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 FORENSICS

2^{ND} YEAR 2^{ND} SEMESTER 2021/2022 ACADEMIC YEARMAIN CAMPUS

COURSE CODE: ICB 1210

COURSE TITLE: ETHICAL HACKING AND PENETRATION TESTING

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.

(i) Hacker [2 Marks]

(ii) Penetration testing [2 Marks]

(iii) Script Kiddie [2 Marks]

(iv) Cracker [2 Marks]

(v) SQL Injection [2 Marks]

(b) Who is an ethical hacker and what is the objective of ethical hacking from the hacker's prospective? [4 Marks]

(c) Briefly discuss the difference between ethical hacking and penetration testing [6 Marks]

(d) An ethical hacker follows processes similar to those of a malicious hacker. The steps to gain and maintain entry into a computer system are similar no matter what the hacker's intentions are. Describe the five phases that hackers generally follow in hacking a system. [10 Marks]

QUESTION TWO **[20 MARKS]**

(a) What is a VPN [3 Marks]

(b) There are several types of hackers.

(i) Explain three types of hacker categories [6 Marks]

(ii) List and Discuss at least 4 skills of a hacker [8 Marks]

(iii) Define hacking tools giving at least an example of a tool used by a hackers. [3 Marks]

QUESTION THREE **[20 MARKS]**

a) Giving an example in each case explain the following attacks as used in ethical hacking [12 Marks]

(i) Denial of Service (DoS) attacks.

(ii) Brute force attacks

(iii) Session Hijacking

(iv) SQL Injection

b) From the above mentioned attacks in Question Three (a), Discuss on how each can be prevented. [4 Marks]

c) What is cryptography? [2 Marks]

d) Differentiate between copyright and trademark. [2 Marks]

e) QUESTION FOUR [20 MARKS]

(a) What is a rootkit and for what purpose is it used for? [3 Marks]

(b) Jack wants to break into Brown Co.'s computers and obtain their secret double fudge cookie recipe. Jack calls Jane, an accountant at Brown Co., pretending to be an administrator from Brown Co. Jack tells Jane that there has been a problem with some accounts and asks her to tell him her password 'just to double check our records'. Jane believes that Jack is really an administrator, and tells him her password. Jack now has a user name and password, and can access Brown Co.'s computers, to find the cookie recipe. This is an example of what kind of attack? Explain [5 Marks]

(c) List and explain 4 types of this attack. [12 Marks]

QUESTION FIVE [20 MARKS]

(a) Security policies are a formal set of rules which is issued by an organization to ensure that the user who are authorized to access company technology and information assets comply with rules and guidelines related to the security of information.

A security policy also considered to be a "living document" which means that the document is never finished, but it is continuously updated as requirements of the technology and employee changes.

Why is security policies important in an organization. [6 Marks]

(b) Briefly discuss the key elements of security policies. [10 Marks]

(c) One example of a security policy is password policy, briefly discuss at least 4 password policies.

[4 Marks]

- END -