NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF SOFTWARE ENGINEERING

QUALIFICATION: BACHELOR OF COMPUTER SCIENCE HONOURS (SOFTWARE DEVELOPMENT)	
QUALIFICATION CODE: 08BCHS	**LEVEL**: 8
COURSE: PROGRAMMING FOR SECURITY PERSONNEL	**COURSE CODE**: PRS821S
DATE: NOVEMBER 2024	**PAPER**: THEORY
DURATION: 2 HOURS	**MARKS**: 100

FIRST OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER	**DR AMBROSE AZETA**
MODERATOR:	**MR VUYOLWETHU MDUNYELWA**

INSTRUCTIONS
1. Answer ALL the questions. 2. Read all the questions carefully before answering. 3. Number the answers clearly.

THIS QUESTION PAPER CONSISTS OF 8 PAGES
(Including this front page)

SECTION A: TRUE OR FALSE

This section consist of 20 questions. Answer all the questions
Each correct answer is allocated 2 Marks
Write True or False for Questions 1 to 20.

1. Passive attacks and Active attacks are types of attacks. **[2 Marks]**
2. Malware stands for Multipurpose software. **[2 Marks]**
3. In order to ensure the security of the data/ information, we need to Decrypt the data. **[2 Marks]**
4. Hackers usually use the computer virus to send good will messages to users. **[2 Marks]**
5. To protect the computer system against the hacker and different kind of viruses, one must always keep firewall on in the computer system. **[2Marks]**
6. A software program or a hardware device that filters all data packets coming through the internet, a network, etc, is known as Cookies. **[2 Marks]**
7. Worm is considered as an unsolicited commercial email. **[2 Marks]**
8. One way to prevent password attack is use of surname as password. **[2 Marks]**
9. Ransomware is a type of malware that encrypts data to make it inaccessible to computer users. **[2 Marks]**
10. External attacks involve someone outside the organization carrying out an attack. **[2Mks]**
11. Denial of Service (DoS) and Distributed DoS are not the same. **[2 Marks]**
12. Passive attacks and Active attacks are types of attacks. **[2 Marks]**
13. Since cyber attackers are now using Artificial Intelligence (AI) tools to carryout attacks, it is essential for organisations to Upgrade their protection mechanism from conventional defense to AI-based defense mechanism. **[2 Marks]**
14. Additional functionalities to cater for the shortcomings of IPV4, includes, security, authentication and integrity. **[2 Marks]**
15. A malware analyst is a cyber security professional trained to study and analyze malicious software (malware) **[2 Marks]**
16. SQL injection is a technique used to exploit user data through web page input by injecting SQL commands as statements. **[2 Marks]**
17. Attachments should always be treated with caution, even if you know the sender **[2 Marks]**
18. Command injection is a database injection technique that exploits a security flaw. **[2Mks]**
19. The netid of the IP Address: 129.198.189.129 is 129.198.110.0 **[2 Marks]**
20. If a user continues to enter a wrong password in the Python code segment below, the print statement will print 5. **[2 Marks]**

```
attempts = 1
while attempts < 7:
  username = input('Enter your username: ')
  password = input('Enter your password: ')
  if username == 'admin' and password == 'admin123':
    print('You have successfully logged in.')
    break          else:
    print('Incorrect credentials. Check if you have Caps lock on and try again.')
    attempts += 1
    continue
```

SECTION B: NETWORK PACKETS

Explain each of the following *send* statement and the possible output, when is executed on Scapy environment.
For instance, the statement send(IP(dst='131.110.120.001')) creates a network packet with destination IP address 131.110.120.001. When executed on Scapy, the output will be:
Sent 1 packets

21. send(IP(ttl=64, src='108.199.4.123', dst = '108.109.120.088')/TCP (sport=125,dport=126)/"Welcome to Python Second Lecture", count=4) **[2 Marks]**
22. send(IP(dst='181.110.120.010'), return_packets=True) **[2 Marks]**
23. send(IP(src='118.199.4.113', dst='120.115.121.012')) **[2 Marks]**
24. send(IP(ttl=64, src='128.99.4.123', dst='135.110.120.130'), count=6) **[2 Marks]**
25. send(IP(ttl=64, src='180.99.4.123', dst='170.110.120.100')/TCP()/"My First Lecture") **[2 Marks]**
26. send(IP(ttl=64, src='128.99.4.123', dst='135.110.120.130')) **[2 Marks]**

SECTION C: CODE SNIPPET

This section consists of 3 questions. Answer **ALL** the questions
Each correct answer is allocated 8 Marks

