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 2025	**PAPER**: THEORY
DURATION: 2 HOURS	**MARKS**: 100

FIRST OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER	**PROF AMBROSE AZETA**
MODERATOR:	**DR OMOBAYO ESAN**

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, AND MULTIPLE-CHOICE QUESTIONS

This section consists of 20 questions. Answer all the questions
Each correct answer is allocated 2 Marks
Write True or False for Questions 1 to 10, or select a, b, c or d for Questions 11 to 20

1. Pharming is hacking approach where cyber-criminals design fake websites or pages for tricking or gaining additional traffic. **[2 Marks]**
2. The existence of weakness in a system or network is known as vulnerability **[2 Marks]**
3. Passive attacks and Active attacks are types of attacks. **[2 Marks]**
4. IT security in any firm or organization is maintained and handled by CEO of the organisation. **[2 Marks]**
5. In order to ensure the security of the data/ information, we need to decrypt the data. **[2 Mks]**
6. Hackers usually use the computer virus to send good will messages to users. **[2 Marks]**
7. To protect the computer system against the hacker and different kind of viruses, one must always keep firewall on in the computer system. **[2Marks]**
8. 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]**
9. Worm is considered as an unsolicited commercial email. **[2 Marks]**
10. One way to prevent password attack is use of surname as password. **[2 Marks]**
11. External attacks involve someone outside the ------- carrying out an attack on: **[2Marks]**
    a. Football field b. Organisation c. Stew d. Potatoes
12. Since cyber attackers are now using Artificial Intelligence (AI) tools to carry out attacks, it is essential for organisations to -------- their protection mechanism from conventional defense to AI-based defense mechanism: a. Destroy b. Sell c. Upgrade d. Remove **[2Marks]**
13. One way to prevent password attack is: **[2 Marks]**
    a. Single username login authentication b. Biometric authentication
    c. Use of surname as password d. Use of student number as password
14. Which of the following is considered as an unsolicited commercial email? **[2 Marks]**
    a. Virus b. QuickHeal c. Spam d. Worm
15. Which software is mainly used to help users identify viruses and avoid them? **[2 Marks]**
    a. Adware b. Malware c. Intrusion detection system d. Wormware
16. One of the following is not a function of Wireshark: **[2 Marks]**
    a. Used for network packet analyser b. Software tool to monitor network
    c. Capture and troubleshoot network traffic d. No real-time packet analyser
17. The solution to avoid security issues with command injection is to use ___within your codes:
    a. Flow control b. Validation c. Comments d. Documentation **[2 Marks]**
18. Ransomware attacks may be described as, **[2 Marks]**
    a. Attackers kidnaping people for money b. Attackers kidnaping data for money
    c. Attackers kidnaping animals for money d. Attackers kidnaping cell phones for money
19. One of the following is not a network attack **[2 Marks]**
    a. Network attacks are unauthorized actions on digital assets within an organizational network
    b. Perpetrators in network attacks tend to target network perimeters to gain access to internal systems
    c. Twitter and Thread owners cage fighting
    d. Violation of user privacy settings and compromise devices connected to the internet

20. One of the following best describe the function of the below python code snippet **[2 Marks]**
    a. The word Greetings is added to the content of all doc files in pack folder
    b. The word Greeting is added to the content of all txt files in pack folder
    c. The word Greetings is added to the content of all txt files in pack folder
    d. The word Greeting is added to the content of all doc files in pack folder

```
#sample python code snippet
import os
def AddToFileContent(directory):
        for root, dirs, files in os.walk(directory):
         for file in files:
          if file.endswith(".txt"): #Target text files for demonstration
          print('Program Execution - Completed!!')
          with open(os.path.join(root,file), 'a') as f:
                  f.write("Greetings")
                  print(' ')
                  print("Please check the txt files inside your pack folder!")
AddToFileContent( ("C:/Users/johanes/OneDrive - NUST/Desktop/pack")
```

SECTION B: 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 displays 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) Given the dataset below in **Table 1**: **(4 Marks)**

Table 1.

