 UNIVERSITI MALAYSIA PAHANG AL-SULTAN ABDULLAH	SUBJECT: Data & Network Security		CODE: BCN2023		MARK: <div>/100</div>
	TOPIC: Chapters 1, 2, 4 & 5				
	ASSESSMENT: Project		NO: 1	TIME: 9 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**. (PO1 Demonstrate knowledge and understanding of the theory and principles of Computer Science specializing in Computer Systems & Networking) – **Chapter 1, 4 & 5**
- C02 Construct **attack** and **defence methods** into computer and network environments. (PO2 Apply appropriate techniques, skills and tools in computer science practices specializing in Computer Systems & Networking) – **Chapter 4 & 5**
- C03 Relate their surrounding environment (i.e., economy, environment, cultural) with the **professional practice** in the context of data network and security. (PO8 Demonstrate **behaviors** that are consistent with **professional standards** and **ethical responsibilities**) – **Chapter 1 & 2**

A. 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 **5 STUDENTS** in a group.
3. Choose **a group leader** who is responsible for task distribution, ensuring group functions as promised and final submission in Kalam/UDAS with Turnitin report.
4. Read the requirements carefully and follow the rubric to complete your task.

B. JOB SCOPE

1. **Project Title:** Campus Network Hardening: A Vulnerability Remediation Exercise
2. **Role:** White hat hackers
3. **Target:** Campus Environment (FTKEE, FTKKP, FTKA, FTKPM, FTKMA, FIST, FIM, PSM, PBM, PSK, Library, KK, PAP, Akademi ADAB, UMPSA Village, BK) – choose and agree in group formation and signing session.
4. **Situation:** You as a group want to discover vulnerabilities of assets in the target environment (computer and network) using several tools you have learned in the lab exercise. After

 UNIVERSITI MALAYSIA PAHANG AL-SULTAN ABDULLAH	SUBJECT: Data & Network Security		CODE: BCN2023		MARK: <div>/100</div>
	TOPIC: Chapters 1, 2, 4 & 5				
	ASSESSMENT: Project		NO: 1	TIME: 9 weeks	

collecting all the possible threats or vulnerabilities, suggest strategies for defence methods and countermeasures to protect those vulnerable assets. Report all findings and prepare a full report.


5. **Feedback:** by the lecturer in group interview week 13 using rubrics (evaluative judgment).
6. **Product (delivery method):** Presentation and report submission.
7. **Signing session:** All agreements must be signed by all parties involved in this project. The agreement needs to be signed after all parties agree on the terms and conditions.

C. PROJECT OVERVIEW

As a **white hat hacker**, your group goal is to simulate a real-world scenario where a security expert is tasked with **hardening** a campus network to prevent **potential threats**. Your task is to plan, design and construct a **vulnerability remediation** exercise to identify **vulnerabilities** and give suggestions for implementing **strategies and measures** to protect the computer and network environments from cyber threats. The concept of this learning strategy is experiential learning whereby learning through experience or learning through reflection on doing. Students apply their knowledge and skills and gain first-hand experience. Skills, knowledge and experience are acquired outside of the traditional classroom setting.

D. PROJECT REQUIREMENTS


1. **Signed Agreement:** Create a professional practice and ethical responsibilities agreement, signed by all parties, including:
 - a. Group contract – as a team, what does the group agree to in terms of several contract items such as but not limited to participation, communication, meetings, conduct, deadlines, conflicts, clause (if in any violation of the above elements, what the team agree to do for a penalty? After that, as a team member, provide roles and contributions by putting them in a table as follows and signed by each team member.

 UNIVERSITI MALAYSIA PAHANG AL-SULTAN ABDULLAH	SUBJECT: Data & Network Security		CODE: BCN2023		MARK: <div>/100</div>
	TOPIC: Chapters 1, 2, 4 & 5				
	ASSESSMENT: Project		NO: 1	TIME: 9 weeks	

No	Student ID	Name	Role & Contribution (describe your role and how do you plan to contribute to this given task)	Signature

- b. Professional practice and ethical responsibilities statement related to this project behaviour (e.g. all dos and don'ts and signed by the project leader, team members and your lecturer) – **use generative AI to construct one.**
- c. List of IP and MAC addresses of the devices used for the project. Every time the team needs to start the activities (vulnerability discovery), record all IP addresses you get from the server. List all MAC addresses associated with the NIC (network interface card) if you connect your computer using cable or WNIC (wireless network interface card) if using wireless as the connection medium.

