**Assessment Specification:**

Practical-based assessment

# (50% of the module mark)

**Assessment Information**

Module Title: **OPERATING SYSTEM SECURITY** Module Code: **COCS71152**

Module Tutors: Asma Patel

**Submission Deadline (via Turnitin ONLY)**: **21st January 2023, 23:59**

## Instructions to candidates

This assignment is the second and final part of the formal assessment for **COCS71152** and is, therefore compulsory. The assignment is weighted at 50% of the course grade. You will be required to work individually, so time management is very important.

When reading this assignment please read all elements fully and understand what is being asked of you, DO NOT rely on your friend to explain what is expected, if you have any issues, please ask the teaching team.

## Your task

You have applied for a job as an IT security engineer. You qualified successfully to the final stage where you are asked to demonstrate practical skills within the area of **operating system security**. Your task is to:

1. To design a methodology, containing at least five steps/techniques, to secure one of the selected Linux operating systems (such as CentOS, Kali Linux or Ubuntu). Methodology could be in the form of a table/bullet points but you should clearly justify proposed steps/techniques, discuss commands/tools that you are planning to use, show their usage and discuss expected results. You can adopt existing operating security methodology, modify it or design your own. Whichever you decide our justification should be supported by the relevant literature. The only information you have been given is that the operating system you are securing, will be facing the external network (the Internet).
2. To practically demonstrate three steps from your methodology. You will need to document it by showing evidence i.e. screen dumps of implemented steps/techniques. This could be, but is not limited to, one of the following security step/technique:
	* Creating a username with a strong password and adding user to a group;
	* Enforcing a password policy that for example updates your system to use sha512 instead of md5 for password protection;
	* Limit SSH access to specific users;
	* Disable unwanted service;
	* Update a system/service;
	* Change file permissions for different users;
	* Add an entry to iptables Firewall Rules;
	* Encrypt files/folders;
	* Show installation of additional packages/tools.

The word count is 1500 words. Your paper must be written in your own words and must include a reference section indicating all your sources of information. You are expected to use appropriate sources for developing your arguments, and an appropriate referencing style as per the University regulations. Your report should be well organised, with appropriate choice of illustrative figures tables and diagrams.

You must ***be very careful not to plagiarise material***.Plagiarism can result in a mark of 0 for the assignment, or even failure of the entire module.

## Plagiarism and Academic Dishonesty

Please do **NOT** copy any other student’s work (or lend other students your work) or copy directly sentences and paragraphs from the Internet unless attributing the section correctly to the author in quotation marks, e.g.

*“The work of Handscomb forms a clear comparison to that of Johnson” Campion (2006).*

In general, try only to quote short sentences and not full paragraphs. Instead, you should as much as possible try to use your own words. As a guide, you should try to limit your usage of direct quotes to around 5 or 7 occurrences within the report. Remember also to put in the full reference in an appropriate style at the end of the report.

Please also note that the content written in the report must be original in relation to your other modules, i.e. you must not copy and reuse content directly from your other modules as this will breach the university’s rules on academic dishonesty. If you are unsure of these rules, please access the following web site:

<http://libguides.staffs.ac.uk/refzone>

## Submission Guidelines

Your final research paper should be word processed and submitted by the deadline. Hence, you need to submit your report at least 15 mins before the deadline.

Your documentation should be submitted in ***electronic format******to the Turnitin plagiarism-checking*** ***service via the link on******the university VLE, Blackboard***. This will be set up near to the deadline to allow you to submit your work. ***Please submit a DOC or PDF version*** of the research paper, otherwise it might NOT be recognised by the Turnitin system. If you have any questions/queries, please contact your tutor.

## Advice

Read the relevant literature, which is extensive, in this area. It is an absolute pre-condition for understanding and justifying any conclusions. It is important that you start your preparation early.

Proof read your work before submitting; check for any grammatical or spelling errors.

If you have any questions or need further clarification on this assignment, please email the tutor.

**Marking criteria**

**Criteria**

**Maximum**

**mark**

**allocation**

**Proposed Security Methodology (at least 5 steps)**

15

**Practical demonstration of (three) security steps/techniques**

30

**Structure, presentation and quality of references**

5

**Total out of 50**