CSC3064 Case Study Assessment

About This Assessment

You recently started a new job as a network security specialist at an IT consultancy firm.

A small company called CatGPT has hired your firm to provide a review of their IT infrastructure. Several different experts at your firm have been tasked with investigating different aspects of the company's IT systems.

Based on some background information provided by the company, you have been allocated responsibility for providing an analysis of security issues related to DNS and discussing how different options could be applied for the company.

You are required to submit a video presentation of up to 8 minutes that concisely presents your analysis and recommendations.

You are required to submit a single mp4 video file via the Canvas Assignments page.

This assessment is worth 60% of the available module marks.

The submission deadline is 16:00 on 31st March.

If you have a question about the assessment, email kieran.mclaughlin@qub.ac.uk
(Please use email rather than Teams)

1. Background Information

CatGPT is a small company that has 10 employees. They recently received significant investment to expand their business. They expect to grow rapidly during the next year to over 40 employees, so they are considering how to grow and improve their IT network, including paying closer attention to cyber security issues. Consequently, the management team has asked your consultancy firm to report on certain aspects of their IT network.

The company serves 100s of customers, who subscribe to the company's CatGPT phone app. The app records the sounds made by people's pet cats, communicates these sounds to a server at the company's premises, which translates the sounds into text in English so people can understand what their cat is saying.

You have been given the following information related to the company network and IT systems:

- The company is based at a single site with office space for staff. The office space contains several PCs and various other hosts, including a code repository server, a media database server, and a GPU server for training AI language models (the models that translate cat noises into text in English).
- The company is provided with two static IPv4 public IP addresses (165.120.2.5 and 165.120.2.6) by its business broadband provider.
- A FortiGate 60B device is used to support network connectivity between the company and the internet, via the ISP. The device is configured to support private IP addressing, as well as a DMZ. It is configured in "NAT mode", as described in Fortinet's documentation for the device.
- For internal networking, a TP-Link TL-SG1016PE switch is used to support a single LAN. Hosts across the LAN share the 192.168.1.0/24 address range. Internet access is provided to the LAN via the NAT functionality of the FortiGate 60B, which uses one of the static public IP addresses provided by the ISP (165.120.2.5).
- The FortiGate 60B provides a DHCP service for the network.
- The FortiGate 60B is configured to obtain a DNS server address automatically from the ISP.
- All hosts in the LAN are connected via physical ethernet cables to the switch.
- The DMZ is home to a second GPU server, which runs inferencing services using trained AI models that can process incoming audio data and return text transcriptions to customer apps. The DMZ allows access from the internal LAN, as well as connections from customer apps to the GPU server via the second static IP address (165.120.2.6).

Note:
The red text above was updated on 13th March to correct a typo.
The IP address 165.120.2.5 was corrected to 165.120.2.6

2. Required Tasks

Overview

The CatGPT company wants to better understand the different options that exist for providing DNS services across the company network. They are aware that different ways of supporting DNS lookups are possible and want to know more about the practicalities of implementing commonly viable arrangements, especially any security implications for different approaches.

To help you start, some arrangements to provide DNS are listed below, which you should consider:

- A self-hosted DNS server, DNS provided by the company's ISP, use of a public DNS server (free or paid) such as Google DNS, Cloudflare DNS, etc.
- Different protocols can be used for communicating DNS requests, including traditional DNS, DNS over TLS, DNS over HTTPS, etc.
- Include any other arrangements you consider to be valid for a small-medium sized company.

You must produce a video report that addresses the two tasks described below.

Task 1: Discuss and compare how different DNS arrangements can be applied to the network

- Using Fig. 1 (Page 4) as a starting point, you should create a set of network diagrams to show how different DNS services and protocol combinations could be deployed for the company.
- For each possible approach, use a relevant network diagram to discuss a detailed step-by-step "walkthrough" where you describe the packet request/response exchanges involved when a host in the company network makes a DNS request.
- You only need to discuss packet exchanges that involve the company network.
- Be sure to discuss technical details such as IP addresses, port numbers and any other pertinent network-related details.
- Many approaches may be possible, leading to several walkthroughs. In each case you do not need to repeat very similar steps already covered by a previous walkthrough.

Task 2: Analyse and compare the security implications of using different DNS arrangements

1. For each approach that you identified in Task 1, clearly describe any firewall policies that should be applied by the Fortinet 60B.
2. For each approach that you identified in Task 1, identify any risks you perceive regarding compromise of the C-I-A principles.
3. The company is aware that some malware has been known to use DNS communications as part of C&C communications. For each approach that you identified in Task 1, explain whether there are any implications (pros and cons) for prevention or detection of such DNS-based C&C communications.
4. Finally, weighing the security implications of the options available, what approach would you recommend the company implements for DNS? Clearly justify your decision. (For marking, the justification is more significant that reaching a "correct" answer).

