JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATION SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE

COMPUTER SECURITY AND FORENSIC

2ND YEAR 2ND SEMESTER 2013/2014 ACADEMIC YEAR

MAIN

COURSE CODE: IIT 3225

COURSE TITLE: ETHICAL HACKING AND PENETRATION TESTING

EXAM VENUE: CL I **STREAM: (BSc. Computer Security and Forensic)**

DATE: 16/04/14 **EXAM SESSION: 9.00 – 11.00 AM**

TIME: 2.00 HOURS

Instructions:

1. **Answer question 1 (Compulsory) and ANY other 2 questions**
2. **Candidates are advised not to write on the question paper.**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room.**

QUESTION 1 30marks

a) Define the following terms as used in hacking and penetration testing
   - i) Ethical hacking (2marks)
   - ii) Ethical hacker (2marks)
   - iii) Vulnerability (2marks)
   - iv) Penetration testing (2marks)

b) Differentiate between the following terms
   - i) Threat and Exploit (2marks)
   - ii) Active and passive reconnaissance (2marks)

c) Whether an attack is perpetuated by an ethical hacker or malicious hacker, all attacks are an attempt to breach computer system security. Security consists of four basic elements explain these elements (8marks)

d) Briefly explain the main phases of hacking (10marks)

QUESTION 2 20marks

a) Giving an example in each case explain the following attacks as used in ethical hacking (12marks)
   - i) Buffer Overflow attacks.
   - ii) Denial of Service (DoS) attacks.
   - iii) Abuse of Trust.
   - iv) Brute force attacks.

b) Explain the function of the tool FIREWALK (4marks)

c) In an attempt to secure his wireless network, Bob implements a VPN to cover the wireless communications. Immediately after the implementation, users begin complaining about how slow the wireless network is. After benchmarsheets the network's speed. Bob discovers that throughput has dropped by almost half even though the number of users has remained the same. Explain why this happens in the VPN over wireless implementation? (4marks)

QUESTION 3 20marks

a) Jack Hacker wants to break into Brown Co.'s computers and obtain their secret double fudge cookie ecipe. Jack calls Jane, an accountant at Brown Co., pretending to be an administrator from Brown Co. Jack tells Jane that there has been a problem with some accounts and asks her to tell him her password 'just to double check our records'. Jane believes that Jack is really an administrator, and tells him her password. Jack now has a user name and password, and can access Brown Co.'s computers, to find the cookie recipe. This is an example of what kind of attack? explain (5marks)

b) List and explain five types of this attack? (15marks)

QUESTION 4 20marks

a) Name and explain two software tools used for OS guessing (6marks)

b) Explain three disadvantages of an automated vulnerability assessment tool. (6marks)

c) i) Define the term zone transfer (2marks)

ii) Briefly explain any three tools used to perform a zone transfer. (6marks)

QUESTION 5 20marks

a) Explain using appropriate commands how the following tools can be used during reconnaissance

i) Whois (3marks)

ii) Dig (3marks)

iii) NS LookUp (3marks)

iv) MetaGooFil (3marks)

b) Having conducted penetration testing, the tester should write a clear report of the procedure and findings. Briefly discuss under the main subheadings the contents of this report (8marks)