UNIVERSITY OF JOHANNESBURG

FACULTY OF SCIENCE

Academy of Computer Science and Software Engineering

Module	**IT00057 / IT08X57** Information Security in the WWW
Campus	APK
Exam	November 2016

Date	25 November 2016	**Time**	08:30
Assessor		Mr F F Blauw	
External Moderator		Prof J van Niekerk (NMMU)	
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

You have been appointed as a penetration tester for **RedRoBank**, a popular bank that thrives on its reputation as a cutting-edge bank that leverages technologies to provide its clients with the best financial services possible.

Due to the ever present threat of potential intrusion, the directors are concerned that the security of their information systems may be the target of data breaches.

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

- Reconnaissance & Footprinting
- Port Scanning & Enumeration
- Exploitation
- Post-Exploitation

[25]

QUESTION 2

RedRoBank employees are complaining that **Norman**, their anti-virus suite, takes too long to scan flash disks and is “hampering our productivity”. Management wants to know whether it is still useful to have anti-virus software despite having firewalls. You respond to their concerns by writing a report that has the following headings:

1. Introduction
2. Description of malware and types of malware
3. Techniques an Anti-Virus uses to detect malware
4. What an Anti-Virus does once malware is detected
5. Conclusion: Do you really need an Anti-Virus?

Bear in mind that this report will be read mostly by non-technical management; as such your explanation and language usage should be for the “layman”.

[20]

QUESTION 3

After the fiasco with the anti-virus, the directors of **RedRoBank** would like to know more about the firewalls they have in place.

3.1. Discuss the major differences between (a) Stateful Inspection and (b) Stateless inspection firewalls. (4)

3.2. Name and briefly discuss the two (2) possible network configurations for an IDPS. You may use diagrams to help you in your discussion. (6)

3.3. Of the multiple approaches that an IDS/IPS system can take to perform its function, discuss the one (1) that you believe is the best. Motivate you answer. (6)

3.4. Honeypots are essentially decoys. Discuss how they can supplement an IDPS. Are they actually of any use, nowadays? (4)

[20]

QUESTION 4

Consider the following parts of code for logging in:

login.html (snippet)

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

login.php

```
6:  function runSQL($query) {
7:    // connect to database, run $query, close connection
8:    // if data is returned, return first record
9:  }

10: // Create a hash from the new password
11: //   $passwordInput - Password received to hash using PBKDF2 over MD5
12: //   $salt - Salt to mix with password
13: function keyFromPassword($passwordInput, $salt) {
14:   hash_PBKDF2("md5", $passwordInput, $salt, 2, 20);
15: }
16:
17: // Call when logging in
18: //   $usernameInput - Username as given by user.
19: //   $passwordInput - Password has given by user.
20: function PerformLogin($usernameInput, $passwordInput) {
21:   $result = runSQL("SELECT * from Users WHERE Username =
      $usernameInput;");
22:   if ($result != FALSE) {
23:     $testPassword = keyFromPassword($passwordInput, $result['salt']);
24:     if ($testPassword == $result['hashedPassword']) {
25:       echo "Welcome back, ".$result['firstName'];
26:     } else {
27:       echo "Sorry, ".$result['firstName'].", your password was incorrect.
          Please try again.";
28:     }
29:   }
30:   else {
31:     echo "Username ".$usernameInput." not found in our records.";
32:   }
33: }
```

Identify **four (4)** potential vulnerabilities. **For each** vulnerability identified, discuss the following:

a) What and where is the vulnerability? (1)

b) Why is it a vulnerability? (2)

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

4×(5) = **[20]**

QUESTION 5

We live in an age where most of our personal data is stored on the information systems of companies that we deal with. **RedRoBank** is of these companies. This data is not only valuable to them, but can also lead to identity theft of their clients if this data were obtained by malicious actors.

In the case of a data breach where all client personal data is stolen, what do you think **RedRoBank** should do? Bear in mind **RedRoBank**'s reputation and monetary value.

[5]

QUESTION 6

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

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

[10]

— END OF EXAM —

Grand Total: [100]