CHUKA UNIVERSITY

UNIVERSITY EXAMINATIONS

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

COSC 853: INTERNET SECURITY

STREAMS: **TIME:3 HOURS**

DAY/DATE: TUESDAY 3/12/2019 **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 or backtrack commands.

SECTION A-COMPULSORY

QUESTION ONE [30 MARKS]

(a)Give a brief description of the key functionalities of each of the following well known network security tools

(i)Scapy **[2 Marks]**
(ii) nmap **[2 Marks]**
(iii)Wireshark **[2 Marks]**
(iv)Hydra **[2 Marks]**

(b) Smurf attack is a typical type of DoS attack. Describe how it works **[5 Marks]**

(c)Differentiate between the following in relation to S/MIME functionality

(i)Enveloped data and signed data **[3 Marks]**
(ii)Clear signed data and signed and enveloped data **[3 Marks]**

(d)With the aid of a diagram demonstrate how you can implement firewalls and intrusion detection system to secure organization's network **[6 marks]**

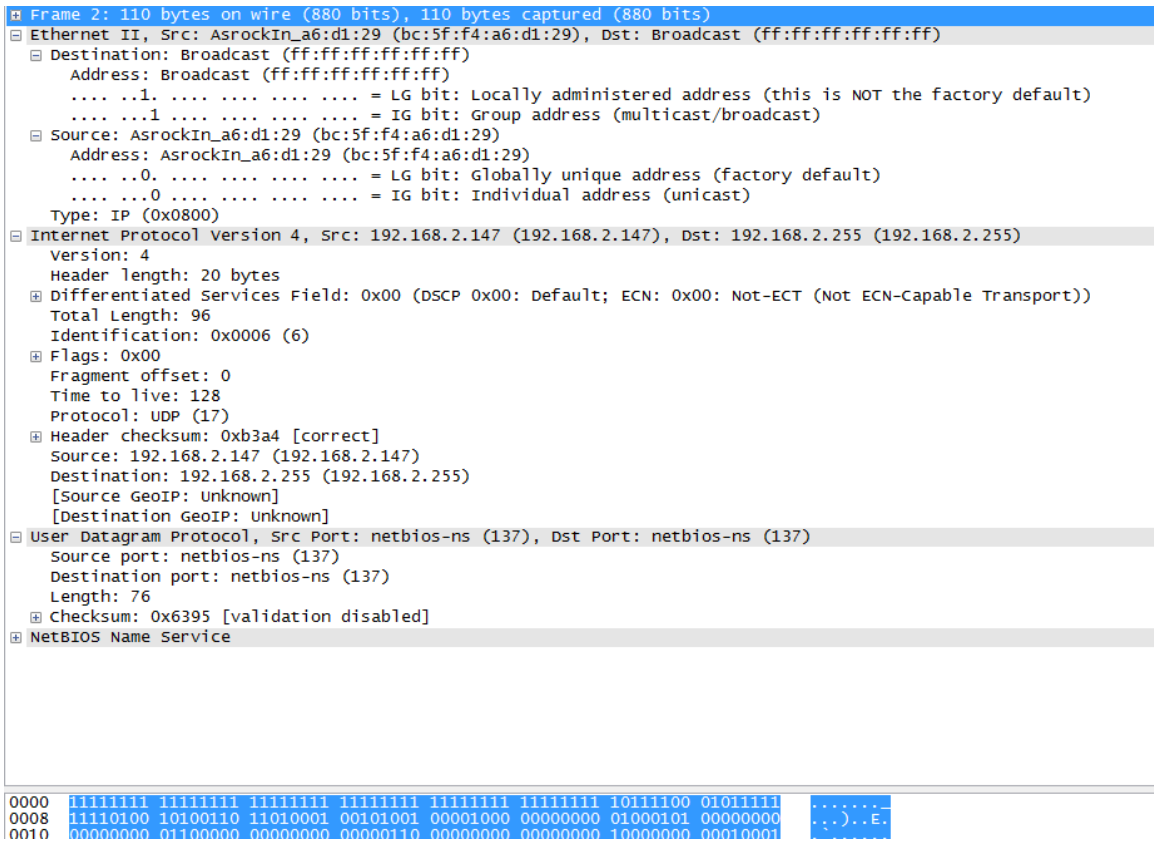
(e) Briefly illustrate using a diagram key steps of pretty good privacy (PGP) security. [5 marks]

QUESTION TWO [15 MARKS]

(a)Write shell commands that creates an ICMP packet with destination address 8.8.8.8.The script should then display the packet and then insert it into the network **[6 Marks]**

(b)Describe the TCP hijacking attack steps **[4 Marks]**

(c)The figure below shows a packet captured and analyzed by wireshark.Study it and provide the following information.



(i)The transport layer protocol used to carry the packet **[1 Mark]**
(ii)The destination IP address of the packet **[1 Mark]**
(iii)The destination port of the packet **[1 Mark]**
(iv)The TTL of the packet **[1 Mark]**
(v)The source MAC address of the packet **[1 Mark]**

QUESTION THREE [15 MARKS]

(a)Using crunch tool, write a command that generates a list of 5 character passwords where the first character is Z ,the second is a lower case,the third is upper case, and the fourth is a number. **[4Marks]**
(b)Using a diagram, illustrate the **FOUR** phases of SSL handshake protocol **[8 Marks]**
(c)Describe **THREE** key services provided by SSL record protocol **[3 Marks]**

QUESTION FOUR [15 MARKS]

(a)Write a script that identifies open ports from a host and scans the services running on them. **[10 Marks]**
(b)Describe the SYN attack steps **[5Marks]**

QUESTION FIVE [15 MARKS]

(a)While describing the role of dual signature in e-commerce transactions, illustrate how it is implemented in secure electronic transactions (SET) protocol **[5 Marks]**
(b) What are the details of the contents of the Purchase Request message generated by the customer in a SET transaction. **[6 Marks]**
(c)Describe **TWO** services provided by PGP protocol giving the algorithm used for each service. **[4 Marks]**
