ABU DHABI POLYTECHNIC
Information Security Engineering Technology Department

Advanced Web Security
(NCS- 321)

Final Examination

Q2 Quarter 2015/2016

2 hours

Instructor Charles

Students answer on the question paper

No additional materials are required

STUDENT NAME									
STUDENT NUMBER									
CRN	1	2	6	0	DEPARTMENT	**ISET**			

READ THESE INSTRUCTIONS CAREFULLY

Write your *name*, *number*, *CRN* and department **clearly** in the boxes above.

Answer **all** questions.

Show **all** you're working and use appropriate **units.** Otherwise, you may lose marks.

Answers those are not **clearly readable**, if any, will not be marked.

Question	Score	CLO
1	/5	1, 4, 5
2	/10	5
3	/20	2, 3, 4, 5
4	/15	1, 3, 4,5
Total	**/50**	

All mobile devices are not allowed during examination.

Abu Dhabi Polytechnic considers cheating or attempting to cheat a serious offense that will result in disciplinary action taken against involved individuals.

	MAXIMUM	Your SCORE
	50	

Abu Dhabi Polytechnic
Information Security Engineering Technology Department

Final Exam Date: 26/11/2016
Exam Duration: 2 hours

Instructions

- This exam has 4 (FOUR) questions. Please attempt all questions.
- Show all solution steps for full credit and state any assumptions explicitly.
- You may only use a simple and standard calculator.

Question 1 Describe the following [5 points]

Consider the case scenario of an online auction website where a user is trying to auction his item. The situation is as such that the website prevents attackers from guessing the passwords of users by temporarily locking accounts that receive too many failed attempts (5 tries) in a given amount of time. Once an account is locked, the attacker (or the user) must wait for a timeout to expire (1 hr) before attempting to login again.

Discuss in detail how the attack happens and propose suitable solution/solutions.

Question 2 Describe the following [Total: 10 points]

Reverse Engineering is vital in reproducing anything based on the extracted information. Explain how information is extracted following WARE approach. Briefly describe all four processes involved within the flow of WARE analysis along with the process diagram. Draw sample diagrams for the processes wherever applicable. Give two examples of tools which assist in reverse engineering.

Question 3 Answer in Short **2 points each [Total: 20 points]**

1. Name atleast one tool and one technique which can be used to prevent SQL injection attack in common web systems

2. What do you mean by Registration Authority and what is their role in-terms of issuing Digital certificates?

3. Define asymmetric Key cryptography and explain why is it better than a Symmetric Key system

4. A standard and good PKI system is necessary for any organization to maintain the different security controls in place. With respect to the same explain in brief what makes a good PKI?

5. What are the issues concerning web industry and why do we choose to reverse-engineer?

6. WARE approach works based on GMT paradigm. Briefly explain the three components involved.

7. Considering classes of vulnerabilities what are the logical attacks found by experts which makes a web application vulnerable.

8. Social engineering is used to manipulate undesired outcome from individuals which they don't perform during normal operations. Keeping that in mind briefly explain what is Click jacking?

9. List 5 steps/ methodologies to avoid getting attacked in a web oriented environment.

10. Information leakage and insufficient authorization are bigger risks threatening the media industry. What solution/solutions would you propose to fix this issue?

Question 4 Multiple choice/ 1 word answers **1 point each [Total: 15 points]**

Fill in or circle the correct answer(s) for each of the following questions, as applicable:

1	2	3	4	5	6	7	8	9	10

1. In cryptography DES (Data Encryption Standard), AES (Advanced Encryption Standard) are examples of
   a. Symmetric key cryptography
   b. Asymmetric key cryptography

Answer: …….

2. In cryptography, a certificate is one which identifies
   a. the certification authority issuing it
   b. names or identifies its subscriber
   c. contains the subscriber's public key
   d. all of the above

Answer: …….

3. Considering Basic PKI Security Functions, making sure that you are communicating with the right person accounts for
   a. Authentication
   b. Non-repudiation

c. Integrity

Answer: …….

4. In SSL_RSA_EXPORT_WITH_RC4_40_MD5 = { 0, 3 }, {0,3} is nothing but
   a. Cipher suite code used in SSL messages
   b. NULL Cipher suite
   c. Hash code
   d. Public Key

Answer: …….

5. Replay Check is a method of copying packets and using the authentication to perform attacks and it is a feature of
   a. SSL (Secure Socket Layer)
   b. TLS (Transport Layer Security)
   c. DTLS (Datagram Transport layer Security)

Answer: …….

6. 

The picture above is an example of ……..
   a. Trojan
   b. Fake scanner page
   c. Fake codec
   d. Code injection attack

Answer: …….

7. Dynamic analysis can be carried out both automatically or manually. Is this statement TRUE or FALSE?

Answer: …….

8. As for the *use case diagrams*, they can be deduced on the basis of the ……..results
   a. Static Analysis
   b. Dynamic analysis
   c. Clustering

Answer: …….

9. Perform rigorous and on-going vulnerability assessments, preferably every week. Because you can't secure what you can't measure.
    a. Asset tracking
    b. Defense in depth
    c. Developmental framework
    d. Measure security

Answer: …….

10. The system should ensure that press releases are only served to authorized users after the embargo date has been passed. This fixes problems encountered due to
    a. Insufficient Process validation
    b. Insufficient authorization
    c. Weak Passwords
    d. Abuse of functionality

Answer: …….

11. The session for a pending trade in a Stock website should have an expiration time set; 20 minutes would be sufficient. This fixes problems encountered due to
    a. Insufficient Process validation
    b. Insufficient authorization
    c. Weak Passwords
    d. Abuse of functionality

Answer: …….

12. Throw up as many roadblocks to attackers as possible. This includes custom error messages, Web application firewalls, and security with obscurity, and so on. This phenomenon addresses
    a. Asset tracking
    b. Defense in depth
    c. Developmental framework
    d. Measure security

Answer: …….

13. Many Web sites today display advertisements hosted by third-party advertising sites. This is an example of
    a. Electronic bomb (e-bomb)
    b. Malicious advertisements
    c. Redirection sites

Answer: …….

14. …… forces a website visitor to execute malicious code in his/her browser
    a. Cross side scripting
    b. DLL injection
    c. Process injection
    d. Information staling

Answer: …….

Good Luck