UNIVERSITY COLLEGE TATI (UC TATI)

FINAL EXAMINATION QUESTION BOOKLET	
COURSE CODE	: BNS 2223
COURSE	: NETWORK SECURITY
SEMESTER/SESSION	: 2-2023/2024
DURATION	: 3 HOURS

Instructions:

1. This booklet contains 5 questions. Answer ALL questions.
2. All answers should be written in answer booklet.
4. Write legibly and draw sketches wherever required.
5. If in doubt, raise your hands and ask the invigilator.

DO NOT OPEN THIS BOOKLET UNTIL YOU ARE TOLD TO DO SO

THIS BOOKLET CONTAINS 7 PRINTED PAGES INCLUDING COVER PAGE

QUESTION 1

In 8 April 2023, a coordinated cyberattack was launched in India against six major airports and healthcare institutions by a hacker group named Anonymous Sudan. The recent cyberattack on multiple airports across the world raised concerns about the level of preparedness necessary to deal with such threats. According to the firm, the attackers used a particular Distributed Denial of Service Attack (DDoS) Python script independently, which identifies open proxies on the Internet and does an average connection of 5 million requests from script executions, as below.

- Type of Attack: DDoS
- Target Sector: Government (Airport)
- Intention: Delay of services

Answer question 1a related to the case study above.

a) State **ONE (1)** requirement for each security objective below that is associated with the passport control system of Istanbul Ataturk Airport;

i) Confidentiality (1 marks)

ii) Integrity (1 marks)

iii) Availability (1 marks)

b) Describe the Script Kiddies profile of attacker (2 marks)

c) How the Repudiation Attacks look like? State **ONE (1)** example of strategy under Repudiation Attack. (3 marks)

QUESTION 2

a) Attackers attempt to exploit weak passwords by using password guessing. Among types of attack in password guessing are **Brute Force, Dictionary Attack** and **Software Exploitation**. Explain **TWO (2)** techniques of password guessing on how they operate. (4 marks)

b) Name **ONE (1)** of a flooding mechanism and describe the method that contributes to the Denial of Service (Dos) attack. (4 marks)

c) Personal Identification Number (PIN) for ATM nowadays uses 6 keys. Answer the following questions.

i) How much time does it take for a cracking software system to crack a PIN number if 1000 keys were searched per second? (1 mark)

ii) Attackers attempt to exploit weak PIN by password guessing in ATM machine. Describe **THREE (3)** methods on how the attacker launches the password guessing attacks. (6 marks)

iii) Explain on how dumpster diving attack is employed in searching victim ATM's PIN? (1 mark)

d) Give the definition of firewall. (1 mark)

e) Identify **FOUR (4)** tasks to be done by firewall. (4 marks)

f) State **THREE (3)** rules of firewall. (3 marks)

QUESTION 3

a) There are two primary types of Intrusion Detection System (IDS) which are Signature and Anomaly detection. Differentiate the way of detection on each of them. (4 marks)

b) IP Security (IPSec) module is used to manage security for individual connections to other modules. Answer all questions related to IPsec, as following;

i) Illustrate the IPSec architecture. (5 marks)

ii) Give the function for each **THREE (3)** module consists in IP Security architecture. (3 marks)

c) Give **FOUR (4)** reasons on why would user use IPSec instead of Secure Sockets Layer (SSL). (4 marks)

d) State **TWO (2)** protocols that employed in IPSec. (2 marks)

QUESTION 4

a) Describe any of **THREE (3)** web security vulnerabilities that you know. (6 marks)

b) Analyze one case of the following case, and answer the question.

The program require the serial number, however Trudy does not have the serial number. Trudy try to find the serial number illegally, by doing the activity by using IDA Assembly and Hex View tool as shown in Figure 1-4 accordingly. Briefly explain on each figure of Trudy's activities in searching the serial number. (8 marks)

```
.text:00401003                push    offset aEnterSerialNum ; "\nEnter Serial Number\n"
.text:00401008                call    sub_4010AF
.text:0040100D                lea     eax, [esp+10h+var_14]
.text:00401011                push    eax
.text:00401012                push    offset aS       ; "%s"
.text:00401017                call    sub_401098
.text:0040101C                push    8
.text:0040101E                lea     ecx, [esp+24h+var_14]
.text:00401022                push    offset aS123n456 ; "S123n456"
.text:00401027                push    ecx
.text:00401028                call    sub_401060
.text:0040102D                add     esp, 10h
.text:00401030                test    eax, eax
.text:00401032                jz      short loc_401045
.text:00401034                push    offset aErrorIncorrect ; "Error! Incorrect serial number.\n"
.text:00401039                call    sub_4010AF
```

