Unit:
Network Security and Cryptography

Assignment title:
Video Zone Streaming Limited

15 credit version

Spring – Winter 2022

Important notes

- Please refer to the *Assignment Presentation Requirements* for advice on how to set out your assignment. These can be found on the NCC Education website. Hover over 'About Us' on the main menu and then navigate to 'Policies and Procedures' then scroll to the 'Student Support' area.
- You **must** read the NCC Education document *Academic Misconduct Policy* and ensure that you acknowledge all the sources that you use in your work. These documents are available on the NCC Education website. Hover over 'About Us' on the main menu and then navigate to 'Policies and Procedures' then scroll to the 'Student Support' area.
- You **must** complete the *Statement and Confirmation of Own Work*. The form is available on the NCC Education website. Hover over 'About Us' on the main menu and then navigate to 'Policies and Procedures' then scroll to the 'Student Support' area.
- Please make a note of the recommended word count. You could lose marks if you write 10% more or less than this.
- You must submit a paper copy and digital copy (on disk or similarly acceptable medium). Media containing viruses, or media that cannot be run directly, will result in a fail grade being awarded for this assessment.
- All electronic media will be checked for plagiarism.

Scenario

Business Overview and Challenge

Video Zone Limited is a video streaming company established in 2001 with its headquarters in London, United Kingdom. The company's primary business is a subscription-based streaming service offering online streaming from a library of films and television series to millions of subscribers around the world. Currently, its streaming service is available in Europe, the United States and Canada only. The company is planning to expand its platform to new customers in Asia, Latin America, Africa, and the Caribbean within the next few years.

Subscribers choose movies and television titles from the main Video Zone website or mobile app. They create an account using an email address and password, can manage their online account, make payments to renew their subscriptions and download movies from the website and mobile app.

Copies of all digital films and movies are stored in its in-house data centre which consists of a huge network of computer servers that can be streamed over the internet to subscribers via the company's website and mobile app. However, the company's data centre is struggling to cope with its growing customer base and inability to deliver real-time streaming of different media file types including video and audio quality in Ultra HD and 4K resolutions. In some cases, customers with low bandwidth internet connections have suffered poor video quality and buffering when streaming online content.

To support its business growth and planned expansion, Video Zone has embarked on a complete redesign of the company's traditional network infrastructure. This will require a phased migration within the next three years of its own data centre to Amazon Web Services (AWS), a public cloud technology infrastructure to scale the online streaming service and cater for new customers.

A competitor video streaming platform was recently hit by a ransomware attack, causing network disruption and significant data loss. Restoration of customer data and digital movies was not complete until six months after the incident. Video Zone is aware of the incident and Thomas, the Chief Information Security Officer (CISO), has created a plan to allow automated backup of data to a Network Attached Storage (NAS) device.

Video Zone has asked all staff to attend an optional social engineering training course. However, a recent review has highlighted that several members of email-based customer service and finance department staff are yet to complete this training.

Network Overview

- Video Zone's data centre located in London consists of about 100 servers. The company also holds personal and financial information on millions of its subscribers on its servers.
- The Video Zone web server hosts both the main Video Zone website and mobile Application Programmable Interfaces (APIs).

- The company has set up a public-facing blog on the web server to engage with its customers about new features to their streaming platform. The details of the exact setup are shown below:

  WordPress version 5.4.2
  Supsystic Contact Form 1.7.5 WP Plugin
  Supsystic Digital Publications 1.6.9 WP Plugin
  Supsystic Data Tables Generator 1.9.96 WP Plugin

- The company uses an internal non-encrypted SMTP server for email communication between staff at the London office.

- During the COVID-19 pandemic, many of Video Zone's network administrators have been working from home. Whenever there is a network issue, they can remotely access the data centre and company internal network using a remote desktop application from their personal computers and fix the issue.

- The Network Attached Storage (NAS) device is kept in-house, in the server room which is always locked and accessible to all staff members.

