COMP1806 **(2024/25)**	**Information Security** **Coursework**	**Contribution** **60% of course**
Module Leader Dr Sakshyam Panda	**Release Date** 11th Oct 2024	**Deadline Date** 22nd Nov 2024

This coursework should take an average student who is up to date with the module content approximately 20 hours. Feedback and grades are normally made available within 21 days from the coursework deadline.

Learning Outcomes: A, B, C, D, E

Plagiarism is presenting somebody else's work as your own. It includes copying information directly from the Web or books without referencing the material; submitting joint coursework as an individual effort; copying another student's coursework; stealing coursework from another student and submitting it as your own work. Suspected plagiarism will be investigated and if found to have occurred will be dealt with according to the procedures set down by the University. Please see your student handbook for further details of what is / isn't plagiarism.

All material copied or amended from any source (e.g. internet, books) must be referenced correctly according to the Harvard reference style.

If you use AI in the process of undertaking your assignment, for example to create an outline of your assignment or to summarize articles, you should acknowledge this by adding a declaration at the end of your work. Check the links below for detailed information on the use of AI for your studies.

- Guidance on how to use AI effectively, and how to reference ChatGPT and other generative AI in your work.
- Declaration of AI Use (also appended to the student guidance).

Your work will be submitted for plagiarism checking. Any attempt to bypass our plagiarism detection systems will be treated as a severe Assessment Offence.

Coursework Submission Requirements

- **An electronic copy of your work for this coursework must be fully uploaded by the Deadline Date.**
- **For this coursework you must submit a single Acrobat PDF document. In general, any text in the document must not be an image (ie must not be scanned) and would normally be generated from other documents (eg MS Office using "Save As .. PDF"). An exception to this is handwritten mathematical notation, but when scanning do ensure the file size is not excessive.**
- **Make sure that any files you upload are virus-free and not protected by a password or corrupted otherwise they will be treated as null submissions.**
- **Your work will not be printed in colour. Please ensure that any pages with colour are acceptable when printed in Black and White.**

Coursework Regulations

- **If you have Extenuating Circumstances, you may submit your coursework up to two weeks after the published deadline without penalty but this is subject to acceptance of your claim by the Faculty Extenuating Circumstances Panel.**
- **Late submissions will be dealt with in accordance with University Regulations.**
- **Coursework submitted more than two weeks late may be given feedback but will be recorded as a non-submission regardless of any extenuating circumstances.**

- **Do not ask the lecturers for extensions to published deadlines - they are not authorised to award an extension.**
- **All courseworks must be submitted as above. Under no circumstances can they be accepted by academic staff.**

Please refer to the University Portal for further detail regarding the University Academic Regulations concerning Extenuating Circumstances claims.

Coursework Specification

Attack vs Defence for Machnine Learning and AI-powered Systems

Admin details

Students are encouraged and allowed to work in teams of 4 or 5 members **(strictly not more than 5).** Half of the team members (at least 2) will be the "Defence" team and the rest of the members will be the "Attack" team. Each team will submit a single coursework file (PDF). **Members of a team must elect a team head who is going to submit the essay to the Moodle area on behalf of the entire team,** while you must include all names of students in this submission. All members of the team will receive the same mark. You must discuss and agree amongst yourselves how the work will be split. **The submission file must strictly adhere the following guidelines to avoid marks reduction, which is usually 10% of the final coursework mark as a penalty for not following the exact guidelines. For example, there is 10% penalty (rounded to the closest 10) if you do not adhere to any of the following:**

- **precisely following the template,**
- **name your file as explained below, and**
- **abide by the rule of a length of strictly 6 pages including references.**

For this coursework, you will need to submit a PDF-format written essay named, e.g. for a team of five members "**COMP1806_2022_Surname1_Surname2_Surname3_Surname4_Surname5.pdf**" where "SurnameX" should be replaced by the surnames of the team memebers. The order of the surnames is irrelevant and you can choose any order for entering the surnames. Alphabetic order is a recommended approach.

The final output will be a **six-pages report** (**including** references) according to the template provided as a separate file in the Coursework folder in Moodle. **This and only this must be used** for preparing your essay. You may organise your sections and subsections the way you find more suitable to your writing style.

Technical details

The goals of this essay are:

- to design a **use case scenario** for assessment.
- to propose and design **an attack graph model** for the selected organisation.
- to propose and discuss different **attacking methods** targeting **Machine Learning (ML)-based assets**.
- to propose and discuss **defending methods** to prevent the exploitation of the ML assets.

You must **select one** of the following use cases for carrying out your coursework:

- healthcare (hospital)
- autonomous vehicles (cars, drones, etc – just one type of them)
- online shopping
- smart homes
- smart cities

Do not forget to cite articles that discuss your attacking and defending methods. You must discuss these methods within the context of your use case rather than blindly repeating their description from the literature. Try to connect the different attacking methods, whenever possible, so that your report has a strong narrative. All articles must be referenced appropriately. Use Google Scholar (https://scholar.google.com/) for finding papers. It also gives you the functionality of copying the reference of any paper you will choose to use. Be consistent and use the same **referencing style, i.e. Harvard**, throughout your essay, as provided in the coursework template.

