**JARAMOGI OGINGA ODINGA UNIVERSITY OFSCIENCE AND TECHNOLOGY**

**END SEMESTER EXAMINATION**

**BSC. COMPUTER SECURITY & FORENSICS YEAR THREE SEMESTER TWO– [2020/2021]**

**SPECIAL/SUPLEMENTARY**

**PAPER: IIT 3322 [COMPUTER SECURITY RISK MANAGEMENT AND CONTROL]**

## INSTRUCTIONS

1. This paper contains FIVE questions. Question One is 30 Marks and the rest are 20 Marks each.

2. Answer question one which is **COMPULSORY** and **ANY OTHER TWO**

3. Be precise and clear in your answers.

## QUESTION ONE [30 MARKS]

a) What do you understand by the terms least privileged and defense in-depth? **(2marks)**
b) What's the difference between an intrusion detection and intrusion prevention system **(2marks)**
**c)** What's the difference between "Sniper style" and "Brute force" In the denial of service attack? **(2marks)**
d) What tools would you used to conduct port scanning, vulnerability & penetration testing respectively? **(3marks)**
e) What is a honey pot and why is it important security control tool **(4marks)**
**f)** What are the four ways that you can mitigate risks associated with computers? **(4marks)**
g) What are four risks associated with penetration testing **(4marks)**
h) State the Four teams that should be involved in contingency planning and contingency operations: **(4marks)**

**i)** Elaborate on the following formula **(5marks)**

$$\text{RISK} = \frac{((\text{Means} + \text{Motive}) * \text{Opportunity}) * \text{Business Impact}}{\text{Controls}}$$

**QUESTION TWO [20 MARKS]**

a) Describe the following in relation to computer security risks **(6marks)**
   - Backdoor
   - Botnets
   - Spyware

b) Why are Botnets very difficult to identify and prevent? **(1marks)**

c) Explain how a backdoor is dangerous within a software application. **(2 marks)**

d) What is an Insider Threat, why is it considered the most dangerous security risk? **(2marks)**

e) What do you understand by the term social engineering? **(1 mark)**

f) Explain four examples of social engineering **(8 marks)**

**QUESTION THREE [20 MARKS]**

a) Distinguish between port scanning and vulnerability scanning **(4marks)**

b) Explain at least two ways in which shoulder surfing can be achieved **(2marks)**

c) What do you understand by the term DNS Cache Poisoning?**( 2 marks)**

d) Describe privilege escalation attack **(2marks)**

e) Using diagram describe how "man in the middle" and "replay attack" can be perpetuated **(10**

**QUESTION FOUR [20 MARKS]**

**a)** You are requested to conduct a security risk assessment of the ICT laboratory in Kisumu learning center. From this exercise you are required to give your assessment of the possible threats pairing them with their respective vulnerabilities, impacts and possible control measures. **(10 marks)**

**b)** Describe at least five types of vulnerabilities that a threat can exploit within an information system. **(10 marks)**

**QUESTION FIVE [20 MARKS]**

**a)** State the components of contingency planning **(3marks)**

b) At what time would an incident become a disaster?**(2marks)**

c) Describe the following terms **(6marks)**

d) What Is Contingency Planning?**(2marrks)**

e) Being part of an incidence response team what are some of the strategies you would employ to stop an incident and attempt to recover control within a computer system. **( 7marks)**