- The diagram of the company's network architecture is shown below:

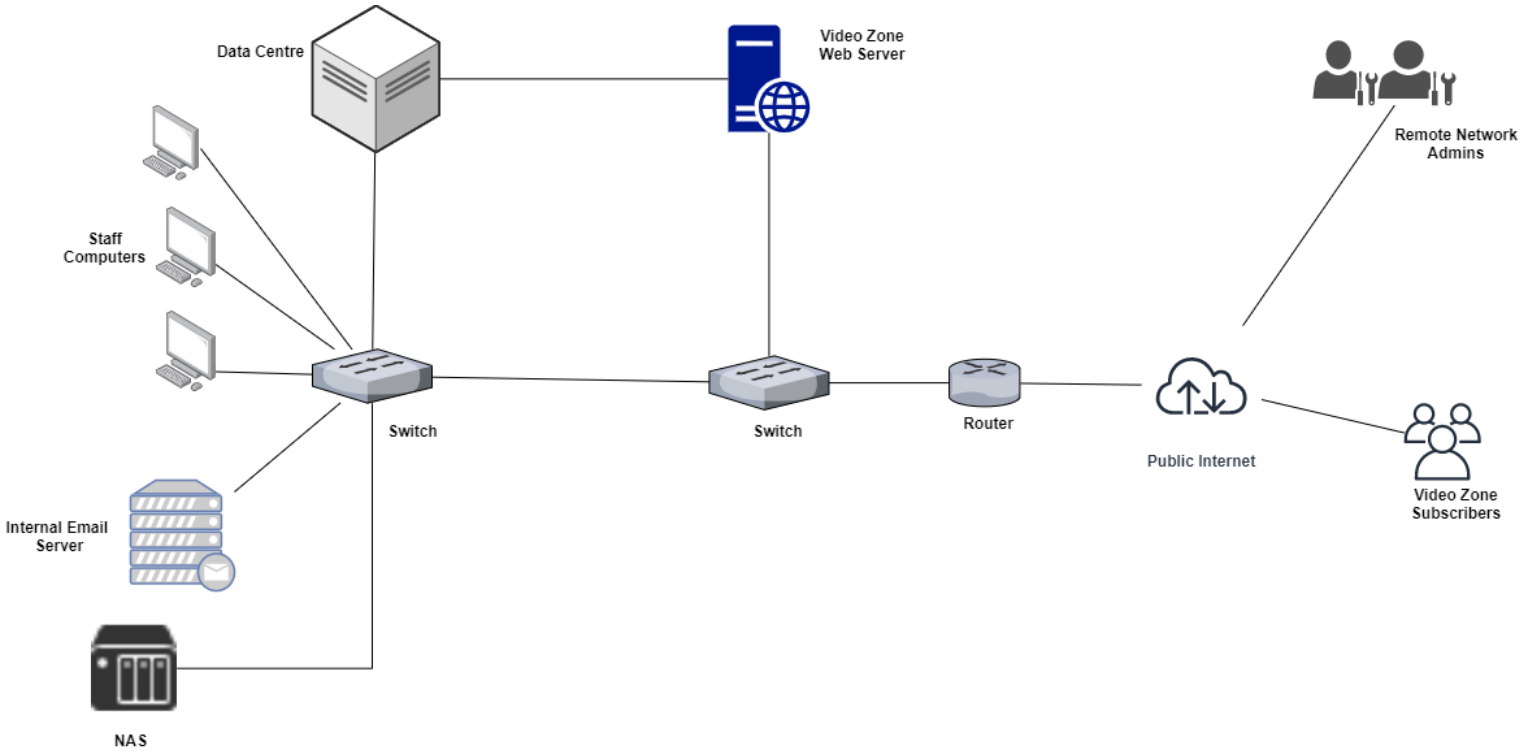

Figure 1. Video Zone Streaming Ltd Network Architecture

Task 1 – Risk Assessment - 15 Marks

This is a complex scenario; you should read it several times to identify what you consider to be critical information that needs to be secured, and where you think the threats may come from. You will need to make some reasonable assumptions here since the scenario does not provide a complete list of data/information or technology employed.

a) Analyse the scenario **and** identify what you consider to be the **FIVE (5) most important** electronically held information assets for Video Zone. Justify your decision. This section of the report should be approximately TWO HUNDRED AND FIFTY (250) words.

b) Create a table (see below) that lists the assets. For each asset identify the main security threats that you think could affect its confidentiality (C), integrity (I) or availability (A). Remember, threats can be accidents **as well as** malicious. There are likely to be multiple threats for each asset **and** the same threats are likely for several assets.