2. **Tools Identification, Assets Discovery and Network Topology:** Identify all tools (software and hardware) that can assist in this project and explain the usage of each tool with its configuration (if any). Create a simplified network topology and assets information of the targeted environment (tools related to footprinting, fingerprinting and enumeration) including:
 - a. IP subnets.
 - b. Device information such as IP addresses, operating systems, services, web browsers, hardware, software versions, network infrastructure, and network configurations (e.g., switches, PCs, servers, if any).
 - c. Wireless access points information, weak and strong signal location (WiFiAnalyzer app), etc.
3. **Vulnerability Identification and Exploitation:** Use hacking techniques to identify and exploit vulnerabilities in the targeted environment, including but not limited to:
 - a. Network scanning and enumeration
 - b. Vulnerability exploitation
 - c. Password cracking
 - d. Social engineering

 UNIVERSITI MALAYSIA PAHANG AL-SULTAN ABDULLAH	SUBJECT: Data & Network Security		CODE: BCN2023		MARK: <div>/100</div>
	TOPIC: Chapters 1, 2, 4 & 5				
	ASSESSMENT: Project		NO: 1	TIME: 9 weeks	

e. Vulnerability Metrics (<https://nvd.nist.gov/vuln-metrics/cvss>)

4. **Remediation:** Once vulnerabilities are identified and exploited, design a remediation plan (the plan needs to be specific to those identified vulnerabilities only and use any standard platform or professional remediation plan. **Use generative AI to construct one**), including but not limited to:
 - a. Patching or updating software.
 - b. Changing passwords or configuring access controls.
 - c. Implementing firewall rules or access lists.
 - d. Configuring intrusion detection/prevention systems.
5. **Documentation:** Document your findings and remediation steps in a detailed report, including:
 - a. All agreement.
 - b. Network topology diagram with subnets and IP addresses and detected devices.
 - c. Vulnerability identification and exploitation steps (explain how the attack worked, then show the steps involved with detailed explanation screenshots).
 - d. Vulnerability metrics and remediation plan.
 - e. Any resources used during the activities (book, technical paper, article, website, YouTube, and others), are **compulsory to be cited** in the report and **listed in the references part**
 - f. Plans, task distributions, and meetings discussion.
 - g. Attach the Turnitin plagiarism result on the last page (project report with a similarity of under 20% will receive full marks for the plagiarism part).

E. DURATION AND SUBMISSION DATES – NINE WEEKS DURATION

Signed agreement (Group) – **W3**


Evaluative judgment - presentation (Group) – **W13**

Project documentation (Group) – **W13**

Individual progress sheet (Individual) – **W2, W3, W6, W7, W9, W10, W12, W13, W14**

Self/peer assessment (Individual) – **W14**

FK

 UNIVERSITI MALAYSIA PAHANG AL-SULTAN ABDULLAH	SUBJECT: Data & Network Security		CODE: BCN2023	MARK: <div>/100</div>
	TOPIC: Chapters 1, 2, 4 & 5			
	ASSESSMENT: Project	NO: 1	TIME: 9 weeks	

F. STUDENT LEARNING TIME (SLT) – PROJECT TIME MANAGEMENT

W2 – 2H (form a group and discuss the content of the Group Contract and Professional Practice and Ethical Responsibilities Statement (Signed Agreement))

W3 – 2H (D1 submit the Signed Agreement)

W6 – 4H (D2, D3)

W7 – 4H (D2, D3)

~~W8 – break~~

W9 – 4H (D4)

W10 – 4H (D4, D5)

W12 – 5H (prepare and submit the report document)

W13 – 1H (evaluative judgment-presentation) 3H (submit corrected report)

W14 – 1H (self/peer review)

G. MARKING CRITERIA AND RUBRICS

The marking criteria and rubrics are as follows.