Question One **[8 Marks]**

(A) The Python program below extracts the first 3 characters in an IPV4 IP Address and display them by appending the first octet to the previous. **(4 Marks)**

```
IP = ["198.454.234.023","177.232.187.001","298.367.823.201","323.419.312.222"]
#Extract the first 3 characters
networks=[]
for address in IP:
networks.append(address[0:3])
print(networks)
```

Sample output:
['198']
['198', '177']
['198', '177', '298']
['198', '177', '298', '323']

Modify the above program to extract the first 4 characters in IPV6 Address below:
8194:1753:8162:1004:0500:2220:17753:8162
6193.4444.1285.5731.2399.0200.1200.6525
7193.3232.1285.5731.7199.3330.4440.1225

and display them by appending the first octet to the previous.
Sample output:

['8194']
['8194', '6193']
['8194', '6193', '7193']

(B) Find the Class, netids and hostids for the following IP addresses: **(4 Marks)**
125. 190. 180. 128
210.110.127.160
191.125.115.090

Question Two **[8 Marks]**

(A) Write a Python program to input two items from the keyboard: IP Address and email. The program should:

- check if the IP Address entered is IPV4 or IPV6, if not either IPV4 or IPV6 then it should report invalid IP.
- Check if the email is valid emails or not. For instance, email with institutional/ organisation's name such as vaate@nust.na, houtw@unam.na, kjteve@ium.na, pchris@unisa.za are valid while public email such as qJohn@yahoo.com and bvpode@gmail.com are invalid. **(4 Marks)**

(B) Write a Python program to check if a number is a spy number or not using the for loop. For example, if the sum of digits equals the product of individual digits in a number, it is a spy. In this Python spy number example, we used a while loop to divide the number into digits and find the sum and the product of the digits. The if statement checks whether the sum equals product, if true, spy number. **(4 Marks)**

Sample output1:
Enter a number to check for spy number: 123
123 is a spy number

Sample output2:
Enter a number to check for spy number: 1124
1124 is a spy number

Sample output3:
Enter a number to check for spy number: 22
22 is a spy number

Sample output4:
Enter a number to check for spy number: 33
22 is a spy number

Sample output5:
Enter a number to check for spy number: 1441
1441 is Not a spy number

Question Three **[8 Marks]**

(A) Write a Python program segment to check network configuration **(2 Marks)**

(B) Modify the Python program below to fill the Columns Address-class and Department in BlueBookip.csv and print out the updated list of the Trusted dataset BlueBookip.csv **(6 Marks)**

```
#A Sample Python programme to Block and Delete Untrusted IP Addresses
import pandas as pd
data1 = pd.read_csv('Desktop/MACHINELEARNING/BlackBookip.csv')
data2 = pd.read_csv('Desktop/MACHINELEARNING/BlueBookip.csv')
action = int(input('Press 1 to Block, or 2 to Delete IP Address: '))
countbb=0
countdd=0
for x in data1.index:
    for y in data2.index:
        if data1.loc[x, 'IPAddresses'] == data2.loc[y, 'IPAddress']:
            if action == 1:
                data2.loc[y,'Status']='Block'
                bb=data2.loc[y, 'IPAddress']
                countbb=countbb+1
                print('#', countbb,'THIS UNTRUSTED IP WAS BLOCKED: ', bb)
            else:
                dd=data2.loc[y, 'IPAddress']
                data2.drop(y, inplace = True)
                countdd=countdd+1
                print( '#', countdd,'THIS UNTRUSTED IP WAS DELETED: ', dd)
            break
        else:
            continue
print ('NEW LIST OF IP ADDRESSES SHOWING PERMITTED AND BLOCKED:')
print(data2.to_string())
print()
print('TOTAL NUMBER OF BLOCKED IP ADDRESSES: ', countbb)
print('TOTAL NUMBER OF DELETED IP ADDRESSES: ', countdd)
```

The above Python program above uses two dataset: BlackBookip.csv and BlueBookip.csv. BlackBookip.csv contains list of Untrusted IP Addresses. BlueBookip.csv contains list of Trusted/Permitted IP Addresses used by organization. Organizations normally validates their IP database by removing any IP contained in BlackBookip.csv from their network IP Address database. The default Status of each IP Address in BlueBookip.csv is marked Permitted. -Each IP Address in BlackBookip.csv is checked against the IP Address in BlueBookip.csv. Any IP Address in BlackBookip.csv that exist in BlueBookip.csv is marked/changed to either Blocked or Permitted in BlueBookip.csv. -It is the security personnel's responsibility to periodically update the organization's IP database by running the above Python program. -The security personnel run the above Python program by selecting 1 for Blocked, or 2 for Permitted.

