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 2024/2025

FOURTH YEAR FIRST SEMESTER FOR THE DEGREE OF BACHELOR OF SCIENCE IN COMPUTER SECURITY AND FORENSICS

CCF 3404: ETHICAL HACKING AND PENETRATION TESTING

DATE: JANUARY 2025 **TIME: 2 HOURS**

INSTRUCTIONS: *Answer question* ***ONE*** *(Compulsory) and any other* ***TWO*** *questions*

QUESTION ONE (30 MARKS)

a) Describe the activities of the following types of hackers (4 Marks)

i. Hacktivist

ii. Insider threat

iii. Organized crime

iv. State sponsored attacker

b) Distinguish between hashing vs encryption algorithms and give an example of each (4 Marks)

c) Discuss the expected qualities of an ethical hacker (4 Marks)

d) You have been assigned to conduct a network infrastructure pen test for Meru University. Describe two resources which must be evaluated (4 Marks)

e) Explain the role of root privileges in Kali Linux OS and give its equivalent in Windows OS (4 Marks)

f) Illustrate and explain the ease of use triangle (3 Marks)

g) Explain then five phases of ethical hacking (4 Marks)

h) List and explain four elements of security (4 Marks)

i) Two hackers attempt to crack a company's network resource security. One is considered an ethical hacker, whereas the other is not. What distinguishes the ethical hacker from the "cracker"? (3 Marks)

QUESTION TWO (20 MARKS)

a) You want to ensure your messages are safe from unauthorized observation, and you want to provide some means of ensuring the identities of the sender and receiver during the communications process. Give and explain the best cryptographic approach for this (4 Marks)

b) Joe and Bob are both ethical hackers and have gained access to a folder. Joe has several encrypted files from the folder, and Bob has found one of them unencrypted. Describe the type of attack vector which is best suited for this. (4 Marks)

c) Distinguish between public keys and private keys (4 Marks)

d) While foot printing a network, describe the nature of information from the following tools: (4 Marks)

   i. Traceroute
   ii. Nslookup
   iii. NMAP
   iv. Whois

e) Write a Google hack which would display all pages that have the phrase "SQL" and "Version" in their titles (4 Marks)

QUESTION THREE (20 MARKS)

a) Distinguish between DNS spoofing vs source routing (4 Marks)

b) Discuss the steps for a generic scanning methodology within an enterprise network (4 Marks)

c) Describe the following activates and give a example of a tool used for each activity: (4 Marks)

   i. Port scanning
   ii. Ping sweeping
   iii. Vulnerability scanning
   iv. SNMP enumeration

d) As an ethical hacker you need to familiarize yourself with some common port addresses and their protocols. Give any four commonly used fort addresses and their associated protocols. (4 Marks)

e) Distinguish between war driving vs war dialing (4 Marks)

QUESTION FOUR (20 MARKS)

a) Define the term sniffing and give an example of a tool used for this activity (4 Marks)

b) Discuss any two defense mechanisms used against sniffing (4 Marks)

c) Illustrate and describe the encapsulations within the TCP/IP protocol suite (4 Marks)

d) You are reviewing a packet capture in Wireshark but only need to see packets from IP address 128.156.44.33. write the packet filter to output this (4 Marks)

e) Passwords in Linux can be stored in one of two places. List and explain (4 Marks)

QUESTION FIVE (20 MARKS)

a) Describe three authentication mechanisms, which are commonly used to secure systems (4 Marks)

b) Discuss four types of password attacks (4 Marks)

c) A security professional employs the tools LNS and S find during a monthly sweep. Explain the nature of information that can be acquired (4 Marks)

d) Describe four social engineering activities and give examples (4 Marks)

e) Define the following terms: (4 Marks)

i. Script kiddie

ii. Phishing

iii. Dumpster diving

iv. Reverse engineering