University of Lincoln
School of Computer Science
Assessment Briefing 2023-2024

The use of AI tools to generate all or part of your assessment submission is **not** permitted unless specifically mentioned below.

Module Code and Title: CMP3750M Cyber Security

Contribution to Final Module Mark:
50%

Description of Assessment Task and Purpose:
This is Assessment 2 and is an individual assignment.

During this module you have had the opportunity to explore a range of tools which can be used for various stages of the Kill Chain. You have also used Wireshark to gain insight into network traffic at a local level.
For this assessment you are required to create a software tool that will scan the network and identify the following:

- TCP traffic
- UDP traffic
- DNS servers
- And one other of your choice. This could be IP, HTTP, SMTP, open ports, user accounts, or similar. Please ensure this is has been approved before you add it to your tool.

Generally, this activity would be done using Python, however, the choice of language is left open to you.

The tool must be tested, and the results presented and discussed.

You must:

- Present a critique on the pro and cons of using network scanning tools - planning and background research.
- Development of scanning tool.
- Testing, formulation of results and write-up
- Critique the possible attacks resulting from the use of this tool.
- Provide a reflection on the activity, what you have learned and the implications of this activity. Positive and negative comments are welcome.

.

Learning Outcomes Assessed:

[LO2] differentiate between types of attacks and critically assess their impact.

Knowledge & Skills Assessed:

Subject Specific Knowledge, Skills and Understanding:

Planning and design, Subject-specific knowledge, Literature searching, Referencing.

Professional Graduate Skills:

Effective time management, working under pressure to meet deadlines, problem solving, logical thinking, evaluation, justification.

Emotional Intelligence:

Self-management

Career-focused Skills:

Network operations, critical analysis, reflection

Assessment Submission Instructions:

Please submit the following to Blackboard:

A report of 1500 words +/- 10% using an appropriate report structure.
References, figures, tables and image titles are not included in the word count.
Your report must contain the following:

- How your tool works.
- What results you are able to get from it.
- A critique on the pros and cons of your software including the attacks that could be initiated.
- Your software tool fully commented.

Date for Return of Feedback:
Please see the School assessment dates spreadsheet.

Format for Assessment:
Please submit 1 file containing your paper to Blackboard using this format:

- Font size 11, 1.5 line spacing, 2cm margins,
- Times New Roman or Arial,
- Harvard referencing.

Feedback Format:
Feedback will be in written format and presented on Blackboard.

Additional Information for Completion of Assessment:
Information on how to write a report can be found at:
https://www.grammarly.com/blog/how-to-write-a-report/?gclid=Cj0KCQjw852XBhC6ARIsAJsFPN2IA77O_xx5GPX5t0S8XY0nohqxHlUG08Hcu0ovQB8wC4fuImJl-IUaAjYKEALw_wcB&gclsrc=aw.ds

The library offers writing development. For more information please refer to:
https://guides.library.lincoln.ac.uk/aws

Assessment Support Information:

Additional Reading

A. Kumar Singh and S. Roy, "A network based vulnerability scanner for detecting SQLI attacks in web applications," *2012 1st International Conference on Recent Advances in Information Technology (RAIT)*, Dhanbad, India, 2012, pp. 585-590, doi: 10.1109/RAIT.2012.6194594.

Pete Davies, Theodore Tryfonas, A lightweight web-based vulnerability scanner for small-scale computer network security assessment, Journal of Network and Computer Applications, Volume 32, Issue 1, 2009, Pages 78-95.

Barnett, Richard J and Irwin, Barry, Towards a taxonomy of network scanning techniques, 2008, Proceedings of the 2008 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries: Riding the Wave of Technology.

Important Information on Dishonesty, Plagiarism and AI Tools:

University of Lincoln Regulations define plagiarism as 'the passing off of another person's thoughts, ideas, writings or images as one's own...Examples of plagiarism include the unacknowledged use of another person's material whether in original or summary form. Plagiarism also includes the copying of another student's work'. Plagiarism is a serious offence and is treated by the University as a form of academic dishonesty.

Please note, if you use AI tools in the production of assessment work **where it is not permitted**, then it will be classed as an academic offence and treated by the University as a form of academic dishonesty.

Students are directed to the University Regulations for details of the procedures and penalties involved.

For further information, see www.plagiarism.org