University of Hertfordshire UH
School of Physics, Engineering and Computer Science

Assignment Briefing Sheet (2020/21 Academic Year)

Section A: Assignment title, important dates and weighting

Assignment title:	Assignment 2: Pentesting Server	Group or individual:	Individual
Module title:	Penetration Testing	Module code:	7COM1068
Module leader:	Alexios Mylonas	Moderator's initials:	C.T.
Submission deadline:	**10.05.2021 23:50**	Target date for return of marked assignment:	**25.05.2021**

You are expected to spend about 15 hours to complete this assignment to a satisfactory standard.

This assignment is worth **%** of the overall assessment for this module.

Section B:

Notes for students

- For **undergraduate modules**:
  - a score of 40% or above represents a pass performance at honours level.
  - late submission of any item of coursework for each day or part thereof (or for hard copy submission only, working day or part thereof) for up to five days after the published deadline, coursework relating to modules at Levels 0, 4, 5, 6 submitted late (including deferred coursework, but with the exception of referred coursework), will have the numeric grade reduced by 10 grade points until or unless the numeric grade reaches or is 40. Where the numeric grade awarded for the assessment is less than 40, no lateness penalty will be applied.
- For **postgraduate modules**:
  - a score of 50% or above represents a pass mark.
  - late submission of any item of coursework for each day or part thereof (or for hard copy submission only, working day or part thereof) for up to five days after the published deadline, coursework relating to modules at Level 7 submitted late (including deferred coursework, but with the exception of referred coursework), will have the numeric grade reduced by 10 grade points until or unless the numeric grade reaches or is 50. Where the numeric grade awarded for the assessment is less than 50, no lateness penalty will be applied.
- Late submission of referred coursework will automatically be awarded a grade of zero (0).
- Coursework (including deferred coursework) submitted later than five days (five working days in the case of hard copy submission) after the published deadline will be awarded a grade of zero (0).
- Regulations governing assessment offences including Plagiarism and Collusion are available from https://www.herts.ac.uk/about-us/governance/university-policies-and-regulations-uprs/uprs (refer to UPR AS14)
- Guidance on avoiding plagiarism can be found here: https://herts.instructure.com/courses/61421/pages/referencing-avoiding-plagiarism?module_item_id=779436
- Modules may have several components of assessment and may require a pass in all elements. For further details, please consult the relevant Module Handbook (available on Studynet/Canvas, under Module Information) or ask the Module Leader.

University of Hertfordshire UH
School of Physics, Engineering and Computer Science

Assignment Briefing Sheet (2020/21 Academic Year)

This Assignment assesses the following module Learning Outcomes (from Definitive Module Document):

1. Critically analyse and evaluate security techniques used to protect complex heterogeneous environments and apply their findings for offering advice regarding solutions to decision makers.
2. Apply advanced and current concepts/issues of computer systems risks, vulnerabilities, threats analysis, and software security in the context of a penetration test
3. Use initiative for autonomously conducting and managing a penetration test, within a complex and unpredictable environment, demonstrating a systematic approach of creatively applying knowledge in unfamiliar contexts for solving problems

Assignment Brief:

Scenario:
Assume that you are working as a consultant for an SME which is building its capability in penetration testing. Your client has asked your employer to conduct the penetration test against a server, as they fear they might have already been breached. To their best of their knowledge, the company assumes that the server offers only the following online services: http, b) ssh, and c) vnc.

This is an **individual assignment** that will assess your ability to conduct a full-scale penetration test. Please ensure that in completing these tasks you deploy the techniques you have been taught in your course and, especially, in this module. If you produce work that is not concise and to the point, then marks may be reduced. The deadline for this assignment is the **10.05.2021**.

Task 3

You are expected to undertake a **grey-box Penetration Test**. To guide your activities, you are expected to use the plans that you have produced in Assignment 1.

Information about the **IP address of target** of your test as well as the **schedule to access** it is available on **Canvas**. Specifically, please navigate to the module on Canvas and select the "**Your Assignment IP address and your Access Schedule**" page, which is available under the "**Module Information**" Unit, in order to find more information.