Deliverables:

- Signed agreement – **W3**
- A written report detailing the project – **W13**
- A presentation (max. 10 minutes) summarizing the project – **W13**
- Individual progress sheet – **W14**

Marks Distribution:

1. Signed Agreement (10 points):

- Completeness of group contract (5 points)
- Sound professional practice and ethical responsibilities statement (as a white hat hacker role) (5 points)

 UNIVERSITI MALAYSIA PAHANG AL-SULTAN ABDULLAH	SUBJECT: Data & Network Security		CODE: BCN2023	MARK: <div>/100</div>
	TOPIC: Chapters 1, 2, 4 & 5			
	ASSESSMENT: Project	NO: 1	TIME: 9 weeks	

2. Tools Identification, Assets Discovery and Network Topology (30 points):

- Accurate analysis of identification of tools and their usage in the project activities (10 points)
- Accuracy and completeness of target's network topology with labelling (5 points)
- Correct identification of devices in the target's environment and their roles (5 points)
- Clear documentation (step-by-step explanation on how team members run the tools from the start until getting the result with screenshots of facts and figures) (10 points)

3. Vulnerability Identification and Exploitation (30 points):

- Effective identification and exploitation of vulnerabilities (10 points)
- Clear documentation of exploitation steps (10 points)
- Successful exploitation of at least 5 vulnerabilities (10 points)

4. Remediation (10 points):

- Effective suggestion for remediation of vulnerabilities (5 points)
- Clear documentation of remediation steps (5 points)

5. Documentation and Presentation (10 points):


- Clarity and organization of report (3 points)
- Turnitin report under 20% similarity (2 points)
- Effective presentation with the use of diagrams and visual aids (5 points)

6. Self/peer review and progress sheet (10 points):

- Self/peer review and reflection (5 points)
- Individual progress sheet (5 points)

Additional Requirements:


- All work must be original and not copied from any sources except stated to use generative AI.
- Students are advised to follow all applicable laws and regulations when conducting the project.

 UNIVERSITI MALAYSIA PAHANG AL-SULTAN ABDULLAH	SUBJECT: Data & Network Security		CODE: BCN2023		MARK: <div>/100</div>
	TOPIC: Chapters 1, 2, 4 & 5				
	ASSESSMENT: Project		NO: 1	TIME: 9 weeks	

Grading Rubrics:

CO1 Rubrics (40%) – Analyse the theory and principles of information security, types of security threats, potential attacks, data cryptography, firewalls, and intrusion detection systems. (PO1 Demonstrate knowledge and understanding of the theory and principles of Computer Science specializing in Computer Systems & Networking) – **Chapter 1, 4 & 5**

Tools Identification, Assets Discovery and Network Topology (30), Documentation and Presentation (5), Self/peer review and progress sheet (5)	Very Weak (1) Or (2)	Weak (2) Or (4)	Fair (3) Or (6)	Good (4) Or (8)	Excellent (5) Or (10)
Accurate analysis of tools' identification and usage in the project activities (10)	Very weak analysis of tools' identification and usage in the project activities. No tool was identified	Weak analysis of tools' identification and usage in the project activities. Provide 1 tool	Fair analysis of tools' identification and usage in the project activities. Provide 2-3 tools	Good analysis of tools' identification and usage in the project activities. Provide 4-5 tools	Excellent analysis of tools' identification and usage in the project activities. Provide more than 5 tools
Accuracy and completeness of target's network topology with labelling (5)	Inaccurate and incomplete with no network topology labelling	Inaccurate and incomplete with weak network topology labelling	Accurate and complete with fair network topology labelling	Accurate and complete with good network topology labelling	Accurate and complete with excellent network topology labelling
Correct identification of devices in the target's environment and their roles (5)	No identification of devices with very weak elaboration	Identified wrong devices with weak elaboration	Identified correct devices with fair elaboration	Identified correct devices with good elaboration	Identified correct devices with excellent elaboration
Clear documentation and step-by-step explanations on how team members run the tools from the start until getting the result with screenshots of facts and figures (10)	Very weak documentation and unclear step-by-step explanations	Weak documentation and unclear step-by-step explanations	Fair documentation and clear step-by-step explanations	Good documentation and clear step-by-step explanations	Excellent documentation and clear step-by-step explanations
Effective presentation with the use of diagrams and visual aids (5)	Very weak presentation with no diagrams / visual aids	Weak presentation with no diagrams / visual aids	Fair presentation with diagrams and visual aids	Good presentation with diagrams and visual aids	Excellent presentation with diagrams and visual aids

