**GRIFFITH COLLEGE LIMERICK**

**QUALITY AND QUALIFICATIONS IRELAND**

**EXAMINATION**

**MASTER OF SCIENCE IN NETWORK AND INFORMATION SECURITY**

**IT INFRASTRUCTURE PROTECTION AND ETHICAL HACKING**

**Module Code: MSCNS-IPEH**

**Lecturer(s): Kevin O’Mahony**

**External Examiners(s): Dr Paul Stynes**

**Date: 4th August 2016 Time: 9.45 – 12.45**

**THIS PAPER CONSISTS OF FIVE QUESTIONS**

**FOUR QUESTIONS TO BE ATTEMPTED**

**SECTION A: COMPULSORY**

**SECTION B: ANSWER ONE QUESTION**

**ALL QUESTIONS CARRY EQUAL MARKS**

**SECTION A: COMPULSORY**

**QUESTION 1**

1. Compare and contrast the main replication deployment scenarios in a cloud computing infrastructure.

**(6 marks)**

1. Explain the significant parameters that should be considered in the design of a fault tolerant mechanism.

**(9 marks)**

1. Discuss the failure behaviour of the network in cloud computing. You must reference a minimum of two findings from the 2010 study by Gill et al. titled “Understanding network failures in data centres: measurement, analysis and implications”.

**(10 marks)**

**Total (25 marks)**

**QUESTION 2**

1. Describe the phases you would expect to perform in conducting a full security test for a company.

**(9 marks)**

1. Evaluate the role of a security tester.

**(8 marks)**

* 1. Describe four techniques used in social engineering.

**(4 marks)**

* 1. Describe what measures could be implemented to counter each of the techniques you select in part (i).

**(4 marks)**

**Total (25 marks)**

**QUESTION 3**

1. Discuss the port scanning step used in a security test.

**(4 marks)**

1. Briefly describe two built in commands and two third party programs you could use when performing an enumeration phase of a security test in a Windows environment.

**(8 marks)**

1. Describe three techniques you could use in password cracking.

**(6 marks)**

1. Explain how you would go about cracking a user’s password on a Windows system. Detail OS commands and third party programs you would use.

**(7 marks)**

**Total (25 marks)**

**SECTION B: ANSWER ONE QUESTION**

**QUESTION 4**

1. Explain the major enhancements WPA implements that address encryption vulnerabilities in WEP.

**(6 marks)**

1. Explain the main three technologies used in WLANs.

**(6 marks)**

1. Detail three hardware and three software tools you would use and for what purpose in performing a security test on a wireless network.

**(6 marks)**

1. Describe the process of 802.1X authentication on a WLAN.

**(7 marks)**

**Total (25 marks)**

**QUESTION 5**

1. Explain the Unicode exploit on older versions of Windows IIS giving an example of how you would invoke it. Why might this exploit still be a security risk and how should we counter it?

**(6 marks)**

1. Discuss the following technologies used by a web application to connect to a database or an external file:
   1. Open Database Connectivity
   2. Object Linking and Embedding Database
   3. ActiveX Data Objects

**(9 marks)**

* 1. Briefly describe any five web application vulnerabilities from the 2013 OWASP ‘Ten Most Critical Web Application Security Risks’ list.

**(5 marks)**

* 1. Explain how to prevent each of the five vulnerabilities you selected in part (i).

**(5 marks)**

**Total (25 marks)**