Email	IP-Address (in Decimal)	IP-Type	Valid Email
qJohn@yahoo.com	186.124. 149.154		
bvpode@gmail.com	8194:17753:8162:0000:0000:0000:17753:8162		
vaate@nust.na	198.139.180.149		
houtw@unam.na	169.189.131.226		
kjteve@ium.na	128.11.3.31		
pchris@unisa.za	8193.0000.1285.5731.99.0000.0000.6525		

Write Python code to do the following:

I. Create a dataset named: verifyIP.csv from **Table 1** to contain the above records.
II. Check each IPs in column IP-Address and report either IPV4 or IPV6 in column IP-Type
III. Search for valid emails and report it. 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: John@yahoo.com and bvpode@gmail.com are invalid.
IV. Fill the column for IP-Address in **Table 2**. It should either be in Binary if IPV4 or Hexadecimal if IPV6.
V. Update the verify.csv file to look like **Table 2** below:

Table 2.

Email	IP-Address (fill this column, IPV4 IPs should be in Binary, while IPV6 IPs should be in Hexadecimal)	IP-Type	Valid Email
qJohn@yahoo.com		IPV4	invalid
bvpode@gmail.com		IPV6	invalid
vaate@nust.na		IPV4	valid
houtw@unam.na		IPV4	valid
kjteve@ium.na		IPV4	valid
pchris@unisa.za		IPV6	valid

(B) Write a Python program that will take a password from the keyboard as input, containing a combination of alphanumeric characters along with special characters, and check whether the password is valid or not with the help of a few conditions. **(4 Marks)**

The primary conditions for password validation are as follows:

I. Minimum 8 characters
II. The alphabet must be between [a-z]
III. At least one alphabet should be of Upper Case [A-Z]
IV. At least 1 number or digit between [0-9]
V. At least 1 special character from: [_ or @ or $]

Sample output1	**Sample output2**	**Sample output3**
Input : R@m@_f0rtu9e$	Input : Rama_fortune$	Input : Rama#fortu9e
Output : Valid Password	Output : Invalid Password	Output : Invalid Password
	Explanation: Number is missing	Explanation: Must consist from: _ or @ or $

Question Three **[8 Marks]**

(A) Briefly explain your understanding of Programming for Security Personnel (use max of 5 lines)**(4Mks)**

(B) Modify the Python program below to fill the Columns Address-class and Department **BlueBookip.csv** and print out the updated list of the Trusted dataset BlueBookip.csv **(4 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 organizations. Organizations normally validate 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	Dept
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 Sc

```
--

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 C: NETWORK PACKETS

Answer **All** questions

Total marks allocated to this session is 12

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

B1. send(IP(ttl=64, src='128.99.4.123', dst='135.110.120.130')) **[2 Marks]**

B2. send(IP(dst='181.110.120.010'), return_packets=True) **[2 Marks]**

B3. send(IP(src='118.199.4.113', dst='120.115.121.012')) **[2 Marks]**

B4. send(IP(ttl=64, src='128.99.4.123', dst='135.110.120.130'), count=6) **[2 Marks]**

B5. send(IP(ttl=64, src='180.99.4.123', dst='170.110.120.100')/TCP()/"My First Lecture") **[2Mks]**

B6. 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]**

SECTION D: CODES/THEORY

Answer **all** questions

Each correct answer is allocated 8 Marks

Question One **[8 Marks]**

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

(B) As a demonstration of cyber security defence and warning, write a Python program that will ask a user if you want to run the exe file named: HBD-GIFT.exe that is inside a folder PROJECT on the Desktop of your computer.
If you say N, the program will terminate with a message **'Good bye, it is better to play safe'** and nothing will happen. But If you say Y the program will display
'Runing of the Executable file HBD-GIFT.exe is ongoing..'
'Please note that your computer may be effected with Trojan horse'
'Please wait for 15 seconds and go check your computer files in the PROJECT folder!' **(4 Marks)**

Question Two **[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 Three **[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 cuss and password is cuss@5
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 20 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 1500 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
---	---	---	---	---
20	---	---	---	---

The Python codes must show the segment for Load, Split, Train, Test and Print on screen to determine the accuracy.

THE END