



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.

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

Privacy & History

Have I visited this website prior to today? Yes, 352 times

Is this website storing information on my computer? Yes, cookies [Clear Cookies and Site Data](#)

Have I saved any passwords for this website? Yes [View Saved Passwords](#)

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)

The page you are viewing was encrypted before being transmitted over the Internet.

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

- The secure protocol being described above [5 Marks]
 - The algorithm used in encrypting the data [5 Marks]
 - The methodology (group) and algorithms used in the key exchange [5 Marks]
 - The hashing algorithm being used [5 Marks]
 - The trapdoor functions used in the identified encryption schemes [5 Marks]
- 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    open  telnet
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
512/tcp   open  exec
514/tcp   open  shell
992/tcp   open  telnets
3306/tcp  open  mysql
5357/tcp  open  wsddapi

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 use 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**-----