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

MEMO

DO NOT PRINT

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]

5 marks for each step – 3 for discussing importance of each step, 2 for linking to impact of the other steps:

The answer should look something like this but may vary

Initial agreement

- **Sets the conditions of the assessment**
  - **Refer to the cost related to further steps not being followed correctly such as vulnerabilities not being discovered or unnecessary testing**
- **Get the agreement in writing (contract) to avoid any potential legal issues later on**
  - **Other steps in the testing process, especially exploit and escalation, would lead to legal action if not part of the agreed testing process**
- **Results in a project management map that provides a structured and formal road map to tasks involved**

Documentation and Reporting

- **you were paid to provide answers – this is where you present them**
- **Document everything and verify your results**
- **Follow up (post-test)**
- **If the client is not provided with a report then they cannot attempt to defend against the vulnerabilities that were discovered as part of the test**
- **Non-technical staff may not realise the severity of the situation of not properly reported on. Know your audience**

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]

-maximum of 4 marks per subsection

Possible comparisons

Type of information:

- OSINT – any of the OSINT Organisational or Individual dimensions
- OSINT is all publicly available – may also be outdated
- Communication is not an absolute, finite thing – social engineering targets may not interpret the message the way it was intended, thus impacting the information your receive
- Information depends on whom you talk too for example you may need to find a more technical employee to get information about potentially vulnerable services on the machines.
- May also refer to information about the physical locations and employees such as physical security or employees carrying key cards (for social engineering as it was covered in the same section as social engineering)

Necessary techniques & skills

- For OSINT - Gathering, processing, analysing publicly available data such as
    - Media
    - Search engines
    - Academic sources
    - Metadata
    - Business reports
- Any reference to technical skills required to interpret and understand the gathered OSINT
- For social engineering
    - Pretexing
    - Observation
    - Elicitation
    - Also accept dumpster diving
    - Phishing

The risks involved as an attacker.

- OSINT – less risk if any due to open-source nature
    - May get picked up on of following a more active approach, but otherwise completely passive or at worst seen as normal traffic/interactions
    - Information may be out of date
- Social engineering – riskier due to direct communication
    - If done poorly could "shut down" the target and not get any information (Too many questions or making the target otherwise suspicious)

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]

Compare signature vs Heuristics based approach for malware detection – 4 marks for each of the two types

2 marks for identifying which is the better solution, based on identified properties. Most likely students will identify heuristics based as the most effective technique due new malware being released, but with a similar function and thus similar activity to be detected. However, any valid argument can be accepted.

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)

Any one of the following attacks:

- **Interception**
- **Interruption**
- **Modification**
- **Replay**
- **fabrication**

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

[10]

