	SUBJECT: Data & Network Security		CODE: BCN2023	MARK: 30
	TOPIC: 4-6			
	LAB ASSIGNMNET NO	2	TIME: 3 WEEKS	

THE LEARNING OUTCOME OF THIS COURSE:

This assignment will be evaluated based on the learning outcome of CO2.

CO2: Construct and organize attack and defence methods into computer and network environments. (Psychomotor).

PLEASE FOLLOW INSTRUCTIONS CAREFULLY


1. This lab assignment is an individual assignment.
2. The mark is 30, which brings 7.5 % out of the total assessment mark.
3. Read the task instructions given carefully and follow the rubric given to complete your task.

THE TASK NEEDS TO FOLLOW

1. Read the instructions carefully
2. In this lab Assignment Part 2 consists of three main tasks.
3. Complete all tasks given
4. Please do it on your own
5. Provide report by using the template that has been discussed in lab session.
6. Use your own words and provide references where appropriate.

SUBMISSION REQUIREMENTS AND MARKS DISTRIBUTION

1. The front page must contain a name, id, section, lecturer's name and date of submission. (1 Mark)
2. Table of Contents (1 Mark)
3. Introduction (1 ½ mark)
4. Task 4 – 10 marks
5. Task 5 – 8 marks
6. Task 6 - 7 marks
7. Conclusion (1 ½ Mark)
8. List Of references (1Mark)

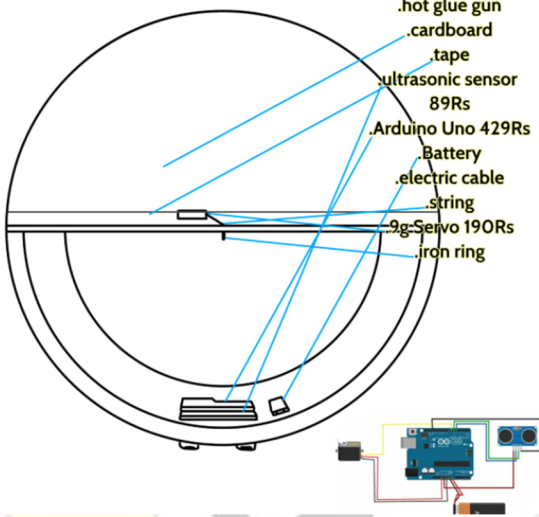
	SUBJECT: Data & Network Security		CODE: BCN2023		MARK: 30
	TOPIC: 4-6				
	LAB ASSIGNMNET NO		2	TIME: 3 WEEKS	


SUBMISSION

Report submission for lab assignment part 2 is on **6th June 2025 before 5.00 PM**

The report file format should be **pdf**.

FORMAT FOR REPORT FOR EACH TASK

Task #	Figure of your Task	Description
4	<p>A. Data is taken from Mycert web site for 4 quarter. The link as below:</p> <ol style="list-style-type: none"> 1. www. 2. www. 3. www.w 4. www. 5. 	
	<p>alat yang diguna</p> <ul style="list-style-type: none"> .hot glue gun .cardboard .tape ultrasonic sensor 89Rs Arduino Uno 429Rs Battery electric cable .string 9g Servo 190Rs iron ring  <p>Figure 1</p>	<p>B. Microsoft excel</p> <ol style="list-style-type: none"> 1. Figure 1 show the component that has been used ...

	SUBJECT: Data & Network Security		CODE: BCN2023		MARK: 30
	TOPIC: 4-6				
	LAB ASSIGNMNET NO		2	TIME: 3 WEEKS	