 UNIVERSITI MALAYSIA PAHANG AL-SULTAN ABDULLAH	SUBJECT: Data & Network Security		CODE: BCN2023		MARK: <div>/100</div>
	TOPIC: Chapters 1, 2, 4 & 5				
	ASSESSMENT: Project		NO: 1	TIME: 9 weeks	


Self/peer review and reflection (5)	Very weak review and reflection	Weak review and reflection	Fair review and reflection	Good review and reflection	Excellent review and reflection
-------------------------------------	---------------------------------	----------------------------	----------------------------	----------------------------	---------------------------------

CO2 Rubrics (40%) - Construct attack and defence methods into computer and network environments. (PO2 Apply appropriate techniques, skills and tools in computer science practices specializing in Computer Systems & Networking) – **Chapter 4 & 5**

Vulnerability Identification and Exploitation (30), Remediation (10)	Very Weak (1) Or (2)	Weak (2) Or (4)	Fair (3) Or (6)	Good (4) Or (8)	Excellent (5) Or (10)
Effective identification and exploitation of vulnerabilities (10)	Very weak identification and exploitation of vulnerabilities	Weak identification and exploitation of vulnerabilities	Fair identification and exploitation of vulnerabilities	Good identification and exploitation of vulnerabilities	Excellent identification and exploitation of vulnerabilities
Clear documentation of exploitation steps (10)	No exploitation steps were provided.	Weak documentation of exploitation steps	Fair documentation of exploitation steps	Good documentation of exploitation steps	Excellent documentation of exploitation steps
Successful exploitation of at least 5 vulnerabilities (10)	Vulnerabilities not successfully exploited	1 vulnerability successfully exploited	2-3 vulnerabilities successfully exploited	4 vulnerabilities successfully exploited	5 and more vulnerabilities successfully exploited
Effective suggestions for remediation of vulnerabilities (5)	Very weak suggestions for remediation of vulnerabilities	Weak suggestions for remediation of vulnerabilities	Fair suggestions for remediation of vulnerabilities	Good suggestions for remediation of vulnerabilities	Excellent suggestions for remediation of vulnerabilities
Clear documentation of remediation steps (5)	No remediation steps were provided.	Weak documentation of remediation steps	Fair documentation of remediation steps	Good documentation of remediation steps	Excellent documentation of remediation steps

CO3 Rubrics (20%) – Relate their surrounding environment (i.e., economy, environment, cultural) with the professional practice in the context of data network and security. (PO8 Demonstrate behaviors that are consistent with professional standards and ethical responsibilities) – **Chapter 1 & 2**

Signed Agreement and Progress Sheet (10), Self/peer review and progress sheet (5), Documentation and Presentation (5)	Very Weak (1) Or (0)	Weak (2)	Fair (3) Or (2) Or (1)	Good (4)	Excellent (5) Or (3) Or (2)
Group Contract (5)	Incomplete signed agreement. Not able to identify roles by group	Partially complete signed agreement. The roles of group members were	Complete the signed agreement. Roles of group members	Complete the signed agreement. Roles and contributions of group	Complete the signed agreement. The roles and contributions of

 UNIVERSITI MALAYSIA PAHANG AL-SULTAN ABDULLAH	SUBJECT: Data & Network Security		CODE: BCN2023		MARK: <div>/100</div>
	TOPIC: Chapters 1, 2, 4 & 5				
	ASSESSMENT: Project		NO: 1	TIME: 9 weeks	