Please look at the Assessment Criteria table, which is provided below, for understanding the expected structure of your report. You are required to present your findings in a factual manner to convince decision makers of a large corporation on business strategies. **Do not provide a narrative of your intelligence gathering activities in the main report.** You may include this in an appendix.

In the Attack Narrative section, you are expected to discuss the attacks you have undertaken and what vulnerabilities you have tested in each attack. In the Vulnerability Details & Mitigation section you are expected to provide a technical explanation of the vulnerabilities you have tested and confirmed (e.g., with a working exploit), as well as offer advice on how to mitigate it. To get full marks for this section you are expected to provide confirmed details and mitigation for three (3) vulnerabilities from the total vulnerabilities that you have found on the target.

You must use the VPN for undertaking this assignment. You must use the allocated to you target (IP address) during your schedule. Failing to do this will result in the deduction of marks.

Assessment Criteria	**Mark Available**
Attack Narrative (not an activity narrative)	20
Vulnerability Detail and Mitigation	20
Report Structure	10
Total	**50**

For clarification questions please make use of the discussion forums on Canvas so that the whole of the student cohort may benefit from the discussion.

Submission Requirements:

You are required to submit a **1500 words text report** in a PDF document using the submission link provided on Canvas. Please note it is your responsibility to ensure you will submit on time. Canvas is a stable platform with a large technical team supporting it. Apropos, it is a software platform. **It is advisable to submit before the day of the deadline**.

You are expected to demonstrate an insight into the implications of the problem introduced in each task by using clear and concise arguments. The report should be well written, showing good skills in creativity and design, as well as well-structured using sections and subsections to ensure its readability**.**

Sentences should be of an appropriate length and the writing style should be brief but informative. Work that is not making sense will be marked down. Write to impress! Aim for excellence. Be pedantic about formatting and presentation.

Marks awarded for:

Please see last page for what the assessors will be looking for in your reports. A rubric will be provided on Canvas.

Type of Feedback to be given for this assignment:

In-course formative feedback and individual personalised summative feedback.

Formative feedback will be given for the tasks through Canvas and during the scheduled sessions as per the module delivery plan. Individual personalised summative feedback will be given through Canvas for the canvas submission. Every week, Review & Reflection questions related to the weekly unit activities will be posted on Canvas. These questions will help you to reflect on the activities you will be undertaking as part of the assessed work for the module, self-assess your work as you progress through the module and help you understand the subject better.

Individual summative feedback will be given through Canvas for the canvas submission.

Feedback is not just the marks and the commentary at the end of the module – it is also the regular verbal advice about your work as you undertake the scheduled activities. If you fail to participate to the scheduled sessions and you fail to engage with the class and with the instructors, you will not receive feedback.

Overall Grade Description

The following descriptions provide the characteristics that would define achievement at the stated levels. An assessment rubric will be made available through Canvas.

Fail (< 40)	Marginal Fail (40 – 49)	Pass (50 – 59)	Merit (60 – 69)	Distinction (>70)
Very limited attack explanation. No vulnerability identification. Very weak report structure. Lack of originality.	Reasonably clear explanation of the attacks against the target VM but it is lacking the appropriate technical depth. At least three vulnerabilities have been identified but the explanation is lacking the appropriate technical depth. No exploitation was attempted, and no mitigation is offered. Report structure is appropriate.	Clear technical explanation of the attacks against the target VM. The web service (port 80) has been fully enumerated. Enumeration findings have clearly informed reasonable exploitation activities. At least three vulnerabilities have been properly identified and discussed at an appropriate technical depth. Some recommendations regarding mitigation are given.	Complete enumeration of the web service (port 80) and at least two more services of the target VM. Enumeration findings have clearly informed complete exploitation and post-exploitation activities. At least three VM vulnerabilities have been identified and discussed at an appropriate technical depth that leads to comprehensive recommendations about possible solutions. Analysis might contain some errors.	High academic learning ability achieved with excellent understanding of the various target VM vulnerabilities (ssh, http, mysql, etc), demonstrating professionalism and methodological thinking in conducting the PenTest. The report can pass professional scrutiny and could be presented to clients.