United Arab Emirates
Ministry of Education

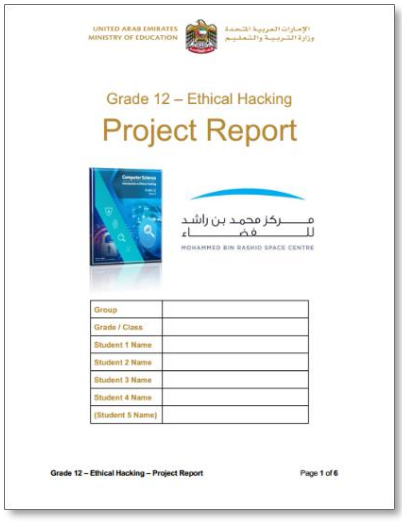
الإمارات العربية المتحدة
وزارة التربية والتعليم

Term 2
Grade 12 -Project Task 2

Teachers Guidelines

Ethical Hacking

Picture 1



Picture 2

PROJECT TASK 2

INTRODUCTION

The **educational system** has databases full of personal information about faculty, staff, and students. Cyber criminals could make money by stealing this personal information and selling it on.

Ethical hacking is an effective way of testing network security, whereby **Scanning** and **Enumeration** are the second and third phases of the process. **Project Task 2 focuses on Units 3 (Scanning) & 4 (Enumeration) of the Grade 12 book.**

Project Task 1 introduced the role of 'Penetration Tester'. As part of Project Task1, Project Task 2 and Project Task 3 & Report 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 Engineer**.

A **Security Engineer** builds and maintains IT security solutions for an organization. They develop security for the company's systems/projects and handle any technical problems that arise. You are asked to

- report on **scanning** in relation to ethical hacking **(Unit 3)**
- report on **enumeration** in relation to ethical hacking **(Unit 4)**
- 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 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)**

PROJECT TASK OBJECTIVES

1. **A.** Using **Unit 3** of the book as a reference, **identify and briefly define** the 3 types of scanning.

   B. Explain in your own words, as to **why** an ethical hacker would want to perform scanning against the educational system.

   C. For all the scanning types in part A, an Ethical Hacker can perform each type of scanning to your educational system and find out what can harm your system.

   Discuss in your group. Find and explain any information which you can detect during **each scanning type**, that could harm your educational system.

2. **A.** Using **Unit 3** of the book as a reference, **identify the different Scanning techniques/tools**.

   B. Telnet commands and **Banner Grabbing** scanning techniques could be used to gather information on your educational system. **Explain how** they could gather information from your educational system.

3. **A.** Using **Unit 4** of the book as a reference, **list the types of enumeration techniques** used by ethical hackers to extract information.

   B. The educational system has many **policies and passwords**. **Which enumeration classification** would be best performed to extract this information **and why?**

   C. The educational system uses many **hardware and network devices**. **Which enumeration classification** would be best performed to extract this information from these devices **and why**?

4. **A.** EthiLAB demonstrates various scanning and enumeration techniques. **Demonstrate how** these techniques return information **for any one command for each of the tools/techniques** of 1) telnet commands 2) banner grabbing 3) nbtstat and 4) SNMP enumeration.

   B. Run only the commands using the software ethiLAB for the example website '**futuresmarteducation.com'.** Follow the steps below:
   - ***Open ethiLAB > Offline Mode***
   - Type the commands for the relevant technique and execute.
   - Take a screenshot or print screen of each of the results and save.

