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 BACHELOR OF SCIENCE IN SECURITY AND FORENSICS

3RD YEAR 1ST SEMESTER 2015/2016 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: IIT 3316

COURSE TITLE: PROTOCOLS AND SYSTEMS FOR INTERNET AND WEB SECURITY

EXAM VENUE: **STREAM: COMPUTER SECURITY & FORENSICS**

DATE: **EXAM SESSION: 2 HRS.**

TIME:

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 1 [30 MARKS]

a) Define the following terms

i) Port Scan **(2 marks)**
ii) Nmap **(2 marks)**
iii) SuperScan **(2 marks)**
iv) Buffer Overflow **(2 marks)**
v) Idle Scanning **(2 marks)**
vi) IPSec **(2 marks)**
vii) SSL **(2 marks)**
viii) TLS **(2 marks)**

b) A browser issued a GET request for a resource and obtained the following two responses as shown below. Answer the following questions:

i) What do 200 represent? **(2 marks)**
ii) What do 404 mean? **(2 marks)**
iii) Identify the main differences response 1 and 2? **(4 marks)**

c) Identifying what sort of network attacks to defend against is critical in attaining the goals of network security. Identify at least six best practices that can be implemented to defend against security threats. **(6 marks)**

QUESTION 2 [20 MARKS]

a) Using two examples each differentiate between routing protocol and routed protocols **(4 marks)**

b) What is HTTP? Using an example of retrieving the JOOUST semester calendar located in the RegistrarAA in the Academics folder, briefly describe how HTTP works. **(6 marks)**

c) List any *four* protocols found in the respective TCP/IP layers. You MUST write their names in full. Identify the ports associated with the four application layer protocols you identified.

Application layer
Transport
Internet
Link **(10 marks)**

QUESTION 3 [20 MARKS]

a) Before any TCP connection between a client and a serve, both running under SSL, is established, there must be almost a process similar to a three-way handshake. This get-to-know-you process is similarly called the SSL handshake. During the handshake, the client and server perform the following tasks. Describe the four task performed. **(10 marks)**

b) What is SET and what type of services does it provide? **(10 marks)**

QUESTION 4 [20 MARKS]

SSL is a widely used general purpose cryptographic system used in browsers. It provides an encrypted end-to-end data path between a client and a server regardless of platform or OS. Secure and authenticated services are provided through data encryption, server authentication, message integrity, and client authentication. Using a diagram describe the process of SSL connection setup. **(20 marks)**

QUESTION 5 [20 MARKS]

a) The call for and desire for security and privacy has led to several security protocols and standards. Among these are: Secure Socket Layer (SSL), Transport Layer Security (TLS), secure IP (IPSec), Secure HTTP (HTTPS), and secure E-mail (PGP and S/MIME). Briefly discuss each of these six security protocols. **(20 marks)**

QUESTION 6 [20 MARKS]

a) What is a DoS attacks? Describe four types of DoS attack **(10 marks)**

b) Spoofing attacks may occur in different forms, for example, DNS, Web and IP spoofing attacks. What is a Spoofing attack? Briefly describe these three types of Spoofing attacks **(10 marks)**