NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF COMPUTER SCIENCE

QUALIFICATION : BACHELOR OF COMPUTER SCIENCE IN (CYBER SECURITY)	
QUALIFICATION CODE: 07BCCS	**LEVEL: 6**
COURSE: NETWORK SECURITY	**COURSE CODE: NWS620S**
DATE: JUNE 2019	**PAPER: THEORY**
DURATION: 2 hours	**MARKS: 70**

FIRST OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER(S)	**Mrs. Mercy Chitauro**
MODERATOR:	**Mr. Joel Eelu**

THIS EXAMINATION PAPER CONSISTS OF 4 PAGES

(Excluding this front page)

INSTRUCTIONS

1. Answer **all questions**.
2. When writing take the following into account: The style should inform than impress, it should be formal, in third person, paragraphs set out according to ideas or issues and the paragraphs flowing in a logical order. Information provided should be brief and accurate.
3. Please, ensure that your writing is **legible, neat** and **presentable.**
4. When answering questions you should be led by the allocation of marks. Do not give too few or too many facts in your answers.
5. Number your answers clearly according to the question paper numbering.
6. Clearly mark rough work as such or cross it out unambiguously in ink.

PERMISSIBLE MATERIALS

1. Calculator.

1. Network Security Introduction and Cryptography.
    a. What is
        i. A passive attack? [1]
        ii. An active attack? [1]
    b. How can you protect your network from passive attacks? [2]
    c. How many keys are required for two people to communicate via an asymmetric cipher? [1]
    d. Briefly explain why 3DES is widely used compared to DES/DEA [3]
    e. Given that 3 DES does not produce efficient software code and that it uses 64-bit block sizes. What elements would be required in algorithm that would work better than 3DES? [2]
    f. Why is the generation of random numbers in network security important? [1]
    g. Give one example were random numbers are used in network security. [1]
    h. Give two requirements for random numbers. [1]

2. Message Authentication
    a. What security measure is required when you need to protect against falsification of data? [1]
    b. What three things are verified to prove message authentication? [3]
    c. Why is encryption alone not suitable for data authentication? [2]
    d. Explain three uses for public key-systems. [3]

3. IPSec is a set of internet standards that ensures security networking for security-ignorant applications. Consider Figure 1 when answering question 3. An IPSec VPN is implemented between RD and RM. The tunnel is terminated at ports 164.10.1.1 and 120.5.2.3. the tunnel uses AES as the encryption standard.

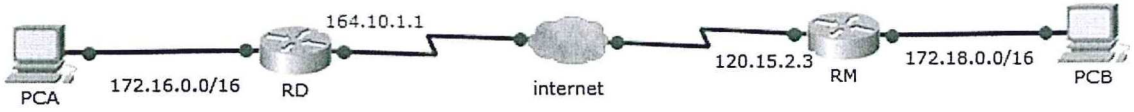

Figure 1: Bakers Fresh branch connection

    a. What type of VPN is implemented between RD and RM? [1]
    b. RD and RM have remote logon, client/server, e-mail, file transfer and web access traffic between them. Which traffic will be encrypted by AES? [2]
    c. State three parameters that are used to identify security associations. Identify the three parameters used by RM in one of its AH security associations. [6]
    d. Where is the security association stated in '3c' stored on RM? [1]

e. RM will use the security association in '3c' on packets originating from 172.18.0.0/16 network and another one for ESP. What type of security association bundle is this? [1]

f. What is a security association bundle? [1]

4. Use figure 2 to answer the following questions

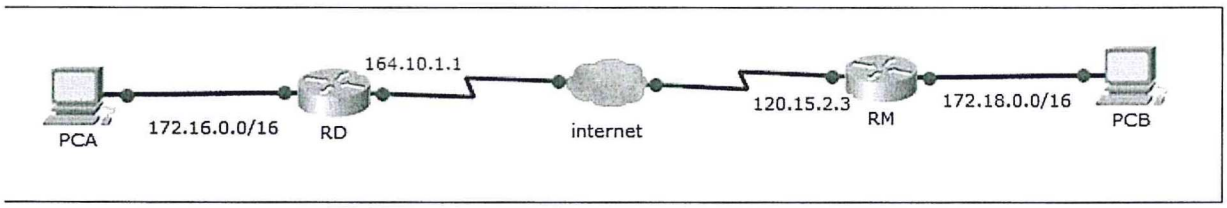

Figure 2: Bakers Fresh Branch Connection

a. Highlight four Pretty Good Privacy (PGP) services that are availed to email users in the 172.16.0.0/16 and 172.18.0.0/16 networks. [2]

b. Explain how PGP encrypts a message sent from user at 172.16.0.253 to user at 172.18.5.13 [2]

c. Does the user at 172.18.5.13 have the key used for encryption before the message is transmitted? [1]

d. Explain your answer in '4c'. [3]

e. Secure/Multipurpose Internet Mail Extension (S/MIME) is another email security standard. S/MIME provides which security services for a MIME? [1]

f. Worms are typically attached to electronic mails so that they access remote systems and replicate.