In Task 2, for subtasks 1, 2 and 3 you should consider how to organise your answers in a consistent and time-efficient format for presentation, for example by using a similarly structured table in each case.

A simplified representation of the company's network configuration is provided below for initial guidance. You should add further complexity and depth of information to create your own diagrams to present the walkthroughs required in Task 1 (see Page 3).

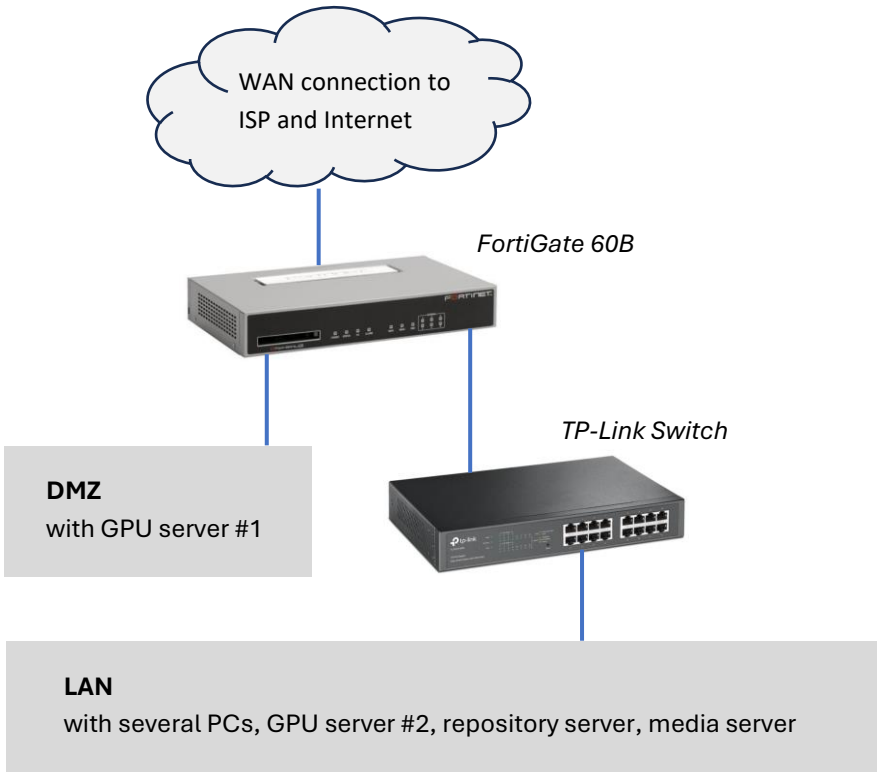

Figure 1: Simple representation of CatGPT's network configuration

3. Guidance About the Video

- Your video is expected to be around **6-8 minutes** long, but not longer than 8 minutes.
- Videos that are over-length will **not be marked beyond the 8 minutes point**.
- You are recommended to use up to 4 minutes to address Task 1, and 4 minutes for Task 2 (using 1 minute for each of the four subtasks in Task 2).
- You are expected to deliver a presentation using PowerPoint (or equivalent software) to address the two tasks.

References

References are generally not required. If you use external material to learn about a topic, this does require specific referencing. The content of your report should be able to stand on its own.

Video Capture

You may use whatever video and audio capture tools you feel work best for you, but you must ensure the audio is clear and that any text is clearly visible.

In the past, students have used OBS, PowerPoint (which can capture very good quality videos with audio), or even a call to yourself using Teams (the quality is not quite as reliable as other options).

Save your video as an **mp4** file, naming it using the name format ***surname_studentnumber.mp4***

Do and Don't

- Do independent research into the issues introduced in the *Background Information* and *Required Tasks* sections.
- Do look for information or techniques that you think other students may overlook.
- Do provide technical depth about specific details in your answers.
- Where applicable, do justify why you have come to a certain conclusion or why you are making a specific recommendation.
- Don't provide generic analysis. Do ensure you discuss the network of *this* company based on the information at hand.
    - Generic discussion can be provided by chatbot, so you need to go beyond this and provide meaningful insights related to the technical details of the case study.

4. Assessment Criteria

100 marks are available in total, divided as follows:

- 40 marks for Task 1
- 40 marks for Task 2
- 20 marks for the quality of how you organise and deliver your presentation.

