

MULUNGUSHI UNIVERSITY

Pursuing the frontiers of Knowledge

Department of Computer Science and Information Technology

Computer Security - ICT 341

FINAL EXAMINATION

DECEMBER 2022

Time: 3:00 Hrs.

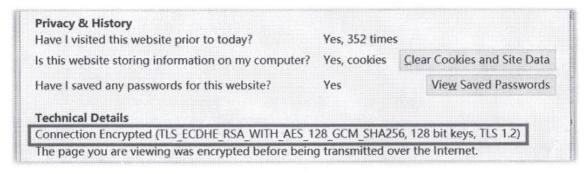
INSTRUCTIONS

There are four (4) questions.

Answer ALL the questions.

Present tidy and readable work.

- 1. Generally, information security is based on certain principles. Attacks breach these principles of security.
 - (a) Describe the 3 major principles of security [6 Marks]
 - (b) List any 4 DOS attacks found in information systems. [4 Marks]
 - (c) Give any 5 properties of DES encryption. [5 Marks]
 - (d) With the help of a diagram, describe AES encryption AND gives any 5 features of AES encryption. [10 Marks]
- 2. Study the extract below obtained from a website that uses secure communication.



Based on the information highlighted in bold, identify the principle of the following and:

- a) The secure protocol being described above [5 Marks]
- b) The algorithm used in encrypting the data [5 Marks]
- c) The methodology (group) and algorithms used in the key exchange [5 Marks]
- d) The hashing algorithm being used [5 Marks]
- e) The trapdoor functions used in the identified encryption schemes [5 Marks]
- 3. Consider the exhibit of network security scan below and answer the questions that follow.

```
Host is up (0.060s latency).
Not shown: 987 filtered ports
PORT
         STATE SERVICE
21/tcp
         open ftp
22/tcp
         open
              ssh
23/tcp
               telnet
         open
80/tcp
         open
               http
135/tcp
         open
               msrpc
139/tcp
               netbios-ssn
         open
443/tcp
         open https
         open microsoft-ds
445/tcp
512/tcp
         open exec
514/tcp
         open
               shell
              telnets
992/tcp
         open
3306/tcp open
              mysal
5357/tcp open
              wsdapi
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 9.88 seconds
```

- (a) State which protocol is used for unsecured and secured remote access services. [5 Marks]
- (b) State which protocol is used for unsecured and secured website services. [5 Marks]
- (c) State which protocol you can used in place of ftp to provide secure file services. [5 Marks]
- (d) State which protocol and port number was used by the WannaCry ransomware in 2017 to propagate on the Internet as a worm and spread the attack. [10 Marks]
- 4. Security attacks are related to threats and vulnerabilities. There are several mechanisms that are implemented to mitigate the security attacks.
 - (a) Differentiate the following terms: threat, vulnerability, and attack. [6 Marks]
 - (b) Describe the 3 factors of authentication. [6 Marks]
 - (c) Differentiate the access control models MAC and DAC. [4 Marks]
 - (d) Describe an access control matrix. [6 Marks]
 - (e) List any 5 secure network protocols. [5 Marks]

	Total [100 Marks]
END OF	EXAM