CATE
ACADEMIC YEAR 2023/24

Assessment Brief

Submission and feedback dates

Submission deadline: Before 14:00 on 28-03-2024

Is eligible for a 48-hour late submission window.

Marks and Feedback are due on 02-05-2024.

N.B. all times are 24-hour clock, current local time (at time of submission) in the UK.

Submission details

Module title and code: Secure Computer Networks -UFCFLC-30-2

Assessment type: Practical Skills Assessment

Assessment title: Practical Skills Assessment

Assessment weighting: 100% of the total module mark

Size or length of assessment: Focus is on quality but not quantity.

Module learning outcomes assessed by this task:

1. Demonstrate an understanding of a range of protocols employed at various network layers.
2. Appreciate the significance of end-to-end security in network communication.
3. Communicate the nature and potential of threats to the security of computer networks, systems, and operating systems.
4. Discuss the relative merits of different solutions to these threats for a given system, business, or application.
5. Analyse a typical business/application for security threats, using appropriate models and leading to proposed solutions.

Completing your assessment

You need to cover all the tasks specified in the assessment brief. To be able to provide some genuine attempt to address the required steps.

What am I required to do on this assessment?

This assignment assesses the following module learning outcomes:

- Discuss the relative merits of different solutions to these threats for a given system, business, or application.
- Analyse a typical business/application for security threats, using appropriate models and leading to proposed solutions.

The marks are as follows:

- A report/documentation on the offence use of LLM focusing on one of the OWASP top 10 LLM. 20%
- A report to demonstrate the practical applicability of the 5 Penetration Testing Methodology (Reconnaissance (both passive and active), Scanning, Gaining Access, Maintaining Access, and Reporting), although it might not be possible to perform lateral movement and clean-up, you still need to discuss the concepts and why this is required. 40%
- A Pecha Kucha pitch/presentation summarising Part II key findings with 20 images, each with a narration of 20 seconds. 40%

Broadly speaking, the assignment requires you to document a report exploring various tools that are used within the penetration testing methodology and on the use of AI tools such as ChatGPT.

The assignment is described in more detail in section 2. Working on this assignment will help you to individually assess and understand how to identify if a system is secure or not. It will also enable you to develop the required practical skills to be able to secure a vulnerable system and advise relevant stakeholders on ways forward.

These skills will enhance your employability and improve your ability to get placements or undertake the task of network analysis and penetration testing.

Where should I start?

You are advised to start with Part I– select an appropriate vulnerability. For Part II, select a company and explore using the appropriate tools. If you are not able to complete the whole Pent test steps on a selected bug crowd programme, then select a vulnerable VM to work on.

What do I need to do to pass?

Comprehensive marking criteria are available in each part, specifying the requirements for achieving a passing mark. In general, to secure a minimum pass mark, you should aim to address the question(s) for that part, providing some evidence, with potential areas of incompleteness or ambiguity. Demonstrating an understanding of the topic is vital, and minor gaps in knowledge may be acceptable.

How do I achieve high marks in this assessment?

Each part has its own comprehensive marking criteria outlining the requirements for achieving a high pass mark. To attain a high pass mark, it is essential to fully address the part requirements. Your work should exhibit exceptional clarity of evidence and reflect a comprehensive grasp of the topic.

How does the learning and teaching relate to the assessment?

- The set of regular lab tasks that we are doing in the module will help you with ideas on potential vulnerabilities in systems.
- We have covered lectures on penetration testing and OWASP top 10 for LLM, this will provide you starting point for your assignment.
- During lectures, we regularly contextualised the teaching materials and provided real-world examples of how this can be applied to this assignment.
- You have been introduced to various tools for ethical hacking, feel free to use other tools that are not covered.
- You have been sign-posted to some free online training materials that will enhance the basic knowledge provided during sessions.

What additional resources may help me complete this assessment?

- If you have questions about this assignment, please post them to the discussion board "*Discussion Area*" on Blackboard.
- Questions during Lab sessions and lectures
- Weekly Mentimeter questions and answers during lectures.

What do I do if I am concerned about completing this assessment?

If you have questions about this assignment, please post them to the discussion board "*Discussion Area*" on Blackboard.

UWE Bristol offers a range of Assessment Support Options that you can explore through this link, and both Academic Support and Wellbeing Support are available.

For further information, please see the Academic Survival Guide.

How do I avoid an Assessment Offence in this module?

Use the support available from UWE Student Adviser if you feel unable to submit your own work for this module.

