Systems - Cyber Threats, Vulnerabilities & Countermeasures (CSI_7_SYS)

Coursework – Specification

Implementation of a Cyber Security Mechanism Assessment

Coursework	Additional Information	Issued	Due Date	%Weight
Coursework 2	**This is an individual-based assessment**	**Week 7**	**16 April 2021**	**60%**

Cybersecurity or information technology security (IT security) is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

Coursework 2

This coursework is individual and worth **60%** of the module total. Your objective is to choose and implement **ONLY ONE** defensive mechanism from the ones listed below, that could be used in the cyber-security field to provide protection against any threat. Describe a **use-case scenario** of using the defensive mechanism, and provide and a step-by-step **implementation** and usage guide. The available case studies for defensive mechanisms are:

1. **Developing and usage of a cryptographic Algorithm in Python** (https://docs.python.org/3/) **or C++** (https://www.cplusplus.com/). For this case study, students have to use a programming language and some cryptographic libraries to develop their own complete application (CLI / GUI) that will interact with the user and provide encryption/decryption by using some cryptographic algorithm.

2. **Web-Security protection** (for example against SQL-Injection, XSS e.t.c.). In this case study, students need to develop and demonstrate their own web-application that will include a defensive solution for a given threat. For this purpose you could use HTML (https://www.w3schools.com/html/) and PHP (https://www.php.net/) languages. Alternatively, you could use an existing tool or mechanism (install, environmental setup, usage e.t.c.) that provides protection over the web, demonstrate and discuss its effectiveness.

3. **Implementation of network security mechanism** (firewall, IDS/IPS e.t.c.). For this case study, students need to setup their own network (physical or virtual) implement their defensive mechanism into it and discuss things as network performance, protocols affected, network operations e.t.c.

4. **Use of neural networks for malware detection.**(e.q. https://github.com/PacktPublishing/Mastering-Machine-Learning-for-Penetration-Testing). For this case study, students have to develop some

code and use data-mining techniques and datasets in order to discuss the use of neural networks in cyber-security field.

You could choose a software or hardware product that could provide a solution.

Only 25 students max are allowed to be allocated into each of the above case studies. So, students need to **express their interest** (*via MS-Teams private message*) in a specific topic *within the first two weeks,* and the First-Come-First-Served policy will be followed. Otherwise, a case study will be randomly assigned to students based on availability. Since each student has been allocated to work on a specific case study for the coursework, can only work on the case study that you have been allocated to. You **CANNOT swap** case studies afterwards. ***Beware***, if a different case study will be submitted than the one that has been allocated, there is a high risk be considered out of topic.

The Final Report

Students are required to write a professional report minimum of **2500 words**, describing the work they have done and briefly justifying any details regarding the defensive mechanism. They must document all of their steps, commands issued, and console output in the form of a **scientific report**. The documentation should be thorough enough that your implementation can be replicated step-by-step by a technically competent reader.

Screenshot Requirements

Along, with the documentation, you have to provide screenshots describing the use-case and the defensive mechanism. All evidence provided needs to be followed by a supportive narrative.

Those screenshots could include information as:

- ✓ Networking environment Attacker(e.q. IP address)
- ✓ Tools (GUI/CLI environment) that have been used.
- ✓ Results that show the effectiveness of the mechanism.
- ✓ Any other evidence that could be used as a proof of concept.

Presentation

Students also need to include a short presentation to present their work. For this purpose you need to create a short video (.mp4), duration up to 10 minutes max, that will explain what you have done. Additionally, those who wish they could present to their classmates (via MS-Teams) during the presentation weeks at the end of the semester.

Submission Details

Students will have to submit **3 different FILES:**

i. The main report (.doc, .docx, .pdf), that will include the documentation of the coursework in a scientific format.
ii. A compressed file (.zip), that will include any source code that has been developed, installation files, link or tools that have been used for the implementation.

iii. The presentation video (.mp4), audiovisual material presenting their work. Alternatively, in case that the size of the video is too big, a YouTube or oneDrive link (in a "presentation_link.txt" file) could be used.

