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

**SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS**

**UNIVERSITY EXAMINATION FOR THE DEGREE OF BSC IN COMPUTER SECURITY AND FORENSIC**

**4TH YEAR 1ST SEMESTER 2015/ 2016 ACADEMIC YEAR**

---

**COURSE CODE: IIT 3413**

**COURSE TITLE: OPERATING SYSTEMS SECURITY**

**EXAM VENUE: MAIN CAMPUS**

**DATE:** **STREAM: BSC FORENSICS**

**TIME: 2 HOURS** **EXAM SESSION:**

---

**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 the meaning of operating system and outline its three major functions (5 marks)

b) You switched on your computer and got a notification that you should “Change windows update settings” and that the current settings of your windows is not recommended. Discuss exactly what action you should take and why. (3 marks)

c) Explain the difference between discretionary and mandatory security policies (2 marks)

d) The host operating system of the mail server in Ndege International Research Centre was released ten years ago and since then, three newer versions have been released. Since it has been very stable, the ICT Manager does not want to change anything in the system.

   i. Do you think he should install a newer version of the operating system? Give valid reasons for your answer. (3 marks)

   ii. In case he cannot buy a new version of the operating system, what advice can you give him to help improve the security of his system? (3 marks)

e) Explain any five risks in the internal or external environment that an operating system hosting an online server may be exposed to and how this can be mitigated. (5 marks)

f) You have taken up a new job as a system administrator and have been tasked with the responsibility of installing a file server for the organization. Outline the six steps you would follow in setting up the server. (6 marks)

g) Explain how active directory or LDAP would help improve the security of a computer network infrastructure offering services to many users. (3 marks)

## QUESTION TWO (20 MARKS)

a) Windows server 2012 provides features that provide improved system management experience. One of these features is improved monitoring through Remote Access Management Console. Discuss the five types of information provided by this service. (10 marks)

b) Once an operating system is installed, it needs to be updated and patched in order to improve its security.

   i. Explain the meaning of patching in this context (2 marks)

   ii. State any two benefits of patching and update (2 marks)

   iii. As a system administrator, describe the ideal environment for patching and updating your newly installed server. Give two valid technical reasons. (6 marks)

## QUESTION THREE (20 MARKS)

a) When addressing server security issues, it is an important to keep in mind several general information security principles. Outline any ten such principles apart from defense-in-depth. (10 marks)

b) System administrators should perform a number of tasks after installing a server operating system in order to harden it. If possible they can configure it as a bastion host.

   i. Explain the meaning of a bastion host. (2 marks)

   ii. One of the major activities in this process is removing or disabling unnecessary services, applications and network protocols. Outline any six common types of services and applications that should usually be removed from an operating system if not required. (6 marks)

   iii. Removing unnecessary services and applications is preferable to disabling them. Give two reasons to support this statement. (2 marks)

**QUESTION FOUR (20 MARKS)**

a) State any four security features found in Linux operating systems that make them ideal for use in hosting online servers. (4 marks)

b) Explain the following information system security models: (4 marks)

   i. Bell-La Padula model

   ii. Biba model

c) Password policy is a very key component of an organization's IT security policy. Outline the six key elements that should be addressed in a password policy. (6 marks)

d) Discuss any two basic tests you would perform on an operating system to check how secure it is. For each case, give an example of the tool you would use to perform the test. (6 marks)

**QUESTION FIVE (20 MARKS)**

a) Organizations should understand that a single security mechanism is generally insufficient. Security mechanisms need to be layered so that compromise of one mechanism is insufficient to compromise the whole system. In the light of this statement, discuss the role played by operating systems in defense-in-depth. (10 marks)

b) In the case of servers, the authorized users who can configure the operating system are limited to a small number of designated server administrators. The users who can access the server, however, may range from a few authorized employees to the entire Internet community. To enforce policy restrictions, if required, the server administrator should configure the operating system to authenticate a prospective user by requiring proof that the user is authorized for such access. To ensure the appropriate user authentication is in place, the system administrator should take certain key steps. Outline any five of those steps. (5 marks)

c) Explain how Kerberos is used in user authentication in networked information system infrastructure. (3 marks)

d) Digital signatures form part of operating system security. Explain how the security of a webmail server can be improved by using digital certificate. (2 marks)