



PENETRATION TESTING PROJECT (FINAL PROJECT)

COURSE : ETHICAL HACKING

COURSE CODE : NWC4123

SUBMISSION : WEEK 14

INSTRUCTIONS TO CANDIDATES:

- 1 This assignment will allocate **35%** of carry marks.
- 2 This is a group project. The members should be no more than 3 persons per group.
- 3 Should you decided to use brute force attacks, you may use the following dictionary accompanied by the questions.
 - a. dictionary.txt
- 4 Student are expected to produce:
 - a. A written technical report.
- 5 Please submit softcopy to the lecture before: **FRIDAY WEEK 14 5:30 pm** .
- 6 Submission will be through LMS.
- 7 Plagiarism, copying and cheating will not be tolerated, where no marks will be awarded and disciplinary actions can be taken.

CLO3: Produce a report on an evaluation of system vulnerabilities through penetration testing techniques and countermeasures.

QUESTION 1: PENETRATION TESTING TECHNICAL REPORT

Item 1

You are required to execute penetration testing on a selected webpage. You **may choose your own preferred webpage or system depending on your own investigation.**

Please use only **ONE (1)** target system

Note that the penetration testing purpose is for analyzing the security capability of the page or system. The student is prohibited altering or making changes on the targeted system or webpage.

Suggested target system are as follows:

<http://megamegapom.free.nf/>

<http://nicelydone.iceiy.com/>

<http://kedaipakkarim.hstn.me/>

PREQUISITES:

After you have picked up your target (item 1), you may execute the following penetration testing activity. The assessment of the testing will be done from your virtual machine (KALI LINUX). By using relevant tools that is available in Kali Linux, you may conduct a systematic penetration testing which comprises of the following components

- a. **Reconnaissance**
- b. **Scanning**
- c. **Gaining Access**

If you unable to penetrate the system with one of the following components, you may state the process that have been done prior.

The following guideline can be used to produce the penetration testing as intended. Should the student decide to provide with alternative framework, the framework must be clearly be stated and incorporated in the penetration testing.

You may refer the penetration testing framework at the following guideline

- <http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html>
- <https://cybergateinternational.com/blog/penetration-testing-methods-presented-and-explained/>
- <https://cybergateinternational.com/blog/understanding-the-five-stages-of-a-penetration-test/>
- <https://owasp.org/www-project-web-security-testing-guide/stable/>

- Penetration Testing: A hands on introduction to hacking by Georgia Wiedman, No Starch Press

DELIVERABLES:

The guideline in how to produce the report is shown as follows. Note that the student may add his or her contents/section which deemed necessary to support the justification of the project.

Bil	Deliverables	Remarks
1	Introduction to the project	<ul style="list-style-type: none"> • The brief explanation on the penetration testing • The plan for penetration testing.
2	Overview of the target	<ul style="list-style-type: none"> • The introduction to the target. • Overview of the target architecture. • Review of possible threats for the target. You may use framework to justify possible threats.
3	Reconnaissance	<ul style="list-style-type: none"> • This section to be prepared by student 1 • Provide the name of the preparer in the beginning of this section. Refer appendix A • The introduction to the reconnaissance methodology. • Demonstrate how the reconnaissance being implemented on the target. You may apply more than TWO (2) methods for this part. • Show the result. • Analyze and justify the result. • Provide the suitable countermeasures to improve the security from being reconnaissance against.
4	Scanning	<ul style="list-style-type: none"> • This section to be prepared by student 2. • Provide the name of the preparer in the beginning of this section. Refer appendix A • The introduction to the scanning methodology. • Demonstrate how the scanning being implemented on the target. You may apply more than TWO (2) methods for this part. • You need to include network diagram to show how the overall infrastructure of the target is being formed. • Show the result. • Analyze and justify the result • Provide the suitable countermeasures to improve the security from being scanned against.
5.	Gaining access	<ul style="list-style-type: none"> • This section to be prepared by student 3. • Provide the name of the preparer in the beginning of this section. Refer appendix A • The introduction to the gaining access methodology. • Demonstrate how the gaining access being implemented on the target. You may apply more than ONE (1) methods for this part. • Analyze and justify the result • Provide the suitable countermeasures to improve the security from being scanned against.

6.	Conclusion	<ul style="list-style-type: none">• Briefly determine the security posture of the target based on the penetration testing.
----	------------	--

SUBMISSION

The submission needs to be in softcopy and are required to be submitted in LMS.

The document needs to include the pledge of ethic and secrecy and need to be **included** on the first page of your report. The pledge can be obtained at the end of this questions.

Chat GPT disclaimer

The use of Chat GPT is scrutinized in this project. The project will mostly revolve on the student capability to write a web application according to the requirement. It is intended to instill student skill in good coding practices and project management. Even though Chat GPT definitely able to produce codes which some way could fulfils the requirement of the project, it does not guarantee the degree of understanding, and knowledge of the author. Therefore, this project will examine the originality and authenticity as well as understanding of the student on the subject matter

QUESTION END

Appendix A

Chapter 2

[title of your work]

[You name and student ID]

Introduction

Writing starts here.....



Ethical Hacking Pledge for Student Project

I, _____ pledge to conduct my ethical hacking project with the utmost integrity and adherence to ethical guidelines. I understand the importance of responsible and legal hacking practices, and I commit to upholding the following principles throughout the duration of my project:

- **Respect for Laws and Regulations:** I will strictly adhere to all local, national, and international laws and regulations governing computer security and hacking activities. I will not engage in any activity that is illegal or unauthorized.
- **Non-Disclosure:** I will treat all information obtained during my testing as confidential and proprietary. I will not disclose any sensitive information, vulnerabilities, or data breaches to unauthorized parties.
- **Responsible Disclosure:** In the event that I discover a security vulnerability, I will follow responsible disclosure practices. I will promptly report the vulnerability to the appropriate stakeholders and provide them with a reasonable amount of time to address the issue before making it public.
- **Limited Scope:** I will only test the systems and networks explicitly defined within the scope of my project. I will not attempt to access or manipulate any systems outside of this scope.
- **No Harm:** I will not intentionally or maliciously damage, disrupt, or compromise the availability, integrity, or confidentiality of any systems, networks, or data. My actions will be focused on identifying and mitigating vulnerabilities.
- **Documentation:** I will maintain accurate and detailed records of my testing activities, methodologies, findings, and communications with stakeholders. This documentation will help demonstrate my commitment to ethical practices.
- **Continuous Learning:** I will stay informed about the latest ethical hacking practices, security trends, and relevant laws. I will continuously improve my knowledge and skills to ensure the highest level of professionalism.
- **Education and Awareness:** I will use the knowledge gained from my project to educate others about the importance of ethical hacking, responsible disclosure, and cybersecurity best practices.
- **Accountability:** I understand that my actions reflect not only on myself but also on the ethical hacking community as a whole. I will hold myself accountable for maintaining the highest standards of ethics and professionalism.

By signing this pledge, I commit to conducting my student project with integrity, responsibility, and respect for ethical hacking principles.

Signature: _____

Date: _____

*to be printed on the first page of the report after cover page