MERU UNIVERSITY OF SCIENCE AND TECHNOLOGY
P.O. Box 972-60200 – Meru-Kenya
Tel: +254(0) 799 529 958, +254(0) 799 529 959, + 254 (0) 712 524 293,
Website: info@must.ac.ke Email: info@must.ac.ke

University Examinations 2023/2024

FIRST YEAR SECOND SEMESTER EXAMINATION FOR THE DEGREE OF BACHELOR OF COMPUTER SECURITY AND FORENSICS AND BACHELOR OF COMPUTER SCIENCE

CCF 3100: FUNDAMENTALS OF PC SECURITY AND PRIVACY

DATE: APRIL 2024 **TIME: 2 HOURS**

INSTRUCTIONS: *Answer question **one** and any other **two** questions*

QUESTION ONE (30 MARKS)

a) Explain three types of intruders in security attacks (6 Marks)

b) List four benefits that can be provided by intrusion detection systems and Intrusion Prevention Systems in protecting an organization information system (4 Marks)

c) Define CIA Triage in the context of PC security and privacy (6 Marks)

d) Explain the importance of user education in effective password management (4 Marks)

e) Distinguish between the following terms as used in PC Security and privacy (6 Marks)

i. Access Control Matrix and Access Control Lists (ACLs)

ii. Security mechanism and security service

iii. Passive attack and active attack

f) Security policies define how an organization deals with security aspects. With use of examples differentiate between user policies and system administration policies (4 Marks)

QUESTION TWO (20 MARKS)

a) State three reasons why physical security is needed in relation to PC Security and privacy (3 Marks)

b) Biometric measurements or personal attributes are used for authentication. These attributes are unique to the individual seeking to authenticate identification.

   i. List any four types of biometrics that are used for authentication (4 Marks)

   ii. Discuss the two types of errors that occur when biometrics are used for authentication. (4 Marks)

c) Pre-emptive techniques have been widely deployed to reduce chances of successful attack. Briefly describe intrusion deflection, infiltration and intrusion deterrence techniques. (3 Marks)

d) Discuss any three threats that operating systems are facing and suggest the defense method for each threat discussed (6 Marks)

QUESTION THREE (20 MARKS)

a) Differentiate between Security Plan, Security Policy and Security Charter (3 Marks)

b) Meru University has been advised by information security experts to use Firewall to protect its network. Define what a firewall is and briefly explain any three types of firewalls that Meru University can use. (7 Marks)

c) Bell and La Padula Model (BLP), Chinese Wall model, Biba model and Clark-Wilson models are commonly security models used to achieve different security services. Outline the security service achieved by each of the above security models. (4 Marks)

d) Discuss the following types of common DoS threats (6 Marks)

   i. Ping of Death

   ii. SYN Flood Attack

   iii. Packet fragmentation and reassembly

QUESTION FOUR (20 MARKS)

a) Discuss the following access control models

i. DAC (2 Marks)

ii. MAC (2 Marks)

iii. RBAC (2 Marks)

b) You have been introduced to the security goals within the context of computer and network security that each organization strives to achieve. Describe any five of these security goals. (10 Marks)

c) Explain how honeypot and honeynets helps in dealing with security attacks (4 Marks)

QUESTION FIVE (20 MARKS)

a) Differentiate between authentication and authorization in relation to PC security (2 Marks)

b) Discuss the following threats (4 Marks)

i. Trojan Horse

ii. Worm

iii. Rootkit

iv. Ransomware

c) Describe how the following work to offer protection against bots

i. CAPTCHA (2 Marks)

ii. 2-Step Verification (2 Marks)

d) Distinguish the following classes of protection as far as operating system security hardening is concerned

i. Information hiding (2 Marks)

ii. Control flow restrictions (2 Marks)

iii. Partitioning (2 Marks)

iv. Code and data integrity checks (2 Marks)

v. Anomaly detection (2 Marks)