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: www.must.ac.ke Email: info@mucst.ac.ke

UNIVERSITY EXAMINATIONS 2020/2021

FOURTH YEAR FIRST SEMESTER EXAMINATIONS FOR THE DEGREE OF BACHELOR OF SCIENCE COMPUTER SECURITY AND FORENSIC

CCF 3404: ETHICAL HACKING AND PENETRATION TESTING

DATE: SEPTEMBER 2021 **TIME: 2 HOURS**

INSTRUCTIONS: Answer Question ONE and any other TWO questions.

QUESTION ONE (30 MARKS)

a) Differentiate between the following terms as used in ethical hacking
   i. Vulnerability assessment and vulnerability analysis (2marks)
   ii. Hacking and ethical hacking (2marks)
   iii. ARP poisoning and DNS poisoning (2marks)

b) A cybersecurity specialist is asked to identify the potential criminals know to attack the organization. Explain three types of hackers who can compromise the network and systems of the organization (3marks)

c) Identify any three well known system ports and specify services running on them. (3marks)

d) Describe any two common password cracking techniques applied by hackers (4marks)

e) Explain four types of exploits which can be conducted on a campus network during penetration testing process (4marks)

f) List four tool that can be used to perform network sniffing (4marks)

g) Hacking has been a part of computing for almost five decades. Discuss three motivations behind the activities of hackers (6marks)

QUESTION TWO (20 MARKS)

a) Differentiate between
   i. Threat and a vulnerability (2marks)
   ii. Network scan and vulnerability scan (2marks)
   iii. Elite hackers and script kiddies (2marks)

b) Discuss any three protocols vulnerable for sniffing in a network (3marks)

c) Identify three advantages and two disadvantages of hacking activities in a network. (5marks)

d) A penetration testing service hired by the company has reported that a backdoor was identified on the network resources have been compromised (6marks)

QUESTION THREE (20 MARKS)

a) Explain the following processes and techniques as used in reconnaissance (2marks)
   i. Foot printing (2marks)
   ii. Scanning (2marks)
   iii. Enumeration (2marks)

b) Discuss three legal requirements that a pen tester needs to understand before scanning an enterprise network for vulnerability (3marks)

c) Consider a web app that displays user posts, like twitter and Facebook. Explain three types of information which a hacker can gather from such sites towards achieving a successful hacking (3marks)

d) Using a diagram illustrate and explain the TCP 3- way handshake (4marks)

e) Explain the structure of NMAP command (4marks)

QUESTION FOUR (20 MARKS)

a) Explain the following tools as used in hacking
   i. Nmap (2marks)
   ii. Metasploit (2marks)
   iii. Cain and Abel (2marks)

b) Hacking on organization systems and networks has been on the increase over years. List any four vulnerabilities that are mostly targeted by hackers (4marks)

c) Name and explain any four hacking tools which network admins can use to perform penetration testing in a network (4marks)

d) DNS is key to the operation of any network where the naming and resolution of those given names is required. However, the flexibility and convenience it provides can be subverted. Discuss three ways in which hackers might take advantage of this. (6marks)

QUESTION FIVE (20 MARKS)

a) Distinguish the following terms.
   i. Black hat hacker and White hat hacker (2marks)
   ii. White-box test vs Black-box test (2marks)
   iii. Hacktivism vs terrorism (2marks)

b) Discuss three ways in which a hacker can use social engineering to gather information about an organization (6marks)

c) Define the term sniffing and briefly explain how sniffing can be achieved in a network (4marks)

d) Identify and explain four tools which can be used during the scanning phase (4marks)