Project Task 2 – Work Plan

Teacher Guidelines:

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

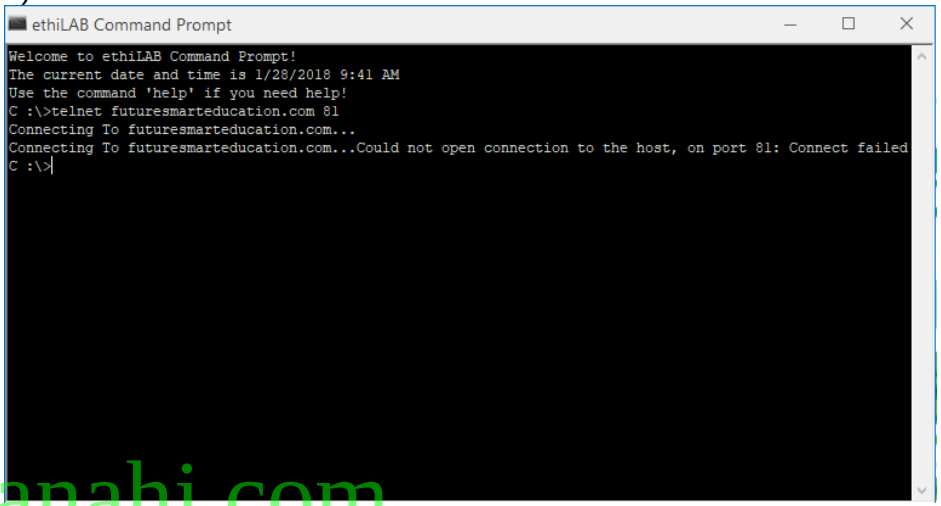
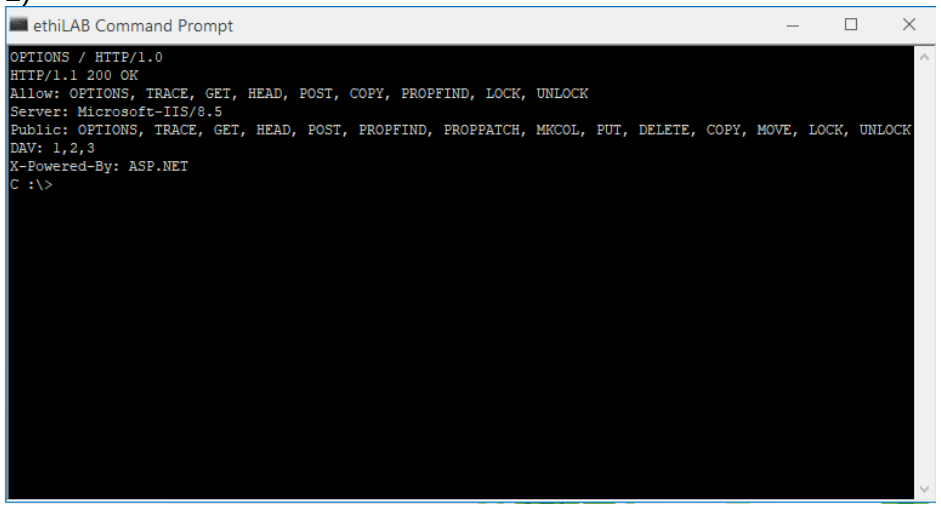
No.	Work Steps	Step Completion & Values
1) A.	Using **Unit 3** of the book as a reference, **identify and briefly define** the 3 types of scanning. • ***Port scanning*** *- is a series of messages is sent to a computer to learn about services and to scans its open ports; through this scan the ethical hacker can determine which port is vulnerable to attack.* • ***Network scanning*** *- a procedure for identifying active hosts on a network, and for scanning IP addresses.* • ***Vulnerability scanning*** *- an automated process of proactively identifying vulnerabilities of computing systems.* ***(Book p65 / PPT Slide 16)***	**1) C.** For all the scanning types in part A, an Ethical Hacker can perform each type of scanning to your educational system and find out what can harm your system. **Discuss in your group. Find and explain any information** which you can detect during **each scanning type**, that could harm your educational system. ***Scanning Type 1: Port Scanning*** *Through port scanning, the Information that could be revealed from the educational system include:* • *the alive host* • *the operating systems involved* • *firewalls* • *intrusion detection systems* • *servers and services* • *physical layout of network* *The educational system contains numerous ports, out of which a few ports are open. Port scanning helps us to identify the ports which are vulnerable(weak) to attack.* *When a student opens his or her email, the education system's server will open a port through which new mail will be downloaded through a connection to the education system's email server. This email can make them a target for any potential hacker.*
1) B.	**Explain in your own words**, as to **why** an ethical hacker would want to perform scanning against the educational system**:** *Scanning process reveals useful information in a system and then use that information for later phases of the penetration testing by ethical hackers.* *Scanning is one of the most important parts of intelligence gathering for an ethical hacker.*	

