TEESSIDE UNIVERSITY

AND

MANAGEMENT DEVELOPMENT INSTITUTE OF SINGAPORE

Course : **Bachelor of Science (Hons) Cybersecurity and Networks (BNSD22311A, BNSD22312A)**

Module Code and Title : **CIS2018-N Server Administration**

MDIS Module Tutor : **Mr Yatim Bin Abdul Ghani**

Assessment : **Individual Report**

Due Date : **31 August 2023**

Total Marks / Weightage : **100%**

TEESSIDE UNIVERSITY - SCHOOL OF COMPUTING, ENGINEERING AND DIGITAL TECHNOLOGIES

ICA SPECIFICATION

Module Title: **Server Administration**	Teeside Module Leader: **Dr Jie Li**
	Module Code: **CIS2018-N**
Assignment Title: **Design and Implementation of a Secure Server Network**	Deadline Date: *(please refer to above)*
	Deadline Time: **2359 hrs**
	Submission Method: Online (Blackboard)

Online Submission Notes:

- Please follow carefully the instructions given on the Assignment Specification
- When an extension has been granted, a fully completed and signed Extension form must be submitted to the SCMA Reception.

Library Support for Academic Skills

Did you know you can book an individual 30 minute tutorial in the Learning Hub with an adviser to help you with your academic skills, writing or numeracy? Or that there are loads of really useful workshops available to help you with your studies and assessments? Have a look at the Succeed@Tees workshops for more details.

FULL DETAILS OF THE ASSIGNMENT ARE ATTACHED
INCLUDING MARKING & GRADING CRITERIA

Contents

1. Introduction

Your assessment is “Design and Implementation of a Secure Server Network”. You are required to write a report to explain your work. In this assessment, you are expected to work **individually**.
This assessment is worth 100% of the total module marks.

2. Your Work

2.1 Introduction

You are required to design and build an internet-connected secure server network for Smith Logistics, which is a medium size warehouse and logistics company.

2.2 Scenario

A recent minor outage has alerted senior management to the importance of the company’s IT system to the day-to-day operations and has given more weight to your company’s recommendation for upgrading.
Currently, the existing network infrastructure has been shoe-horned onto an ageing server which is running Windows 2003 Small Business Server with clients as old as Windows XP and some as new as Windows 10. The company acknowledges that, given recent network and computer system breaches such as WannaCry, that they need to update their IT infrastructure and are looking to create a more secure IT infrastructure with room for expansion.
Due to the current company data governance framework, the company has no plan to move to a cloud solution yet, apart from the email service, such as Office 365. Therefore, the current plan is to upgrade their existing network to a fault tolerant server network, which can spread existing workloads across multiple servers. You will also need to build Windows 10 clients which you can join to the domain to use to help document that all the services are working correctly.

The required workloads across the servers are:

- Internally facing
    - Active Directory Domain Services
    - DNS
    - DHCP
    - Internal File Sharing Services
- Externally facing
    - Web Server – Apache, PHP and MySQL

The company has limited budget for this upgrade. Therefore, you have to consider how many servers and which operating systems are required, in order to achieve such requirement.

Smith Logistics has emphasised that they want to take this opportunity to strengthen their network security and are looking for you to explain what security considerations and/or improvements you can make as you outline the solution.

Smith Logistics store a lot of information and data, and they want to ensure that their servers, in particular, their file server has the appropriate disk redundancy in place so that they can tolerate disk failures without having to depend upon a backup solution. They also acknowledge that given they are rebuilding their entire server infrastructure they will also need to revisit backup options and have therefore asked you for advice both on disk redundancy and backup solutions.

They are also concerned about application compatibility so have requested that you create a mock-up of the proposed environment which they can then use to test their in-house applications and externally facing website. This will allow them, in the event there are any issues to resolve these before the final switch is made. As such you will be required to make detailed documentation of the environment you create for testing to ensure that it can be accurately re-created for the live migration.

2.3 Your Report

You are to assume the role of the assigned technical lead for this proposal and have been tasked with creating the initial mock environment and associated documentation.

