UNIVERSITY OF LONDON

Coursework Brief

MSc Computer Science

Module: CSM060, Information Security

Coursework: October to December 2023 study session – End of Term Coursework Assessment

Submission Deadline: Wednesday, 3 January 2024 by 13.00 Greenwich Mean Time

- Please note: You are permitted to upload your Coursework in the final submission area as many times as you like before the deadline. You will receive a similarity/originality score which represents what the Turnitin system identifies as work similar to another source. The originality score can take over 24 hours to generate, especially at busy times e.g. submission deadline.
- If you upload the wrong version of your Coursework, you are able to upload the correct version of your Coursework via the same submission area. You simply need to click on the 'submit paper' button again and submit your new version before the deadline.
- In doing so, this will delete the previous version which you submitted and your new updated version will replace it. Therefore your Turnitin similarity score should not be affected. If there is a change in your Turnitin similarity score, it will be due to any changes you may have made to your Coursework.
- Please note: When the due date is reached, the version you have submitted last, will be considered as your final submission and it will be the version that is marked.

- **Once the due date has passed, it will not be possible for you to upload a different version of your coursework assessment. Therefore, you must ensure you have submitted the correct version of your coursework assessment which you wish to be marked, by the due date.**

Coursework is weighted at 100% of final mark for the module.

Coursework Description:

The Coursework assessment is aimed at determining the students understanding of the core aspects of Information Security.

The task requires you to demonstrate the ability to investigate security issues in an organisation based on the background information provided below and to present the outcomes of your investigation with clarity as a formal report.

In the first part of the coursework you will assess security risks, threats and vulnerabilities to an organisation by synthesising the findings of security assessment reports produced by different tools, discussed below. In the second part, you will present your findings of any vulnerabilities identified, and propose appropriate information security protection mechanisms.

You will present your findings and recommendations in a report (approximately 3,000 words excluding references, figures, and tables).

Background

Birkbeck College has implemented a new e-commerce application to sell College insignia-branded merchandising through the site http://infosec.updrs.net:443.

The server software was implemented internally and operated from within the College's main data centre. As this is the first major internal development effort of a commercial nature for the College, the Security Manager has requested that a full security assessment is performed. ACME Networks, where you work as Lead Security Consultant, has been hired to perform the required security review of the service and software.

The first step in your investigation is to produce three reports generated by state-of-the-art security tools (covered in the lab section of Topic 6), specifically:

- OWAS ZAP, a black-box web app vulnerability analysis scanner.
- SSL Lab black-box deep analyser of the cryptographic configuration of the server.
- Njsscan, a white-box JavaScript source code analysis of the software produced.

In the second phase of your analysis, your task is to synthesise the technical reports generated by the tools above, analyse their findings and produce a report for the Security Manager on the cyber security risks to this system including your recommendations for mitigating the risks identified.

Your report should address the following:

1. The purpose and scope of the assessment carried out.
2. The assessment methodology followed.
3. Summary and detailed findings of the assessment with risk levels.
4. Actions to mitigate the risks identified.
5. Implications of the above for the College and its ability to conduct its business.

Further Details

Your report should include information about your method of analysis: that is the technical approach you took to analysing the server and how you analysed the data generated by the assessment tools. You should provide evidence of vulnerabilities and include a clear explanation as to why they pose risks. You should propose a solution to address the risks you identify and justify them with supporting research in particular with reference to published advisories such as CVE (cve.org).

In your report, you should follow a formal procedure to evaluate risk levels and the potential impact of threats and vulnerabilities on Birkbeck. You will also be assessed on your ability to identify and prioritise risks in a consistent and comprehensive manner.

To prepare your report, you should conduct your research using a variety of sources including those provided in the module reading list and provide references in the report. Moreover, in reaching your conclusions you should consider the ITS and Data Protection policies of the College available via https://www.bbk.ac.uk/about-us/policies/corporate-policies.

