	SUBJECT: Ethical Hacking	**CODE:** BCY2043	**MARK**: /100
	TOPIC: Chapters 3-6		
	ASSESSMENT: Project	**NO:** 1	**TIME:** 6 weeks

The learning outcomes that will be evaluated in this project are:

C02 Analyze theory and principles of information security, element of security, hacking cycle, hacktivism and ethical hacking.
C03 Construct attack and defence methods into computer and network environments.
C04 Demonstrate communication effectively in written and oral form through report and presentation session.
CO5 Relate their surrounding environment (i.e. economy, environmental, cultural) with the professional practice by demonstrating usage of data and ethical hacking methods and tools.

INSTRUCTIONS

1. The total mark of this project is 100 that will bring **25% assessment marks**.
2. This project is a group project with a maximum of **4 students** in a group.
3. Choose a group leader; group leader is responsible for task distribution, report submission in Kalam etc.
4. Read the instruction carefully and follow the rubric given to complete your task.

TOOLS

- Session hijacking / MITM
    - Burp Suite
    - OWASP ZAP
    - Firesheep HTTP
    - netool toolkit
    - WebSploit Framework
    - ssstrip
    - CookieCatcher
    - Metasploit
    - Ghost Phisher
    - Evilginx

- Phishing
    - Ghost Phisher
    - Wifiphisher
    - ReelPhish
    - King Phisher

1. Choose **ONE (1)** attack from the list above. Provide **real case study** related to the attack.
2. Given the list of tools. Choose only **ONE (1)** tool from the list or any available tool. Each tool should be selected by only **ONE** group. Write the tool your group has chosen at the link provided.
3. Study how to use the tool. Explain how the selected tools can be used to prevent such attack.
4. Plan and document your attack activities including (**5 requirements**):
    - **who is involved (attacker and victim),**
    - **when to conduct the attack,**
    - **OS / platform / host (attacker and victim)**
    - **the steps of the attack, and**
    - **how many trials taken.**

    Show the steps involved with the detailed explanations. For each trial of attack, show the result with logic justification.
5. Justify the selection of the tools that you have chosen.
6. Simulate your defense mechanism. Show the important steps. Discuss the results.
7. Simulate your defense mechanism (for example, firewall, IDS, IPS, AV, honeypot). Discuss the results.

REQUIREMENTS

1. Front page must contain project name, group name and members.
2. Document your task distribution, meetings discussion etc. in your report.
3. Any resources that have been used during the activities (book, technical paper, website and other), **compulsory to be cited in report and list them in report references.**
4. Please ensure that, in the last page of your report you attach the Turnitin plagiarism result of your project report (If the lecturer finds any form of plagiarism, this will lead to **0** marks in 25%project)
5. Please refer the rubric to complete your report.
6. Present your work.

Submission Due date: End of week 14, 11.59 PM

1. Report (softcopy-pdf)