In submitting this assignment, you make the following declaration: not fact-checking and providing citations for any of the work included information obtained from using AI tools will result in an Assessment Offence or mark of zero for that part.

The most common forms of Assessment Offence for this module are related to Plagiarism, contract cheating, falsification, and Collusion. **Do not share your work with others**.

For the research part, ensure the words and work are your own. Do not cut and paste work from other sources. Provide the required fact-checking for part I. Changing a few words or the order of the text or using an online paraphrasing tool does not constitute making this your own work. Ensure your work is cited and the reference list is to UWE Harvard standard.

You are reminded that that is an **INDIVIDUAL** assessment. Working together with others in the completion of this work is regarded as collusion.

Section 2: Tasks to be completed.

There are three parts to be completed for this coursework:

Part I) The use of AI within teaching and learning to test or improve the Knowledge Skills and Ability (KSA) framework is gaining much attention. In this task, you are tasked to explore the use of AI tools for offensive Cyber Security and document your findings. This needs to be done by focusing on one of the OWASP Top 10 for LLM Applications v1.0.1. This will include code examples, examples of vulnerabilities, attack scenarios, preventions etc. This demonstrates the K- knowledge aspect of the KSA framework. You need to fact-check the output from such tools and back it up with appropriate in-text citations, so do not assume that the output from these tools is correct. Hence, you are required to demonstrate the skills of reflection and critiquing text and outputs from AI tools.

Part II) Documentation of the tool and techniques used for penetration testing methodology:

You will need to document using various tools as appropriate for each step and all steps that need to be covered in your report. In this section, you are required to apply what you have learned from Part I where appropriate on a selected company – demonstrating the S – Skills of the KSA framework.

Perform and document as many stages as possible against one of the bounty list of programs, such as https://bugcrowd.com/programs. At least perform the passive reconnaissance phase within the scope provided by the selected company. There is no need to find a bug on the site; you only need to demonstrate the stages. Do not execute any attacks out of scope as listed by the company or any active attack. Staying within the scope means you are within the required legal limits, and the company is participating in the program, which is also legal.

Note: If you are unable to complete an attack against a bug bounty site, then repeat your Pen Test on a vulnerable machine from Vulnerable By Design ~ VulnHub:

Your report should cover at a minimum:

a) Describe what you discovered about the victim system and what tools you used. This should include, for example, open ports and available services.
b) Describe all successful attacks you executed against the system. This should include the attack vector(s) (e.g., service), the tool you used, and how you achieved access/privileged access.
c) Recommend solutions on how to secure (i.e., fix) the vulnerabilities discovered.

Part III) Provide a Pecha Kucha presentation of 20 images in slide format each image will have a 20-second narration/explanation. This will cover your key findings in Part II of this assignment. Hence, the whole pitch should last exactly 6 minutes and 40 seconds. Anything more than that will be marked down.

Section 3: Deliverables

- A written report for Part I and II in a format that can be opened by most computers is to be submitted ONLINE via Blackboard on or before **28/03/2024 @2pm** as an electronic copy in either DOC or PDF format, **no ZIP or compressed format**. Please name the file using your student number.
- A pre-recorded pitch for Part III with your voice and face showing in the recording, using a format that can be opened by most computers. Submission without face showing will get a 0% for this part.

Only one report file is to be submitted with a section for each of Parts I and II.

- A link to your OneDrive Folder or GitLab repository– code/scripts should be properly cited. Please ensure that you have enabled access to your repository by the module leader and module team.
- Instructions – readme file on how to use or where the code/scripts are used.
- You need to submit a detailed report, with screenshots – needs to be clear and readable, to describe what you have done and observed.
- You also need to explain the observations that are interesting or surprising. Please also list the important code snippets and screenshots that need to be readable and explained.
- Simply attaching code or screenshots - need to be clear and readable- without any explanation or demonstration of your understanding of the Learning Outcomes will not receive credits.

All screenshots in the report for command line prompts, must have your student number and date and time in the user prompt, need to be clear and readable. You should also use red colour to indicate root privilege and Blue as a regular user. Or, if you have disability issues in terms of colour, use two different suitable colours and make this clear in your report. Failure to comply with this, the report will get 0 marks.

Marks and Feedback

Your assessment will be marked according to the following marking criteria (see section 4). You have access to BB Discussion area to ask any question and get feedback during lab and lectures sessions. A final assignment feedback will be issues with or before the marks are made available.

You can use these to evaluate your work before you submit it.

