UNIVERSITY OF JOHANNESBURG

FACULTY OF SCIENCE

Academy Of Computer Science and Software Engineering

Module	**IT00057 / IT08X57** Information Security in the WWW
Campus	APK
Examination	November 2014

DATE	7 November 2014	**SESSION**	08:30 – 10:30
ASSESSORS		FF Blauw WS Leung	
EXTERNAL MODERATOR		Prof HS Venter *(University of Pretoria)*	
DURATION	120 minutes	**MARKS**	100

Please take careful note of the following:

1. Answer **ALL** questions in the ANSWER SHEET supplied.
2. Do NOT write in pencil. **Anything in pencil <u>will not be marked</u>.**
3. Write neatly and legibly.
4. Answers must pertain to the material covered during the course of the module.
5. This question paper consists of 4 pages, including this cover page.

QUESTION 1

You have been appointed as a penetration tester for ABND, a Fortune 501 international consulting firm that boasts a wide range of clients ranging from government to large corporate entities with offices located on various continents.

Due to the ever present threat of corporate espionage, the directors are concerned that the security of their information systems (hosting sensitive client information) 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 answer should discuss the various phases of penetration testing including:

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

[30]

QUESTION 2

You have been tasked to improve the remote authentication system of ELSA (Extended Lifeform Securing Authentication). This authentication system currently only requires a username and password. However, due to recent events with the eyeCl0ud, the management of ELSA has decided that additional authentication will be required. At this stage, expensive systems such as biometrics cannot be afforded.

Briefly discuss one method to improve the ELSA system and why it will improve the authentication. In your discussion, provide an outline and explanation of the technology you want to implement.

[10]

QUESTION 3

Does antivirus software work? Your discussion should include the following topics:

- How easy is it for one to author malware?
- Briefly discuss various approaches that an antivirus may employ to detect malware.
- If an infected file is detected, what does the antivirus software do to restore it?
- From a holistic view, is antivirus software effective at combating malicious software?

[10]

QUESTION 4

4.1. WEP (Wired Equivalent Privacy) had three goals, two of which were:

- Confidentiality
- Access Control

Briefly discuss these TWO aspects and how the WEP implementation failed. (6)

4.2. "Shell Shock" is a bug that was discovered in the Bourne Again Shell (BASH). Briefly discuss this vulnerability and how it can be exploited. (4)

[10]

QUESTION 5

5.1. Rate the computation and security performance of the following types of firewall with one of the following ratings: Best, Good, Average, and Worst.

Firewall Type	Computation	Security
Stateless		
Stateful		
Circuit-level		
Application-level		

(4)

5.2. Name and briefly discuss the two possible network configurations for an IDPS. (4)

5.3. What is canoncalisation and how could it be used to bypass an IDPS? (2)

[10]

QUESTION 6

TakeSomeMore are planning to launch an online shopping platform. You have been asked to assess their web application for possible vulnerabilities. Note: You will only be investigating the web system, not the network and hardware surrounding it. Discuss the approach you will take as well as the aspects you will be looking at.

[10]

QUESTION 7

7.1. Discuss how proxies could be considered a useful tool for hackers. (4**)**

7.2. Discuss the role of memory forensics as a defence and analysis technique for security testers concerned with information security in the WWW. (6)

[10]

QUESTION 8

Considering the guest lecture, discuss two of the primary threats discussed and exploited.

[10]

— END OF EXAMINATION ☺ —

GRAND TOTAL [100]