NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

Faculty of Computing and Informatics

Computer Science Department

QUALIFICATION: BACHELOR OF COMPUTER SCIENCE HONOURS	
QUALIFICATION CODE: 07BACS	**LEVEL: 8**
COURSE: PRACTICAL NETWORK SECURITY	**COURSE CODE:** PTS811S
DATE: JUNE 2019	**SESSION: 1**
DURATION: 2 Hours	**MARKS: 80**

FIRST OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER(S)	Dr Fungai Bhunu Shava
MODERATOR:	Mr Kudakwashe Madzima

THIS QUESTION PAPER CONSISTS OF 3 PAGES
(Excluding this front page)

INSTRUCTIONS

1. Answer ALL the questions.
2. Write clearly and neatly.
3. Number the answers clearly.
4. Do not use additional materials
5. Cross out any work which should not be marked.
6. No pencil work allowed except for diagrams where requested.

Use the scenario below to answer the questions where reference is made to it. The answers should be relative to the context.

Scenario: Smart has become a buzzword in homes, businesses, cities and nations; this is enhanced by the connectivity of virtually all things/devices we use in homes and workplaces. This allows for individuals to monitor and remotely control all their devices in the home from their smart mobile device as well as access business and national services information from anywhere anytime. Organisations are keen on cutting costs in every possible way and this brings the implementation of green technologies which are energy and cost efficient. However, all connected things need to secure all information at rest, in transit or during processing to maintain CIA and hence individual and organisation reputation. Trends from 2017 as per first takehome activity have shown that any individual or organisation with an online presence is a potential target for cyber criminals. Ransomware, cryptocurrency mining, fileless malware, cross operating system attacks, hardware vulnerabilities (top stories on Huawei, USA, UK, China; Spectre and Meltdown), emerging disruptive technologies (Bring Your Own Device (BYOD), Internet of Things/Everything (IOT/E), Machine Learning (ML) and Artificial Intelligence (AI)) attacks. This was made worse by organizational security practices witnessed over the years. Organisational security culture is very poor as evidenced by lack of security basics such as updates, patches, implementing basic security measures, failure to learn from past experiences, failure to improve cyber defences. Organisations are still vulnerable as they are not growing.

Trending solution in 2018 security reports include Cyber resilience, proactive approach to security, a goal of data visibility to ensure cyber resilience, implementing the zero trust model. Namibia University of Science and Technology (NUST) will not be left out in being part of the solutions. As a Chief Security Officer (CSO) you have been appointed to ensure Information security at NUST and to proactively contribute to the needed solutions for the republic of Namibia.

1. Introduction to Security **[16 marks]**
    a. Who are the potential targets for cyber criminals? [1 mark]
    b. What attitude/s do you need to develop towards InfoSec if you will win in fighting the cyber criminals? [3 marks]
    c. In lab 1 you were given six tools to help you gather information about your IT lab environment. Among them were NMAP, Wireshark, Netstat, and Microsoft Baseline Analyser (MBSA).
        i. Explain why this exercise is important to a CSO, detail the role of each tool listed? [6 marks]
        ii. Explain how this information can help in implementing some of the proposed solutions highlighted in the scenario? [6 marks]

2. Policing [10 marks]

In assignment two you were tasked to use five to ten current and relevant articles including white papers to design a process to implement a Zero Trust Model for BYOD at NUST. This speaks to one of the proposed solutions in the scenario. To effectively do this, a policy needs to be in place.

Determine the important components of a Zero Trust Model Policy and use them in designing a relevant policy for the NUST community. [10 marks]

3. Firewalls [11 marks]

    a. What is the purpose of a Firewall in the smart NUST network? [2 marks]
    b. With the aid of a detailed explanation, what would be the best firewall type to recommend for any organisation that fits the provided scenario? [9 marks]

4. Intrusion Prevention Systems [8 marks]
    a. To ensure intrusion prevention in a timely manner within a smart organisation, sensors are integrated with real-time monitoring systems, to collect data from end user devices for processing and analysing. Which type/s of IPS is suitable for the scenario above? Why? [6 marks]
    b. What would you recommend for the proposed smart organisation, an IPS or IDS? [2 marks]
5. AAA [10 marks]
    a. What benefits would a smart organisation enjoy from implementing AAA? [7 marks]
    b. Name three protocols that can be used to implement AAA in smart environments such as smart NUST? [3 marks]

6. Cryptography [10 marks]
    a. Using the smart city as an example, differentiate between key exchange and key agreement and state which one would be more appropriate. [4 marks]
    b. Using the smart organisation setup define steganography. [4 marks]
    c. How can one securely transmit an email over the NUST network without the fear of insider threat? [2 marks]

7. Internet security [15 marks]
    a. Define any two types of insecurities or attacks that need your attention in a smart organisation described in the scenario. [4 marks]
    b. The smart computing services to be introduced at NUST are accessible via the Internet using NUST devices or personal networks as individuals are more comfortable using the Bring Your Own Network (BYON) model. What are the

risks associated with Internet usage especially coupled with BYON in a smart NUST environment? [6 marks]

c. How best can NUST ensure that their network is safe? [2 marks]

d. In module 7, you were tasked to research on the use of IM an SMS over the Internet. What are the benefits and security risks associated with this in a smart organisation? [3 marks]

END!