   i. What is a worm? [2]

   ii. Which other means do worms use to access remote sites besides attaching to emails? [2]

g. In a worm's lifetime it goes through the same phases as that of a virus. Explain the difference between worm's propagation phase and a virus's propagation phase. [4]

5. Intruders

a. Classify and explain the type of intruder explained below.

i. An outside individual who takes over your web server and pretends to be the webmaster and modifies content on your web pages. [2]

ii. A sales person in your company who escalates their rights to that of the system administrator. [2]

b. What would be your advice to network security administrator of a company that is experiencing intrusion as given in '5a' [2]

c. A Firewall is designed to protect the premises network from Internet-based intrusion and to provide a single choke point where security and auditing can be imposed. Table 1 is an example of a packet filtering firewall.

Table 1: Packet Filter Rules

Rule	direction	Src Address	Dest Address	Protocol	Dest Port	Action
A	in	External	Internal	TCP	25	Permit
B	Out	Internal	external	TCP	>1023	Permit
C	Out	Internal	external	TCP	25	Permit
D	In	external	internal	TCP	>1023	Permit
E	either	Any	any	any	any	deny

Explain what will happen to the packets in Table 2 in a network with a summary address of 33.10.0.0/16 considering the packet filter rules in Table 1. [4]

Table 2: Packets in network 10.0.0.0/8

Packet	Src Address	Dest address	Protocol	Port	**Action**
I.	11.13.4.9	33.10.10.25	TCP	25	
II.	48.16.10.45	33.10.63.1	TCP	23	
III.	33.10.24.33	12.13.14.16	TCP	2023	
IV.	11.13.4.9	33.10.25.9	TCP	995	

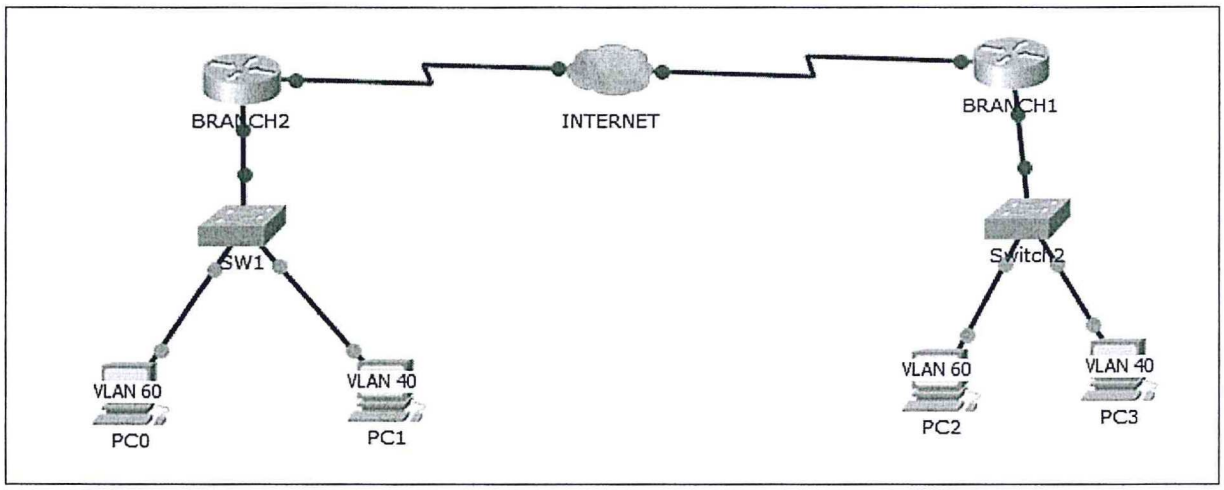

Figure 3

7. Consider Figure 3. Assume that this network has no security implementations at the moment. Describe 5 security measures that can be added to this network. For each security measure:

   a. State what it is that will be added? [3]

   b. Explain how it adds security. [3]

   c. Where possible; how it is achieved? [3]

Good luck!!