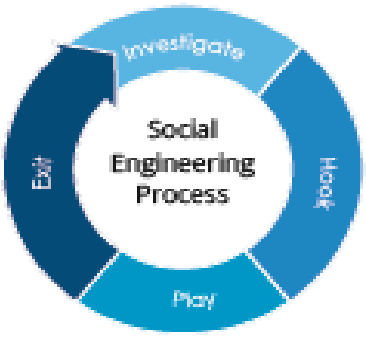
Term 3
Grade 12 - Project Task 2

TEACHERS GUIDELINES

SIS No **Name:**		**Date:**	
		Grade	
Group:	**N / A (Not Applicable)**	**Start Time:**	
Signed		**Finishing Time:**	

Ethical Hacking

Picture 1



Picture 2

TEACHERS GUIDELINES

Project task 2 is an individual task. This task will be a take home assessment and requires a detailed research from the students to answer the questions. **Please follow the Project Guide to check on the details for maintaining the student's documents electronically.** Teachers will have to maintain all the electronic documentation for each student as a part of evidence collection.

Students may require few guidance in understanding the roles of the social engineering victims, dialogue or scenario writing.

Guide the students in carrying out the research and adding references wherever required.

The answers may differ based on the research carried out. Please take professional judgement in grading the students.

PROJECT OBJECTIVE

To understand the concepts covered in the Unit 7,8 term 2 book "Introduction to Ethical Hacking", in the context of Sniffing & Social Engineering. The project task will be covering all student learning outcomes (SLO's) in the Unit 7,8.

EQUIPMENT REQUIREMENTS

Pen/Pencil, Laptop or Computer with internet connection, Paper, Printer, Term book.

PROJECT TASK INTRODUCTION

Research, using the internet or books, and complete questions with suitable answers.

STUDENT GUIDELINES

In this task you will perform research on different sniffing & social engineering attacks based on Unit 7, 8 (term 2 book). Follow the documentation guidelines below:.

- When the question demands explanation, a clear answer to justifying the question must be provided. There is **no word limit**.
- The documentation format should follow **font Arial with text size 11 or 12**
- Discuss with your teacher regarding your mode of document submission. **(hardcopy or softcopy)**

United Arab Emirates
Ministry of Education

الإمـارات العـربيـة المتحدة
وزارة التربيـــة والتعليـــم

Project Task 2 – Work Plan

No.	Work Steps	Step Completion & Values	Remarks
Q1	Read the article below and fill in the boxes with the suggestions provided for protecting the users from packet sniffers.		

ARTICLE

There are two important actions that can protect users from packet sniffers and other eavesdropping attacks.

First, use encryption! If you encrypt sensitive data and passwords while in transit, you'll render packet sniffers useless. Encryption can be implemented in a number of ways: SSL (HTTPS) connections to Web servers, encrypted SSL or TLS connections to mail servers, or other application-specific techniques. Alternatively, you can use a virtual private network (VPN) to encrypt entire communications links, regardless of protocol.

Second, use a switched network. In this case, a packet sniffer will only be able to eavesdrop on connections taking place on its own local switch port. If you assign each system to an individual switch port, there simply won't be any packets for the packet sniffer to intercept.

Ref:
https://searchsecurity.techtarget.com

Suggestion 1 (from article): Encryption	→	**How are the users protected?** Sensitive data and passwords can be protected.
Suggestion 2 (from article): Using switched network.	→	**How are the users protected?** A packet sniffer can only do eavesdrop on connections taking place on its own local switch port.
Suggestion 3 (your suggestion): Use sniffing tools	→	**How are the users protected?** Can be used to monitor the network traffic.

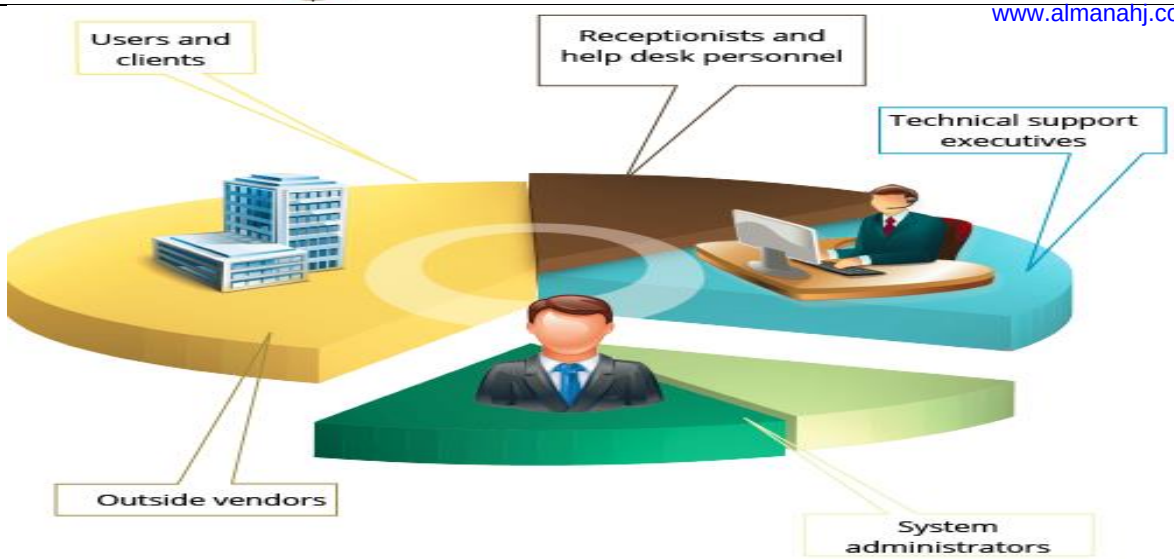
Q2	**Read the scenario and answer** • Asma wants to know the use of sniffing tools. The first one has been given. Complete the other three uses of sniffing tools to guide Asma.	1) Sniffing tools can be used for packet capturing. 2) Can collect confidential information like user name, password ect. 3) Can discover network misuse. 4) Can help to filter network traffic.	
	• Ahmed tries to send an email to his manager. But his manager keeps saying "NO email received from your side". But Ahmed surely used his managers correct email address. What is this spoofing attack?	DHCP spoofing attack	
	• Salama tried to log into her email account by using her company's email address, but when she tries to log into her email account from the company's web site another fake website appeared. What is this spoofing attack?	DNS spoofing attack	
	• A technical engineer figures out there's a high network traffic in one of the department. When he tries to solve the problem, he finds many broadcasting packets. What is this attack?	MAC flooding	
	• Mohammed tries to send an email to Faizal's PC but someone else in same the department received that email and not Faizal. What is this spoofing attack?	ARP flooding	