The filenames need to have the format:

i. studentID_name-coursework_report.doc (example: 123456_John_Doe-coursework_report.doc)
ii. studentID_name-support_materials.zip (example: 123456_John_Doe-support_materials.zip)
iii. studentID_name-presentation.mp4 (example: 123456_John_Doe-presentation.pdf)

Marking Criteria

Criteria	Excellent (100-71%)	Comprehensive (70-61%)	Pass (60-51%)	Weak (50-41%)	Poor (40-0%)	Total Marks /60
Report Structure and Readability **(Marks 10%)**	Sophisticated, consistent, error free application of relevant topics conventions with great attention to detail. Excellent writing, structure, spelling, grammar and referencing.	Comprehensive application of relevant topics conventions with few errors. Very good writing, structure, spelling, grammar, but with minor errors.	Generally correct application of relevant topics conventions, with some errors and / or inconsistencies. The length of the report is at least 2500 words Sufficiently written with little structure, spelling, grammar with some errors	Poorly written with confusing structure, spelling, grammar and / or errors. Below the minimum of 2500 words	Poorly written, less than 2500 words, with no academic style, structure, spelling, grammar and/or multiple errors.	
Abstract and Introduction **(Marks 10%)**	A well-articulated abstract and introduction that provides a clear, logical, and succinct description of content, objectives, scope and requirements. The organization of the review, which draws the reader's attention to a central concern, debate, or contention.	A well-articulated abstract and introduction that provides a clear, logical description of content, objectives, scope, requirements and organization of the review	Satisfactory abstract and introduction that has a good reflection and description of the content, objective, scope, and organization of the report.	An abstract that articulates some key components of the report. An introduction that outlines the content, scope, and organization of the report	Either no abstract or introduction, or one that poorly or partially situates the reader in the context of the concern, debate, or contention addressed in the report	
Conclusions and Critical Analysis **(Marks 10%)**	Excellent breadth, accuracy and detail in understanding key aspects of subject. Contributes to subject debate. Very good awareness of ambiguities and limitations of knowledge. Provides high-level summary, very accurate and detailed. Very high-quality analysis developed independently. Sustained evaluation and synthesis of resources.	Good depth of understanding of key aspects of subject shown Evidence of coherent knowledge. Very good contribution to subject debate. Very good understanding and interpretation of results.	Demonstrated good understanding of key aspects of subject. Some evidence of coherent knowledge and own critique. Sufficiently summarize the report with good interpretation of results	Weak evidence of superficial understanding of subject. Inaccuracies, does not summarize well the report or lack of succinctness. Some attempt at evaluation and some synthesis of resources.	Little or no evidence of understanding of subject. Inaccuracies. Lack of understanding and interpretation of results, no critical analysis or does not summarize the report.	
Defensive Mechanism						
Description of the mechanism and Use Case(s) **(Marks 15%)**	Shows breadth, accuracy and detail in understanding key aspects of subject. Contributes to subject debate. Some awareness of ambiguities and limitations of knowledge. Knowledge and understanding are consistent and accurately developed with a level of criticality.	Accurate and extensive understanding of key aspects of subject. Evidence of coherent knowledge. Knowledge and understanding are basic/relatively superficial.	Accurate understanding of key aspects of subject. Evidence of coherent knowledge. Knowledge and understanding are detailed and satisfactory.	Some evidence of superficial understanding of subject. Minor Inaccuracies. Knowledge and understanding shows consistent gaps.	Little or no evidence of understanding of subject. Many Inaccuracies. Knowledge and understanding are poor and lacks academic rigor.	
Implementation and scenario Execution **(Marks 30%)**	Excellent problem-solving ability and implementation of the proposed methodologies and solutions. Ability to Adapt to unforeseen practical and theoretical challenges to achieve project objectives. Well crafted technical solution, addressing all aspects of the user requirements.	Very good problem-solving ability and implementation of the proposed methodologies and Solutions. Adapt to practical and theoretical challenges to achieve project objectives.	Sufficient problem-solving ability and implementation of the proposed methodologies and solutions. Some adaptation to practical and theoretical challenges to achieve project	Limited problem-solving ability and implementation of the proposed methodologies and Solutions. Limited exploration of possible solution(s) using established approaches to	Poor or lack of problem-solving ability and implementation of the proposed methodologies and solutions. Little or no exploration of solution(s). Question or	

		Comprehensive technical solution, addressing various aspects of the user requirements.	objectives identified goals. Good technical solution, addressing most aspects of the user requirements.	resolve practical and theoretical problems. Weak attempt at the technical solution, addressing only few aspects of the user requirements.	problem unresolved. Poor attempt at technical proposition.	
Presentation **(Marks 25%)**	Showed excellent confidence & composure. Very clear, persuasive and compelling with skilful use of the presentation format. Presentation addresses the needs of the audience very well.	Were mostly confidence & composed. presentation is clear, mostly persuasive, compelling and skilfully presented. Presentation addresses the needs of the audience to a large degree.	Good use of the presentation format and skills. Presentation takes into account the needs of the audience.	Presentation format is adequate. Showed some confidence & composure, but has room for improvement. Presentation may sometimes not take into account the needs of the audience.	Showed no confidence or composure. presentation format is not used adequately, and the needs of the audience are not taken into account.	
Comments:						**Final Mark:**