



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

Examination Answer Books

12 Pages

Instructions to Candidates

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	PI47607
2	Title of Examination Paper	Advanced Cybersecurity
3	Module Code	ACCA6000
4	Date and Time of Examination	16/5/2018 9am - 11am
5	Examination Venue	Townhill Gym
6	Seat Number	G008
7	Number of Answer Books handed in	1

List the numbers of the questions you have attempted	Office Use
1	10
2	15
3	16
Total	41

(Gweler yr ochr arall am y fersiwn Cymraeg)

Complete, fold and seal
(see note 2 below)

SURNAME: Phillips

FORENAME(S): Tordani

- ① a) i) A virus is created by a malicious attacker with the intent to corrupt a targeted system or network. These viruses can be transferred to a system in a number of ways, such as opening e-mail links from unknown senders, directly connecting infected devices such as DVDs, CDs and USBs, and ~~and~~ downloading applications from third party sites.

Once a system is infected, the virus can compromise the confidentiality, integrity and availability of data and resources. Viruses typically try to hide their presence within a system, e.g. as within another program or image.

- ii) Devices can show certain characteristics which can indicate the presence of viruses. These include slowing of a device or system, typically as viruses prevent certain actions or consume memory / network bandwidth. Data being transmitted to an unknown destination can hint to viruses capturing data to send to the attacker. The addition of programs or software from unauthorised sources, such as certain websites or CDs, could potentially hint to the presence of malicious software.

- iii) Countermeasures can be taken to prevent viruses from infecting computer systems. Installation of Anti-virus, such as McAfee and Norton, can prevent viruses from downloading or they can be used to find viruses already present. Anti-malware software, such as Malwarebytes, can also be used in a similar manner.

Routine ~~network~~ scans, such as port, network and vulnerability scans should be done to look for any weak point which can be exploited. Port scans searching for certain traffic ~~or used~~ ~~ports~~ such as ICMPs. Solarwinds is an example of port scan software. Network scans ~~can~~ are used to map the network and look at traffic traversing it. ~~Examples~~ Examples of software used is NMap, which can be used to map the network and look for TCP, UDP, etc. traffic. Vulnerability scans look for active, passive and network ~~vulnerabilities~~ vulnerabilities and an example of software is Nessus.

Not downloading links from unknown e-mails or untrusted sites can prevent viruses from downloading to a Computer system.

Locking and ~~also~~ deactivating unused ports will prevent unauthorised devices from connecting to the network.

Scan all CDs, DVDs, USBs, etc. with anti-virus software to ensure they are safe to open.



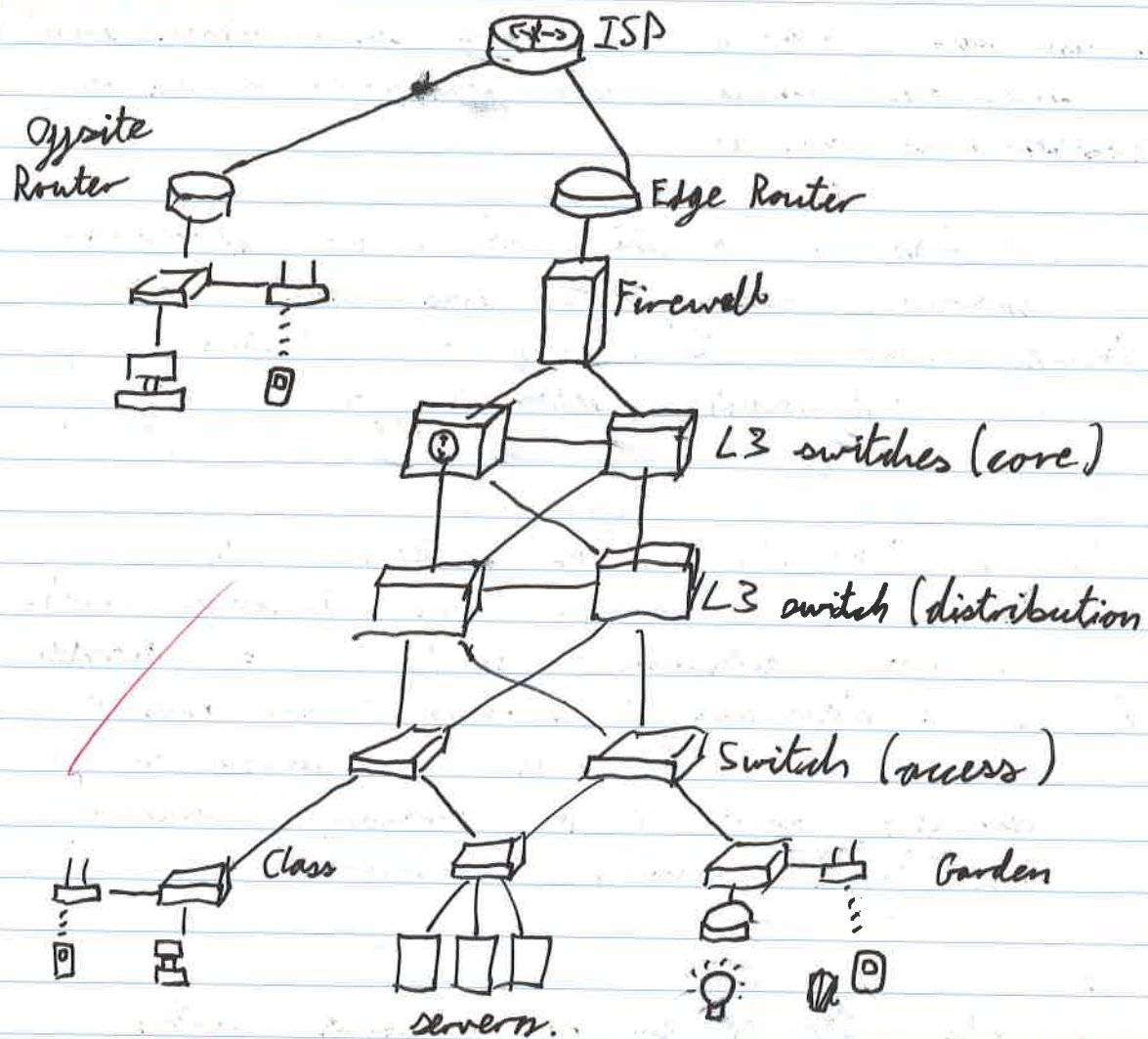
Ensure all software, such as the operating system(OS) and anti-viruses, are up to date, as older OS ~~are~~ are not supported and can have extra vulnerabilities while older virus scans may be inadequate at detecting newer viruses.