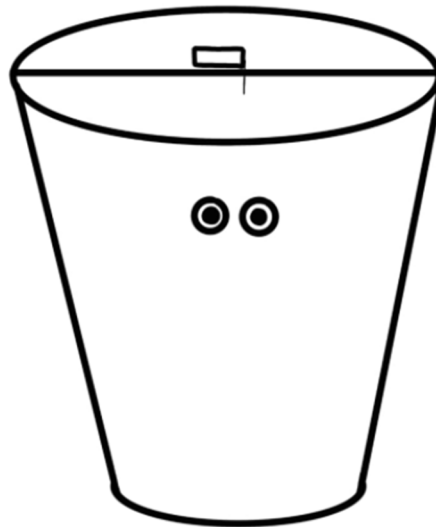


Figure 2

2. As shown in Figure 2, this is the design for final product

5	
6	


TASK 4 – 10 MARKS

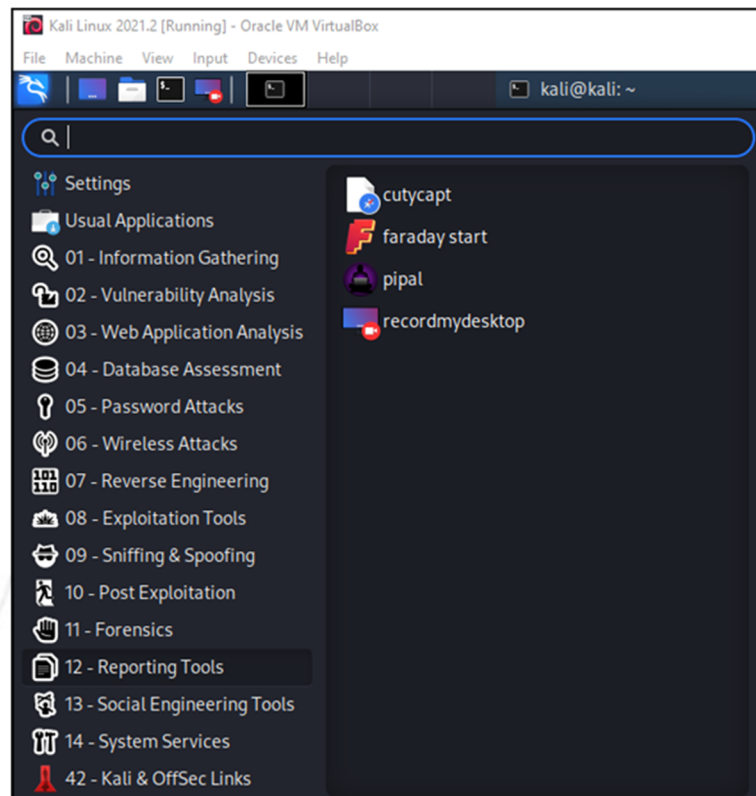
A. Exploit Vulnerability Using Metasploit

1. Find **THREE (3)** exploits for Windows 7 in a lab virtual machine other than the one used in the lab module.
2. Run the exploits and record all the steps and screen capture. Explain and give some information about the exploits that you launched.
3. Report your findings.

B. Web Vulnerability Scanning

1. Explore Kali Linux applications and tools from 01 until 14 as in the picture below:

	SUBJECT: Data & Network Security		CODE: BCN2023		MARK: 30
	TOPIC: 4-6				
	LAB ASSIGNMENT NO		2	TIME: 3 WEEKS	




2. Run XAMPP Web Server (on Windows machine).
3. Find **TWO (2)** suitable tools/scripts to launch vulnerability scanning towards the web server service. You can use Kali Linux or any tools/scripts from outside the Kali Linux machine for this task.
4. Report your findings on how to use the tools/scripts and what result you get from the vulnerability scanning activity.
5. Compare the results between the two tools/scripts that you used.

Provide a step-by-step screen snapshot with the explanation

TASK 5 – 8 MARKS

A. Using A Firewall to Stop Attacks

1. Search for any third-party firewall software on the Internet.
2. Install and run the firewall into a lab virtual Windows 7 machine. Make sure the Windows firewall is off.
3. Run back the **THREE (3)** exploits from your previous task (Task 4A lab assignment 2). Make sure the attacks are still successful.

	SUBJECT: Data & Network Security		CODE: BCN2023		MARK: 30
	TOPIC: 4-6				
	LAB ASSIGNMENT NO		2	TIME: 3 WEEKS	

4. Now run the third-party firewall and set it up to make sure that the attacks earlier can be stopped by the firewall.
5. Show inside the firewall logs or its screening area that it has stopped the attacks successfully.

Provide a step-by-step screen snapshot with an explanation.


TASK 6 - 7 MARKS

A. Capture Wireless Access Data Transmission

1. Create and set a Wi-Fi hotspot network environment with a wireless connection using your computer. Connect your phone to the hotspot.
2. Show how you set the network and connected your mobile phone to your Wi-Fi hotspot network. Show a step-by-step screen snapshot of how you configure it until the phone can fully connect to the wireless and get an Internet connection. Report on the wireless security configuration.
3. Run the Wireshark program on your computer and capture traffic from the Wi-Fi hotspot network. Try to log in and access the e-banking system, UMPSA's Kalam website and <http://testphp.vulnweb.com/login.php> website using your phone. Stop the Wireshark capture traffic.
4. Record and report your findings about the data that appeared in the Wireshark from accessing the websites.

B. Access Point Security

1. Suggest any wireless access point used in the market to strengthen security in a home wireless environment. Based on its function, justify your choice of the access point based on the security point of view.
2. Provide a reference for the product selection.

	SUBJECT: Data & Network Security		CODE: BCN2023		MARK: 30
	TOPIC: 4-6				
	LAB ASSIGNMNET NO		2	TIME: 3 WEEKS	

MARKING GUIDE

Item	0	In between	Full mark
Front page	Not provide		Provide all
TOC	Not provide		Provide Correct
Introduction	Not provide		Provide Correct
Task 4	Not provide	Missing task and not complete	Provide all and complete
Task 5	Not provide	Missing task and not complete	Provide all and complete
Task 6	Not provide	Missing task and not complete	Provide all and complete
Conclusion	Not provide		Provide Correct
List of references	Not provide		Correct and complete