Asset	**Threat**	**CIA?**	**Likelihood**	**Impact**	**Risk**
E.g. Customer data	Server failure	**A**	Low	Medium	Low
	Employee theft	**C**	Low	High	Medium

c) Complete the columns of the table by assessing the **likelihood** of the threat being successful and the **impact** that it would have on the company. In this scenario you should consider Low/Medium **and** High definitions as follows:

	Likelihood	**Impact**
Low	Less than once per year	Inconvenience may affect operation for a day or two
Medium	Once per year to once per week	Operation may be impacted for over a week, loss of customers.
High	Several times a week	Company may not survive – lost reputation and customers

d) Now complete the Risk column by using the following Risk matrix.

		Impact		
		Low	Medium	High
Likelihood	Low	Very Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	Very High

Task 2 – Controlling the risks – Explanation - 40 Marks

Once you have identified the highest risks, you need to make recommendations on how to control those risks, i.e., what security you will put in place.

a) Discuss each of the threats you have identified in Task 1b) **and** recommend what security implementations to mitigate the risks. For higher marks, consider including alternative countermeasures to mitigate the risks and provide clear justifications. Where you use a technical term, you should explain it.

20 Marks

b)

i) Provide detailed explanations about **THREE (3)** different types of attacks to which the public-facing blog setup is vulnerable. **For extra marks**, provide references to exploits and security advisory notes for each vulnerability.

10 Marks

ii) Outline a strategy that could be used to detect the presence of **ALL THREE (3)** of the vulnerabilities featured in your answer to Task 2b) i) **and** describe technical solutions that would prevent the exploitation of the vulnerabilities described in your answer to Task 2b) i).

10 Marks

This section of the report should be approximately SEVEN HUNDRED AND FIFTY (750) words.

Task 3 – Securing the network - 30 Marks

Thomas, the CISO has suggested that Virtual Private Network (VPN) technology, a Demilitarised Zone (DMZ) and firewalls might be useful to help secure the corporate network.

a) Explain the key features of a VPN **and** how it could be applied here to address risk(s) associated with staff working remotely. Explain the suitable type of VPN connection option that is appropriate for the scenario **and** justify your recommendations.

5 Marks

b) As part of securing the corporate network, discuss the use of firewalls to secure the entire network **and** of a Demilitarised Zone (DMZ). Draw a new network diagram from Figure 1, showing new components which include firewalls, a VPN connection for staff working remotely **and** a DMZ. You must include all components from Figure 1 in your new diagram **and** justify your network design.

15 Marks

c) Discuss how you will improve the security on the internal email server **and** Network Attached Storage (NAS) device. You must provide a detailed discussion of any appropriate technology **and** methods in your recommendations.

10 Marks

This section of the report should be approximately FOUR HUNDRED AND FIFTY (450) words.

Task 4 – Maintaining Security - 5 Marks

Explain any actions you would recommend for ensuring security is taken seriously by all staff, especially the staff members of the email-based customer service and finance department. Discuss how you would monitor the effectiveness of the social engineering training course.

This section of the report should be approximately ONE HUNDRED AND FIFTY (150) words.

Task 5 Reflective commentary - 10 Marks

Reflect on what you learned from completing the assignment.

- Explain any problems you had **and** how you went about solving them.
- Explain anything you would do differently if you were to start it again.

This section of the report should be approximately ONE HUNDRED AND FIFTY (150) words.

Submission requirements

- The report should be well written, checked and proofed. Also, the report should be presented in a format and style appropriate for your intended audience. You must also include a list of references and you must use Harvard referencing and avoid plagiarism throughout your work.

- Your answers to the tasks should be combined in a single word-processed report with an appropriate introduction. The report should be 1750 words +/- 10% in length (excluding tables).

- Familiarise yourself with the NCC Education Academic Dishonesty and Plagiarism Policy and ensure that you acknowledge all the sources which you use in your work.

- You must submit a paper copy and digital copy (on disk or similarly acceptable medium).

- Media containing viruses, or media which cannot be run directly, will result in a fail grade being awarded for this assignment.

Candidate checklist

Please use the following checklist to ensure that your work is ready for submission.

Have you read the NCC Education document *Academic Misconduct Policy* and ensured that you have acknowledged all the sources that you have used in your work?	❑
Have you completed the *Statement and Confirmation of Own Work* form and attached it to your assignment? **You must do this.**	❑
Have you ensured that your work has not gone over or under the recommended word count by more than 10%?	❑
Have you ensured that your work does not contain viruses and can be run directly?	❑