6

Passwords and encryption can be used to secure systems and data from theft or unauthorised personnel.

10

② a)



IOT is the a network of smart devices, equiped with sensors, actuators and an internet connection to communicate. As these devices are connected to the internet, they are vulnerable to attacks. These include man-in-the-middle and flooding. To secure these devices, such a motion sensors to control lighting etc., encryption methods should be utilised to ensure data confidentiality. This prevents unauthorised parties from accessing network data from these devices.



All unused ports should be shutdown and all devices should use passwords and ~~enable~~ encryption.

Firewalls should be installed near network edge which connects to the ~~internet~~ internet. This is to monitor traffic entering and leaving the network for malicious software.

BYOD policies must be enforced to determine what is and is not acceptable to do, to download on to, etc. ~~these~~ with these devices. Anti-virus software must be used to prevent malicious ~~software~~ software and viruses from affecting BYOD and all network devices.

~~Web~~ Servers are vulnerable to a number of attacks and must be protected with encryption and anti-virus.

Remote connections can be established with tunnels or remote access, such as SSH. SSH ~~encrypts~~ encrypts the connection for added security. Proper privileges must be set up to determine who can access network resources.

Cloud systems must take steps to ensure data confidentiality, ~~not~~ integrity and availability, such as encryption ~~and~~ and backup data. Redundancy in network design can also improve performance.

③ a) Symmetric encryption is where ^{all} ~~both~~ devices ~~with~~ communicating must have the same encryption key. This form of encryption is between 80 and 256 bits. Data is encrypted in either block or stream method. Block ~~sends~~ encrypts segments and sends those out while stream sends the data as a constant stream.

Examples of this encryption method are DES, 3DES and AES. DES is an older method used before a company can upgrade to AES. It encrypts the data a single time before transmitting. 3DES is the same as DES, however, the encryption method is performed 3 times. AES is an advanced version that ~~also~~ encrypts multiple times.

Asymmetric encryption is where the encryption key is different from the decryption key. This improves security ~~as~~ since if an attacker gains the encryption key, they cannot decrypt it. This method of encryption encrypts between 516 and 4096 bits.

Examples of Asymmetric encryptions are Diffie-Hellman (DH) and RSA.

- b) There are multiple ways of attempting code breaking and cryptography attacks. These include an attacker feeding his own information into an encryption key to determine and analyse the outcome, known as own key attack.

An ~~other~~ attacker can physically persuade someone via torture or coercion, known as a Rubber hose method.

An attacker can use partially decrypted information as a base to discover the decryption key.

Brute force method involves trying multiple key to identify the correct method, however, this method is slow and unreliable.

Offline methods involve trying to decrypt data before it leaves the network while online method involves capturing streamed or sent information.

Older methods of code breaking involved looking for pattern in the text to reconstruct the information.

Partial Key attacks are where the attacker has part of the decryption key which can be used to decrypt the rest.