Write a report which should at a minimum contain:

- A network diagram, including IP addresses. **(10%)**
- A recommendation and explanation of chosen disk redundancy and backup solutions for the final build (does not need simulating). **(10%)**
- Documentation for each network services component, such as AD DS, DNS and DHCP, describing briefly it's function and explaining what dependencies it may have and/or how it interacts with other components on the network. **(20%)**
    - Documentation might include IP Addresses of servers, DHCP Options, DNS Forward Lookup zones, Websites setup, etc.
    - You do not need to discuss any network devices, e.g., switches and routers.
- Documentation of a proof-of-concept network, evidencing the setup and configurations made using screenshots. **(25%)**
    - Client machine evidence should be used to demonstrate that the wider system works.
    - Internet connectivity is expected for both servers and clients.
- Recommendations of potential hardware based upon recommended specifications for operating systems and services along with indicative pricing. **(5%)**

- The report is expected to address any potential legal, ethical or security issue that may be present throughout the body of work. **(5%)**

Your report could also optionally include:

- Pro-active advice on identifying single points of failure and possible recommendations to mitigate or eliminate these. **(5%)**
- Pro-active advice for improving security and possible recommendations for future actions. **(5%)**
- Pro-active security advice including policy recommendations for the new network. **(5%)**

3. Deliverables and submission instructions

3.1 Structure of Report

The report should be around **3,500** words (with +-10% allowance), and must include the following sections:

- Cover page (A standard Assignment Front Sheet with your name and student ID)
- Table of contents
- Introduction
- Your works
- Conclusion
- References
- Appendices (if applicable)

The words in the table of contents, references, and appendices will not be counted above the word limit (3,500 words).

3.2 Submission deadline

An electronic version of the report must be submitted to Blackboard in PDF or Microsoft Word format by 2359hrs on *(please refer to the cover page)***.**

Important: No paper copies of the reports will be accepted.

NOTE: If you feel that your circumstances warrant an extension, and that you would benefit from one, you **must see your Module Leader** *(please refer to the cover page)* **before the deadline**. We cannot issue extensions after the deadline has passed.

4. Learning Outcomes

- Communicate effectively and professionally in writing using appropriate tools.
- Analyse a range of server solutions to make evidenced-based decisions on the combination of technologies that gives the best solution for a specified business scenario.
- Demonstrate their ability to manage a range of common services and justify the methods of delivering those services.
- Identify and discuss server administration concepts, principles and practices.
- Identify and offer solutions to a range of server monitoring problems.
- Evaluate a range of solutions that provide a secure server configuration to meet business requirements.
- Demonstrate understanding of a range of server monitoring techniques with due consideration of potential legal, professional and ethical issues.

5. Marking Scheme

Tasks	Description	Marks
A network diagram, including IP addresses	• Clearly shows the understanding of the given situation. • All given issues have been addressed. • Well-designed network, various subnetting technologies have been applied.	7-10
	• Shows the understanding of the issues relating to the given situation. • Most of given issues have been addressed, but not all of them. • Well-designed network, but no subnetting technologies were involved.	4-6
	• Demonstrate a limited understanding of the issues relating to the given situation. • Designed network may include some components to provide limited functions.	1-3
	• No network diagram is provided.	0
A recommendation and explanation of chosen disk redundancy and backup solutions for the final build (does not need simulating).	• Shows a clear understanding of disk redundancy and backup solutions. • Discusses a range of disk redundancy and backup technologies. • Recommend and explain the chosen technologies.	7-10
	• Shows an understanding of disk redundancy and backup solutions. • Recommends and explains the chosen technologies.	4-6
	• Demonstrate a limited understanding of disk redundancy and backup technologies. • Recommend a workable solution without explanation.	1-3
	• No disk redundancy and backup solutions are included.	0