Professional practice and ethical responsibilities statement (5)	and no individual commitment stated.	identified vaguely. Individual commitment stated.	identified. Clear individual commitment stated.	members identified. Detail individual commitment stated.	group members are clearly identified and evidenced. Precise individual commitment stated.
Individual progress sheet (5)	Not able to identify the reference. No contribution was made to group's progress	Able to use one reference for group development. Little contribution made to group progress	Able to use more than one reference for group development. Important contribution made to group progress	Able to use more than one reference and from two forms of sources for group development. Significant contribution made to group progress	Able to use more than two references and from two forms of sources for group development. Significant and important contribution made to group progress
Turnitin percentage (3)	51% and above		21% - 50%		less than or equal 20%
Clarity and organization of report (2)	Not follow the format and some contents provided		Some format used and all content provided		All format use as required and provide all content, reference

H. REPORT FORMAT:

1. The front page must contain the project name, group number and name, group members name and student ID, and lecturer's name.
2. Provide the content based on tasks and the rubric provided.

I. SUBMISSION DEADLINE: END OF WEEK 13 BEFORE 5.00 PM (6/6/2025)

1. Report (softcopy – Portable Document Format pdf) with format Group<#number>_Project.pdf.
2. Turnitin Report (attached after the last page of the Project Report).

 UNIVERSITI MALAYSIA PAHANG AL-SULTAN ABDULLAH	SUBJECT: Data & Network Security		CODE: BCN2023	MARK: /100
	TOPIC: Chapters 1, 2, 4 & 5			
	ASSESSMENT: Project	NO: 1	TIME: 9 weeks	

Appendix 1

Group Contract (5%)	BCN 2023: DATA & NETWORK SECURITY Signed Agreement
--------------------------------	--

Objective

The objective of this group contract is to make sure that your team will work successfully throughout the course. As you will be working with your group members throughout this semester, you need to be accountable for your group performance in this course. Hence, the group needs to agree on how you are going to work, the quality of work your group will produce and actions to be taken for those group members who are not meeting the group contract/expectation. In case of any dispute, the lecturer will refer to the group contract for action to be taken on individual (s) who fail to perform.

To form a team and team contract

Find team members of a maximum of 5 students. Perform the following activity.


- Declare and identify individual strengths.
- Identify individual roles in the team.
- Agreed on meeting time, venue, communication means and approaches to arrive at any decisions.
- Develop team/group social contract.

Deliverable / To submit

Submit this document; group social contract and keep one copy for your group.

Group Number/Name: ???

Contract Item: As a Team, we agree to	
• Participation	
• Communication	
• Meetings	


 UNIVERSITI MALAYSIA PAHANG AL-SULTAN ABDULLAH	SUBJECT: Data & Network Security		CODE: BCN2023		MARK: <div style="font-size: 2em; text-align: center;">/100</div>
	TOPIC: Chapters 1, 2, 4 & 5				
	ASSESSMENT: Project		NO: 1	TIME: 9 weeks	

<ul style="list-style-type: none"> Conduct 	
<ul style="list-style-type: none"> Deadlines 	
<ul style="list-style-type: none"> Conflict 	

Clause In any violation of the above, we agree	
--	--


Please ensure that the item in the clause is effective and feasible.

No	Student ID	Name	Role & Contribution (describe your role and how you plan to contribute to this given task)	Signature

 UNIVERSITI MALAYSIA PAHANG AL-SULTAN ABDULLAH	SUBJECT: Data & Network Security		CODE: BCN2023		MARK: <div style="font-size: 2em; text-align: center;">/100</div>
	TOPIC: Chapters 1, 2, 4 & 5				
	ASSESSMENT: Project		NO: 1	TIME: 9 weeks	

Assessor: Mr. Abdullah Mat Safri

Date Received:

 UNIVERSITI MALAYSIA PAHANG AL-SULTAN ABDULLAH	SUBJECT: Data & Network Security		CODE: BCN2023		MARK: <div>/100</div>
	TOPIC: Chapters 1, 2, 4 & 5				
	ASSESSMENT: Project		NO: 1	TIME: 9 weeks	

Professional Practice and Ethical Responsibilities Statement (5%)	BCN 2023: DATA & NETWORK SECURITY Signed Agreement
--	--

Objective

The objective of this professional practice and ethical responsibilities statement is to make sure that your team will align with the code of ethics and professional conduct. As you will be doing some vulnerability assessments and non-destructive hacking activities, you need to be accountable for every action you perform. Hence, the group needs to build the statement, and all members should understand and comprehend the statement perfectly.