	Our system is an educational system. Scanning is required for our system. If we as an ethical hacker do the scanning process to our educational system, we can get more information about the host or system which is going to be a target to the hacker. We can then reveal the useful information about that target host or system. Then we as ethical hackers can use that information for the penetration testing. ***(Book p62-64 / PPT Slide 15)***	*When we do the port scanning we can identify this threat and protect our education system.* ***(Book p65-66 / PPT Slides 18,19)*** *https://whatismyipaddress.com/port-scan* **Scanning Type 2: *Network Scanning*** *Network Scanning provides information about which IP addresses map to live hosts that are active on the Internet and what services they offer.* *Ping sweep is a network scanning procedure that could be used for the educational system.* *Using Ping sweep, an ethical hacker would ping the entire range of educational system's network IP addresses to find out which ones are online or alive.* *Once the hacker knows which machines are alive on the educational system, they can focus on which machines to attack and work from there.* *The IP's could be student, principal or faculty addresses.* *By doing the network scanning, we can protect our education system from the hackers to know about out hosts on network and the IP addresses.* ***(Book p68-69 / PPT Slides 22-23)*** *http://www.binarytides.com/ping-sweep-network-nmap/*

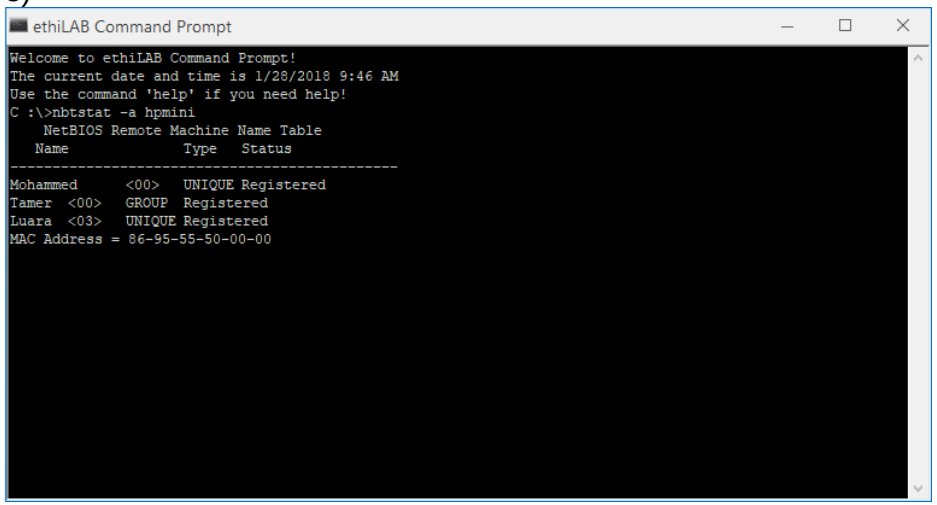
		Scanning Type 3: Vulnerability Scanning *One type of vulnerability scan is the web application security scanner.* *If we perform the web application security scanner to our education system, we could check for hundreds of vulnerabilities(weaknesses).* *Students and teachers visit the educational system's web site for a number of purposes. When they are visiting the web site they may find some link or re direction which can force the user to download a file (called drive-by downloading).* *By performing a vulnerability scan, we as ethical hackers can identify this weakness that could harm our web site users.* *After identifying this weakness, our web site users can be protected from visiting irrelevant web sites or downloading harmful files.* ***[OR]*** *Another example would be to use a computer worm on the educational system.* *A computer worm is a piece of code that roams around a network, looking to exploit known vulnerabilities in machines.* *If the worm is located in a vulnerable target (any computer/host/system) on the educational system, it could infect the host machine and then the worm will start to use that machine and begin looking for other machines on the educational system's network that are similarly vulnerable.* ***(Book p69-70 / PPT Slides 24-26)*** *www.sans.org/reading-room/whitepapers/threats/vulnerabilities-vulnerability-scanning-1195*

