University of Northampton

CSY2084 – Ethical Hacking and Penetration Testing			
Date of Issue:	22nd March 2024	**Last Date for Submission:**	19th May 2024 23:59
		Module Tutor:	Tolulope Odunsi

Assignment Guidelines – Please read carefully.

1. The University of Northampton's Policy on Plagiarism & Mitigating Circumstances will be strictly implemented.

2. This is an individual assignment.

3. Write your name and student ID on the first page (title page) of your word document.

4. This assignment must be completed and submitted electronically to the correct submission point 'Coursework Submission' on the module's NILE page.

5. You must follow the submission guidance provided under the section '**Assessment Submission**'. **Failure to follow the above submission guidelines may result in a capped or fail grade**.

6. Answers to all parts of the assignment MUST be submitted to achieve a passing grade for the assignment.

7. The module tutor reserves the right to invite you for a viva-voce to discuss your submission. **Failure to give a convincing viva-voce will result in a grade of F**.

Introduction:

This assignment accounts for 75% of the module marks. It covers the materials covered in the module from pre-engagement planning to post-exploitation.

Scenario:

XYZ Accounting, a local accounting firm, has recently begun to store more client data electronically. With a growing client base and a reputation for providing high-quality financial services, the firm relies heavily on its internal network infrastructure to manage client data, financial records, and other sensitive information. Concerned about the increasing threat landscape and the potential risks associated with cyberattacks, the management team of the firm decides to take proactive measures to strengthen the security of their internal network by contacting you to conduct a vulnerability assessment and penetration test on their internal network ONLY. The network consists of 1 Linux Server, 1 Apache webserver and a couple of windows machines or nodes.

High level Objectives of the Accounting Firm:

1. Vulnerability Assessment: A comprehensive scan of their internal network to identify weaknesses and misconfigurations in their systems and software. This will help them understand the inherent vulnerabilities on their network.
2. Penetration Testing: A simulated cyber-attack on their internal network. This will test the effectiveness of their existing security controls and identify any exploitable weaknesses. The pen test will be limited to the internal network only, simulating an attack by someone who has gained access internally.

Benefits of this service to the Accounting Firm:

1. Improved security posture: By identifying and addressing vulnerabilities, the accounting firm can make their network more secure and reduce the risk of a data breach.
2. Increased client confidence: By taking steps to secure their data, the accounting firm can demonstrate to their clients that they take data security seriously.
3. Compliance with regulations: A government regulation requires that the firm implement security measures to protect sensitive data. Conducting a vulnerability assessments and penetration testing will help them comply with this regulation.

Assignment Specifications:

Task A: Pre-engagement Planning Activities

1. Describe how you will go about getting a legal contract with this accounting firm.
2. Discuss the penetration testing methodology you will use in conducting the test.

Task B: Conducting Penetration Test

This assessment focuses on your ability to report your findings after completing a penetration test:

3. Using your lab as the internet network i.e., 10.0.0.0/24, find all the possible vulnerabilities on all the nodes on the network (this should not include the ones that have been covered in class).
4. Write a report detailing the activities (with screenshots and report from tools used) you carried out at each stage of the penetration test namely reconnaissance, vulnerability analysis, exploitation, and post-exploitation.
5. Report all successful exploits and you may also record unsuccessful exploits to show the client the rigour you went through in carrying out the test.
6. Tabulate your recommendations and let the client know the order they should follow in remediating the vulnerabilities you have discovered.

Technical Requirements:

1) You need to complete a scan of the target network to identify all existing vulnerabilities using Kali Linux tools, relevant tools from GitHub and TTPs (Tactics, Techniques and Procedures). For each one, present a summary, include the risk level, risk matrix, and recommendation to mitigate the vulnerability.

2) You need to conduct a comprehensive exploit attempt of the vulnerabilities using Kali Linux tools, relevant tools from GitHub and TTPs (Tactics, Techniques and Procedures).

3) Produce a Final Penetration Test Report based upon the tools and techniques you used and the results of your exploitations. Provide evidence (i.e., screenshots, test outputs) of all the steps you carry out and document the commands and tools you use during the test.

In your report, create a section on pre-engagement planning activities and another section for the final report. Your report will include a title page, table of content, and bibliography. Ensure all imported material is properly cross-referenced, pages and sub/sections heading are numbered, and figures include caption.

Assessment Criteria:

Pre-engagement Activities (15%)
Reconnaissance (15%)
Vulnerability Analysis (25%)
Exploitation and post-exploitation (30%)
Final Report Documentation (15%)

A marking rubric has also been created for this brief, please check it for detail assessment criteria.

Assessment Submission:

To submit your work, please go to the 'Submit your work' area of the CSY 2084 Ethical Hacking and Penetration Testing on the NILE site and submit it as a single MS word document or PDF to Turnitin under '**Assignment 1**'. It is important that you submit your work to the correct submission points, and that your work is submitted on time.

Your assignment must be submitted on or before 11.59pm on Sunday, 19th May 2024.

Assessment Guidance

Academic Practice

The University of Northampton policy will apply in all cases of copying, plagiarism or any other methods by which students have obtained (or attempted to obtain) an unfair advantage. Support and guidance on assessments and academic integrity can be found from the following resources:
SkillsHub: https://skillshub.northampton.ac.uk/academic-integrity/

Completing The Assignment:

This assignment must be completed and submitted electronically in the assignment point in NILE - BEFORE the submission deadline for your class.

Begin your work early, as the assignment is a substantial task that requires planning and effort to complete satisfactorily.

Getting Feedback:

The assignment will be marked by your tutor and then second marked by another tutor. This process can take up several weeks. Once all the required marking and second marking has been completed, your grade and your feedback will be uploaded to NILE.

Backing up Files:

Always keep a back-up copy of all work submitted for assessment in case of unforeseen submission problems. Accidental loss of file will not be a satisfactory reason for an extension.