JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR SCIENCE IN COMPUTER SECURITY AND FORENICS

1ST YEAR 1ST SEMESTER 2018/2019 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: **IIT 3113**

COURSE TITLE: **PC SECURITY AND PRIVACY**

EXAM VENUE: **STREAM: BSC COMP SECURITY**

DATE: DECEMBER 2018 **EXAM SESSION:**

TIME: 2.00 HOURS

INSTRUCTIONS:

1. **Answer Question 1 (Compulsory) and ANY other two 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 ONE **[30 MARKS]**

(a) Define the following terms and concepts as applies to Information Security. [4 Marks]
   (i) Threat
   (ii) Vulnerability
   (iii) Malware
   (iv) DNS Poisoning

(b) Differentiate between the following as applies to PC Security and Privacy [6 Marks]
   (i) Phishing and Vishing
   (ii) Trapdoor and Backdoor
   (iii) Antivirus and Anti-Spam

(c) Give any <u>two</u> proactive and <u>two</u> reactive security measures that can be used to improve PC Security. [4 Marks]

(d) Below are some of the security incidences that occurs while PC is in use. For each case, identify with supporting answer which goals of security is violated. [8 Marks]
   (i) Mwaura crashes Annette's PC
   (ii) Oliver hacks into his Equity Bank Ltd payroll system
   (iii) Atieno defaces the homepage of MCA's website
   (iv) Mwende cracks into Angela's facebook account and use it to chat with Tom.

(e) Outline important steps required when: [6 Marks]
   (i) Detecting and removing malware that has invaded a PC
   (ii) Installing and configuring personal firewall in a PC

(f) Using a suitable illustration, briefly explain recommendation practices that can be adopted to enhance use of passwords as an access control mechanism. [2 Marks]

QUESTION TWO **[20 MARKS]**

(a) Using a well labelled diagram, briefly explain how the following can be used to secure computing assets. [12 Marks]
   (i) Honeypots
   (ii) Intrusion Detection Systems
   (iii) Firewalls
   (iv) Protocol Analyzers

(b) Biometrics is one of the authentication approaches employed to improve security. Identify two strengths and weaknesses of this approach. [4 Marks]

(c) "Understanding the importance of information security is fundamental to anyone who uses computing assets". Do you agree with this statement? Explain your answer. [4 Marks]

QUESTION THREE **[20 MARKS]**

(a) Define the following concepts as applies to PC Security and Privacy. [4 Marks]
   (i) Operating System Hardening
   (ii) Access Control Methods

(b) For each of the listed concepts in 3(a) above, discuss the industry best practices that can be used implement them. [8 Marks]

(c) Briefly explain the vulnerabilities and mitigations associated with network devices. [4 Marks]

(d) Give countermeasures that can be used against *Data Remanence* and *Dumpster Diving*. [4 Marks]

QUESTION FOUR **[20 MARKS]**

(a) The following statements might be TRUE or FALSE as applies to computer security. For each case, support the choice of your answer. [8 Marks]
   (i) Physical access allows attacker to plug into an open Ethernet jack.
   (ii) Multiple factor authentication makes it difficult for an attacker to have correct materials for authentication.
   (iii) In denial of service attack, the attacker tries to exhaust resources of the host.
   (iv) Like in Single Sign-on, Reduced Sign-on uses single credential for many systems.

(b) Consider three computers that connect to the internet through a proxy server with their IP Addresses as follows: Computer A is on 10.122.0.3, Computer B is on 192.168.1.23, Computer C is on 192.168.1.133 and Server S is on 192.168.1.1. in this case, explain whether; [6 Marks]
   (i) Computer B can claim it is Computer C to the Server S.
   (ii) Computer A can claim it is Computer C to the Server S.

(c) A professor asked during their PC Security and Privacy class why computers are considered insecure, two students Jane and Peter provided the following answers:

   Peter Most PCs use insecure operating systems

   Jane Most PCs runs buggy, vulnerable and even malicious codes.

   Comments on the accuracy on each of the answers provided by the students above. [6 Marks]

QUESTION FIVE **[20 MARKS]**

(a) Briefly explain how the following enhances security of computing assets. [6 Marks]
   (i) Audit Log Analysis
   (ii) Penetration Testing

(b) "Social engineering relies heavily on the six principles of influence established by Robert Cialdini"
   (i) Explain the term social engineering in the context of information security. [2 Marks]
   (ii) While referring to the Cialdini's theory, expand on the six principles. [6 Marks]

(c) "Computer system can be exploited for both fraud and theft by both automating traditional methods of fraud and by using new methods". Discuss. [6 Marks]

- END –