NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

# FACULTY OF COMPUTING AND INFORMATICS

## DEPARTMENT OF COMPUTER SCIENCE

| | |
|---|---|
| QUALIFICATION : BACHELOR OF COMPUTER SCIENCE | |
| QUALIFICATION CODE: 07BACS | LEVEL: 6 |
| COURSE: NETWORK SECURITY | COURSE CODE: NWS620S |
| DATE: JANUARY 2020 | PAPER: THEORY |
| DURATION: 2 HOURS | MARKS: 70 |

| SUPPLEMENTARY / SECOND OPPORTUNITY EXAMINATION QUESTION PAPER | |
|---|---|
| EXAMINER(S) | MRS MERCY CHITAURO |
| MODERATOR: | DR ATTLEE GAMUNDANI |

**THIS EXAMINATION PAPER CONSISTS OF 3 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. Public key encryption schemes can be used for conventional encryption and digital certificates.
   a. What else can public key encryption schemes be used for? [1]
   b. Suppose that Romanus wants to send a message to Tjitjiri. Describe how a public key encryption scheme can enable Romanus to send a digitally signed message to Tjitjiri. [4]
   c. What is the drawback to the digital signature method described in (1b)? [1]
   d. What could be a more efficient way of obtaining a digital signature? [2]
   e. Give a practical example of the solution you mentioned in (1d) [1]
   f. Explain how the solution in (1d) can provide a digital signature [3]

2.
   a. State and describe two ways that enable message authentication. [4]
   b. Given the simple hash function utilizing bitwise XOR; with a block size of four bits. What will be the hash of message blocks given below. Give your answer in base 10.
      i. Block 1 $=3_{10}$; block two $=4_{10}$ [5]
   c. What is the purpose of the Diffie Hellman key exchange algorithm? [2]

3. Kerberos uses as its basis the symmetric Needham-Schroeder protocol. It makes use of a trusted third party, termed a Key Distribution Center (KDC), which consists of two logically separate parts: An Authentication Server (AS) and a Ticket Granting Server (TGS). Kerberos works on the basis of "tickets" which serve to prove the identity of users.
   a. What is shared between the KDC and each entity (client or server) in the network? [1]
   b. What does the KDC generate so that two entities can communicate? [1]
   c. In Kerberos operations there is no direct communication. What is provided by the TGS that allows a user to get access on a server? [1]
   d. Considering Kerberos operation, when Ngatu receives a ticket from Vilima, how does she know it came from Vilima? [2]

4. IPSec

   a. At which level of the OSI does IPSec operate? [1]

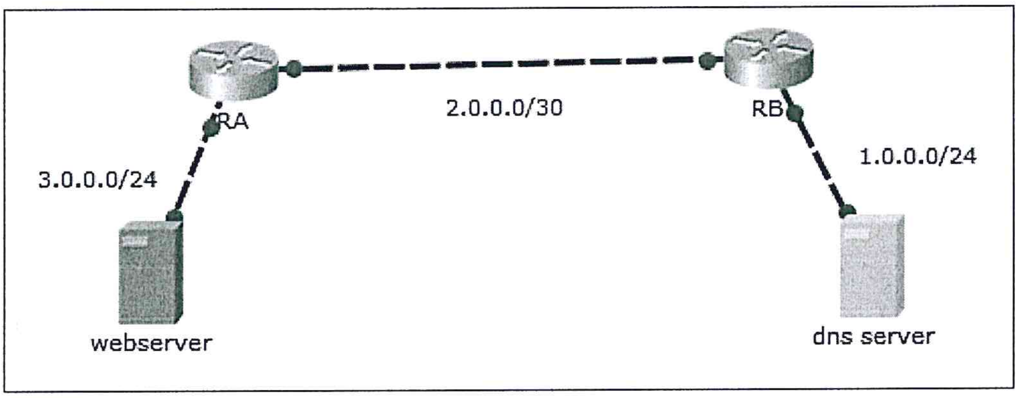

*Figure 1*

   b. Consider Figure 1.

      ii. What will be the benefit for **RA**'s routing protocol if IPSec is implemented? [2]

      iii. What is a security association in the context of RA and RB? [2]

      iv. What are three components that will be found in the triple security association between **RA** and **RB** that is defined at RA? [3]

      v. Where are security associations for **RB**? [1]

5.

   a. Draw Table 1 in your answer sheet and fill in the respective control to the given firewall technique. [4]

*Table 1: Firewall techniques and controls*

| **Firewall technique** | **Control** |
|---|---|
| Controls how particular services are used | i. |
| Determines the types of Internet services that can be accessed, inbound or outbound | ii. |
| Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall | iii. |
| Controls access to a service according to which user is attempting to access it | iv. |

   b. A packet filter firewall is typically set up as a list of rules based on matches to fields in the IP or TCP header. If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard the packet. If there is no match to any rule, then a default action is taken.

      i. Describe two default firewall policies possible. [4]

   c. What type of devices or systems are kept in the demilitarized zone? [1]

6. One function of an intrusion detection is to audit system configuration for vulnerabilities and misconfigurations.
   a. What will be the result of such an audit? [2]
   b. Which of pattern based or heuristic IDS would be able to carry out the audit in (6a)? [2]
   c. Explain how an Intrusion Prevention System IPS extends the functionalities of an IDS. [2]
   d. How would you protect an IDS from network attacks? [2]

7. Using your knowledge of SSL. Explain how SSL circumvents the attack given.
   a. Brute-force cryptanalytic attack: An exhaustive search of the key space for a conventional encryption algorithm. [2]
   b. Man-in-the-middle attack: An attacker interposes during key exchange, acting as the client to the server and as the server to the client. [2]

8.
   a. Highlight four Pretty Good Privacy (PGP) services. [2]
   b. Explain how PGP encrypts a message. [2]
   c. Does the receiver have the key used for encryption before the message is transmitted? [1]
   d. Explain your answer in '8c'. [3]
   e. Secure/Multipurpose Internet Mail Extension (S/MIME) is another email security standard. S/MIME provides which security services for a MIME? [2]
   f. In S/MIME Terminology what does it mean to say, ***"When S/MIME creates a message digest to be used in forming a digital signature it MUST support SHA – 1 and it SHOULD support MD5"***? [2]

Good luck!!