Documentation for each network component, describing briefly it's function and explaining what dependencies it may have and/or how it interacts with other components on the network	• Shows a clear understanding of each network component. • Briefly describes the function of each network component. • Explains how each network component interacts with others.	14-20
	• Shows an understanding of each network component. • Describes the function of each network component in details. • Briefly explains how each component interacts with others.	8-13
	• Demonstrates a limited understanding of each network component. • Did not describe the function of each network component. • Did not explain how each network component interacts with others.	1-7
	• The report does not describe any network component.	0
Documentation of a proof-of-concept network, evidencing the setup and configurations made using screenshots	• Demonstrates the configurations. • The screenshots are proof of concept network.	20-25
	• Demonstrates the part of the configuration. • The screenshots are provided but can only proof the part of works.	11-19
	• Demonstrates the part of the configuration. • No screenshots are provided.	1-10
	• No demonstration or evidence are given	0
Recommendations of potential hardware based upon recommended specifications for operating systems and services along with indicative pricing	• Shows a clear understanding of company requirement. • Shows a clear understanding of specifications for hardware, and server operating systems. • Recommendations fits well with the company's current situation. • Good explanation.	4-5
	• Shows an understanding of company requirement. • Shows an understanding of specifications of the server operating system. • Recommendations is reasonably well.	2-3
	• The recommendation has been given but may not be suitable for the company.	1
	• No recommendation is given.	0
The report is expected to address any potential legal, ethical or security issue that may be present throughout the body of work	• Potential legal, ethical or security issues have been clearly addressed.	3-5
	• Potential legal, ethical or security issues have been mentioned, but not fully addressed.	1-2
	• Did not mention any of potential legal, ethical or security issue.	0
Pro-active advice on identifying single points of failure and possible recommendations to	• Identifies single points of failure, as well as to recommend the solutions.	3-5
	• Identifies the single points of failure, but no solution has been given, or the given solution cannot mitigate the identified failure.	1-2

mitigate or eliminate these	• No such topic is included.	0
Pro-active advice for improving security and possible recommendations for future actions	• Identifies security issues. • Recommends some possible actions for improvement.	3-5
	• Identifies security issues, but no recommendation is given.	1-2
	• No such topic is included.	0
Pro-active security advice including policy recommendations for the new network	• Explains the potential limitations of current policies. • Reasonable recommendations are given.	3-5
	• Explains the security limitations of current policies, but no recommendation is given.	1-2
	• No such topic is included.	0
Spelling, grammar, academic style, reference, etc.	• The structure of the report follows the requirement, which is introduced in Section 4.4. • No spelling error, and may have minor grammar issues.	7-10
	• The structure of the report follows the requirement, which is introduced in Section 4.4. • A number of spelling errors.	1-6
	• The structure of the report does not follow the requirement, which is introduced in Section 4.4 of this document.	0

6. Criteria

90%-100% • Exceptional work with presentation of a very high standard for the logical design and the report • There is coherence of ideas and demonstration of a thorough knowledge and understanding of network infrastructure, security etc. supported by wide reading with very effective use of source material and accurate referencing.
80%-89% • Outstanding work with presentation of a very high standard for the logical design and the report • There is of ideas and demonstration of a thorough knowledge and understanding of network infrastructure, security etc. supported by wide reading with effective use of source material and accurate referencing.
70%-79% • Extremely good work with presentation of a high standard for the logical design and the report • There is coherence of ideas and demonstration of thorough knowledge and understanding of network infrastructure, security etc. supported by reading with use of source material and accurate referencing.
60%-69% • The work is well presented and coherently structured for the logical design and the report. • There is evidence of a sound knowledge and understanding of network infrastructure, security etc. Most material used has been referenced / acknowledged.
50%-59% • Presentation is acceptable but with some errors.

• There is knowledge and understanding of network infrastructure, security etc. Some use of relevant source material.
40%-49% • Presentation is acceptable but attention to structure and style is required. The content is relevant but largely descriptive. • There is evidence of a reasonable level of knowledge and understanding but there is limited use of source material to support the design.
39% and below – Fail. • The work is poorly structured and presented. • Some material is irrelevant. Content is based largely on taught elements with very little evidence of reading around the topic