UNIVERSITY
OF
JOHANNESBURG

Faculty of Science

Academy of Computer Science and Software Engineering

Module **IT08X57**
Information Security in the WWW

Campus APK

Exam 4 Novermber 2021

Date 4 November 2021

Time 08:30

Assessor Mr R Spijkerman

External Moderator Prof M Olivier
(University of Pretoria)

Duration 120 minutes

Marks 100

Please take careful note of the following:

1. Answers may be typed, or hand-written and photographed.

2. Answers must pertain to the material covered during the course of the module.

3. Discussion questions do not have dedicated marks for format and structure, but please attempt to keep your discussion cohesive.

4. Where possible, upload your submission as a single PDF document.

5. Please DO NOT compress (ZIP, RAR, etc.) your submission.

6. This question paper consists of **three (3)** pages, including this cover page

7. Submit to Eve as well as Dropbox (https://www.dropbox.com/request/EKK5sEKCusldoYzRm8XR)

Question 1

Discuss the importance of the following steps in the generic testing process:

- Initial Agreement
- Documentation and Reporting

Your discussion should also refer to the impact of the other steps in the testing process.

[10]

Question 2

During the information gathering stage of the testing process, one might look to Open-source Intelligence (OSINT) or attempt to gain information through social engineering. Within this context, compare OSINT and social engineering with regards to:

- The type of information that can be gained.
- The necessary techniques and skills.
- The risks involved as an attacker.

[10]

Question 3

Cryptojacking malware allows an attacker to mine cryptocurrencies using a victim's resources without their knowledge or consent. At a large scale, this can be extremely lucrative and as such new cryptojacking malware is constantly being released.

Compare the two techniques antivirus software might use to detect malware and discuss which technique you believe would be more successful against cryptojacking malware.

[10]

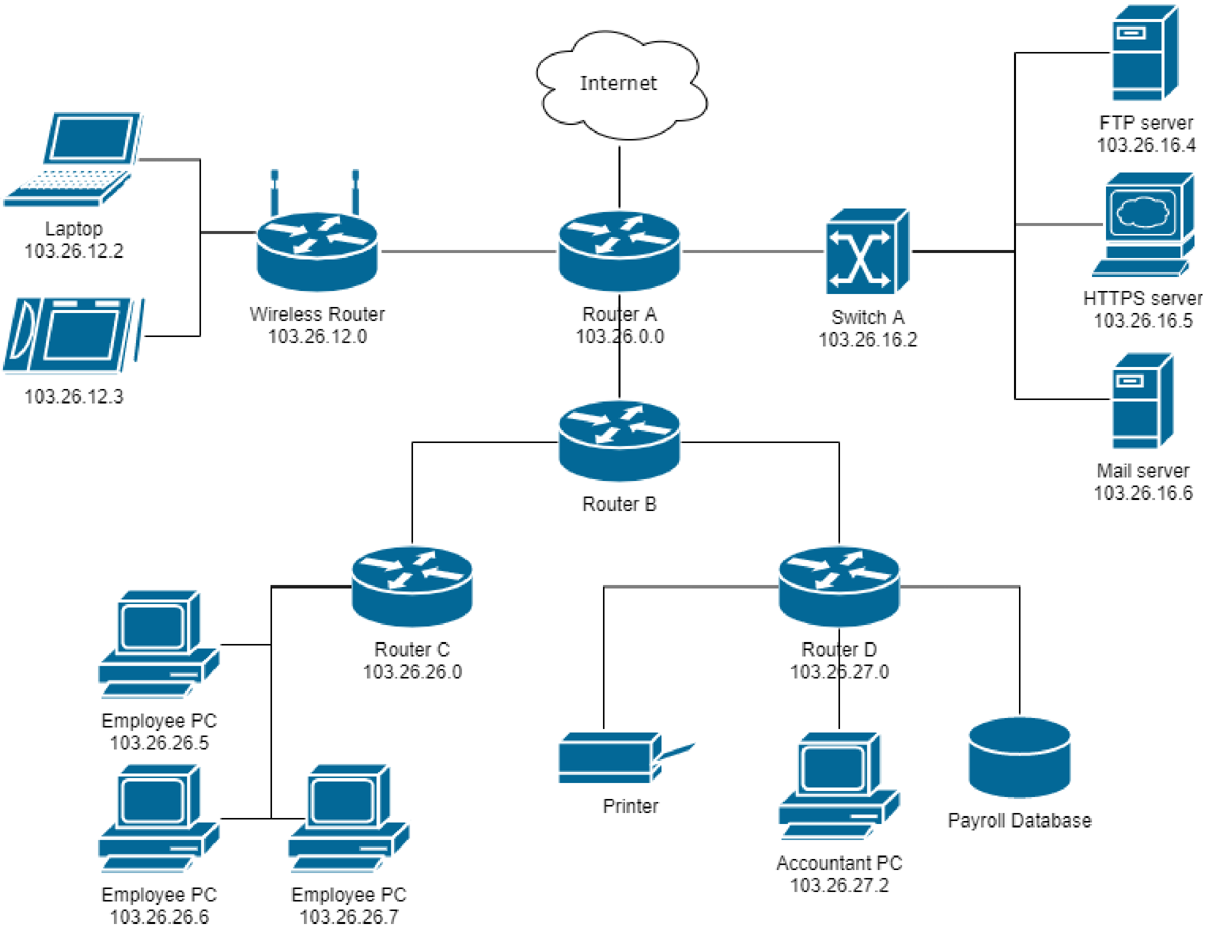
Question 4

4.1. With the aid of a diagram, describe any **one (1)** type of Man-in-the-Middle attack between Jack and Sally. (5)

4.2. How would you enable such a Man-in-the-Middle attack? (5)

[10]

