



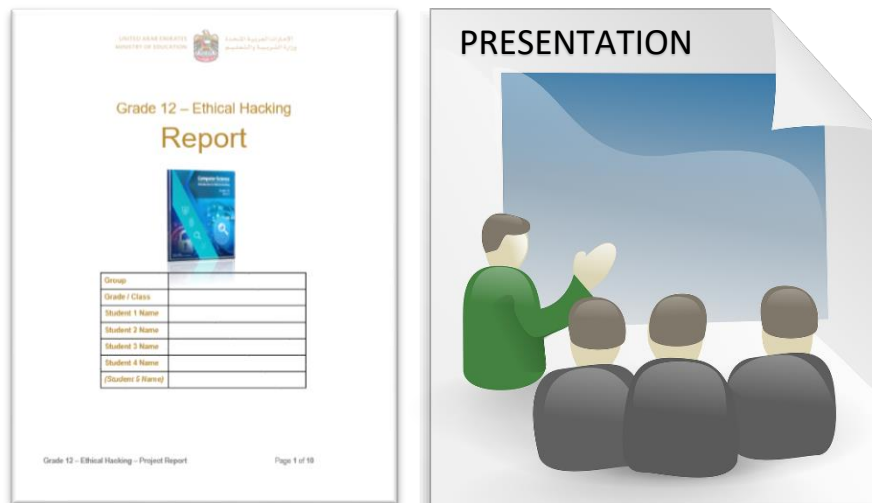
Term 2 Grade 12 – Project Task 3

Teacher's Guidelines

Ethical Hacking



Picture 1



Picture 2



IMPORTANT NOTICE

Dear teachers, in case your school is facing any software issues with **EthiLAB**, please ensure that you create a ticket by completing the online form which was sent by operations.

The link for the online form is as follows:

https://forms.office.com/Pages/ResponsePage.aspx?id=ZN_eq0qrBUuqA_TbXZ4iiz-35SJZDP1KqLNM-zZZCCdUQjBUMzkwQ0RLRFNNVvhHSEnkWDFDMIFIOC4u

Project Task 3

Introduction

From the footprinting, scanning and enumeration phases, we can use this information to break into, or gain access to, the educational system (**System Hacking**).

Project Task 3 focuses on Unit 5 (System Hacking) of the Grade 12 book.

Project Task 1 introduced the role of 'Penetration Tester', Project Task 2 introduced the role of 'Security Engineer'. Project Task 3 will introduce the role of 'Security Analyst'.

As part of the project you will take up the roles of:

- **Penetration Tester**
- **Security Engineer**
- **Security Analyst**
- **Information Security Manager**



Student Guidelines

In this project task you will imagine that you and your group members started working for the information security team, as a **Security Analyst**.

A **Security Analyst** detects and prevents cyber threats to an organization. They find out the weaknesses of the infrastructure (software, hardware and networks) and find creative ways to protect it. You are asked to

- report on **system hacking** in relation to ethical hacking (**Unit 5**)
- Work together as a **group**, with even contribution from all group members to complete the project task together
- When the question demands explanation, a clear answer to justifying the question must be provided. There is **no word limit** for your documentation.
- The documentation and report format should follow **font Arial with text size 11 or 12**
- Discuss with your teacher regarding your groups mode of document submission. **(hardcopy or softcopy) – To edit this document in Microsoft Word, please open the actual .PDF file with Microsoft Word, and convert the document.**

Project Task Objectives

A System hacking cannot be accomplished in a single activity but is accomplished through various steps. **Write what each of the 6 steps are, and include a brief description of what each step involves.**

B. To recover passwords from a computer system, special techniques are required. **Write the 5 techniques** for password-cracking **and briefly explain each.**

C. Discuss in your group. List 3 pieces of advice that would you give to the students that use the educational system to help defend themselves against password cracking? **For each, give a reason as to why** it would protect them on the educational system.

Project Task 3 – Work Plan

Teacher Guidelines:

Answers may vary. We request the teachers to take professional judgement for marking the project.

No.	Work Steps	Step Completion & Values
A	<p>System hacking cannot be accomplished in a single activity but is accomplished through various steps. Write what each of the 6 steps are, and include a brief description of what each step involves.</p> <p>1)</p> <p>2)</p> <p>3)</p> <p>4)</p> <p>5)</p> <p>6)</p> <p><i>1) Cracking passwords – Password cracking could be used to help a user recover a forgotten or lost password, or it can also be used to gain unauthorised access to a system.</i></p> <p><i>2) Escalating privileges - Privilege escalation grants the attacker elevated access to the network and its associated data and applications. The goal is to gain administrative access to the network and its associated applications.</i></p> <p><i>3) Executing applications - When the attacker remotely executes malicious applications on the victim's machine.</i></p>	<p>C. Discuss in your group. List 3 pieces of advice that would you give to the students that use the educational system to help defend themselves against password cracking? For each, give a reason as to why it would protect them on the educational system.</p> <p>1)</p> <p>2)</p> <p>3)</p> <p><i>1) Don't use a password that can be used in a dictionary.</i></p> <p><i>A dictionary password could be easily password cracked on the educational system by using an active online attack such as the password guessing dictionary technique.</i></p> <p><i>2) Avoid storing passwords in an unsecured location.</i></p> <p><i>If students store their passwords on their local machine, their passwords can be easily extracted using automated mechanisms such as a USB drive.</i></p>



4) *Hiding files* - The attacker can hide files on a system to prevent their detection. These files can then be used to launch an attack on the system.

