JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING

UNIVERSITY EXAMINATION FOR THE DEGREE OF MASTERS OF IT SECURITY AND AUDIT

1ST YEAR 1ST SEMESTER 2018/2019 ACADEMIC YEAR

KISUMU CAMPUS

COURSE CODE: IIT 5112

COURSE TITLE: ADVANCED INFORMATION SYSTEMS SECURITY

EXAM VENUE: **STREAM: IT SECURITY & AUDIT**

DATE:14/08/19 **EXAM SESSION: 9.00 – 12.00NOON**

TIME: 3.00 HOURS

INSTRUCTIONS

1. **Answer THREE questions**
2. **Question 1 is compulsory**
3. **Candidates are advised not to write on the question paper**
4. **Candidates must hand in their answer booklets to the invigilator while in the examination room**

QUESTION 1 [20 MARKS]

An organization's servers provide a wide variety of services to internal and external users, and many servers also store or process sensitive information for the organization. NIST Special Publication 800-44 Version 2, Guidelines on Securing Public Web Servers is an answer to IT security professionals tasked with server security. You have been asked to do a 15 minute presentation using PowerPoint slide (bullets only) on installing a Windows Server as a domain controller. The guidelines below will assist you to articulate your key points. Your response should be inform of bullets for your presentation (strictly no discussion or explanations required).

i) Install new virtual machines
ii) Create Windows Server file
iii) Create a Windows Client/Linux clients OS
iv) Install guest operating systems (1 Server and 1 or more Client OS) on the virtual machines
v) Install Windows server
vi) Add roles, features and services
vii) Install Domain Controllers (DC)
viii) Add computer(s) to your domain (Create Computer Objects)

QUESTION 2 [20 MARKS]

You have been invited to attend an interview for the position of the corporate IT Security Officer. This position requires in-depth knowledge of the server security. You have been told that part of the interview will involve questions related to server security because management feels that this is an area that most University curriculum has paid less attention.

a) Briefly discuss how you would set up local storage and assign access rights (using NTFS rules) to 3 different groups. **(10 marks)**
b) Briefly discuss how you would install application or software restriction policies using the concept of organizational units and Group Policy Object (GPO). Use specific examples for clarity. **(10 marks)**

QUESTION 3 [20 MARKS]

a) Penetration testing is "security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation". The purpose of penetration testing is to exercise system protections (particularly human response to attack

indications) by using common tools and techniques developed by attackers. Discuss any four benefits of penetration testing of your server. **(8 marks)**

b) Vulnerability scanners are automated tools that are used to identify vulnerabilities and misconfiguration of hosts. Many vulnerability scanners also provide information about mitigating discovered vulnerabilities.
   i) Identify any three capabilities provided by vulnerability scanners **(6marks)**
   ii) Identify any three weaknesses of vulnerability scanners **(6marks)**

QUESTION 4 [20 MARKS]

The most critical aspect of deploying a secure server is careful planning before installation, configuration, and deployment. Careful planning will ensure that the server is as secure as possible and in compliance with all relevant organizational policies. Briefly discuss ten important things to consider when planning for server deployment

QUESTION 5 [20 MARKS]

Since server security is tightly intertwined with the organization's general information system security posture, a number of IT and system security staff may be involved in server planning, implementation, and administration. Briefly describe any 3 roles of the following IT security personnel in an organization

a) Chief Information Officer **(5 marks)**
b) Information Systems Security Program Managers **(5 marks)**
c) Information Systems Security Officers **(5 marks)**
d) Server, Network, and Security Administrators **(5 marks)**