Question 5



The owner of the above network has deployed antivirus software to all of the applicable machines on the network. There are, however, still several security vulnerabilities depicted in the diagram. Choose any **two (2)** vulnerabilities present in the above network. For each chosen vulnerability you must:

- Briefly introduce and discuss the security vulnerability. (3)
- Discuss a potential improvement and how it should be implemented the above network. (7)

(10)x2

[20]

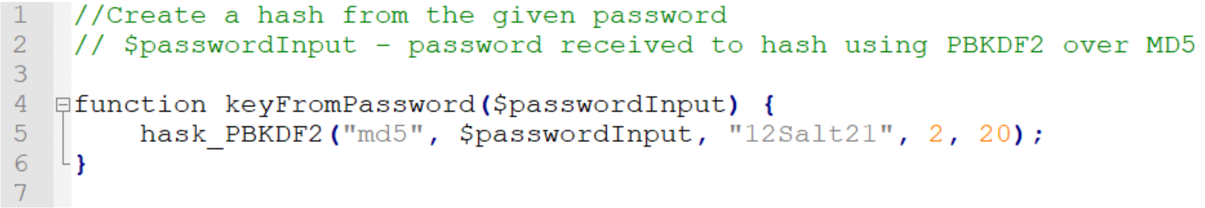
Question 6

The Open Web Application Security Project (OWASP) is a not-for-profit organisation whose aim is to find and fight web application vulnerabilities. They regularly publish a TOP TEN list of vulnerabilities.

For each of the following examples, below, identify the OWASP Top 10 vulnerability and discuss the following:

a)	The vulnerability and its impact.	(2*3)
b)	How the vulnerability can be detected.	(2*3)
c)	One (1) method of fixing the vulnerability.	(2*3)

Example1.php

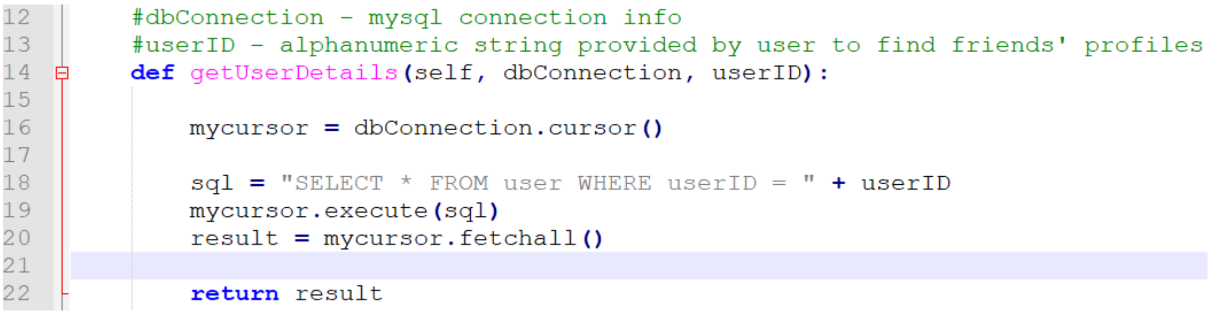


```php
//Create a hash from the given password
// $passwordInput - password received to hash using PBKDF2 over MD5

function keyFromPassword($passwordInput) {
    hask_PBKDF2("md5", $passwordInput, "12Salt21", 2, 20);
}

```

Example2.py



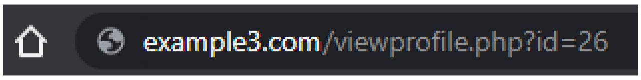
```python
#dbConnection - mysql connection info
#userID - alphanumeric string provided by user to find friends' profiles
def getUserDetails(self, dbConnection, userID):

    mycursor = dbConnection.cursor()

    sql = "SELECT * FROM user WHERE userID = " + userID
    mycursor.execute(sql)
    result = mycursor.fetchall()

    return result
```

Example 3



example3.com/viewprofile.php?id=26

[18]

Question 7

Consider any **three (3)** design flaws that may exist in authentication systems and discuss the points below for each flaw:

a)	What the design flaw is.	(2*3)
b)	How it might be discovered and attacked.	(2*3)

[12]

Question 8

Consider your research project for this semester, briefly discuss the vulnerability you identified. Refer to:

- The vulnerability's origin,
- How the vulnerability might be used during the penetration testing process.
- A countermeasure or fix for the vulnerability.
- The effectiveness of the countermeasure.

[10]

END

[Total: 100]