This agreement is designed to ensure that all activities are conducted within legal and ethical boundaries and to protect both the project participants and the target's assets (network, system and endpoint) being tested.

Deliverable / To submit

Submit this document; professional practice and ethical responsibilities statement and make one copy for each member.

Example of the Statement

Professional Practice and Ethical Responsibilities Agreement

Project Title: [Insert Project Title]

Project Team Members:

- [Name of Team Member 1]
- [Name of Team Member 2]
- [Name of Team Member 3]
- [Name of Team Member 4]
- [Name of Team Member 5]

Target Environment:


- [Name of Target]
- [Area]

Date of Agreement: [Insert Date]

1. Scope of Work

The project team is authorized to conduct ethical hacking activities on the following systems and components:

- [List of Systems and Components]
- [Specific IP Addresses, URLs, or System Names]

 UNIVERSITI MALAYSIA PAHANG AL-SULTAN ABDULLAH	SUBJECT: Data & Network Security		CODE: BCN2023		MARK: <div>/100</div>
	TOPIC: Chapters 1, 2, 4 & 5				
	ASSESSMENT: Project		NO: 1	TIME: 9 weeks	

2. Permission and Authorization

<fill this part>

3. Legal and Ethical Responsibilities

<fill this part>

4. Code of Ethics

<fill this part>

5. Confidentiality

<fill this part>

6. Reporting and Documentation

The project team will provide regular updates and final reports to the lecturer. These reports will include:

- **Summary of Activities:** A detailed summary of the ethical hacking activities conducted.
- **Vulnerabilities Identified:** A list of all vulnerabilities identified, along with their severity and potential impact.
- **Recommendations:** Recommendations for remediation and improvement of the system's security.

7. Termination

This agreement may be terminated by lecturer upon written notice. Upon termination, the project team will cease all activities and provide a final report to the lecturer.

8. Signatures

By signing below, the project team members and the lecturer agree to the terms and conditions outlined in this agreement.


Project Team Members:

- [Name of Team Member 1] _____ [Date]
- [Name of Team Member 2] _____ [Date]
- [Name of Team Member 3] _____ [Date]
- [Name of Team Member 4] _____ [Date]
- [Name of Team Member 5] _____ [Date]

Lecturer:

- [Name of Lecturer] _____ [Date]

This agreement is designed to ensure that all ethical hacking activities are conducted in a professional, legal, and ethical manner. It is important to review and understand all the terms and conditions before signing. If you have any questions or concerns, please discuss them with the lecturer.

 UNIVERSITI MALAYSIA PAHANG AL-SULTAN ABDULLAH	SUBJECT: Data & Network Security		CODE: BCN2023		MARK: <div>/100</div>
	TOPIC: Chapters 1, 2, 4 & 5				
	ASSESSMENT: Project		NO: 1	TIME: 9 weeks	

Appendix 2

Individual Progress Sheet (5%)	BCN 2023: DATA & NETWORK SECURITY
---	--

Student ID and Name: Group No/Name: Project Title :		
Week	My weekly log	References used / Notes
2	Eg. Group Formation and Discussion 1. Kick off meeting – understand project requirement. 2. Roles and responsibilities distribution among group members. 3. Generate project idea for group. My task 1. Contribute one idea – xxxxx 2. My roles in group project - xxxxx	References: 1. Article - xxxxx 2. YouTube channel – xxxxx 3. Asdasda Notes: 1. Understand term for security objectives – confidentiality, integrity, availability. 2. Find white hat hacker roles and functions. 3. Comprehend vulnerabilities, threats, attacks, risks and responsible disclosure.
3		
6		
7		
9		
10		
12		
13		
14		