**A picture containing text

Description automatically generatedSoftwarica College of IT & E-Commerce**

ST4063CEM The Security Professional

**Assignment Brief 2022 (Regular)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Module Title**  The Security Professional | | **Ind/Group**  Ind | **Cohort**  Sept 2023 | **Module Code**  ST4063CEM |
| **Coursework Title**  Coursework Component | | | | **Handout date:**  TBD |
| **Module Leader**  Robert Vanwey | | | | **Due date:**  TBD |
| **Estimated Time (hrs):** ST4063CEM Expects 100 hours of self-study over the semester.  **Word Limit\***: 3000 words | **Coursework type:**  One coursework scenario report and one practical skill test | | | **% Of Module Mark**  Coursework:50%  Practical skills test:50% |
| **Submission arrangement online via Softwarica Moodle:** Phase Tests will be conducted via the ST4063CEM module page. ALL project details on the course Moodle Pages.  **Mark and Feedback date:** Mark from Phase Tests immediately with feedback to follow the next week. Mark and feedback from Individual project viva expected within 3 weeks.  **Mark and Feedback method:** All marks are delivered by Moodle. Phase Test feedback is delivered in class while Individual project viva feedback is usually delivered in the file of comments from the viva marker. | | | | |

|  |
| --- |
| **Module Learning Outcomes Assessed:**  1. Show strong cybersecurity leadership skills both practical and theoretical which is crucial for a secure culture, and management styles affect teams and organizations differently.  2. Define and describe threat, vulnerability, and risk in the context of cybersecurity and exploit one of the vulnerabilities.  3. Develop a targeted CV for a chosen cybersecurity career, highlighting relevant qualifications, skills, and experience.  4. Demonstrate core technical skills appropriate for level 4 students in cybersecurity, including a good understanding of Windows and Linux, and the ability to use standard tools. |
| Coursework First Component includes one element:   1. Scenario report (50%)   Coursework Second Component includes one element:   1. Skill Test (50%)     These make up 100% of the module mark. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. **Skill Test (50%)**   Practical skills test performed in the labs of the Skills Development 1 module and a bit intermediate. The passing grade for this assessment is 75%. Specifics of the test will be provided at the time of the test. It will be designed to assess the various concepts and skills taught in this module.   1. **Scenario Report (50%)**   This individual coursework is handled by everyone. The Coursework is specific to the students from the Ethical Hacking and Cyber Security degree course. This assignment is intended to assess your wider understanding of the subject. The bulk of the marks is awarded for the discussion element and the technical aspects. Focusing on both the technical, you are expected to examine (Why, How, and What) this means in terms of security, and the legal and ethical context. In many of the theoretical topics there is no clear-cut answer, so remember to strengthen your argument with relevant citations from appropriate sources.  **Task and Marks Distribution:**  You are tasked with simulating a cybersecurity project for a CTF company that has a broken access control vulnerability. The company has equal funds at the start, but decisions made during the project will lead to different outcomes. Your role is to analyze the impact of the simulated attack on the system's security, identify the broken access control vulnerability and the threat exploited, and evaluate risk assessment and mitigation strategies. The project will conclude with the submission of a tailored CV and cover letter for a cybersecurity job, showcasing your qualifications, skills, and experience while demonstrating your understanding of key competencies.   1. In the given scenario how would one penetrate the system and find vulnerabilities within it? **[25]** 2. Identify the threat, vulnerability, and risks considering the vulnerability. **[20]** 3. Suppose you are the leader of a cybersecurity company then explain how professional communication and teamwork in the context of red teaming and blue teaming concerning vulnerability and how management and leadership can affect the overall decision-making task should be carried out along with appropriate frameworks). **[25]** 4. Suppose you are applying to a company that is hiring a cybersecurity analyst. Now make a CV and a cover letter for the job based on the skills and experience gained. Necessary assumptions can be made**. NOTE: You must cover this question on a separate page otherwise mark will be reduced. [20]**   **Specifically, your report should include the following.**   1. Title page/Cover Page. 2. Executive summary 3. Table of Contents: This should list the report sub-sections in decimal notation and should be auto-generated. 