اونيۏرسيتي مليسيا فهڠ السلطان عبدالله UNIVERSITI MALAYSIA PAHANG AL-SULTAN ABDULLAH	**SUBJECT:** Data & Network Security	**CODE:** BCN2023	**MARK**: /100
	TOPIC: Chapters 1 - 6		
	ASSESSMENT: Project	**NO:** 1	**TIME:** 10 weeks

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

C01 Analyse the theory and principles of information security, types of security threats, potential attacks, data cryptography, firewalls, and intrusion detection systems.
C02 Construct attack and defence methods into computer and network environments.
C03 Relate their surrounding environment (i.e., economy, environment, cultural) with the professional practice in the context of data network and security.

INSTRUCTIONS

1. The total mark of this project is 100 which will bring 25% from overall assessment marks.
2. This project is a group project with **4 STUDENTS** in a group.
3. Choose a group leader; the group leader is responsible for task distribution, report submission in Kalam/UDAS etc.
4. Read the instructions carefully and follow the rubric to complete your task.
5. Use the template provided or your own for the project report.

REQUIREMENTS

1. Set up **THREE (3)** new virtual OS connected under the same subnet (it is advised to set up the OS in a virtual environment and bridge the network connection to use the same subnet as the host OS). Two OS (Windows and Linux) will be the victim, and one OS will be the attacker. Record the IP address and subnet used for this project.

2. **TWO (2)** members will be an attacker (Red Team) and **TWO (2)** members will be a defender (Blue Team). Read here for more information on the Red and Blue Team concept. https://purplesec.us/red-team-vs-blue-team-cyber-security/

3. The Blue Team needs to:
    a. Set up **TWO (2)** virtual OS; one is a Linux Operating System, and the other is a Windows Operating System — set up in the Windows OS to have web service, up and running. Any web service can be set up.
    b. Networking services like file and printer sharing, web browsers, NETBIOS, and others must be turned on, up and running.
    c. In the Linux OS, install everything related to networking services, up and running.

d. Harden the **TWO (2)** virtual OS with the latest patches and updates after the Red Team has successfully done the attack and gets results from the intrusion activities. Use a firewall, IDS and other security measures to secure the OS.
e. Search for the Blue Team concepts and activities on the Internet and record findings. Apply the findings to both computers where possible.
f. Report everything from the first searching activities to the end of attack and defence activities under the Blue Team concept.

4. The Red Team needs to:
   a. Search the Red Team concepts and activities on the Internet. Record everything about the Red team related to attack and defence activities.
   b. Search for attacks and tools that can be used to launch attacks towards the Windows and Linux OS.
   c. Report everything from the first searching activities to the end of attack and defence activities under the Red Team concept.

5. Run **FOUR (4)** attacks for Windows and **FOUR (4)** for Linux computers. Explain how the attack happened, then show the steps involved with the detailed explanation screenshots. Report everything under Blue Team and Read Team respectively when doing attack and defence activities.

6. Report how the Blue Team countermeasures the attack and what are the mitigation plans, etc. Provide findings on the Blue Team mitigation plan/defence mechanism.

7. Any resources used during the activities (book, technical paper, website, and others), are **compulsory to be cited** in the report and **listed in the references part.**

8. Document your plan, task distribution, meetings discussion in your report.

9. Please ensure that, on the last page of the report, attach the Turnitin plagiarism result of the project's report (under 20% similarity will get full mark for plagiarism part).

10. Please refer the rubric to complete your report.

Report Format:

a) The front page must contain the project name, group number, group members name and lecturer's name.
b) Make a full report using the template given or your own.
c) Provide the content based on tasks and the rubric provided.

Submission Deadline: End of week 13 BEFORE 5.00 PM (3/1/2025)

1. Report (softcopy – Portable Document Format pdf) with format Group<#number>_Project.pdf.