PUSL3132
Ethical Hacking

20 CREDIT MODULE

ASSESSMENT: 50% Coursework

MODULE LEADER: Professor Nathan Clarke

MODULE AIMS

- To introduce and understand the role and responsibilities of a penetration tester, including relevant legal and operational consequences.
- To introduce strategies that can be utilised in enabling a structured and methodical analysis of organisational systems and vulnerabilities.
- To introduce the tools and techniques that are applied within the field and be able to explain the findings in a meaningful fashion.

ASSESSED LEARNING OUTCOMES (ALO):

1. Demonstrate a systematic understanding and critique the roles and responsibilities of a Penetration Tester with consideration for legal and ethical issues.
2. Apply appropriate tools and techniques that can be used to both attack and defend systems in given scenarios.
3. Interpret and analyse results from a range of tools and document findings in an appropriate manner.

Coursework Assessment

With the ever-increasing complexity of technology, it is imperative that organizations are able to robustly test and evaluate the security of their computer systems and networks. Penetration testing forms a critical component of that evaluation.

Scenario Overview:

Clarke's Ceylon Team are a traditional Sri Lankan tea producer. The Managing Director has decided to ensure the organisation is fully digital in all its operations. The MD is however concerned about the risks posed by this move and has hired the services of a penetration testing consultant (you!).

Your task is to perform a thorough examination of the company and provide a detailed report on the security and vulnerabilities of their systems. It is expected you will identify and explain the methodology taken, provide a rationale to explain what tests/tools are being used in addition to evaluating the vulnerabilities that exist within the system. It is important you reflect on the legal and ethical implications of this approach. Given the size of the organization, they do not have a testbed available – so testing will be performed on operational systems – so please consider and mitigate the impact of the evaluation. Based upon the examination, the report should also contain the necessary information for the company to mitigate the identified risks. ***It is critical that you undertake a practical-based pen-test of the systems and document this in your report.***

In order to facilitate the examination, a virtual environment has been created with a number of critical systems you would expect. This has been created on an isolated subnet and additional information will be provided by the academic on how to access this.

This is a group report consisting of between 3-4 members. Additional instructions will be provided on how to select your groups via the DLE. You are free to structure your report as you feel appropriate, but the following key aspects need to be addressed as part of the submission (please also refer to the assessment criteria with which your report will be assessed against); also provide commentary detailing what the different options are when you present and analyse various key terminologies (e.g. file systems and computer systems):

- Introduction (i.e., what you are covering and why, how the report is structured)
- Background (i.e. literature detailing why penetration testing is required and common mistakes made)
- Testing Methodology (i.e., testing strategy and rationale for the approach and tools selected)
- Evaluation (i.e., results of the penetration test with accompanying narrative for a novice to understand)
- Mitigation (i.e. what controls and configurations are required to improve the level of security and reduce the likelihood of compromise)
- Your conclusion (i.e., what are the critical findings and mitigations)

Assessment Criteria:

The overall length of the report (excluding appendices) should not exceed the word limit, which is dependent upon the size of the group.

Group Size	Word Limit
3	4000
4	5000

Relevant supporting information may be included as appendices if required. The report will be assessed on the depth and breadth of your analysis and overall quality of presentation. It will be expected to have appropriate introduction and conclusion sections, and to be supported by references.

The marking scheme will be structured as follows:

- Introduction (5%)
- Background (10%)
- Testing Methodology (15%)
- Evaluation (35%)
- Mitigation Recommendations (25%)
- Conclusions and Supporting Evidence (references) (10%)

It is important that all members of the group contribute towards all sections of the report. It is NOT appropriate for one member to complete the background section and another group member to complete the evaluation.

In terms of marking, all group members will receive the same marks. However, should a group member not actively contribute to the creation of the report, please ensure you email me (nclarke@plymouth.ac.uk) and **all members of the group** (to ensure transparency) and I will note this against your group. Upon assessing the submission, I will ensure the report is marked on an individual basis.

Use of Artificial Intelligence and Machine Learning:

- You may use AI to assist in undertaking research on what a penetration test is, how to undertake a test and to explore tools and techniques you may use. Please take considerably care over the quality and reliability of the information you find – it can often be incorrect. I would recommend you use traditional methods and ensure good quality citations.
- You may use AI to grammar check your final report.
- You may **NOT** use AI to write any aspect of the report. No sentences or paragraphs should be included where the idea/concept or purpose of the sentence has not first been written by you.