1. UWE Bristol's UWE's Assessment Offences Policy requires that you submit work that is entirely your own and reflects your learning, so it is important to:
    - Ensure you reference all sources used, using the UWE Harvard system and the guidance available on UWE's Study Skills referencing pages.
    - Avoid copying and pasting any work into this assessment, including your previous assessments, work from other students or internet sources!
    - Develop your style, arguments, and wording, so avoid copying sources and changing individual words but keep, essentially, the same sentences and/or structures from other sources!
    - Never give your work to others who may copy it.
    - It is an individual assessment, develop your work and preparation, and do not allow anyone to make amends on your work (including proof-readers, who may highlight issues but not edit the work) and

    When submitting your work, you will be required to confirm that the work is your own, and text-matching software and other methods are routinely used to check submissions against other submissions to the university and internet sources. Details of what constitutes plagiarism and how to avoid it can be found on UWE's Study Skills pages about avoiding plagiarism.

Section 4: Marking Criteria/grid.

Marking criteria for **Part I**

Introduction and Context (15 marks)	Clarity of Introduction (5 marks) 0-39%: Unclear or absent introduction, lacking a clear statement of purpose. 40-59%: Basic introduction, with limited clarity and purpose. 60-69%: Adequate introduction but lacking in full clarity and purpose. 70-79%: Clear introduction, effectively setting the context and purpose. 80-89%: Very clear and engaging introduction, demonstrating a strong sense of purpose. 90-100%: Excellent introduction, perfectly setting the stage for the research.	Background and Context (5 marks) 0-39%: Minimal or no background information provided. 40-59%: Basic background information, lacking depth. 60-69%: Adequate background, providing some relevant context. 70-79%: Good background information, giving a solid foundation for the research. 80-89%: Very good background, offering comprehensive context and relevance. 90-100%: Excellent background, demonstrating an exceptional understanding of the context.	Justification for Selection (5 marks) 0-39%: Lack of justification for selecting the OWASP Top 10 LLM issue. 40-59%: Basic justification, with limited rationale. 60-69%: Adequate justification, but lacking depth. 70-79%: Good justification, providing clear reasons for the selection. 80-89%: Very good justification, demonstrating a thorough rationale for selection. 90-100%: Excellent justification, offering a compelling and well-founded reasoning for the selection.	
Analysis and Discussion (40 marks)	Depth of Analysis (10 marks) 0-39%: Superficial analysis, lacking depth and detail. 40-59%: Basic analysis with limited exploration. 60-69%: Adequate depth, covering key aspects of the OWASP Top 10 LLM issue. 70-79%: Good depth of analysis, providing substantial insights. 80-89%: Very good depth, demonstrating a thorough examination of the issue. 90-100%: Excellent depth, offering comprehensive and insightful analysis.	Critical Evaluation (15 marks) 0-39%: Limited critical evaluation, lacks depth and insight. 40-59%: Basic critical evaluation, with minimal depth. 60-69%: Adequate critical evaluation, but lacking thoroughness. 70-79%: Good critical evaluation, providing insightful perspectives. 80-89%: Very good critical evaluation, demonstrating depth and a nuanced understanding. 90-100%: Excellent critical evaluation, offering a comprehensive and nuanced assessment.	Comparison and Contrast (10 marks) 0-39%: Limited or no comparison with other relevant issues. 40-59%: Basic comparison, with minimal relevance to other issues. 60-69%: Adequate comparison but lacking in depth. 70-79%: Good comparison and contrast with other relevant issues.	Use of Evidence and Support (5 marks) 0-39%: Inadequate or no use of evidence to support the analysis. 40-59%: Basic use of evidence, with limited relevance. 60-69%: Adequate use of evidence, supporting key points. 70-79%: Good use of evidence, enhancing the credibility of the analysis. 80-89%: Very good use of evidence, demonstrating

