MAKERERE UNIVERSITY

COLLEGE OF COMPUTING AND INFORMATION SCIENCES

DEPARTMENT OF NETWORKS

END OF SEMESTER I EXAMINATION 2019/20

YEAR OF STUDY: I

COURSE NAME: SYSTEMS AND NETWORK SECURITY

COURSE CODE: MCN 7103

DATE: 26th November 2019 TIME: 4.00PM – 7.00PM

INSTRUCTIONS:

1. All answers must be written in the answer sheet provided.
2. Attempt **ALL** questions in section A and **ANY THREE** questions from section B
3. Clearly indicate the question Number that you are attempting
4. Begin each section B question on a new Page

SECTION A (40 marks)

1. Write short notes about the following terms as applied to network and systems security. [2 Marks each]

a) Vulnerability
b) Timing attack
c) Network security
d) SYN flooding
e) threat
f) Cracker
g) Hacker
h) White hat
i) Black hat
j) Repudiation

2. Name the 3 primary vulnerabilities that plague networks implementations. [3 Marks]
3. Explain cryptanalysis and its defense mechanism. [3 Marks]
4. What are the two states of data? [2 Marks]

5. IP scans and Port scans are common hacking tools. But they can also be used by administrators. How do administrators use these tools? [3 Marks]
6. Explain backdoor and its possible defense mechanism. [3 Marks]

7. Who is a hypothetical hacker [2 Marks]

8. Explain social engineering including the methods used to implement it. [4 Marks]

SECTION B (20 Marks each)

Question 1 – Security fundamentals

a) Briefly describe how you could implement Closed Access model for network security.[6 Marks]
b) One of the biggest reasons to create and follow a security policy is compliance with the law. Any business is potentially liable should a hacker or a virus take down the operation. Similarly, if a business is running a publicly held e-business and a catastrophic attack seriously impairs the business, a lawsuit is possible and therefore due diligence is part of the legal process.

i. What is due diligence? [2 Marks]

ii. Explain the three aspects of focus in the due diligence process. [6 Marks]
iii. Explain the meaning of due care process. [3 Marks]

c) In any fast-growing industry, changes are to be expected, and in the IT industry, the types of potential threats to network security are always evolving. Explain three potential consequences of breaching security of the computer network? [3 Marks]

Question 2 –Asymmetric encryption

a. Describe three reasons why public key encryption will not replace symmetric key encryption. [6 Marks]

b. The concept of public-key cryptography evolved from an attempt to attack two of the most difficult problems associated with symmetric encryption. Explain the two most difficult problems associated with symmetric encryption. [6 Marks]

c. Explain the four essential steps for public key encryption procedure. [8 Marks]

Question 3 –symmetric encryption

a) Rail fence is an example of transposition techniques. Using rail fence, decipher the following cipher text and clearly show the formula if the key is 7146325. [4 Marks]
asstetighndnmtchbhnotioiieig

b) Explain the term steganography and provide 4 examples. [5 Marks]

c) Use the steganography technique to decipher the hidden message in the text below. [6 Marks]

Dear George;

Greetings to all at Oxford. Many thanks for your letter and for the summer examination package. All Entry Forms and Fees Forms should be ready for final dispatch to the Syndicate by Friday 20th or at the very latest, I'm told by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16+ proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours;

d) Explain Shannon's confusion [3 Marks]

e) Differentiate block cipher from stream ciphers. [2 Marks]

Question 4 – Attacks, Threats & vulnerabilities

a) Describe the four primary classes of attacks. [8 Marks]
b) Explain traffic analysis and provide the defense mechanism for it. [4 Marks]
c) Differentiate between DoS and DDoS. [4 Marks]
d) Explain any four examples of malware in network systems. [4 Marks]