**JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY**

**SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS**

**UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR SCIENCE IN SECURITY AND FORENICS**

**4thYEAR 1st SEMESTER 2018/2019 ACADEMIC YEAR**

**MAIN CAMPUS**

---

**COURSE CODE: IIT 3411**

**COURSE TITLE: IT SECURITY ARCHITECTURE AND DESIGN**

| | |
|---|---|
| **EXAM VENUE:** | **STREAM:** |
| **DATE:** | **EXAM SESSION:** |
| **TIME: 2.00 HOURS** | |

---

**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) What's the one main drawback of network taps and protocol analyzers? **(1 mark)**

**b)** Explain two vulnerabilities associated with the **File Transfer Protocol (FTP) ( 2 marks)**

c) Explain what you understand by the two these two secure network technologies **NAC** and **PAT** ( **2 marks)**

d) Briefly explain three disadvantages of Hide-Mode Mapping in NAT **(3marks)**

e) State the three actions that an IDS can take when it receives a suspicious packet (3marks)

f) When outlining penalties for violations what are the three critical things that a policy should be emphasized? **(3marks)**

g) In a Stateless Packet Filtering it allows or block packets based on information in the protocol headers state the three features within the protocol header that it looks at before making a decision whether to block or allow packets **(3marks)**

h) State the at least four critical area where IDS network sensors should be placed to ensure efficiency **(4marks)**

i) What are the inherent Benefits of a security policy? **(4marks)**

j) What are the goals associated with Proxy Servers **(5marks)**

## QUESTION TWO [20 MARKS]

a) Explain the critical aspects that a secure VPN design should address **(14marks)**

b) Several advantages such as No need to modify firewall settings to support VPN traffic, Configuration scales more easily and can deal with congested servers are attributed to Setting up a VPN parallel to your firewall inside the DMZ. Briefly explain three disadvantages attributed to this scenario **(6marks)**

**QUESTION THREE [20 MARKS]**

a) State and explain the various steps in an intrusion detection **(14 marks)**

b) State Three ways for detecting a potential intrusion **(3 marks)**

c) State at least three ways in which you can harden an operating system to resist attacks **(3 marks)**

**QUESTION FOUR [20 MARKS]**

a) Briefly explain the advantages and disadvantages of IDS triggering mechanisms **(8marks)**

b) State the Seven Steps to Creating a Security Policy **(7marks)**

c) Sate the three IP packet header fields used by packet filtering **(3marks)**

d) What is a protocol analyzer? **(2marks)**

QUESTION FIVE [20 MARKS]

a) State and explain the various components that make up an intrusion detection system (IDS) **(10Marks)**

b) State and briefly explain at least 5 advantages associated with subnetting as a way of securing a network infrastructure **(5 marks)**

c) Briefly explain at least 5 convergence vulnerabilities especially in relation to VOIP

**(5 marks)**