2) A.	Using **Unit 3** of the book as a reference, **identify the different Scanning techniques/tools:** • *Telnet Commands* • *Banner Grabbing* • *Nmap* • *Angry IP scanner* ***(Book p71-77 / PPT Slide 16)***	**2) B. Telnet commands** and **Banner Grabbing** scanning techniques could be used to gather information on your educational system. **Explain how** they could gather information from your educational system. **<u>Telnet Commands</u>:** *Telnet commands can be used to search for all open ports in a telnet command loop.* *TCP port (port 80) of our educational system is a very important port. To check if a TCP port is open or reachable on the educational system it is possible to use the telnet command.* *Using the 'portqry' telnet command it would be possible to find the open range of ports using the educational system's URL for a specific accepted protocol (TCP, UDP) running behind the port.* ***(Book p71-72 / PPT Slides 27-32)*** **<u>Banner Grabbing</u>**: *Banner grabbing is a technique used to gain information about a computer system on a network and the services running on its open ports.* *Banners are the welcome screens that can reveal software version numbers and other system information on network hosts.* *The educational system's login screen contains banner information. It is intended for administrative use but could also provide access to a hacker.* *This banner information for the educational system could potentially identify the operating system, the version number, and the specific service packs.* ***(Book p73-74 / PPT Slide 33-40)***

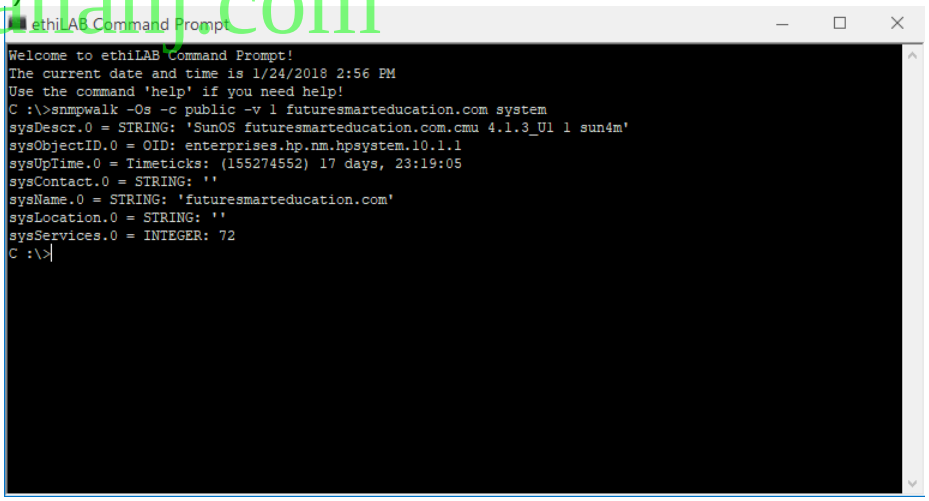
3) A.	Using **Unit 4** of the book as a reference, **list the types of enumeration techniques** used by ethical hackers to extract information • *Extract usernames using email IDs* • *Extract information using the default passwords* • *Brute Force (guessing) active directory* • *Extract usernames using SNMP* • *Extract information using DNS zone transfer* • *Extract (capturing) user groups from Windows* ***(Book p86-87 / PPT Slide 11)***	**3) B -** The educational system has many **policies and passwords**. **Which enumeration classification** would be best performed to extract this information **and why**? *Our group suggests that a NetBIOS enumeration classification is best, as it is used to obtain the policies and passwords and the list of computers that belong to the educational system's domain.* *This enumeration classification also helps to obtain the list of shared resources (printers, servers etc) of the individual hosts on the educational system's network.* ***(Book p89 / PPT Slide 11-15)*** **3) C** - The educational system uses many **hardware and network devices**. **Which enumeration classification** would be best performed to extract this information from these devices **and why**? *Our group suggests that the Simple Network Management Protocol (SNMP) enumeration classification is best, as it is used to manage, monitor and maintain hardware devices connected to the educational system's network, such as hosts, routers, and in general any device that supports the network.* ***(Book p95 / PPT Slide 11-13)***

