

# CO4509 - Computer Security

## Assignment 2

Martin Bateman  
mbateman@uclan.ac.uk

April 28, 2020

Due date: 31<sup>st</sup> May 2020 11:59pm

Weighting: 50%

Size: 12 pages, 3000 words

## Assignment Description

WidgetsInc has contracted Benny Vandergast Inc to develop their new web-based store. Benny Vandergast Inc has provided a VMware virtual machine for testing. WidgetsInc have decided to give you the job of evaluating the security of the system provided by Benny Vandergast Inc.

You should perform a security evaluation on the provided virtual machine image. You have not been supplied with either the IP address of the system or any usernames and passwords, you have to discover these as part of your investigation.

## Requirements

Your report should include:

- A description of how you investigated the security of the system.
  - include fully cited information on tools and techniques you used.
- A description of the results obtained.
- A proposal on how to secure the system.
  - you should address each of the security issues you find.

## Learning Outcomes

2. Propose and justify suitable security for a networked computer system.
3. Use a range of security-related tools.
4. Critically evaluate tools and techniques for system security.
6. Research and report on a security-related topic, using appropriate literature.

## Submission

The assignment work should be submitted as a Word document or Portable Document Format to the correct assignment slot on Blackboard<sup>1</sup> before 11:59pm on the 31<sup>st</sup> May 2020.

## Late work

Late work must be submitted to Blackboard in the required assignment slot.

## Penalties for late submission

Except where an extension of the hand-in deadline date has been agreed (using extenuating circumstances forms), lateness penalties will be applied in accordance with University policy as shown in Table 1<sup>2</sup>.

(Working) Days Late	Penalty
up to 5	maximum mark 50%
more than 5	0%

Table 1: Late submission penalty

## Extenuating circumstances

If you believe that you have circumstances that justify an extension of the hand-in deadline for your assignment work, you should use the Extenuating Circumstances procedure. Extensions (to a maximum of 10 working days) can be granted when there are serious and exceptional factors outside of your control. Everyday occurrences such as colds and hay fever do not normally qualify for

---

<sup>1</sup><http://portal.uclan.ac.uk/>

<sup>2</sup>[https://www.uclan.ac.uk/study\\_here/student-contract-taught-programmes.php](https://www.uclan.ac.uk/study_here/student-contract-taught-programmes.php)

extensions. Where possible, requests for extensions should be made before the submission date.

The University considers extenuating circumstances to be conditions that significantly impact on your work. Normally these will cover more than one module. Requests for consideration of extenuating circumstances in respect of assignment work submission, should be made using the MyUCLan<sup>3</sup>. You should speak to your Academic Advisor prior to submitting. Whilst extenuating circumstances are being considered, you should inform relevant module leader, and continue with the assignment.

## Feedback

Feedback will be given to the class within 15 working days of the assignment hand-in date. This may be done in the first fifteen minutes of the lecture. This will be followed by individual written feedback tying to the Learning Outcomes listed in the assignment brief, together with any additional helpful feedback such as areas for improvement and areas for improvement.

## Plagiarism

The University uses an electronic plagiarism detection system where your work could be uploaded, stored and cross-referenced against other material. You should know that the software searches the WWW, an extensive collection of reference material and work submitted by members of the same cohort to identify duplicates.

For detailed information on the procedures relating to plagiarism, please see the current version of the University Academic Regulations<sup>4</sup>.

## Reassessment and Revision

Reassessment in written examinations and coursework is at the discretion of the Course Assessment Board and is dealt with strictly in accordance with University policy and procedures. Revision classes for referrals will take place during 'reassessment revision, appeals and guidance week' as marked on the academic calendar.

The mark for the reassessed component is subject to a maximum of 50%.

---

<sup>3</sup><http://myuclan.uclan.ac.uk/>

<sup>4</sup>[https://www.uclan.ac.uk/study\\_here/student-contract-taught-programmes.php](https://www.uclan.ac.uk/study_here/student-contract-taught-programmes.php)

## Assessment criteria

	Fail (10)	Pass (50)	Merit (60)	Distinction (70)	80	(80)
<i>Investigation</i> (30)	Fail Brief description.	Investigation is superficial. Some security issues have been identified via the use of automatic tools. Only investigates one area of the system e.g. just web shop, OS or the running services.	Investigation includes multiple aspects (OS, services, application etc). Or goes in depth into a single aspect of the system.	Good coverage across three or more aspects (OS, services, application etc). Or goes in depth into a two aspects.	Excellent coverage across all aspects of the system. Pass-words have been recovered rather than overwritten.	
<i>Implications</i> (30)	Brief description.	Poor or obvious implications for each vulnerability found. Or only some implications are addressed or the implications don't match up with the severity of the problem.	Limited description of the issue and the implications. Either all aspect covered but to a superficial level or only goes into detail of a few of the issues found.	Good description of the issue and its implications. All issues addresses.	Excellent description of the issue and its implications. Accurate and concise description of each issue. Each issue includes a description of how to exploit the problem.	
<i>Securing</i> (30)	Brief description doesn't really secure the system.	Poor or obvious way of securing the system, e.g. overall recommendation of just firewall/patching rather than the way of dealing with each problem.	Limited description of how to secure the issues found.	Good description of how to secure the issues found. Each identified issues is addressed.	Excellent description of how to secure the problems found.	
<i>Documentation</i> (10)	Very poor. For example not referenced, doesn't address the question or very poor spelling and grammar making it hard to understand.	Some items are referenced. Poor grammar, spelling.	Referenced. Good spelling, grammar. Layout is consistent and make sense.	Good quality documentation. All items referenced, figures are labelled.	Excellent. Publishable quality.	