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

3rdYEAR 1st APRIL 2018/2019 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: ICT 3317

COURSE TITLE: FIREWALLS AND NETWORK DEFENSE SECURITY

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) Distinguish between Permissive versus restrictive policies (2marks)

b) State Attacks detected by an IDS sensor (2marks)

c) Explain what a firewall is and what it can and cannot do (2marks)

d) A VPNs do not reduce the need for a firewall expound (2marks)

e) State Attacks detected by an IDS sensor (2marks)

f) State the three Options for defining rules in a firewall policy (3marks)

g) Lists the three General steps to create a firewall policy (3marks)

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

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

j) When Managing Firewalls to Improve Security what are some of the guidelines that you should adhere to (4marks)

k) Sate the four critical steps when developing security policies from risk assessment (4marks)

QUESTION TWO [20 MARKS]

a) State the eight general steps in creating a bastion host (8marks)

b) What are some of the advantages and disadvantages of Installing VPN software on the firewall itself? (6marks)

c) When Designing a VPN you need assess organization's needs and goals state at least four critical consideration you look at in relation to this statement. (4marks)

d) Firewalls are not a standalone solution expound the statement (2marks)

QUESTION THREE [20 MARKS]

a) Explain the several ways in which Firewalls can be deployed. (14marks)

b) Rules for blocking traffic are done case-by-case using a firewall, state the three rule actions that usually applied when blocking traffic (3marks)

c) 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)

QUESTION FOUR [20 MARKS]

a) When configuring firewall rules what are the critical components that you should pay attention to? (6marks)

b) You are contracted to set up a firewall for Jooust, as an expert explain where you would place a packet filter firewall (6marks)

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

d) Briefly explain four ways in which you can harden a bastion Host (4marks)

QUESTION FIVE [20 MARKS]

a) Briefly describe the following common attacks and explain the defense mechanisms to be applied.(10 marks)

i. DOS
ii. SYN Flood
iii. Virus
iv. Trojan
v. Social engineering
vi. Malicious port scanning
vii. ICMP massage abuse
viii. Finding vulnerable host on the internal network to attack
ix. Man in the middle
x. RPC attacks

b) What are the General steps for reviewing log files? (5marks)

c) What are the goals of a Proxy Servers? (5marks)