



12 Pages

1. Please give the information requested in the boxes below.
2. Enter your name in the space provided to the right, fold over and seal down (using the label provided) to hide your name.
3. The answers must be legibly written. The Examiners can either ignore illegible script or have it typed and the expense of typing charged to the candidate.
4. Write your answers in ink.
5. Begin each answer on a fresh page. Do all rough work in the answer book and cross it through.
6. No part of this book is to be torn out; it must be handed in complete.
7. If more books than one are used, fasten them together using the tags available from the invigilator(s).
8. **Every book must be handed in. In no circumstances may answer books, used or unused, be taken out of the examination venue.**

1	Student Number	2232921
2	Title of Examination Paper	NETWORK AND CYBERSECURITY ESSENTIALS
3	Module Code	ACCA4024
4	Date and Time of Examination	10:00 22/11/2023
5	Examination Venue	LR6
6	Seat Number	N/A
7	Number of Answer Books handed in	1

[illegible]

(Gweler yr ochr arall am y fersiwn Cymraeg)



Prifysgol Cymru
University of Wales
Y Drindod Dewi Sant
Trinity Saint David

Llyfr Atebion Arholiadau

12 Tudalen

Cyfarwyddiadau i Ymgeiswyr

1. Rhwch yr holl wybodaeth y gofynnir amdani yn y blychau isod.
2. Rhwch eich enw yn y lle a ddarparwyd ar y dde, plygwch et a'i sellio i lawr (gan ddefnyddio'r label a ddarparwyd) i guddio'ch enw.

1. Rhaid i'r atebion fod mewn llawysgriflen ddarlennadwy. Gall yr Arholwyr naill ai anwybyddu sgript annarllennadwy, neu drefnu iddi gael ei theipio a chael yr ymgeisydd i dalu.
2. Ysgrifennwch eich atebion mewn inc.
3. Dechreuwch bob ateb ar dudalen newydd. Gwnewch unrhyw fras nodiadau yn y llyfr atebion a thynnu llinell drwyddynt.
4. Ni ddylid rhwgo unrhyw ran o'r llyfr. hwn; rhaid ei gyflwyno yn gyfan.
5. Os defnyddir mwy nag un llyfr, rhwymwch hwy gyda'i gilydd gan ddefnyddio'r tagiau sydd ar gael oddi wrth y gwyllwyr/gwyliwyr.
6. Rhaid dychwelyd pob llyfr. Ni chaniateir mynd â llyfrau atebion, wedi eu defnyddio neu heb eu defnyddio, allan o'r lleoliad arholi o dan unrhyw amgylchriadau.

(See the other side for English version)

1	Rhif Myfyriwr	
2	Taith y Papur Arholiad	
3	Cod y Modwl	
4	Dyddiad ac Amser yr Archoliad	
5	Lleoliad yr Arholiad	
6	Rhif Sedd	
7	Nifer y Llyfrau Atebion a gyflwynwyd	

[illegible]

Lenwch, plygwh a seliwh
(gweier nodyn 2 isod)

CYFENN:

ENW(AU) CYNTAF:

Q1

B

✓

Q2

A

✓

Q3

D

✗

Q4

B

✓

Q5

A

✓

Q6

D

✓

Q7

B

✓

Q8

C

✓

Q9

A

✗

Q10

D

✗

Q11

D

✗

Q12

B

✓

Q13

D

✓

Q14

A

✓

Q15

B

✓

Q16

B

✓

Q17 B ✓

Q18 B ✓

Q19 A ✓

Q20 B ✓

Q21 B ✓

Q22 A ✓

Q23 D ✓

Q24 A ✗

Q25 B ✓

Q26 B ✗

Q27 D ✓

Q28 B ✓

Q29 C ✓

Q30 D ✗

Q31 A ✓

Q32 C ✓

Q33 A ✗

Q34 D ✓

Q35 A ✗

Q36 B ✓

Q37 A ✗

Q38 A ✗

Q39 A ✓

Q40 B ✓

30

Q41 route information from source to destination

Q42 OSI MODEL 3 LAYER of network OSI refer to (operating system interconnection). is responsible to facilitate communication data transmission between different network. its primary work is to manage the data packet route to intended destination.

DATA PACKET ROUTE:- it analyse the route, select more efficient one and send to data packet in based of factors.

LOGICAL ADDRESS:- uniquely identifying the device on network on the system

PHYSICAL LAYER:- physical layer of the network

Describe mechanically, electrically, functions. to maintain the procedure, activate, de-activate.

of network data transmission.

Data link:- Use to describe network exchange.

BUT fibre optic and coaxial both use for transmission media. they're different in construction and function also.

fibre optic has higher data transmission rate. it works in long distance and immunity to interference

compared to coaxial it has slower data transmission speed and doesn't work fast in long distance. Susceptibility to interference.

Phishing:- Hacker use tricky techniques to reveal information to victim such as bank card details, passwords. they show legitimate entities. it done through email, fake web pages, text messages

Denial of service (DoS):- result of this attack victims data disrupt by hacker.

MALWARE:- Ransomware, virus, trojan horse, Adware, spyware

These all are harmful, and damage the software

computer system or unauthorise access.

ADware: irritate staff while work in computer

SPYware: - hack data widely and give third party for various reason.

Q5

use encryption WPA3

use Password strong implementation.

VPN's extra layer of network