



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) + **sign** 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.**

SURNAME: cut forth

FORENAME(S): Laurance

1	Student Number	P146632
2	Title of Examination Paper	Advanced Cybersecurity
3	Module Code	ACCA6000
4	Date and Time of Examination	16/5/18
5	Examination Venue	Gym
6	Seat Number	Gold
7	Number of Answer Books handed in	1

[illegible]

(Gweler yr ochr arall am y fersiwn Cymraeg)

 28%

Q1

ai) ~~Detection~~, during a network scan, the virus is detected and ~~quarantined~~ when this happens
 Detection, analysis, Quarantine, Analysis, Storage/Removal
 Storage/Removal

ii) There are many indicators that could suggest a virus has affected a PC :-

Slow/no start up, probably the biggest indicator something is wrong is when the ~~PC~~ ^{PC} is slow or does not load the operating system

missing/not working Applications, this can indicate multiple problems such as a virus, if so the virus has corrupted or Deleted the data

• incorrect Browser Homepage, this is most commonly caused by malware being installed as cookies from a users web browser. When opening the browser it will take the user to a third party site

• Network activity; abnormal traffic coming from the device such as Broad cast ping to discover other network devices

• Email spam, viruses can infect multiple devices by sending Group Emails to every user on a network, the Emails have copies of the virus that install themselves when the email is opened

Q 1

iii

To prevent virus infections on a computer system there are some ^{simple} steps that can be taken

Firewall usage:

• up to date system, many viruses target specific versions of a software, because of an exploit found in them. once this exploit is discovered the manufacturer will create a patch to secure it. by updating the software the user is limiting the number of potential threats.

• Email Security, viruses are able to be stored in Emails. because of this simple procedures need to be taken to protect the users device:

- Scanning Emails before opening
- Not using links found in the email
- Don't open Emails from unknown sources e.g. Spam

• Download Security: ~~don't~~ viruses can be hidden in the data of a download. to protect a pc:-

- Don't use torrent sites e.g. line.wire
- Many of the Downloads are just viruses
- Don't use unsecured web sites
- Scan the Download before opening it

Scheduled system scans, There is no real way to protect a pc ~~100%~~ from malware. Such as viruses. So one of the best ways to secure the device is to ensure it will be infected. So to ensure it's safe it is advised that the user set up a full system scan to run automatically. This will help secure the device by ensuring the detection and removal of any virus.

7



Q2

IOT and smart city security issues

As the New University of Wales Trinity Saint David (UWTSD), Network will incorporate Internet of Things Technology. it is important to know what sort of threats there are:

Threats

~~Malware, for example viruses, in a IOT~~

In a IOT environment many users with different devices will connect to the UWTSD Network. Some of these devices will be infected. Some of the users will have ill intent, but there are too many threats to list, but here is some of them.

- Malware: This can be spread by infected devices connecting to the network. Malware ranges from simple viruses to ~~malware~~ Trojans and key loggers.

- Out of date Software/Hardware, this that enables attackers to use known attack vectors that newer models don't have.

- Hacking: as this is a ~~IoT~~ network Hackers will use man in the middle attacks to gain access to the network, gaining access through the use of a 3rd party device like an unsecured USB phone.

- Rogue access points, used to gather network data by relaying traffic through themselves, this is done to steal users data and monitor a network.

malicious and being damage, people are a group of crackers capable of great and terrible things. Some users on the network will attempt to disrupt it to achieve a goal such as protesting X causes by defacing the university's website or damaging property such as the wireless access points. people will also damage property by accident such as tripping over or dropping a device.

Next page

22

* Theft of Data and Hardware, every thing can be stolen from the personal data of a university network user to a light server

* unauthorised access, could say unsecured devices and unsecured networks, allows too much access to a user such as giving a student admin rights

All of the mentioned threats and more, will affect the university's IOT Network. So how to protect a network is important and is the most relevant information to the university :-

- Staff and Student Training, provide training on how to keep a user's Device Secure
- Physical Security to protect Hardware and record any damages
- checking the configuration of the server to make sure the correct permissions are applied.
- Network scans, to check the university's devices for vulnerabilities
- keeping any devices up to date, both software and hardware. This limits the amount of threats that can be used
- firewalls and Anti-virus software, the use of tools such as 360 Security (Anti-virus), will help protect a network from malware

14



Q3

i

Symmetric encryption, other well known as private key encryption is the method of encrypting data to be transported to another device (such as Email).

This method is used when a reply is needed from the recipient is required.

SSL

ii Asymmetric, slower, does not require replies

Has two types of encryption

Block encryption, packets are encrypted in blocks.
 Each block has to reach destination before decryption can begin.

Stream encryption - each bit is encrypted as it is sent out