Sample Run1:

```
Press 1 to Block, or 2 to Delete IP Address: 1
# 1 THIS UNTRUSTED IP WAS BLOCKED: 58.147.128.0
# 2 THIS UNTRUSTED IP WAS BLOCKED: 199.5.192.0
--
```

NEW LIST OF IP ADDRESSES SHOWING PERMITTED AND BLOCKED:

SN	IPAddress	Total IPs	Assign Date	Owner	Status
1	58.147.128.0	8192	15/06/2005	Afghanistan	Blocked
2	199.5.192.0	4096	05/01/2011	Afghanistan	Blocked
3	150.55.192.0	4096	02/07/2007	Afghanistan	Permitted

Sample run2:

Press 1 to Block, or 2 to Delete IP Address: 1
1 THIS UNTRUSTED IP WAS BLOCKED: 58.147.128.0
2 THIS UNTRUSTED IP WAS BLOCKED: 199.5.192.0
--

NEW LIST OF IP ADDRESSES SHOWING PERMITTED, BLOCKED AND ADDRESS-CLASS:

SN	IPAddress	Total IPs	Assign Date	Owner	Status	Address-Class	Department
1	58.147.128.0	8192	15/06/2005	Afghanistan	Blocked	A	Software Eng
3	150.55.192.0	4096	02/07/2007	Afghanistan	Permitted	B	Computer Science

--

TOTAL NUMBER OF BLOCKED IP ADDRESSES: 23
TOTAL NUMBER OF DELETED IP ADDRESSES: 23
TOTAL NUMBER OF IP ADDRESS-CLASS A: 50
TOTAL NUMBER OF IP ADDRESS-CLASS B: 34

HOW TO CALCULATE ADDRESS-CLASS

First Octet	Address-Class	Department
1-126	A	Software Eng
128-191	B	Computer Science

SECTION D: CODES/THEORY

Answer **all** questions
Each correct answer is allocated 8 Marks

Question One **[8 Marks]**

(A) Explain the security risk with the codes below and rewrite the codes to avoid command injection attack. **(4 Marks)**

```
import os
Num1=input("Enter an integer Arithmetic Expression : ")
print ("Result =", eval(Num1))
```

(B) Modify the Python program segment below to avoid command injection. **(4 Marks)**

```
import os
Num1=input("Enter an integer Arithmetic Expression : ")
print ("Result =", eval(Num1))
```

Question Two **[8 Marks]**

(A) Write a Python program to accept username and password with 5 times maximum entering. if the user enters up to 5 maximum (unsuccessful) username and password, the Account will be locked, and the message below will be displayed on the screen: Account locked as a result of failed login. **(4 Marks)**

This is a case of an attacker trying to gain illegal access to a system by guessing login details-username and password. At each failed login, the incorrect username and password must be saved into a new csv or MS Excel or Text file named: *failed_logins*

The correct username is nuadm and password is nuadm@2
If the user enters the correct username and password, the system will log the user in and report: You have successfully logged in

The system must also update the file by entering the correct username encrypted with asterisks (*)

The content of the failed_logins.csv file should be:

SerialNumber	**UserName**	**Password**	**Status**
1	josephine	jose123	Fail
2	abcbank	abcbank	Fail
3	bank	bank123	Fail
4	cba	cba333	Fail
5	jacob	steven	Fail
6	*****	*******	Successful

(B) Assume the malware_dataset.csv below with 1000 records, write a Python program to determine if a file is a malware or not, depending on the following condition: **(4 Marks)**

If File Name contains letter m, then file is a malware.
If File Size is greater than 2000 bytes, then file is a malware.
If file Type is unknown, then file is malware
1 means file is a malware and 0 means file is not a malware.

SN	File Name	File Size (bytes)	File Type	Malware
1	file1.mxe	2048	unknown	1
2	file2.exe	90096	unknown	1
3	file3.mxe	8192	unknown	1
4	file4.exe	1024	exe	0
5	file5.exe	804	exe	0
---	---	---	---	---
1000	---	---	---	---

The Python codes must show the segment for Load, Split, Train, Test and Printing of the classifier to determine the accuracy.

Question Three **(8 Marks)**

(A) Discuss six differences between IPV4 and IPV6. **(4 Marks)**

(B) Write a Menu driven Python program to run the following MS Operating System (OS)/Windows commands by selecting a number 1, 2, 3, 4, 5, 6, 7, 8 or 9. You are to find/search the Internet for the right OS commands for each option. When option 9 is selected, the program should exit. If none of the options is selected the program should display 'Incorrect Choice', and go back to the menu. **(4 Marks)**

Press 1. To know the IP Address of a website: www.trinityuniversity.edu.ng
Press 2. To know the user that is login
Press 3. To know the version of the Operating System
Press 4. To know the running processes
Press 5. To display all open network connections and listening ports
Press 6. To display all users
Press 7. To check the password policy of the account
Press 8. To find out the wi-fi network you are connected to
Press 9. Exit

THE END