JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR SCIENCE IN COMPUTER SECURITY AND FORENSICS

4th YEAR 2ND SEMESTER 2018/2019 ACADEMIC YEAR

KSUMU CAMPUS

COURSE CODE: IIT 3441

COURSE TITLE: ADVANCED LINUX /UNIX SYSTEM ADMINISTRATION

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 is the difference between a packet-filtering firewall and a proxy-server firewall? Can the two be used together? **(4 marks)**

b) What function is attributed to "sudo" and "apt-get" command in Ubuntu **(2 marks)**

c) How would you verify if the necessary Postfix packages are installed by running: **(2 marks)**

d) State two alternate IMAP/POP3 servers that postfix can work with **(2 marks)**

e) state the three standard format mail box delivery formats that postfix can work with **(3 marks)**

f) State the strengths attributed to postfix over other MTA`s. **(2 marks**)

g) Why is postfix a suitable alternative to sendmail **(2 marks)**

h) what do you understand by the term dovecot **(2 marks)**

i) how would you verify that the DNS is working correctly in Ubuntu **(2 marks)**

j) Explain what you understand by the following principles when securing a network system **(6 marks)**

g) Explain why linux is becoming popular **(3 Marks)**

QUESTION TWO [20 MARKS]

a) List the Components that would typically form LDAP directory for a small enterprise **(4 marks)**

b) Using a diagram show realistic schematic LDAP hierarchical structure **(8 marks)**

c) List three advantages and disadvantages associated with LDAP **(6marks)**

d) Name two commands associated with testing network connectivity **(2marks)**

QUESTION THREE [20 MARKS]

a) What is the difference between an authoritative and a non-authoritative answer to a DNS query? How could you ensure that an answer was authoritative? **(5 marks)**

b) What's the difference between exclusionary and inclusionary filter? **(2 marks**

c) From the Terminal windows notice the difference in curser symbol "$" and "#" what do they entail. In what way would you query a DNS Server **(2marks)**

d) State and explain the two types of mail clients clearly bring out their differences **(4marks)**

e) What do you understand by the term FQDN and what does it entail? **(2 marks)**

QUESTION FOUR [20 MARKS]

To help you manage your LDAP directory, state atleast three GUI tools available out there **(3marks)**

What's the primary drawback to some hardware firewalls? **(2mark)**

What's the best approach that most security experts believe is the way to go in handling firewall filters and rules **(2marks)**

Describe what you understand by the following terms in relation to open source email system **(10 marks)**

- Postfix
- Dovecot
- Clam AV
- Thunderbird

- SquirrelMail

What is the linux command that is used to view the internet protocols configuration **(1mark)**
Which file does Linux use to resolve hostnames? **(1marks)**
What ports has the IANA declared reserved? **(1 mark)**

QUESTION FIVE [20 MARKS]
Briefly explain the function of each of the following DNS records: SOA, PTR, A, MX, and CNAME. **(10 marks)**
What is LDAP (2marks)
What do you understand by the term postfix **(2marks)**
when installing & Configuring Dovecot POP3/IMAP Server for Ubuntu state the two packages that you would require **(2marks)**
A user is logged into the Linux workstation, what is the best way to login to root from a shell prompt for Ubuntu and Centos? **(2 mark)**
You are working in Linux when a program hits a flaw and stops running. Which commands can be used to end the process? **(2 mark)**