<table>
<tr><td rowspan="3">اونيۏرسيتي مليسيا ڤهڠ السلطان عبدالله
UNIVERSITI MALAYSIA PAHANG
AL-SULTAN ABDULLAH</td><td colspan="2"><b>Course:</b> Network Programming</td><td rowspan="3"><b>MARKS:</b>
/40</td></tr>
<tr><td><b>Code:</b> BCN3033</td><td><b>Team/individual:</b>
Team (3 - 4)</td></tr>
<tr><td><b>Type of Assessment:</b>
Project 1</td><td><b>Name of Assessment:</b>
Rootkit</td></tr>
</table>

Title of Project 1: Relations of network functions and rootkit @ root exploit

===

1. Background

A rootkit is a term from Linux that is derived from two words, "root" and "kit". “Root” is referred as administrator of Unix-based OS (Linux, BSD, Ubuntu). It acts as a user account with full privileges and unlimited access. Similar to Windows, a term used for user that has root access is known as administrator. On the other hand, "kit" refers to a program or tool that allows attackers to gain root or administrative access of the OS. Therefore, by combining "root" and "kit”, these words refer to a malware for the unauthorized user (attacker) used to gain root privileges to the victim’s OS. An attacker is capable to execute administration action (create folder, delete file, delete user, install more malware and others) remotely from other locations, if the attacker is able to establish a network communication with the victim’s computer.

During Network Programming course, we have discussed about the important network functions (for example socket (), bind (), accept () and listen ()) in C/C++ language. However, this project is to test your understanding of server and client code in rootkit code and apply your understanding to build a rootkit in any type of OS (Ubuntu, Redhat, Kali Linux, Windows, or MacOS). Learning to write a rootkit is useful to understand most of the network programming related concepts and its importance in our daily life, especially in the security point of view.

In this project, construct a rootkit from different OS (Attacker (Ubuntu) attacks Victim (Windows) or vice versa) in one virtualbox. Our lab has equipped both Ubuntu and Windows, and you may test and try it there.

2. Course outcome

a) Demonstrate the programming language and techniques in relation to the networking concept
b) Write, construct and run the network programming
c) Organize new ideas related to the network programming

3. General instructions

CO1:

a) Use the Cover page prepared for you (see Appendix A)
Analyze both differences as well as similarities of network functions in our lesson (socket (), bind (), and others) with the network functions existed in the rootkit code.
From your analysis, ***construct*** a table of summary, followed by the explanation in paragraphs. That explanation should provide your understanding of:

   i. the differences of parameters in network functions in between our note and in rootkit code; **[10 Marks]**

CO2:

b) With the help of the network functions, ***construct a rootkit*** code in any language (C, C++, Java, or Python). And provide the ***steps with multiple screenshots*** of successfully attacking the victim's computer using the rootkit.
[10 Marks]

c) ***Execute and demonstrate*** the rootkit and show that you are able to execute administrator privileges without the victim's permission. **[10 Marks]**

d) ***Create*** a ***video*** to prove the rootkit executions. The requirements of the video are as follows:

[5 Marks]

   i. Maximum of 15 minutes only
   ii. The video file extension is either .avi or .mkv
   iii. The video should teach the viewers to understand the steps, be able to attack the victim's computer with rootkit successfully and stop it effectively by following the steps in the video. Provide the google drive link in your report and ensure the link is accessible by my email (firdausza@ump.edu.my)

CO3:

e) ***Create*** a solution to detect or stop the rootkit from executing malicious actions or steps to prevent the rootkit from attacking the OS at initial phase. **[5 Marks]**

Marking rubrics

CO	Criteria	Level of achievement						Weight	Score gained	Marks	Total
		0	1	2	3	4	5				
CO 1 (10)	a) Understanding of the network functions in the rootkit code	Unable to answer at all	Able to provide minor explanation only	Able to explain the rootkit code like 25% of it.	Able to explain the rootkit code like 50% of it.	Able to explain the rootkit code like 70% of it.	Able to explain the rootkit code clearly, shows that the students understand the code well.	1	5	5	5
	b) Demonstrate the rootkit information in the report	Not provided the demonstration to use the rootkit	Just provide minor info in to demonstrate the rootkit.	Just provide the basic steps to demonstrate the rootkit, hard to understand and the reader unable to demonstrate it according to the information.	Provide the basic steps to demonstrate the rootkit, with figures, and screenshots. And the reader able to demonstrate it according to the information.	Able to provide all steps to demonstrate the rootkit clearly, with figures, screenshots and easier to understand. Or the reader able to demonstrate it according to the information.	Able to provide all steps to demonstrate the rootkit clearly, with figures, screenshots and easier to understand. And the reader able to demonstrate it according to the information.	1	5	5	5
CO 2 (25)	b) Construct a rootkit code	Not provided	Copy and paste rootkit code exactly from the internet without change anything	Copy and paste rootkit code exactly from the internet and just change the title and comment only	Construct a rootkit and shows understanding only 25% of the code	Construct a rootkit and shows understanding only 50% of the code	Construct a rootkit and shows true understanding of the code	2	10	10	10
	c) Execute the rootkit	Not provided	Have error and unable to run the rootkit.	Have error, and able to run the rootkit sometimes.	Have error, and able to run the rootkit.	Rootkit code running however has still minor problem @ error	Rootkit code running without any error	2	10	10	10
	d) Video	Not provided	Provide the video but still the reader unable to understand the steps and unable to execute the rootkit according to the video	Provide the video but still the reader unable to understand the steps but able to execute the rootkit according to the video, sometimes.	Provide the video but still the reader unable to understand the steps but able to execute the rootkit according to the video	Provide the video and the reader understand the steps and able to attack the victim with rootkit successfully however, unable to stop it	Provide the video and the reader understand the steps and able to attack the victim with rootkit successfully and stops it effectively by following the steps in the video	1	5	5	5
CO 3 (5)	e) Propose solution to stop or avoid the rootkit	Not provided	Provided but able to run the function about 20%	Provided and run the function about 40%	Provided and run the function about 50%	Provided and run the function about 80%	Provided and able to run the function successfully.	5	5	5	5
	Total									40	40

4. Appendix A: Front cover

UMPSA

اونيۏرسيتي مليسيا ڤهڠ السلطان عبدالله

UNIVERSITI MALAYSIA PAHANG
AL-SULTAN ABDULLAH

BCN3033

Network Programming

PROJECT 1

(Your project title here)

Your name and Stud ID

(Your group member’s name, stud ID and their tasks in this project)

Student ID	Name	Task @ contribution in this project 1

Lecturer:
Dr Ahmad Firdaus bin Zainal Abidin

Course outcome	Marks (weight score | percentage)
CO1	/10
CO2	/25
CO3	/5
	/40