Criteria	Fail (<40%)	3rd/Pass (40%+)	2.2 (50%)	2.1 (60%+)	1st (70%+)	Grade
Introduction	The introduction fails to describe the subject domain, the context or structure of the report.	A sound introduction into the subject domain and purpose. Lacks in supporting evidence.	A logical introduction with evidence of planning and structure.	A concise and clear introduction with appropriate context and structure being provided. Good number of appropriate references.	An excellent, concise and clear introduction with appropriate context and structure being provided. Well referenced with supporting evidence throughout.	**/5**
Background	Too little relevant background material at an appropriate level.	An appropriate level of background material has been identified and discussed	An good level of background material has been identified and discussed.	A robust level of background material has been identified and discussed. Utilising good quality sources.	An excellent level of background material has been identified and discussed. Good quality sources used throughout.	**/10**
Testing Methodology	No meaningful reference to a logical testing approach.	Evidence of a sound yet simple approach to the pen test.	Good evidence of understanding and applying testing methodologies	Excellent evidence of understanding and applying testing methodologies.	A comprehensive methodology, reflective of current practice and mindful of additional operational factors.	**/15**
Evaluation	Little meaningful practical testing and poor discussion of the results.	Clear yet basic demonstration of undertaking a pen test across the principle phases.	A good demonstration of pen testing with accompanying presentation and analysis of the results	Excellent use of pen testing throughout and a detailed presentation and analysis of the results	A comprehensive and complete pen test using appropriate tools and a well structured presentation of the results with accompanying analysis and discussion.	**/35**
Mitigation Recommendations	No meaningful and logical mitigations provided.	Evidence of appropriate mitigations but with limitations on the coverage and analysis.	Good evidence of appropriate mitigations with accompanying analysis.	A very good set of appropriate mitigations with accompanying rationale and analysis.	A complete set of mitigations, well aligned to results from the pen test with accompanying analysis and discussion.	**/25**
Conclusions & References	The conclusions do not flow from the presented report. Few if any relevant references.	Some attempt at deriving appropriate conclusions has been made. They do logically flow from the analysis presented. Some evidence of appropriate references	Some relevant and interesting insights that logically flow from the report.	A solid attempt at concluding the report, logically applied. Failed to provide an insight into the implications. Good use of a number of relevant sources in an appropriate manner	The concluding remarks are a logical extension of the arguments presented. Clear and concise. Evidence of a good understanding of the implications of the analysis. An excellent set of appropriate peer-reviewed references	**/10**
Feedback/Overall	*Additional feedback*					**/100**

General Guidance

Extenuating Circumstances

There may be a time during this module where you experience a serious situation which has a significant impact on your ability to complete the assessments. The definition of these can be found in the University Policy on Extenuating Circumstances here: https://www.plymouth.ac.uk/student-life/your-studies/essential-information/exams/exam-rules-and-regulations/extenuating-circumstances

Plagiarism

All of your work must be of your own words. You must use references for your sources, however you acquire them. Where you wish to use quotations, these must be a very minor part of your overall work.

To copy another person's work is viewed as plagiarism and is not allowed. Any issues of plagiarism and any form of academic dishonesty are treated very seriously. All your work must be your own and other sources must be identified as being theirs, not yours. The copying of another persons' work could result in a penalty being invoked.

Further information on plagiarism policy can be found here:

Plagiarism: https://www.plymouth.ac.uk/student-life/your-studies/essential-information/regulations/plagiarism

Examination Offences: https://www.plymouth.ac.uk/student-life/your-studies/essential-information/exams/exam-rules-and-regulations/examination-offences

Turnitin is an Internet-based 'originality checking tool' which allows documents to be compared with content on the Internet, in journals and in an archive of previously submitted works. It can help to detect unintentional or deliberate plagiarism.

It is a formative tool that makes it easy for students to review their citations and referencing as an aid to learning good academic practice. Turnitin produces an 'originality report' to help guide you.

Referencing

The University of Plymouth Library has produced an online support referencing guide which is available here: http://plymouth.libguides.com/referencing.

Another recommended referencing resource is Cite Them Right Online; this is an online resource which provides you with specific guidance about how to reference lots of different types of materials.