**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 FORENICS**

**4th YEAR 2ND SEMESTER 2015/2016ACADEMIC YEAR**

**MAIN CAMPUS**

---

**COURSE CODE: IIT 3441**

**COURSE TITLE: ADVANCED LINUX /UNIX SYSTEM ADMINISTRATION**

**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) Explain what an MX record is. Why are MX records important for mail delivery? **(2 marks)**

b) 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? **( 3marks)**

c) What does CentOS stands for **(1mark)**

d) How would you Perform System Upgrade in CentOs. **( 1mark)**

e) From the Terminal windows notice the difference in curser symbol "$" and “#" what do they entail **(2marks)**

f) From the Ethernet Device dialog box, you click on statically set IP address, and enter the Address, Subnet mask and Default gateway address as desired and clicked “OK” to save. On the terminal when you invoke “ifconfig” IP settings dint change to the desired. Explain what could be the problem and how it can be solved. **(2marks)**

g) You are running linux OS on CLI how would you know the hostname? **(1mark)**

h) What role does Webmin Play in a linux server **(1mark)**

i) What do you understand by the term BIND what function does it serve **(2marks)**

j) State two ways in which you would query a DNS Server **(2marks)**

k) What’s the difference between exclusionary and inclusionary filter **(4 marks)**

l) What do you understand by **“httpd”** **(1mark)**

m) What purpose does **dig** and **nslookup** serve **(2marks)**

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

o) All firewalls work only on inbound traffic; they do not limit or block outgoing traffic is this statement true or false justify your answer **(2marks)**

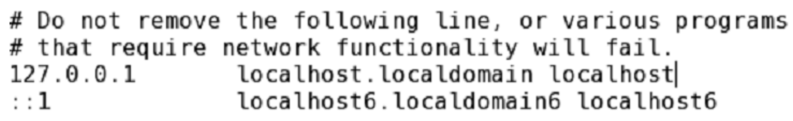
## QUESTION TWO [20 MARKS]

a) Amongst UNIX and Linux systems which OS would you recommend for each of the following applications. Explain your choices. **(8 marks)**

i. A single user working in a home office
ii. A university computer science lab
iii. A corporate web server
iv. A server cluster that runs the database for a shipping company

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

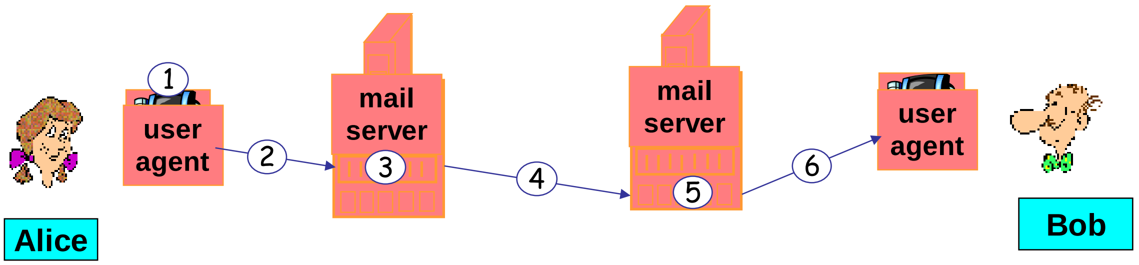
c) Which file stores the piece of information below **(1mark)**



```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1        localhost.localdomain localhost
::1              localhost6.localdomain6 localhost6
```

d) What is a slave DNS what critical function does it server within the internet environment **(2marks)**

e) Using the Scenario Below explain process 1-6 **(6marks)**



f) What ports has the IANA declared reserved? **( 1 mark)**

## QUESTION THREE [20 MARKS]

a) Suppose that a user at your site has started a long-running process that is consuming a significant fraction of a machine's resources. **(4 marks)**

   i. How would you recognize a process that is hogging resources?

   ii. Assume that the misbehaving process might be legitimate and doesn't deserve to die. Show the commands you would use to suspend the process temporarily while you investigate.

   iii. Later, you discover that the process belongs to your boss and must continue running. Show the commands you'd use to resume the task.

   iv. Alternatively, assume that the process needs to be killed. What signal would you send

b) Draw a simple, imaginary network diagram that connects a machine in your computer lab to Amazon.com Include LAN, and WAN components. Show what technology is used for each component. **(10 marks)**

c) What is the linux command that is used to view the internet protocols configuration**(1mark)**

**d)** Which file does Linux use to resolve hostnames? **(1marks)**

e) Explain the two kinds of servers handle incoming e-mail messages? **(4marks)**

## QUESTION FOUR [20 MARKS]

**a)** Outline the differences between Kickstart, JumpStart, and Ignite-UX. **(3 marks)**

**b)** Today, most office buildings house computer networks and are wired with UTP Ethernet. Some combination of routers and switches is needed to support these networks. List at least three functions of each of each. **(6marks)**

**c)** Explain how you would access webmin on a linux server. **(2marks)**

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

**(6 marks)**

   i. Postfix
   ii. Dovecot
   iii. Clam AV

**e)** Distinguish between Thunderbird and SquirrelMail **(2marks)**

**f)** Which command creates a file system? **(1 mark)**

## QUESTION FIVE [20 MARKS]

a) Explain the function of each of the following DNS records: SOA, PTR, A, MX, and CNAME. **(5marks)**

b) Briefly explain the difference between a user agent (MUA), a delivery agent (DA). Then explain the difference between a mail transport agent (MTA) and a mail submission agent (MSA).

**(4 marks)**

c) You want to change the hostname of your server from “localhost.locadomain" to: "server01.4thyearcsf.com". To do so, you need to edit a file in the directory.

i. What is the name of this file? **(1mark)**

ii. What is the full command you will invoke from the terminal to aid you change the file?

**(1mark)**

iii. You have saved the changes you made to this file but upon checking whether the hostname has changed you realized it still states localhost.locadomain. What could be the problem? Show the full command you would invoke to finally change the hostname

**(2marks)**

d) Explain what you understand by the following principles when securing a network system

**(6marks)**

- **Separation of Duties**
- **Least Privilege**
- **Defense-in-depth**

**e)** You are working in Linux when a program hits a flaw and stops running. Which command can be used to end the process? **(1 mark)**