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

4th YEAR 1st SEMESTER 2016/2017 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: IIT 3411

COURSE TITLE: IT SECURITY ARCHITECTURE AND DESIGN

EXAM VENUE: **STREAM:**

DATE: DECEMBER 2016 **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) Why does fiber optic media have a significant security advantage over other transmission Media **(2marks)**

b) What security implementation principle recommends division of responsibilities so that one person cannot commit an undetected fraud? **(1marks)**

c) What do you understand by the term subnetting **(1 mark)**

d) Briefly explain two important features a VLAN would provide in a network infrastructure **(2 marks)**

e) What way would you reduce the risk of attack in file transfer protocol **(1 mark)**

f) What do you understand by term convergence in relation to network design? **(2 marks)**

g) What do you understand by NAT, what are the two important functions it provides on a network **(3marks)**

h) What is a demilitarized zone **(2mark)**

i) What is a Non-routable address? **(2marks)**

j) What are cookies, how do they pose a risk on a network (2marks)

k) What two uses can you gain from the data collected in a Honeypot **(2 marks)**

l) Distinguish between statefull and stateless packet filtering **(2 marks)**

m) On what principle does NIDS works**(1 mark)**

n) Security for virtualized environments can be a concern for two reasons explain **(2 marks)**

o) State three ways to reduce the risk introduced by USB devices on a network **(3 marks)**

p) Firewalls are not a standalone solution explain **(2 marks)**

QUESTION TWO [20 MARKS]

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

b) State at least six advantages associated with convergence **(6 marks)**

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

d) By the use of a diagram explain how Network Address Translation Works **(4marks)**

QUESTION THREE [20 MARKS]

a) Assume you are an attacker state and explain five steps that you would use to conduct an attack on a network scenario **(10 marks)**

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

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

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

e) Briefly explain at least five methods a network attacker can use to view switch traffic **(5 marks)**

QUESTION FOUR [20 MARKS]

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

b) Differentiate between Security patch, Hotfix & Service pack **(3 marks)**

c) State at least 6 advantages to an automated patch update service **(6 marks)**

d) For Windows-based systems, there are two defenses against buffer overflows state and explain how they work **(4 marks)**

e) Explain ARP poisoning **(4 marks)**

QUESTION FIVE [20 MARKS]

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

b) State and explain the functions of at least 5 Network Security Devices**(10 marks)**

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

d) VPNs do not reduce the need for a firewall it's recommended always use a firewall as part of VPN security design by Installing VPN software on the firewall itself. Explain three advantages and disadvantages of Installing VPN software on the firewall itself **(6 marks)**