			80-89%: Very good comparison, offering a thorough analysis of similarities and differences. 90-100%: Excellent comparison and contrast, showcasing a deep understanding of the issue within the broader context.	a strong foundation for the analysis. 90-100%: Excellent use of evidence, with a comprehensive and well-integrated approach.
Conclusion and Recommendations (20 marks)	Summary of Findings (10 marks) 0-39%: Ineffective summary, lacking clarity or completeness. 40-59%: Basic summary, with limited emphasis on key findings. 60-69%: Adequate summary but lacking full clarity or emphasis on key findings. 70-79%: Good summary, effectively highlighting key findings. 80-89%: Very good summary, offering a clear and concise overview of key findings. 90-100%: Excellent summary, effectively capturing and emphasizing the most important findings.		Recommendations and Solutions (10 marks) 0-39%: Weak or no recommendations provided. 40-59%: Basic recommendations with limited feasibility.60-69%: Adequate recommendations but lacking in depth or practicality. 70-79%: Good recommendations, providing practical and well-founded solutions. 80-89%: Very good recommendations, offering well-thought-out and feasible solutions. 90-100%: Excellent recommendations, demonstrating a thorough understanding of practical solutions.	
Presentation and Writing (15 marks)	Structure and Organisation (5 marks) 0-39%: Poorly structured, with no logical flow or organisation. 40-59%: Basic structure, with some confusion in organisation. 60-69%: Adequate structure but lacking in full clarity or logical flow. 70-79%: Good structure, with a clear and logical organisation. 80-89%: Very good structure, facilitating a smooth flow of information. 90-100%: Excellent structure, with a clear, logical, and compelling organisation.	Clarity of Expression (5 marks) 0-39%: Incoherent expression, with frequent grammar and language issues. 40-59%: Basic clarity, with occasional grammatical or language issues. 60-69%: Adequate clarity, but some improvement needed in language use. 70-79%: Good clarity of expression, with only minor language concerns. 80-89%: Very good clarity, with clear and concise language. 90-100%: Excellent clarity of expression, with flawless language use.	References and Citations (5 marks) 0-39%: Inadequate or no use of references and citations. Major inaccuracies or lack of proper citation style or not UWE citation style. 40-59%: Basic use of references, with some inaccuracies or missing citations. Inconsistent adherence to citation style. 60-69%: Adequate use of references, but improvements needed in accuracy and consistency of citation style. 70-79%: Good use of references, with accurate citations and adherence to the chosen citation style.	

			80-89%: Very good use of references, demonstrating a strong understanding of citation conventions and accurate citation style. 90-100%: Excellent use of references, with meticulous accuracy and consistent adherence to the chosen citation style. Demonstrates a thorough understanding of citation conventions.

Marking criteria for **Part II**

	0-39%	40-49%	50-59%	60-69%	70-84%	85-100%
	Provides a little demonstration of pen testing skills but is not able to provide details of live passive attacks and little or no evidence of exploits for vulnerable VMs. No reflection and critiquing of results or no citations of sources, and use of inappropriate sources. Missing executive summary for the report. Maily focused on vulnerable VM but not on a selected site. No required meta-data on command prompt as instructed.	Able to provide minimal details of passive attacks and minimal coverage of the pentest methodologies, required and poor coverage. Some references and citations but mainly websites but not peer-reviewed materials. some reflection and critiquing of results including sources and no citations to most of the facts and content of the assignment.	Provided evidence of all required tasks – passive attacks, exploits and demonstrated and applied to the selected company but with little or no context and unclear explanation of the report. Missing citations and references. Minimal evidence of reflection and critiquing of results and other research, and a poor list of references and citations.	Fully addressed the required task pen test methodologies) with a clear report, but failed to contextualise this with other resources, references, and reports. Little evidence or attempt at reflection and critiquing of sources, minimal citation or sources or use of inappropriate sources and/or missing citations.	Provides clear evidence of independent vulnerability testing and your critical evaluation while discussing the scenarios, providing comprehensively critiqued countermeasures, and justifying them. This should be detailed with sufficient citations to relevant references. Good coverage of the selected company, tools and vulnerabilities, pen test methodologies/steps, in-depth coverage of legal and ethical issues on pen testing and clear points and arguments. Provide excellent coverage of the role of social engineering in attacks and pen-testing. Some evidence reflection and critiquing of sources including some citations.	Publishable material: well-presented evaluation of attacks, a clear strategy on how to mitigate such attacks, and well-cited materials on all pen test methodologies addressed: A clear, comprehensive, complete, and well-documented solution to the chosen target site and/or Vulnerable VM and/or live passive attack for a selected participating site/company, together with a detailed report, demonstrating an excellent understanding. Has provided excellent reflection and critiquing of sources including citations sources. Outstanding description of the selected attacks and detailed coverage on the exploit walkthrough and use of additional sources and appropriate citations, An outstanding demonstration of your evaluation and attack strategy. Uses appropriate terminology accurately; professionally presented in both layout on the page and logical structure; impressively presented in an appropriate style; grammatically of an extremely high standard.

