Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAM
SEMESTER II
SESSION 2021/2022

COURSE NAME	:	SECURITY ASSESSMENT AND TESTING
COURSE CODE	:	BIS 33703
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JULY 2022
DURATION	:	3 HOURS
INSTRUCTION	:	1. ANSWER ALL QUESTIONS 2. THIS FINAL EXAMINATION IS AN **ONLINE** ASSESSMENT AND CONDUCTED VIA **CLOSED BOOK** 3. STUDENTS ARE **PROHIBITED** TO CONSULT THEIR OWN MATERIAL OR ANY EXTERNAL RESOURCES DURING THE EXAMINATION CONDUCTED VIA CLOSED BOOK

THIS QUESTION PAPER CONSISTS OF **FIVE (5)** PAGES

Q1 Compare phase 4 of Penetration Testing Execution Standard (PTES) and Zero Entry Hacking (ZEH) penetration test methodologies.

(10 marks)

Q2 Write a suitable Google search based on **Figure Q2** and **Table Q2** by using **THREE (3)** Google hack operators.

Figure Q2

Table Q2

URL1	http://reg.upm.edu.my/eISO/portal/audit_dalam/2013/NCR%20DAN%20OFI%20AUDIT%20DALAMAN%2019.03.2013.xls
URL2	http://reg.upm.edu.my/eISO/portal/audit_dalam/2013/Penemuan%20Audit%20Dalaman-Paparan%20Web%208.0.4.2013.xls
URL3	http://reg.upm.edu.my/eISO/portal/audit_dalam/2013/NCR%20DAN%20OFI%20AUDIT%20DALAMAN%2018.03.2013.xls

(6 marks)

Q3 Write a suitable Google search based on **Figure Q3** and **Table Q3** by using **FOUR (4)** Google hack operators.

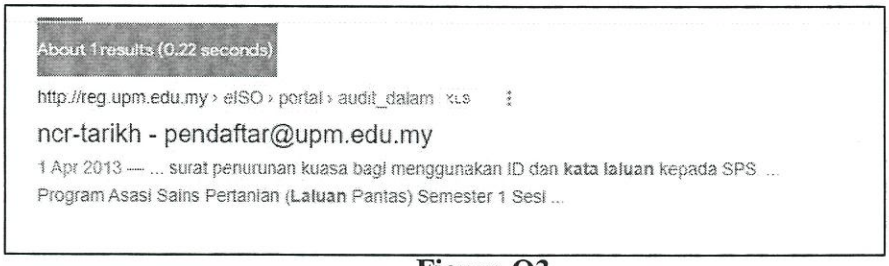

Figure Q3

Table Q3

URL	http://reg.upm.edu.my/eISO/portal/audit_dalam/2013/Penemuan%20Audit%20Dalaman-Paparan%20Web%208.0.4.2013.xls

(6 marks)

Q4 Write a suitable google hack search for the following questions:

(a) Search for all google sites in Malaysia.

(3 marks)

(b) Exclude Google Translate (https://translate.google.com.my) for google hack from **Q4(a)**.

(3 marks)

(c) Search for port 10000 for google hack from **Q4(b)** .

(3 marks)

Q5 Write **ONE (1)** search for all devices in 3.25.177.0, in Australia, runnning secure shell (ssh) service for a specific SSH-2.0-OpenSSH_6.6.1 version in shodan.io using **FOUR (4)** search filters. You can refer to **Figure Q5** below.

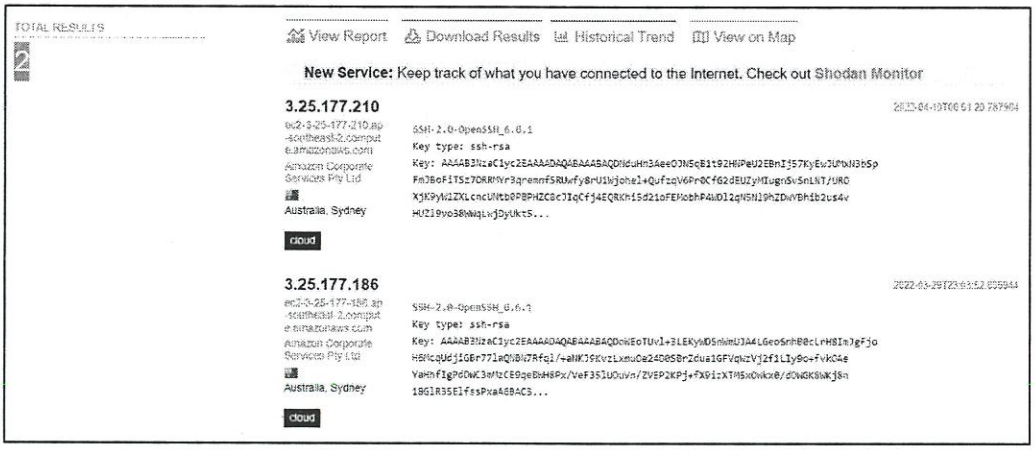

Figure Q5

(13 marks)

Q6 Your organization is currently having a medium security posture(security environment). Your organization already have it's own Blue Team.

Justify whether your organization need to establish a Red Team.

(10 marks)

Q7 Your organization is currently having a low security posture (security environment). The management request for your expertise to decide whether to go for White Box, Black Box or Gray Box penetration testing.

(a) Suggest a suitable penetration testing category, based on the information given above.

(1 mark)

(b) Justify your answer in **Q7(a)** by giving **THREE (3)** points.

(9 marks)

Q8 You are given these sites, namely www.uthm.edu.my, www.google.com.my and www.utem.edu.my. Simple Mail Transfer Protocol (SMTP), Lightweight Directory Access Protocol(LDAP) and Domain Name Server(DNS) are the protocols related to these sites. Assume that you are using Windows 10, and currently you are at root directory D (D:).

(a) Write **ONE (1)** nmap command.

(5 marks)

(b) Explain the command given in **Q8(a)**.

(5 marks)

Q9 Discuss **THREE (3)** advantages of google cache in penetration testing. Justify your answer.

(10 marks)

Q10 A company called Pentesz was requested to run a penetration testing service for UMW Technology Sdn Bhd (UTSB). At the end of the penetration test activity, Executive Summary and Technical Report has been prepared for UTSB.

(a) Discuss **ONE (1)** importance of the report for the CEO of UTSB.

(5 marks)

(b) Discuss **ONE (1)** importance of the report for the IT Technical staff of UTSB.

(5 marks)

Q11 Why an external auditor company is approached for auditing the security system of a company? Justify your answer.

(6 marks)

-END OF QUESTIONS-