The assessment of the essay is based on the Assessment criteria in the form of a Rubric on the next page. You will need to **use the knowledge acquired during weeks 1-6**. It is left to you to decide the technical depth of your report as this choice is reflected in the marking scheme.

Marking Scheme – Rubric

The following Rubric matrix demonstrates the exact criteria that your report will assessed against

Grade	Description
Assessment Domain 1: Knowledge and understanding of content (25%)	
Assessment description: Accurate knowledge and critical and comprehensive understanding of the well-established principles, theories, and concepts of their area(s) of study, and of the way in which those principles have been developed. Demonstrates an awareness of different ideas, contexts, and frameworks, and recognition of those areas where the knowledge base is most or least secure.	
0%-29%	Little or no understanding of the discussed and analysed information security concepts. There is very little evidence of engagement with the key elements. Overall, a very unsatisfactory attempt.
30%-39%	A poor understanding of the discussed and analysed information security concepts. There is insufficient evidence of engagement with the key elements. Overall, an unsatisfactory attempt.
40%-49%	Has demonstrated a satisfactory level of understanding of the discussed and analysed information security concepts. There are a few notable omission SECs and there is limited evidence of engagement with all key elements. Overall, a satisfactory attempt at these criteria.
50%-59%	Has demonstrated a good understanding of the discussed and analysed information security concepts. There is also some good evidence of engagement with most key elements with some omission of detail.
60%-69%	There is a very good systematic understanding of the discussed and analysed information security concepts. There is also some very good evidence of engagement with all key elements.
70%-79%	Demonstrates an excellent systematic understanding of the discussed and analysed information security concepts. There is also excellent evidence of engagement with all key elements.
80%-100%	Demonstrates exceptional systematic understanding of the discussed and analysed information security concepts. There is exceptional evidence of engagement with all key elements.
Assessment Domain 2: Use of Research informed evidence (20%)	
Assessment description: An ability to present, evaluate and interpret qualitative and quantitative data, to develop lines of argument and make sound judgements in accordance with basic theories and concepts of their subject(s) of study. Comprehensive range of evidence which is interpreted with insight in its application of context. Some perception and persuasion demonstrated. Explicit understanding of other stances. Range of evidence and critical engagement embedded in work. Can collect and interpret appropriate data and successfully undertake research with a degree of autonomy.	
0%-29%	There is almost no evidence of engagement in relevant background reading. There is no real understanding of the techniques needed for analysis or enquiry into the research around the discussed and analysed information security concepts. You need to spend time researching and engaging with module materials to develop an understanding into these concepts and the research that supports them.
30%-39%	There is a failure to engage with enough relevant literature and, where background reading is referred to there is little evidence that it has been understood. You have little understanding of the techniques needed for analysis or enquiry into the research around the discussed and analysed information security concepts. You need to read much more widely and improve your understanding into these concepts and the research that supports them.
40%-49%	Satisfactory reference is made to background reading, but it is limited in nature and draws on a restricted number of authors. There is some limited evidence of techniques of enquiry. There is some evidence that the literature has helped to inform your thinking and satisfactory evidence of