5) *Covering tracks* - At this stage the attacker disables logging, clears log files, eliminates evidence, plants additional tools, and covers their tracks to remove any evidence of having done any damage.

6) *Penetration testing* - The last stage of system hacking is to evaluate the security posture of the target network or system.
(Book p104 / PPT Slide 9)

B

To recover passwords from a computer system, special techniques are required. **Write the 5 techniques** for password-cracking and **briefly explain each.**

- 1) _____:
- 2) _____:
- 3) _____:
- 4) _____:
- 5) _____:

1) **Dictionary attacks:** The dictionary is a text file that contains a list of known words up to and including the entire dictionary. An attack of this type takes the form of a password cracking application that has a dictionary file loaded into it. The application uses this list to test different words to recover the password. Dictionary attacks are more useful than brute force attacks, but this attack does not work with a system that uses passphrases.

3) *Never use passwords such as date of birth or mobile number.*

Information gathered during footprinting and scanning may reveal students' personal information, such as such as date of birth or mobile number. If students use this information as their password, it could be easily guessed.

PPT Slide 21, 15

www.almanahj.com



2) **Brute-force attacks:** In this type of attack, every possible combination of characters is attempted until the correct one is uncovered. The time taken will depend on the length and complexity of the password.

3) **Hybrid attack:** This type of attack builds on the dictionary attack, but words are modified with the addition or substitution of special characters, such as Eth@ica0l instead of Ethical.

4) **Syllable attack:** This type of attack is a combination of both a brute-force attack and a dictionary attack. It is used when a password is not a standard word or phrase. It also uses every possible combination of every word in the dictionary.

5) **Rule-based attack:** This type of attack is an advanced attack and is used when the attacker has some information about the password, such as knowing that a password contains a two- or three-digit number.


(Book p108-110 / PPT Slide 19-26)

www.almanahj.com



Rubrics & Marking Rubrics Guidance

- 1) Print the rubrics for each student and fill in the student details.
- 2) Check the work for each task and circle the cell which you feel is appropriate with respect to the task completion. The top row indicates each cell's points.
- 3) Enter the mark for each of the task in the space give below and find the total out of 20. An example is shown below.

 UNITED ARAB EMIRATES MINISTRY OF EDUCATION		Marking Rubrics – Computer Science - Project Task 3 <i>(please print for each student)</i>				
Student ID	12345678	Student Name	Abdullah Ahmed Mohammed Omar	Grade	7	
Q	Excellent 5	Very Good 4	Good 3	Satisfactory 2	Inadequate 1	No Attempt 0
Q 1	All 6 system hacking steps are identified with a brief description	All 6 system hacking steps are identified with a brief description	All 6 system hacking steps are identified with a brief description		1 to 6 system hacking steps are identified. No explanation given	No attempt made
	All 5 password cracking techniques are identified and briefly explained.	All 5 password cracking techniques are identified and briefly explained.	All 5 password cracking techniques are identified and briefly explained.	2 to 5 password cracking techniques are identified with a weak description.	1 to 5 password cracking techniques are identified. No explanation given.	No attempt made
	3 valid password cracking advice listed	3 password cracking advice listed, 2 valid, 1 incorrect	2 valid password cracking advice listed	2 password cracking advice listed, 1 valid, 1 incorrect	1 valid password cracking advice listed	No attempt made
	3 valid password protection reasons listed	3 password protection reasons listed, 2 valid, 1 incorrect	2 valid password protection reasons listed	2 password protection reasons listed, 1 valid, 1 incorrect	1 valid password protection reason listed	No attempt made
Point	0	4 + 4	3	0	1	0
PROJECT TASK 3 TOTAL =					12	/ 20 points



Marking Rubrics – Computer Science - Project Task 3 *(please print for each student)*

Student ID _____ Student Name _____ Grade _____

	Excellent 5	Very Good 4	Good 3	Satisfactory 2	Inadequate 1	No Attempt 0
	All 6 system hacking steps are identified with a brief description	All 6 system hacking steps are identified with a brief description	All 6 system hacking steps are identified with a brief description	3 to 6 system hacking steps are identified with a weak description.	1 to 6 system hacking steps are identified. No explanation given	No attempt made
	All 5 password cracking techniques are identified and briefly explained.	All 5 password cracking techniques are identified and briefly explained.	All 5 password cracking techniques are identified and briefly explained.	2 to 5 password cracking techniques are identified with a weak description.	1 to 5 password cracking techniques are identified. No explanation given.	No attempt made
	3 valid password cracking advice listed	3 password cracking advice listed, 2 valid, 1 incorrect	2 valid password cracking advice listed	2 password cracking advice listed, 1 valid, 1 incorrect	1 valid password cracking advice listed	No attempt made
	3 valid password protection reasons listed	3 password protection reasons listed, 2 valid, 1 incorrect	2 valid password protection reasons listed	2 password protection reasons listed, 1 valid, 1 incorrect	1 valid password protection reason listed	No attempt made
Point	+	+	+	+	+	+

PROJECT TASK 3 TOTAL = / 20 points