CHUKA UNIVERSITY

UNIVERSITY EXAMINATIONS

FIRST YEAR EXAMINATION FOR THE AWARD OF DEGREE OF MASTER OF SCIENCE IN COMPUTER SCIENCE

COSC 854: SECURITY ARCHITECTURE AND DESIGN

STREAMS: Y1S2 **TIME:3 HOURS**

DAY/DATE: WEDNESDAY 4/12/2019 **2.30 P.M – 5.30 P.M**

INSTRUCTIONS:

1. Answer Question **ONE** and any other **TWO** questions
2. Marks are awarded for clear and concise answers
3. Where scripts are to be written, use Kali linux commands.

SECTION A-COMPULSORY

Question ONE [30 Marks]

(a)A Small Business That Has a Basic Internet Presence

A small sales company wants to set up an Internet connection but does not intend to sell products directly over the Internet. The owner of the business has read several horror stories about companies being taken over by attackers and has specifically asked for as secure a design as possible, but does not have a large budget.

Following are the specific design requirements and business needs that the company has established:

- The workstations and Windows servers are the primary resources that must be protected. The company needs to establish an information Web site for its customers, but the site is not considered essential to the business operations.
- The company does not know of any individuals or organizations that would specifically want to do them harm, but it does store customer information, including credit card data, on its Windows servers.
- Employees must be able to send and receive email.
- Employees must be able to browse suppliers' web sites.
- The company is not expected to get a large volume of traffic.
- The design must be secure, but the budget for security devices and software must be kept as low as possible.

- The external connection that has been arranged with the ISP is a *burstable* Lease line provisioned for a continuous usage of 5 Mbps.

Given the above requirements, identify with the aid of some diagram, the critical features of the security design needed to secure the organization network [12 Marks]

(b)Describe THREE benefits of security architecture approach [6 Marks]
(c)Many standards including ISO 27001 standard conforms with SABSA architecture steps. Describe the activities in each of the following steps of SABSA architecture:
(i)Business Driver [2 Marks]
(ii)Business attributes [2 Marks]
(iii)Threat analysis [2 Marks]
(iv)Impact analysis [2 Marks]
(v)Control Objectives [2 Marks]
(vi)Security Services [2 Marks]

QUESTION TWO [20 MARKS]

(a)Graham—Denning Model defines a set of basic rights in terms of commands that a specific subject can execute on an object. Describe **SIX** primitive protection rights, or rules of how these types of functionalities should take place securely [6 Marks]

(b)Harrison-Ruzzo-Ullman Model is an operating system level computer security model. Describe its key concerns [4 Marks]

(c)Describe **FIVE** Components of Java Security architecture [5 Marks]

QUESTION THREE [15 MARKS]

(a)SABSA is a business-driven security framework for enterprises that is based on risk and opportunities associated with it. Describe the requirements of the five horizontal layers of SABSA framework **[**10 Marks]

(b)Using a diagram illustrate the relationship between SABSA and COBIT [5 Marks**]**

QUESTION FOUR [15 MARKS]

(a)Discuss **FIVE** characteristics of a good security architecture [10 Marks]

(b)Security architecture controls comprise people, process and technology controls. Describe **FIVE** characteristics of security architecture controls [5 Marks]

QUESTION FIVE [15 MARKS]

(a)Describe the following concepts as applied in Computer systems security architecture**.**
(i)Security Kernel [2 Marks]
(ii)Trusted Computing base [2 Marks]
(b)Personnel security is a system of policies and procedures which seek to mitigate the risk of workers (insiders) exploiting their legitimate access to an organisation's assets for

unauthorised purposes. A manufacturing farm has hired you to assist them in developing a comprehensive personnel security program. What are the key elements you would consider in your design [6 Marks]

(c)Operations security is an information risk management process that encourages managers to view operations from the perspective of an adversary in order to protect sensitive information from falling into the wrong hands. Describe **FIVE** steps of operations Security Process. [5 Marks]