Q3

Social engineering attackers search for targets of opportunity, or potential victims. Confidential information can be collected from targeted victims.

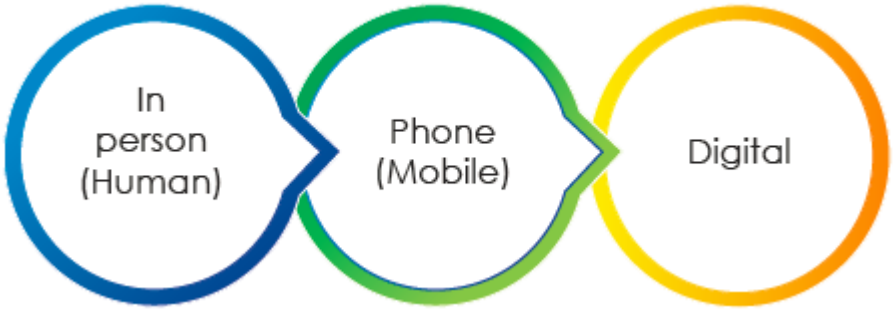
Write any two information for each of the following targets that can be collected through social engineering attacks

Please ask your teacher to clarify the targets roles if needs be.



Answers may vary.

1. Receptionists and help desk personnel.
   a) Any employees email address.
   b) Company details.
2. Technical support.
   a) system information
   b)
3. System administrators.
   a) username , pass word
   b)
4. Outside vendors.
   a) timing
   b)
5. Users and clients.
   a) places and timing
   b)

Q4	Instead of hacking the system, humans are hacked in social engineering attacks. The three main different types of social engineering attacks happen in person or through phones (mobile) or through digital medias. Consider any hacker who works in a multinational company. • Write and explain clearly any **one way** that hacker would hack the company details using all the three types of social engineering attack. • Write your suggestions/recommendations to the company's employees on how to protect from such social engineering attacks.	 **For this answer try to write a dialogue or a story-based scenario between the hacker with any person in the company using any social engineering types for hacking. Follow the social engineering process.** **– refer the book pages from 183 – 189** Answers may vary. Answers must adapt any one of the types of the social engineering attack from the book (183 – 189). An example is shown In person – **Dumpster diving** The hacker (in the IT administrator room): Hi, how are you? IT admin: Good. How can I help you? The hacker: Can you please reset my password? IT admin: Please give me some time. I will get back to you shortly. (IT admin leaves his room). The hacker starts to look and collect the small bits of paper in the dust bin which may contain important information like the email/password/keys of the employees.	

		Your suggestions/recommendations – A paper shredder in the company can be used by the IT admins to destroy important printouts. Using Phone (mobile) - Text message attack (smihing) the attacker sends the victim an sms message from an unknown number and warns that they are about to receive a code asking them to verify their google account by replying to the message . Your suggestions/recommendations - ensure that the text message from the a formal organization by phone them	

		Using Digital - phishing phishing scams are the most common types of computer-based soical engineering attack . they use false emails , chats or websites designed Your suggestions/recommendations - ensure from from your site unless if reliable site or not	

Q5	Your family and friends are probably unaware of social engineering attacks. Create a questionnaire that contains 5 **social engineering questions (A4 paper)**. Each questionnaire should be answered by at least 10 different people (family, teachers and friends). **An example is shown:** **1. Have you shared your password with anyone whom you know?** ○ **YES** ○ **NO** **2. Have you ever clicked a link on the internet or on email that lead you to download dangerous files?** ○ **YES, I have** ○ **NO, I have not** ○ **Not sure**	Answers may vary. The questionair should relate to social engineering.	

Marking Rubrics

Ⓐ Check of Dimension and Function

No.	Points	0	2
1	Can identify the methods for protecting from packet sniffing.	No efforts made	
2	Can differentiate different types of spoofing attacks.	No efforts made	
3	Can identify the information collected using social engineering.	No efforts made	
4	Can prepare a dialogue or story for social engineering attacks in an organization.	No efforts made	
5	Can prepare a social engineering attack awareness questionnaire.	No efforts made	

Ⓑ Visual Checks

No.	Inspections	0	2
1	Suggestions to prevent from packet sniffing are listed.	No efforts made	
2	Different spoofing attacks are identified.	No efforts made	
3	Can list the information collected using social engineering.	No efforts made	
4	Suggestions are provided for the social engineering prevention attack in an organization.	No efforts made	
5	Questionnaire is answered by different age group of people.	No efforts made	