4) A.	EthiLAB demonstrates various scanning and enumeration techniques. **Demonstrate** how these techniques return information **for any one command for each of the tools/techniques** of 1) telnet commands 2) banner grabbing 3) nbtstat and 4) SNMP enumeration. **1) Telnet command (Scanning):** ***telnet [Host URL] [Port number] (To check if a TCP port is open or reachable is to use the telnet command)*** ***(Book p71-72 / PPT Slides 27-32)*** **2) Banner Grabbing (Scanning):** ***telnet [domain] [FTP port]*** ***SYST (To Identify the running operating system and FTP server version)*** ***(Book p73-75 / PPT Slides 33-40)*** **3) nbtstat (Enumeration):** ***nbtstat – a hpmini (To get the NetBIOS hpmini table of a remote computer)*** ***(Book p90-92 / PPT Slides 15-24)*** **4) SNMP (Enumeration):** ***snmpwalk (To retrieve a subtree of management values under a system variable)*** ***(Book p97-99 / PPT Slides 30-34)***	**4. B)** Running the command on ethiLAB produces the following results: 1)  2) 

3)



4)



United Arab Emirates
Ministry of Education

الإمـارات العـربيـة المتحدة
وزارة التربيـــة والتعليـــم

Marking Rubrics – Computer Science - Project Task 2 *(please print for each student)*

Student ID _____ **Student Name** _____ **Grade** _____

Q	Excellent 5	Very Good 4	Good 3	Satisfactory 2	Inadequate 1	No Attempt
Q 1	• All 3 types of scanning are identified and defined • Clear explanation for scanning given. • All scanning types' information is clearly explained with suitable examples.	• All 3 types of scanning are identified and defined • Clear explanation for scanning given. • 2-3 scanning types' information are clearly explained with suitable examples.	• All 3 types of scanning are identified and defined • Explanation for scanning given. • 1-2 scanning types' information are clearly explained with suitable examples.	• All 3 types of scanning are identified • Explanation for scanning given. • 1-3 scanning types' information are explained with no suitable examples.	• All 3 types of scanning are identified • Unclear Explanation for scanning given. • No scanning types' information are clearly explained without suitable examples.	No attempt made
Q 2	• All 4 scanning techniques/tools are listed • Both techniques have been clearly explained.	• All 4 scanning techniques/tools are listed • One or both techniques have been clearly explained.	• All 4 scanning techniques/tools are listed • Both techniques have been vaguely explained.	• All 4 scanning techniques/tools are listed • Only 1 technique has been vaguely explained.	• All 4 scanning techniques/tools are listed • No technique has been explained clearly.	No attempt made
Q 3	• All 6 enumeration techniques are listed • Identified the correct enumeration classification for both scenarios and clearly explained.	• All 6 enumeration techniques are listed • Identified the correct enumeration classification for one or both scenarios, but only one clearly explained.	• All 6 enumeration techniques are listed • Identified the correct enumeration classification for both scenarios, but neither clearly explained.	• All 6 enumeration techniques are listed • Identified the correct enumeration classification for only one scenario and not clearly explained.	• All 6 enumeration techniques are listed • Did not identify the correct enumeration classification for either scenario.	No attempt made
Q 4	All 4 commands using ethiLAB software have been demonstrated with evidence.	Any 3 commands using ethiLAB software have been demonstrated with evidence.	Any 2 commands using ethiLAB software have been demonstrated with evidence.	Any 1 command using ethiLAB software has been demonstrated with evidence.	Commands using ethiLAB software have been attempted, but no evidence or with errors.	No attempt made
Point	+	+	+	+	+	+

TOTAL = / 20 points