<table>
<tr><td></td><td>use of some techniques of analysis when researching into the discussed and analysed information security concepts.</td></tr>
<tr><td>50%-59%</td><td>Some good relevant reading is evident and demonstrates good understanding of the issues. There is evidence of some use of established techniques of analysis and enquiry when researching into the discussed and analysed information security concepts. There is also some evidence of good commentary on aspects that include are mostly current research and scholarship into the discussed and analysed information security concepts.</td></tr>
<tr><td>60%-69%</td><td>A very good range of appropriate literature is used. Views are discussed and arguments presented with reference to this literature, and there is evidence of very good deployment of established techniques of analysis and enquiry when researching into the discussed and analysed information security concepts. There is also evidence of very good commentary on aspects of current research and scholarship into the discussed and analysed information security concepts.</td></tr>
<tr><td>70%-79%</td><td>You provide an extensive range of current and appropriate literature to support your strong arguments and different perspectives, and you provide excellent commentary and strong scholarship into the discussed and analysed information security concepts. An excellent ability to deploy established techniques of analysis and enquiry when researching into the discussed and analysed information security concepts.</td></tr>
<tr><td>80%-100%</td><td>An extensively wide range of current and appropriate literature is presented to support your strong arguments and different perspectives, and you provide exceptional commentary and advanced scholarship into the discussed and analysed information security concepts. An exceptional ability to deploy established techniques of analysis and enquiry when researching into these concepts.</td></tr>
<tr><td colspan="2"><b>Assessment Domain 3</b>: Evaluation and analysis (20%)</td></tr>
<tr><td colspan="2"><b>Assessment description</b>: Demonstrates systematic thinking and the ability to critical evaluate arguments and make judgements. Use a range of established techniques to initiate and undertake critical analysis of information, and to propose solutions to problems arising from that analysis. An understanding of the limits of their knowledge, and how this influences analyses and interpretations based on that knowledge.</td></tr>
<tr><td>0%-29%:</td><td>No argument is provided to demonstrate your understanding of knowledge available on the discussed and analysed information security concepts. You present no evidence of a hypothesis and no real exploration of any literature.</td></tr>
<tr><td>30%-39%:</td><td>Little in the way of argument is provided to demonstrate your understanding of knowledge available on the discussed and analysed information security concepts. You present no real hypothesis and explore very little literature around this.</td></tr>
<tr><td>40%-49%:</td><td>A satisfactory ability to present some elements of an argument using your understanding of the knowledge you have researched around the discussed and analysed information security concepts. You present some evidence of a hypothesis and some exploration of this.</td></tr>
<tr><td>50%-59%:</td><td>You demonstrate a good ability to devise and present a mostly clear argument using your understanding of the knowledge you have gained around the discussed and analysed information security concepts. You present evidence of a clear hypothesis and at times you justify your approaches to exploring this.</td></tr>
<tr><td>60%-69%:</td><td>You demonstrate a very good ability to devise and sustain a clear argument. Very good understanding of some of the limits in the knowledge available around the discussed and analysed information security concepts. Very good hypothesis presented and a justified approach to exploring this.</td></tr>
<tr><td>70%-79%:</td><td>An excellent ability to devise and sustain a comprehensive argument. Excellent understanding of both the limits and the gaps in the knowledge available around the discussed and analysed information security concepts. Strong hypothesis presented and well-justified approaches to exploring this.</td></tr>
<tr><td>80%-100%:</td><td>An exceptional ability to devise and sustain a comprehensive argument. An exceptional understanding of both the limits and the gaps in the knowledge available around the discussed and analysed information security concepts. Very strong hypothesis presented and well-justified approaches to exploring this.</td></tr>
<tr><td colspan="2"><b>Assessment Domain 4</b>: Communication, Organisation and Presentation (20%)</td></tr>
<tr><td colspan="2"><b>Assessment description</b>: Produce a coherent and well-structured assessment which effectively communicates information, arguments, and analysis in a variety of forms to specialist and non-specialist</td></tr>
</table>

audiences and deploy key techniques of the discipline effectively. Emerging evidence of innovation and/or well-judged experimentation. Use of clear, accurate English, well organised, with flow and progression.	
0%-29%	No structure presented and the assessment includes a significant number of errors in Standard English. It lacks academic style, and this impedes flow. Further proofreading clearly needed and additional support for academic writing.
30%-39%	Little structure and the work are hampered by errors in Standard English. It lacks academic style and does not flow well. Further proofreading clearly needed and additional support for academic writing.
40%-49%	The structure is satisfactory overall but does need improvement. Many errors appear in the use of Standard English (possibly due to poor proof reading). The work does not flow well in several places, and this affects clarity.
50%-59%	A good structure for the most part. The work observes many academic conventions in style and content and is mostly presented in Standard English, with some errors and omissions. Some sentence structure also needs revision, and this can affect the flow of your work in places.
60%-69%	A very good structure – with clear presentation and organisation of ideas. The work observes almost all academic conventions in style, content and is presented well, mostly using Standard English throughout. The majority of this work uses a style which flows well.
70%-79%	Excellent structure and very well organised ides. The written English is of a very high standard and the work observes all academic conventions in style and content. Excellent flow and style and a pleasure to read.
80%-100%	This assessment is exceptionally well structured and organised. The written English is of an extremely high standard and observes all academic conventions in style and content. The assessment flows exceptionally well and is a pleasure to read.
Assessment Domain 5: Referencing and coverage (15%)	
Assessment description: Sources used are all acknowledged in the text and reference list/bibliography using correct academic citation – including online sources. Bibliography is wide and extensive, and sources cited in text are predominately primary sources. Evidence of broad, independent reading from appropriate sources.	
0%-29%:	The assignment lacks a reference list/bibliography, or it is incorrectly laid out. Referencing system within the assignment (i.e., Harvard) has not been followed and you need further support with this.
30%-39%	The reference list/bibliography has many errors in its layout. Many references in the main text are incomplete or incorrect and may be missing from the bibliography. You need further support with this.
40%-49%	The assignment includes citations within the main body and has a reference list /bibliography. However, this referencing is often inaccurate and/or there are several omissions. Reading list is short and limited. An over reliance on secondary sources
50%-59%	Literature is not always correctly referenced within the text and/or reference list/bibliography. Almost all texts are included in bibliography. Reading list is good in terms of number of sources but there are several secondary sources.
60%-69%	Sources used are almost all acknowledged in the text and the reference list/bibliography, mostly using correct citation – including most online sources. A very good approach to academic practice. Bibliography is very good in its breadth and depth and most sources are primary sources.
70%-79%	Sources used are all acknowledged in the text and the reference list/bibliography, using correct citation – including online sources. Follows an excellent, professional approach to academic practice. Bibliography is also excellent in its breadth and depth and all sources are primary sources.
80%-100%	Sources used are, without exception, acknowledged in the text and the reference list/bibliography, using correct citation – including online sources. Follows an exceptionally strongly professional approach to academic practice. Bibliography is also exceptional in its breadth and depth and all sources are primary sources.