



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.**

Complete, fold and seal
(see note 2 below)

SURNAME:

Griffins

FORENAME(S):

Dale Scott

1	Student Number	P146062
2	Title of Examination Paper	Advanced cybersecurity
3	Module Code	ACC A6000
4	Date and Time of Examination	16/05/2019 09:00
5	Examination Venue	Gym
6	Seat Number	6003
7	Number of Answer Books handed in	1

List the numbers of the questions you have attempted	Office Use
1	14
2	20
3	15
Total	49

(Gweler yr ochr arall am y fersiwn Cymraeg)

65%

plain text upper,

1Ai A virus is a piece of code that is written to slow down, monitor or create a backdoor into a device. The stages of a virus life are

- ① Creation - The virus is created
- ② Spread - the virus is spread over the internet
- ③ Infection - the virus infects a device when opened.
- ④ Propagation - The virus spreads around the network to infect more devices.
- ⑤ Execute - the virus is opened and the code is run on the system.
- ⑥ Propagation - The virus spreads around the network to infect more devices
- 6 - Reporting - the virus could log information to be sent back to the creator.

1Aii If a virus has infected a device within the network or multiple devices the first thing that would inform a network administrator is an anti-virus, this should detect and remove the virus automatically. However, if the virus got passed the anti-virus then the infected device will receive performance issues. These issues will be a reduction in speed, A network monitoring tool like SolarWinds should detect this. Another thing that may notify of a virus is the network/device behavior that will be seen in a management toolset.

1Aiii A virus can sometimes be avoided by user training and the correct policies & configurations being implemented. The countermeasures that can be implemented are discussed on the next page.

- Fire-wall / - Can be used to block certain unwanted traffic from within the network.
- ACL / - ACL is like a firewall it is a sequential list of permit or deny statements & can block certain traffic.
- Anti-Virus / - An anti-virus can be used to scan web pages & block malicious websites & files.
- Updates / - Ensuring a device is fully up to date will help prevent viruses from accessing the device.
- Email Scanning / - Ensuring all email attachments are scanned before opening.
- Training / - Training staff to know the vulnerabilities and have a basic knowledge of network security is another method.
- Permissions / - Stopping people who don't need access to downloading files is another method, this can be achieved by granting correct permissions.
- Applications / - Only download applications from trusted stores or websites.
- Monitoring tools / - Monitoring tools like Solarwinds can be used so they can detect suspicious activity & alert the administrator.

2A1 Future trends in cybersecurity will include current threats that will be discussed below. It will also include more sophisticated attacks. IoT devices are also a major security weakness within networks.

- Brute force attacks - password cracking
- Dictionary attacks - password cracking
- Network scanning attacks - Exploiting vulnerabilities
- Man-in-the-middle attacks - modifying transaction
- Man-in-the-browser attacks - like man in the middle but harder to detect.



Dedicated Denial of Service - A service is overwhelmed with requests, so more i/o devices are launched more servers are created.

- Keyloggers - log information & send back to attacker
- Ransomware - A major threat that is likely to happen again, when data is encrypted and a ransom is demanded.

The attacks that are listed are likely to be the future attacks for the next 1-2 years by. That time more sophisticated attacks will be released. Quantum Computers are likely to bring password cracking up to a major threat when they are made widely available.

Cloud-based Service security issues

- o weak authentication & accounting.
- o ~~lack~~ weak data encryption
- o unsecure access
- o Risk of data loss
- o lack of proper data management
- o no control of data on cloud

Internet of Things & Smart City security issues

- o lack of authentication & accounting
- o lack of encryption
- o privacy issues
- o Devices launched into market without security being considered.
- o Risk of losing control of devices ~~system~~ to hackers.
- o Can be exploited to become part of botnets for DDoS attacks.
- o unable to install security to protect devices.
- o Risk of insecure data transmission
- o possible data loss

Web Markup language (HTML5 vulnerability) and database application system security.

- o lack of authentication & accounting
- o lack of encryption
- o improper management
- o improper data handling
- o Data loss.

How will these affect the network?

Future trends in cyber security will affect the network by more vulnerabilities being added when adding in IoT Devices. Additionally Byod will increase this by adding possibly unsecured devices into the network.

Cloud based services security issues will affect the network as IoT devices can be ~~man~~ managed via cloud services. Also there may be cloud services used within the network this will greatly increase the risk. Remote access will also increase the risk of this data being accessed on insecure systems.

Internet of things and smart city security issues will affect the network as there is ~~for~~ IoT devices. These are used to monitor classrooms, carpets, lighting, smart garden. This will monitor and add more devices as they are required creating a bigger security issue.

Web Markup language and database application system security issues will affect the network as internet access is used for the network. Remote access is also using internet access. Database within the network will also create the issue.

Q3A Symmetric encryption algorithm uses a pre-shared key. The same key is used to encrypt the data & decrypt the data. Symmetric encryption uses block ciphers, this splits the data into blocks of 64 or 128 bits to be sent. This encryption method is commonly used for Virtual Private Networks between routers. Examples used up to 256 bit encryption. ↑

- o DES
- o 3DES
- o AES

10

Asymmetric encryption algorithm uses a private & public key. The private key is normally used to encrypt the data. The public key is when used to decrypt the data. Sometimes it can be the opposite way around. This encryption type uses both block & stream ciphers. This encryption algorithm uses up to 4096 bit encryption and can be all the way up to 15424 bit against quantum computers. This is used for Virtual Private Networks & mainly HTTPS.

Examples

- o RSA
- o Elliptic Curve
- o DH.

3b. Some cryptography attacks include plain text cipher attack, encrypted cipher attack, plain text attack. Cryptographers are employed to break encryption ciphers. They are usually very good at maths. Code breaking techniques include brute force attacks, Dictionary attacks, rainbow crans and password guessing attacks. Password cracking can be used for code breaking to gain access to the network.

5

15