A suggested structure for your report is provided below. You do not have to follow the exact structure of this template which is only a suggestion to assist your work. Several samples of completed

reports produced by commercial providers is also provided for reference and inspiration.

Table of Contents
A table of contents should be included in the report.

List of Tables:
Provide an itemised list of all tables included in the report.

List of Figures:
Provide an itemised list of all figures included in the report.

Structure of the main report body

You should include the following components in the main body of your report:

1. **Executive Summary**: The executive summary should provide an overview of the key points of the report including findings and mitigations. Its purpose is to be shared with individuals who may not have time to review the entire report but must be aware of the key points, such as senior management. The level of details should be such that the reader is able to make informed decisions for the organisation based just on reading the executive summary.

2. **Background**: Describe the organisational context within which this report has been commissioned and its goal and aims. Make reference to relevant organisational policies, role of the commissioning individual and target audience. Make reference to the capabilities of the team conducting the assessment and preparing the report, their track record and any other relevant information such as compliance with international standards.

3. **Assessment Scope**: Describe in detail the specific objectives of the report and the areas covered. Clearly identify security and risk aspects that are included and issues that are beyond the scope of this work. Describe how the report can and cannot be used in the specific organisational setting.

4. **Summary of Findings**: Summarise the key overall findings giving your overall assessment for this service. Identify issues in broad areas and relate them to organisational risks. Address both technical and management concerns.

5. **Summary of Recommendations**: Summarise the key overall recommendations including a go/no-go recommendation for this service. Identify recommendations at various levels including service operation, management of the software development process, integration of risk management policies and controls and refer to specific roles within the organisation.

6. **Detailed Analysis:** This section should include the following elements:

   (a) **Assessment Methodology**: Describe how you collected evidence to inform your report and how you analysed this evidence to reach your conclusions. This should include both elements of the discovery process and fact finding, industry best practice, consideration for corporate policies and your formal approach to assessing and managing risk.

   (b) **Methodology for Security Test Reporting**: Describe what specific technical tests were performed as part of the assessment, justify the purpose of each and detail the areas that they cover. Provide a description of how each test has been performed and any assumptions made. Moreover, describe how you evaluated and prioritised each finding of the technical assessment of the system.

   (c) **Detailed Findings**: Present each technical finding in detail giving reference to related information such as security advisory repositories. For each, describe technical mitigation measures required and identify responsibilities for their implementation.

(d) **Business Risks**: Relate technical risks to risks for the organisation overall i.e. such as those that relate to its ability to carry out its business process and provide a service to its stakeholders including but not limited to students, staff and sponsors.

7. **References:** Any references used in the report should go in this section and correct citation should be used in the text where relevant.

It is of utmost importance that students use their own words in completing the coursework (see note on plagiarism below).

Assessment Criteria:

Please refer to Appendix C of the Programme Regulations for detailed Assessment Criteria.

Plagiarism:

This is cheating. Do not be tempted and certainly do not succumb to temptation. Plagiarised copies are invariably rooted out and severe penalties apply. All assignment submissions are electronically tested for plagiarism. More information may be accessed via: https://learn.london.ac.uk/course/view.php?id=3

Penalties for exceeding the word count:

The content within the main body of text comprises the overall word count, including in-text citations, references, quotes, heading and sub-headings.

- You MUST state an accurate word count (excluding the list of references) at the end of your work. If you do not state an accurate word count your mark will be reduced by 5 marks.
- The content within the main body of text comprises the overall word count, including in-text citations, references, quotes, heading and sub-headings. The cover page, reference list and any appendices do not count towards the overall word count.

- For Coursework elements and the project, there is a maximum word limit. If you exceed the word limit, we will reduce the mark you receive as follows:

Excess number of words over the word limit	**Penalty applied**
More than 10% up to and including 20%	5 marks deducted from original mark.
More than 20%	You will receive a mark of zero (0) for your work.