to server gained through one vulnerability Some post exploitation tasks completed, for example dumping passwords, or creating a persistent backdoor	Good discussion of security issues found. Issues are classified and discussed using a well-known risk rating system (i.e., OWASP) Suggestions for mitigating flaws are given, Suggestions are relevant to the issues detected	Clear report structure and presentation. Appropriate introduction and conclusions, summarising reports contents. Limited use of references to support arguments.

40 to 49%	Appropriate tools used to discover the structure of network, and services running on it. Limited discussion of the results, and how they link to exploitation phase	Some success in compromising desktop. Relevant vulnerabilities identified and compromised. Limited (user level) access gained on the system	Some success in compromising server, access to server gained through a single vulnerability. Limited post exploitation tasks completed.	Limited discussion of security issues found. Generic suggestions for improving security, given. However, no specifics for issues detected	More than one of: Poor report structure and presentation Introduction / conclusions limited to re-iterating coursework brief with no context added. Limited use of references to support arguments made
Fail 30, 35%	Results of scanning are presented, (i.e., though a screenshot) no discussion on analysis of the results	Limited success in compromising desktop. Vulnerabilities successfully identified, but not exploited	Limited success in compromising server, potential vulnerabilities identified, but not exploited	Limited discussion of the issues found, no recommendations for addressing security issues	Poor report structure and presentation, Introduction and conclusions limited to re-iterating the coursework brief Limited use of references to support arguments
Fail 0 to 29%	Limited or not attempt made	No attempt made	No attempt Made	No Attempt Made	Poor report structure and presentation, literature not used to support arguments made.