Your work will be assessed according to the indicative criteria provided as guidance below, and in accordance with the QUB Undergraduate Conceptual Equivalents Scale:
https://www.qub.ac.uk/directorates/media/Media,837251,smxx.pdf

	80-100%	**70-79%**	**60-69%**	**50-59%**	**40-49%**	**0-39%**
Task 1 **[40% weighting]**	Exemplary depth of insight across a comprehensive range of approaches. Rigorous detail and insight provided in walkthroughs. Network diagrams are uniquely informative and used highly effectively.	Excellent insight across a comprehensive range of approaches. Rigorous detail and insight provided in walkthroughs. Network diagrams are highly informative and used very effectively.	Very good analysis across a broad range of approaches. Very good level of detail and insight provided in walkthroughs. Network diagrams are informative and used effectively.	Good analysis across a reasonable range of approaches. Good level of detail and insight provided in walkthroughs. Network diagrams are informative and generally used effectively. Any misunderstandings are minor.	Evidence of understanding across a reasonable range of approaches. Level of detail and insight provided in walkthroughs is acceptable but may be limited in scope. Network diagrams are satisfactory but might have been used more effectively.	Inadequate analysis. Weak explanation with significant gaps or irrelevant material. Walkthroughs are confusing, missing key information, or show lack of understanding.
Task 2 **[40% weighting]**	Unique and comprehensive insights regarding firewall policies. Unique and comprehensive insights regarding CIA analysis. Unique and comprehensive insights regarding implications for C&C. Outstanding justification of proposed approach.	Strong and thorough insights regarding firewall policies. Strong and thorough insights regarding CIA analysis. Strong and thorough insights regarding implications for C&C. Excellent justification of proposed approach.	Very good insights regarding a good range of firewall policies. Very good range of insights regarding CIA analysis. Clear analysis regarding implications for C&C. Very good justification of proposed approach.	Accurate but incomplete insights regarding firewall policies. Good range of insights regarding CIA analysis. Good but incomplete analysis of implications for C&C. Good justification of proposed approach but may lack some depth.	Acceptable but limited insights regarding firewall policies. Reasonable but more obvious insights regarding CIA analysis. Reasonable analysis of implications for C&C, but lacking depth. Fair justification of proposed approach but may lack some depth.	Limited or weak limited insights regarding firewall policies. Limited insights regarding CIA analysis. Limited understanding of implications for C&C. Justification of proposed approach is not convincing.
Reporting and Organisation **[20% weighting]**	Uniquely informative in presentation approach. Stands out prominently as exceptional in quality. Diagrams are exceptional in technical detail.	Exceptionally clear. Concise throughout. Excellent organisation of information. Excellent balance of time allocated to each point of discussion. Presentation stands out in quality. Diagrams are excellent in technical detail.	Very clear and professional reporting style. Concise. Information is effectively organised. Well-balanced time allocated to each point of discussion. Minimal flaws. Diagrams are very good in technical detail.	Mostly clear reporting style. Could be more concise. Presentation good but could be better organised. Could improve balance of time, e.g. too much time on one topic at the expense of others. Minor flaws. Diagrams are accurate but may lack some depth of technical detail.	Clarity is acceptable, but with notable flaws. Not all information is presented clearly. Lacks concision. Crams in too much content. Too little content. Minor issues with video audio or visuals. Diagrams have some errors and lack some depth of technical detail.	Lacks clarity. Presentation is disorganised. Discussion does not match content on the screen. Discussion is difficult to follow. Pace too fast to follow. Audio edited to increase speed. Diagrams are unsatisfactory and difficult to follow.

5. Submission

Save your report as an **mp4** file and submit according to the instructions in Canvas.
Please name your file using your surname and student number, e.g. **einstein_40401234.pdf**

---

6. Assessment Aims

The broad aim of the report is to demonstrate and assess your **depth of understanding** across module topics, and your **ability to apply** that understanding to analyse a scenario.

- You may wish to study and apply the lecture notes, but you are also encouraged to look at topics more deeply to support your analysis of the case study.
- There is not a tick-box list of X items that you *must* identify in your report. However, you should aim to address a diverse range of relevant network security issues with a good depth of technical detail throughout.
- This is an open-ended investigation. Two students could approach the presentation quite differently and achieve an equally good mark.

---

7. Plagiarism and Collusion

This is an independent piece of work and must be completed solely by you. You must not discuss or share your analysis with anyone else. The analysis that you present must be your work, and your work alone.

This is an open-ended investigation. You are encouraged to find information and present points of analysis that you believe others may have missed.

By submitting the work, you declare that:

- I have read and understood the University regulations relating to academic offences, including collusion and plagiarism: http://www.qub.ac.uk/directorates/AcademicStudentAffairs/AcademicAffairs/GeneralRegulations/Procedures/ProceduresforDealingwithAcademicOffences/
- The submission is my own original work and no part of it has been submitted for any other assignments, except as otherwise permitted.
- I certify that that the submission is my own work, all sources are correctly attributed, and the contribution of any AI technologies is fully acknowledged.