Marking criteria for **Part III**

Content (40%)	Understanding of Ethical Hacking (10 marks) 0-39%: Demonstrates minimal understanding of ethical hacking principles. 40-59%: Shows basic understanding but lacks depth and clarity. 60-69%: Adequate understanding with some depth and clarity. 70-79%: Good understanding with clear explanations. 80-89%: Very good understanding with detailed and insightful explanations. 90-100%: Excellent understanding, providing a thorough and insightful exploration.	Presentation Structure (10 marks) 0-39%: Structure is confusing or non-existent. 40-59%: Basic structure with weak transitions. 60-69%: Adequate structure with some coherence. 70-79%: Good structure with clear transitions. 80-89%: Very good structure, facilitating a smooth flow. 90-100%: Excellent structure, enhancing the overall presentation.	Depth of Content (10 marks) 0-39%: Superficial content, lacking depth. 40-59%: Basic content with limited details. 60-69%: Adequate depth with some detailed information. 70-79%: Good depth, providing substantial information. 80-89%: Very good depth, with thorough coverage of key aspects. 90-100%: Excellent depth, demonstrating a comprehensive exploration.	Relevance of Information (10 marks) 0-39%: Irrelevant or tangential information. 40-59%: Basic relevance, with some off-topic points. 60-69%: Mostly relevant information. 70-79%: Highly relevant information with minimal off-topic content. 80-89%: Very relevant information, directly contributing to the topic. 90-100%: Excellent relevance, every piece of information directly supports the topic.
Delivery (30 marks)	Clarity of Speech (7 marks) 0-39%: Incoherent speech, difficult to understand, no or poor quality of video (no face) . 40-59%: Basic clarity, occasional difficulties in understanding. 60-69%: Adequate clarity with some room for improvement. 70-79%: Clear and articulate speech. 80-89%: Very clear and articulate, enhancing overall comprehension. 90-100%: Excellent clarity, making the presentation highly engaging.	Engagement with Audience (8 marks) 0-39%: Minimal or no engagement with the audience. 40-59%: Limited engagement, occasional interaction. 60-69%: Adequate engagement with some audience interaction. 70-79%: Good engagement, maintaining audience interest. 80-89%: Very good engagement, actively involving the audience.	Use of Visual Aids (7 marks) 0-39%: Ineffective or no use of visual aids. 40-59%: Basic visual aids with limited relevance. 60-69%: Adequate use of visuals, enhancing understanding. 70-79%: Good use of visuals, directly supporting key points.	Time Management (8 marks) 0-39%: Poor time management, significantly over or under the allotted time. 40-59%: Basic time management with noticeable deviations. 60-69%: Adequate time management, with minor deviations. 70-79%: Good time management, staying close to the allotted time. 80-89%: Very good time management, with minimal deviations. 90-100%: Excellent time management, precisely adhering to the allocated time.

		90-100%: Excellent engagement, capturing and maintaining audience attention.	80-89%: Very good use of visuals, enhancing overall presentation. 90-100%: Excellent use of visuals, contributing significantly to audience understanding.	
Ethical Considerations (15%)	Ethical Stance (7 marks) 0-39%: Lack of consideration for ethical aspects. 40-59%: Basic understanding of ethical considerations. 60-69%: Adequate consideration of ethical principles. 70-79%: Good understanding of ethical implications in hacking practices. 80-89%: Very good consideration of ethical aspects, demonstrating awareness. 90-100%: Excellent ethical stance, with a deep understanding of ethical principles.		Legal and Moral Implications (8 marks) 0-39%: Minimal or no discussion of legal and moral implications. 40-59%: Basic acknowledgment of legal and moral considerations. 60-69%: Adequate discussion of legal and moral implications. 70-79%: Good understanding and presentation of legal and moral aspects. 80-89%: Very good exploration of legal and moral implications. 90-100%: Excellent analysis of legal and moral implications, demonstrating a comprehensive understanding.	
Overall Impression (15 marks))	Creativity and Originality (7 marks) 0-39%: Lack of creativity or originality, only audio, over allowed time limit. 40-59%: Basic creativity, with limited original ideas. 60-69%: Adequate creativity and some original perspectives. 70-79%: Good creativity, introducing original ideas. 80-89%: Very good creativity, showcasing innovative thinking. 90-100%: Excellent creativity and originality, presenting unique and innovative perspectives.		Confidence and Professionalism (8 marks) 0-39%: Lack of confidence and professionalism. 40-59%: Basic confidence, occasional lapses in professionalism. 60-69%: Adequate confidence and professionalism. 70-79%: Good confidence and professionalism, maintaining a professional demeanour. 80-89%: Very good confidence and professionalism, presenting with a high level of expertise. 90-100%: Excellent confidence and professionalism, demonstrating mastery of the topic with a polished presentation.	