UNIVERSITY OF JOHANNESBURG

# FACULTY OF SCIENCE

Academy of Computer Science and Software Engineering

|  |  |
|---|---|
| Module | IT08X57<br>Information Security in the WWW |
| Campus | APK |
| SSA | January 2020 |

|  |  |  |  |
|---|---|---|---|
| Date | January 2020 | Time | 08:30 |
| Assessor |  | Mr F F Blauw |  |
| External Moderator |  | Prof B L Tait<br>(UNISA) |  |
| Duration | 120 minutes | Marks | 100 |

The question paper consists of 4 pages

Instructions:

- Answer all questions.
- Please write neatly and legibly.
- Do not write in pencil.
- Ensure that all diagrams are neatly drawn.
- Unless otherwise stated, diagrams do not constitute complete answers.

## QUESTION 1

In Information Theoretic Security, it is stated that to achieve perfect secrecy the size of the key must be equal or greater to that of the message, as shown below:

$$|\mathcal{K}| \geq |\mathcal{M}|$$

where $\mathcal{K}$ is the space of all keys and $\mathcal{M}$ is the space of all messages.

However, distributing such a long key would defeat the purpose of secret message exchange. Describe how this drawback is overcome.

**[10]**

## QUESTION 2

Due to the ever-growing threat of potential intrusion, companies – great and small – are concerned that the security of their information systems may be the target of data breaches. These companies are hiring security testers to test the security of their information systems. However, does the testing strategy differ depending on the size of the organisation?

Provide a comprehensive strategy in which you describe how you will carry out a security test from start (being appointed) to finish (reporting your findings) all the while referring to the size of the company. Your essay should discuss the various phases of penetration testing, including:

- Information Gathering
- Scanning & Enumeration
- Exploit
- Post-Exploitation

**[30]**

## QUESTION 3

3.1. Discuss the major differences between (a) Stateful Inspection and (b) Stateless inspection firewalls. (6)

3.2. Discuss IDPS (IDS/IPS) system in terms of its setup and operation. In your discussion make sure discuss the types of approaches and IDPS can take to perform its function. (15)

3.3. Of the multiple approaches that an IDS/IPS system can take to perform its function, which is the best? Motivate you answer. (2)

**[25]**

## QUESTION 4

Consider the following parts of code for logging in:

`login.html` (snippet)

```
<form action="login.php" method="GET">
  Username: <input type="text" name="username"/><br/>
  Password: <input type="text" name="password"/><br/>
  <input type="submit" value="Log in"/>
</form>
```

`login.php`

```
function runSQL($query) {
  // connect to database, run $query, close connection
  // if data is returned, return first record
}

// Create a hash from the new password
//   $passwordInput - Password received to hash using PBKDF2 over MD5
//   $salt - Salt to mix with password
function keyFromPassword($passwordInput) {
    hash_PBKDF2("md5", $passwordInput, "salt123", 2, 20);
}
// Call when logging in
//   $usernameInput - Username as given by user.
//   $passwordInput - Password has given by user.
function PerformLogin($usernameInput, $passwordInput) {
    $result = runSQLPrepared("SELECT * from Users WHERE Username = ?", $usernameInput);
    if ($result != FALSE) {
        $testPassword = keyFromPassword($passwordInput);
        if ($testPassword == $result['hashedPassword']) {
            echo "Welcome back, ".htmlspecialchars($result['firstName']);
        } else {
            echo "Sorry, ".htmlspecialchars($result['firstName']).", your password was incorrect. Please try again.";
        }
    }
    else {
        echo "Username ".htmlspecialchars($usernameInput)." was not found in our records.";
    }
}
```

Identify **five (5)** potential vulnerabilities (of different types – for example, do not show two *SQL Injection vulnerabilities*). **For each** vulnerability identified, discuss the following:

a) Where is the vulnerability? Why is it a vulnerability? (3)

b) Suggest one (1) method of fixing the vulnerability. (2)

5×(3) = **[20]**

**QUESTION 5**

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

- Origin of the vulnerability
- Reason for the vulnerability
- Countermeasure / Fix for vulnerability
- Critique of countermeasure

**[15]**

***— END OF EXAM —***

**Grand Total: [100]**