Open University *of* Mauritius

Open University *of* Mauritius

BSc (HONS) APPLIED ICT [OUbs017]

EXAMINATION FOR:		November/December 2020
MODULE	**:**	Network Security [OUbs0173114]
DATE	**:**	Wednesday 09 December 2020
DURATION	**:**	2 Hours

INSTRUCTIONS TO CANDIDATES

1. This question paper consists of **FOUR (4) QUESTIONS**.
2. Answer **ALL Questions**.
3. Always start a new question on a fresh page.
4. Total marks: **100**

This question paper contains 4 questions and 5 pages

ANSWER ALL QUESTIONS

QUESTION 1 [20 MARKS]

a) With the help of examples, explain the following terms:

i. Trap door

ii. Logic Bomb

iii. Login Spoofing

iv. Privilege Escalation Attacks

(8 marks)

b) AAA security process describes the network or applications way of identifying a user and ensuring the user is whom they claim to be. Describe the security process and provide an example for each.

(6 marks)

c) An operating system, also called OS, is a collection of system programs, tools, and utilities that manage computer hardware resources and offer common services for client application software.

i. Describe the Windows OS security model.

ii. Describe the Linux OS security model.

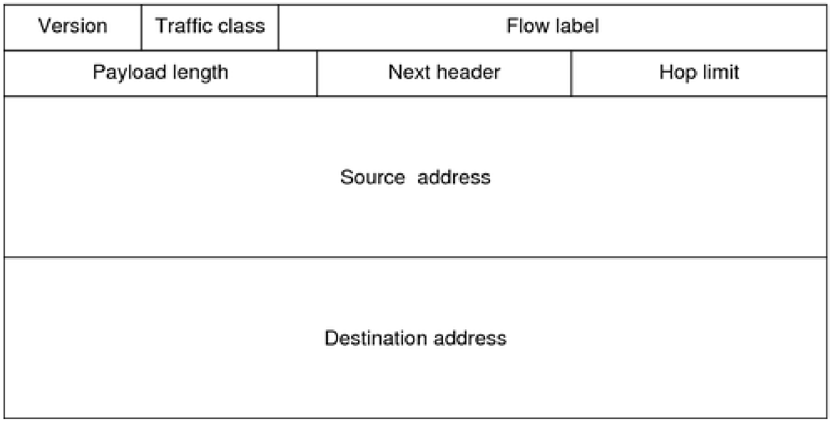
(6 marks)

QUESTION 2 [25 MARKS]

a) IPv6 is said to be more secure than IPv4. Describe the security features in IPv6 and describe the main security vulnerability of IPv4.

(4 marks)

b)



The image above depicts the format of an IPv6 Packet header format. Briefly indicate the purpose of the following IPv6 header fields:

i. Version.

ii. Payload Length.

iii. Next header.

iv. Hop limit.

v. Source IP address.

vi. Destination IP address.

(12 marks)

c) What is the purpose of creating a DMZ during firewall implementation?

(3 marks)

d) With the help of diagrams, describe **three (3)** types of firewall and their purpose.

(6 marks)

QUESTION 3 [30 MARKS]

a) Successful BYOD deployments have turned an initial risk management initiative into a broader programme of business enablement, elaborate on this statement.

(6 marks)

b) Explain the concept of Single Sign-On (SSO). Provide **two (2)** advantages and **two (2)** disadvantages.

(6 marks)

c) Security in mobile devices is becoming a common threat. However, very few mobiles come with native security mechanism.

i. Describe mobile security threats.

ii. Illustrate on the counter measures that could be used.

(6 marks)

d) Discuss what is meant by network forensic. Provide an example of a network forensic case.

(6 marks)

e) Intrusion detection and prevention are two broad terms describing application security practices. What is the role of an IDS and IPS and describe the operation of a signature-based IDS.

(6 marks)

QUESTION 4 [25 MARKS]

a) IP Traceback is the name of the method used to cross verify the authenticity of the source of an IP address. Describe what is meant by packet marking and how it works.

(5 marks)

b) List and briefly describe the **five (5)** stages of a typical intrusion process in a network.

(10 marks)

c) Database security threats are numerous and may involve the following:

i. SQL Injection

ii. Privilege Abuse

iii. Unmanaged Sensitive Data

iv. Misconfigured Database

v. Limited Security Expertise and Education

With the help of examples, discuss the above threats.

(10 marks)