4. Introduction 5. Body of the report: Appropriate headings in the body of the report should be used. 6. Conclusion 7. Reference list: All references must be in CU APA 7th Referencing Style.   (*Note: The word count would only be counted from the introduction to the conclusion section while the first page should be well designed,* *and the CV and cover letter must be in Picture Format at the end of the document after references.)*  **Plagiarism Note**  As with all assessed work, both the research and written submission should be your work. When submitting this work, you are explicitly indicating that you have read the rules on plagiarism as defined in the University regulations and that all work is, in fact, your own, except were explicitly referenced using the accepted referencing style.  **Mark Distribution:**   |  |  |  | | --- | --- | --- | | S.N. | Task | Marks | | 1 | Penetrate the system and understand vulnerabilities within the system | 25 | | 2 | Identify the threat, vulnerability, and risks considering it as a chosen sector | 20 | | 3 | Suppose you are the leader in a cybersecurity company then explain how professional communication and teamwork in the context of red teaming and blue teaming concerning the vulnerability and how management and leadership can affect the overall decision making. (The task should be carried out along with appropriate frameworks) | 25 | | 6 | Making of proper CV and cover letter. | 20 | | 7 | Referencing and Documentation | 10 | |  | **Total** | 100 |     **Note:**  The Individual Coursework is assessed by the module leader that takes place at the end of the semester by giving some configuration work in the Lab. Students should attend their allocated slot and can only take them at another time under exceptional circumstances with the permission of their Course Director.   1. Students are encouraged to use their user-defined data structure rather than the built-in data structure of a given language. 2. You are expected to use the Coventry University APA style for referencing. For support and advice on this, students can contact the Centre for Academic Writing (CAW). 3. Please notify your academic services team and module leader for disability support. 4. The college cannot take responsibility for any coursework lost or corrupted on disks, laptops, or personal computers. Students should therefore regularly back up any work and are advised to save it on cloud-based services. 5. If there are technical or performance issues that prevent students from submitting coursework through the online coursework submission system on the day of a coursework deadline, an appropriate extension to the coursework submission deadline will be agreed upon. This extension will normally be 24 hours or the next working day if the deadline falls on a Friday or over the weekend. This will be communicated via your Module Leader. 6. Collusion between students (where sections of your work are like the work submitted by other students in this or previous module cohorts) is taken extremely seriously and will be reported to the academic conduct panel. This applies to both coursework and exam answers. 7. A marked difference between your writing style, knowledge, and skill level demonstrated in class discussion, and test conditions and that demonstrated in a coursework assignment may result in you having to undertake a Viva Voce to prove the coursework assignment is entirely your work. 8. If you make use of the services of a proofreader in your work, you must keep your original version and make it available as a demonstration of your written efforts. 9. You must not submit work for assessment that you have already submitted (partially or in full), either for your current course or for another qualification of this college, apart from resits, where for the coursework, you may be asked to rework and improve a previous attempt. This requirement will be specifically detailed in your assignment brief or specific course or module information. Where earlier work by you is citable, i.e., it has already been published/submitted, you must reference it. Identical pieces of work submitted concurrently may also be self-plagiarism. |

**Learning Outcomes matrix:**

|  |  |
| --- | --- |
| **Question No.** | **Learning Outcomes Assessed** |
| **Coursework 1** Scenario report | **1, 2, and 3** |
| **Coursework 2 –** Skill Test | **4** |

**Mark allocation guidelines to students**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 0-39 | 40-49 | 50-59 | 60-69 | 70+ | 80+ |
| Work mainly incomplete and /or weaknesses in most areas | Most elements completed; weaknesses outweigh strengths | Most elements are strong, with minor weaknesses | Strengths in all elements | Most work exceeds the standard expected | All work exceeds the standard expected |