Figure 1: Analysis of Attack by IDA Assembly

```
.text:00401003  04 50 68 84 80 40 00 E8-7C 00 00 00 6A 08 8D 4C
.text:00401013  24 10 68 78 80 40 00 51-E8 33 00 00 00 83 C4 18
.text:00401030  85 C0 74 11 68 4C 80 40-00 E8 71 00 00 00 83 C4
.text:00401040  04 83 C4 14 C3 68 30 80-40 00 E8 60 00 00 00 00
```

Figure 2: Analysis of Attack by Hex View

```
.text:00401003                push    offset aEnterSerialNum ; "\nEnter Serial Number\n"
.text:00401008                call    sub_4010AF
.text:0040100D                lea     eax, [esp+10h+var_14]
.text:00401011                push    eax
.text:00401012                push    offset aS       ; "%s"
.text:00401017                call    sub_401098
.text:0040101C                push    8
.text:0040101E                lea     ecx, [esp+24h+var_14]
.text:00401022                push    offset aS123n456 ; "S123n456"
.text:00401027                push    ecx
.text:00401028                call    sub_401060
.text:0040102D                add     esp, 10h
.text:00401030                test    eax, eax
.text:00401032                jz      short loc_401045
.text:00401034                push    offset aErrorIncorrect ; "Error! Incorrect serial number.\n"
.text:00401039                call    sub_4010AF
```

Figure 3: Analysis of Attack by IDA Assembly

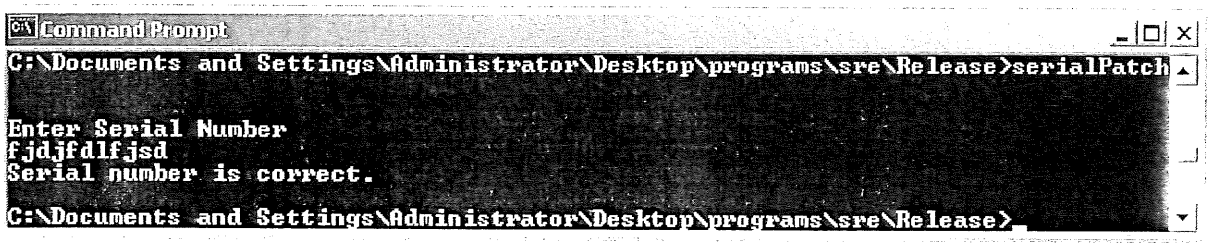

Figure 4: Serial Number is Obtained

a) The symbol in Figure 5 indicates a system being used or provided. It can be seen at certain places. Based on the figure, answer all questions below.

i) What does the symbol represents? Identify **TWO (2)** components of Figure 5. (3 marks)

Figure 5: Network Medium

ii) Describe **TWO (2)** wireless LAN threats. (4 marks)

iii) Explain **TWO (2)** steps on how a Wi-Fi system can be set up in secure manner. (4 marks)

QUESTION 5

a) Calculate the key that will be used by Alice and Bob to communicate using the Diffie Helman technique. Values given are;

n=11, g=7, x=3, y=6 (4 marks)

b) Calculate the public key as the pair (n, e) and the private key as the pair (n, d) by using the RSA Asymmetric Key cryptography. Values given are:

p=7, q=5, e=11, d=11 (4 marks)

c) Encrypt the message 'How are you' into the ciphertext by using one Time-Pad *NCBTZQARX* (7 marks)

d) Generate the message 'go to town' to the cipher text by using the technique of Simple Columnar Transposition Technique. Use five column, and order of column for cipher text are 32154 (5 marks)

e) Use the answer of cipher text generated from question 6d) to be encrypt again by using Simple Columnar Transposition Technique with 2 Rounds. (5 marks)

----------**End of question**----------