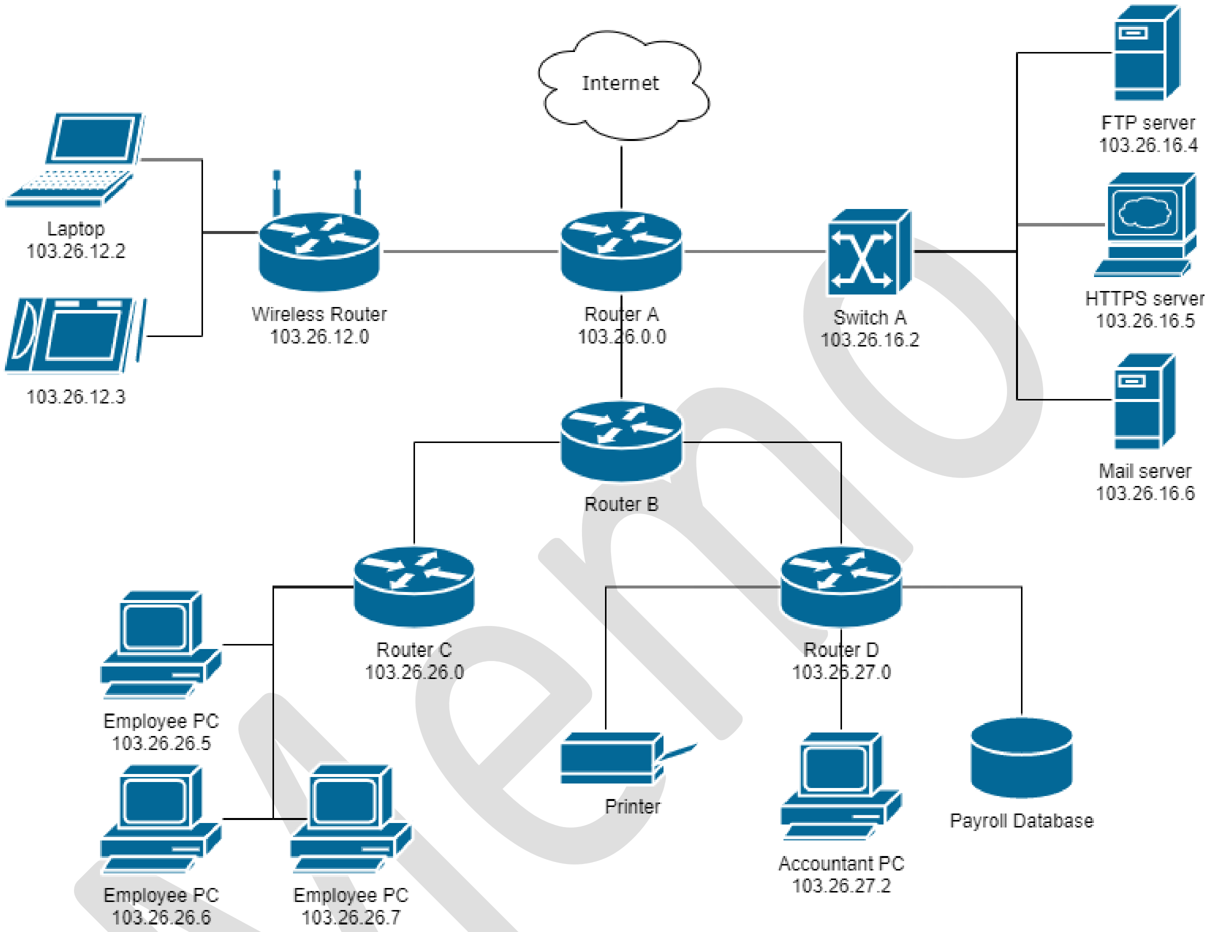
Network sniffing to capture packets

Different types of sniffing:

- **Active sniffing**
  - **Interact directly with target machine**
  - **e.g. ARP spoofing; MAC flooding**
  - **Discuss ARP spoofing & MAC flooding and why it is done**
- **Passive sniffing**
  - **Sit on network and capture packets sent and received**

- **Targets hub-based or wireless networks**

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]

Possible vulnerabilities:

- **No DMZ**
- **No NAT**
- **No IDS or IPS**

- **No firewall – between network and Internet or for internal secure areas**
- **Any other valid vulnerability that is depicted on the diagram**

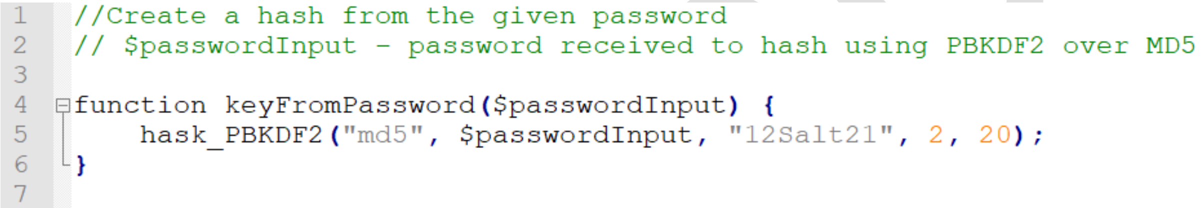
Question 6

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



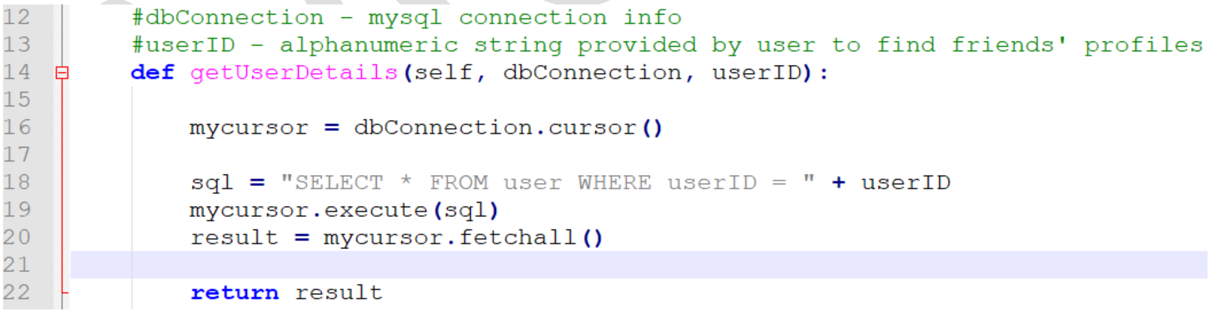
```
//Create a hash from the given password
// $passwordInput - password received to hash using PBKDF2 over MD5

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

Sensitive data exposure

Weak password hashing techniques

Fixed with a better hashing algorithm & not a static salt & more iterations for PBKDF2

Example2.py

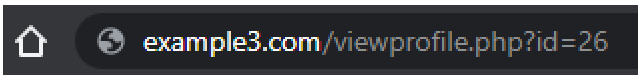


```
    #dbConnection - mysql connection info
    #userID - alphanumeric string provided by user to find friends' profiles
    def getUserDetails(self, dbConnection, userID):

        mycursor = dbConnection.cursor()

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

        return result
```

Injection

Fixed with sanitised input

Example 3



example3.com/viewprofile.php?id=26

Insecure direct object reference

Fixed by always checking user access

[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]

Any of the following

- **Allowing bad passwords**
- **Brute forcible login**
- **Verbose failure message**
- **Vulnerable transmission**
- **Predicable usernames**
- **Password change – either not allowed or forced**
- **Forgotten passwords**
- **Remember Me**
- **Authorisation issues**
- **Nonunique usernames**
- **Poor Multi-factor authentication**
- **Insecure credential storage**

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]

Student answer

END

[Total: 100]