**Mark allocation guidelines to students:** **marking rubric.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Criteria** | **0** | **1** | **2** | **3** | **4** |
| **Topic 1 (25 marks)**  Penetrate the system and find vulnerabilities within it. | Not Submitted or Late Submission | Some attempts were made to penetrate the system but were unable to do so. | Some penetration was attempted, but lacking experience and knowledge | Adequate penetration was attempted, demonstrating a good understanding of theories and practical issues with evidence of reading beyond the recommended minimum | Extensive knowledge of defense and offense with the mindset of a leader, demonstrating an excellent understanding of theories, practical issues, and strong evidence of reading beyond the recommended minimum. |
| **Topic 2 (20 marks)**  Identify the threat, vulnerability, and risks of the vulnerability | Not Submitted or Late Submission | Limited understanding of the threat, vulnerability, and risks in the chosen sector. | Adequate identification of the threat, vulnerability, and risks in the chosen sector using a risk matrix. | Comprehensive identification of the threat, vulnerability, and risks in the chosen sector using a detailed risk matrix and clear mitigation strategies. | A thorough analysis of potential threats, vulnerabilities, and risks to the chosen sector. Demonstrates professional level understanding and applies critical insight. Comprehensive use of risk matrix to evaluate and prioritize risks. Extensive evidence of additional research. |
| **Topic 3 (15 marks)**  Making proper communication mechanisms for teamwork the vulnerability | Not Submitted or Late Submission | A limited range of sources was used with unclear presentation and analysis. Addresses most objectives with some omissions and unclear structure. | The task is covered but lacks detail or clarity in communication mechanisms. Some relevant sources were used but limited critical analysis. | Adequate explanation of communication process and tools for teamwork. Demonstrates a good understanding of communication theories and practical issues. Shows evidence of additional reading. | Thorough understanding of effective communication mechanisms for teamwork. Clear explanation of professional communication process and tools used. Proper use of relevant sources, strong critical analysis, and evidence of reading beyond the recommended minimum. |
| **Topic 4**  **(10 marks)**  Importance of decision-making and impact in terms of the vulnerability along with the framework | Not Submitted or Late Submission | Limited understanding of management leadership and its impact on cyber security decision-making. Lacks framework design. | Basic understanding of management leadership and its impact on cyber security decision-making. Provides an incomplete framework but lacks depth and critical analysis. | Good understanding of management leadership and its impact on cybersecurity decision-making. Provides adequate framework with evidence of critical analysis and evaluation. | Extensive understanding of management leadership and its impact on cybersecurity decision-making. Provides comprehensive and sophisticated framework with extensive evidence of additional research or reading. Demonstrates the ability to apply knowledge and insights to real-world scenarios. |
| **Topic 4**  **(20 marks)**  CV and Cover Letter | Not Submitted or Late Submission | Some understanding is demonstrated but is incomplete. The CV and cover letter lack basic information and proper formatting, and the language used is inadequate. | The CV and cover letter are adequate but lack depth and detail. Some information is not relevant, and the language used is too general. | The CV and cover letter are well-structured and contain relevant information. The language used is appropriate and demonstrates a good understanding of the targeted industry. | The CV and cover letter demonstrate a proper level of attention to detail and professionalism. The language used is precise and effective, indicating a clear understanding of the targeted industry and the applicant's strengths and accomplishments. Adequate evidence of research or reading beyond the recommended minimum is provided. |
| **Topic 5**  **(10 Marks)**  Proper  Reference, Report Structure | Not Submitted or Late Submission | General report style with some errors in formatting and structure, limited use of figures and tables, and inconsistent or missing referencing. | Adequate general report style with appropriate formatting and structure, some use of figures and tables, but still lacking in referencing or with errors in referencing. | Well-structured report with good use of figures and tables, with proper referencing, and some evidence of reading beyond the recommended minimum. | Well-structured report with a consistent structure, effective use of figures and tables, comprehensive and extensive referencing, and extensive evidence of reading beyond the recommended minimum. |