**ASSIGNMENT BRIEFING SHEET**

|  |
| --- |
| **ASSIGNMENT AIMS:**  To assess students on skills taught and researched on distributed systems. |
| **LEARNING OUTCOMES ASSESSED:**  Knowledge and understanding of:   1. *Requirements for security services* 2. *Features of distributed systems which make security and integrity problematic And should be able to:* 3. *Identify and evaluate threats to the security and integrity of distributed systems* 4. *Select and deploy context appropriate counter measures* 5. *Explain the issues involved in their work and justify and explain the approach taken* |
| **SUBMISSION REQUIREMENTS:**  The assignment should be submitted via E-learning Portal for assessment 15:00 on Friday 1st March 2022. |
| **FEEDBACK FROM THIS ASSIGNMENT**  Feedback for this assignment will be as described and returned via E-learning. |
| **MARKS AWARDED FOR:**  Marks will be allocated as indicated on the attached marking scheme. |

|  |
| --- |
| STUDENT COMMENTS ON THE ASSIGNMENT *(optional- for your continued academic and personal development you are encouraged to review your achievement and reflect on your progress in your studies).*   * What did you do well? * What could you have done better? * What would have enabled you to do it better? |
| MARKER’S COMMENTS *(markers may elect to provide feedback or comments by alternative means on students’ submissions, e.g. eLearning portal, detailed marking plan, etc.)* |

**BIT4209 – Distributed Systems**

## Assignment

You are to answer the following question and submit for evaluation.

Some parts of the question will require research beyond the material discussed in the course. This is intended and is part of the assessment.

As one of the biggest names in coffee farming brands, Njemu Coffee Estate is a leading farming company working on different coffee products such as green beans, Mbuni and cherry. This estate is one the most respected brands in the farming industry and its excellent coffee is very popular amongst coffee lovers around the globe. Currently the company has a main office and five branches located at various places in the Kirinyaga - Kenya miles away from each other. Njemu Coffee Estate employs fifteen agronomist and thirty administration staff. Each of the employees has his/her own computer and/or laptop. Each office has a local network including various servers, switches and other devices. All four offices’ networks are linked together through the Internet and using leased lines as the main communication infrastructure. In each site, various servers were dedicated for certain services and operations such as email, WWW, online sales and e-payments, special coffees and processing, data storage, etc. Njemu Coffee Estate would like to review its business strategy and current portfolio including asset management and investment. The strategic management office would like to ensure the security of all its assets including coffee stocks, data and communication links between the main office’s network resources and the other five branch offices’ local networks. The major concerns amongst the management team are the protection of all their critical coffee blend and pre-seasonal products, information leakage, harmful malware, and any possible unauthorised access to data and/or design files and network resources. In order to provide the level of security demanded by this solution, Njemu Coffee Estate ’s security infrastructure should be designed, deployed, and managed with KEBS and International Standards Organization (ISO) guidelines in mind.

The Web server’s API performs storage and all the necessary data processing. The services Web applications and all entities will communicate using the HTTP Protocol, Node.js, MongoDB and a protocol specific to MongoDB. The Njemu Coffee Estate ’s system architecture is designed to allow the applications to be hosted on up to four distributed entities as follows:

* + MongoDB
  + API (Node.js)
  + Web Portal (PHP, Nginx)
  + Computer and Mobile Devices

The system was designed to allow easy scaling of each part of the system as required. There is a central server for storage and available for remote access using VPN. The system and added functionalities should be evaluated in terms of their performance with specific client data and security operations. This includes extensive system configuration, performance testing, security assessment and penetration testing for the service applications and servers. This is to ensure that the service applications are not just working but meet the overall objectives of the company and provide an integrated secured suite of useful results that are meaningful and commercially valuable. The management team would like to ensure the security of its designs and data as well as secure communication links between the main office’s network resources and their clients and customers. The major concerns amongst the management team are the protection of all their critical designs

and services, information leakage, harmful malware, and any possible unauthorised access to data and/or financial operations and reports. Such unauthorised activities could be achieved through SQL injection and/or cross site scripting XSS attacks.

The management team decided to hire a security consultant to review and upgrade the existing network security infrastructure. Muchiri, the newly employed security consultant proposed a number of security controls such as a user authentication mechanism to avoid identity spoofing. A data integrity technique was suggested to avoid data alteration and to ensure database security.

However, Muchiri thinks that the current firewalls are working well and are able to control incoming and outgoing traffic access so will be kept, but require reconfiguration. In order to improve security, Muchiri believes that an intrusion detection system is required in each host to help in identifying any malicious and/or unauthorised activities. Despite the interesting security solutions proposed by Muchiri, his security assessment was incomplete in terms of identifying Njemu Coffee Estate ’s assets and analyzing risks of attacks. Issues such as the development of security policies to identify the required protection and deployment of security mechanisms were not part of his work. Muchiri’s proposed solutions were not specific and detailed in terms of the encryption algorithms and security protocols to be employed, authentication methods to be used as well as intrusion detection techniques and methods.

You have been contacted by Njemu Coffee Estate **to review their Web service application and security requirements, design and implementation.** Your report should attempt **to provide a clear, unambiguous statement of the security architecture quality of Njemu Coffee Estate ’s service applications and system infrastructure.** You will gather extra information through several means such as published reports and papers to obtain the relevant necessary information. **This process includes a review of the current system and to provide an architectural diagram of Njemu Coffee Estate system and network. This should be based on the information provided by Njemu Coffee Estate in previous sections.** You will perform comparisons with relevant standards and be **able to identify the major assets, risks to attacks such as SQL injection and XSS attacks. You will develop policies to overcome the security vulnerabilities and to minimize their impact on Njemu Coffee Estate .** In your report, the company’s online Web-based service through its architecture should be evaluated in terms of its security provisions. The Njemu Coffee Estate ’s security posture should be presented by **identifying its critical information and systems that need to be protected.** This is to allow you **to propose the necessary security mechanisms and solutions to meet Njemu Coffee Estate ’s security needs.** These efforts will highlight the good practices and findings about this company and consider various technical standards such as ISO information security standards, relevant documents, etc. This **is to study and specify the requirement details and evaluation of Njemu Coffee Estate ’s system architecture and services in terms of meeting the necessary security needs and controls.**

The final outcomes and results are intended **to provide the company with a list of recommendations and any necessary justifications to improve their security.** The implementation of any recommendations contained in your report should not guarantee the elimination of all security threats but should allow keeping the risks as minimum as possible. To achieve this, you will need **to identify and clarify security issues for the core system, technical review and assessment of system architecture as follows:**

* + Identify Njemu Coffee Estate ’s major assets and risks to attacks, security assessment to the whole system and develop necessary policies to address all the security issues and to support the security requirements
  + Identify and assess potential security threats and/or vulnerabilities, with specific attention to threats to critical designs and financial stored data or during transmission
  + Identify technical constraints/requirements of web services and remote access control e.g. authentication and login passwords, authorization and firewalls
  + Security concerns of financial operations such as online payments and sensitive data confidentiality and integrity including service availability
  + Design and document security controls and mechanisms, data and server replication

protection and real-time monitoring of end-user system usage

* + Identify technical constraints/requirements of secure content management, data access,

rapid recovery and backup e.g. safeguard against disaster

* + Procedure for performing security testing of core system and APIs, review of source code

and fixing faults that are identified from tests e.g. ‘Field test’ using live customer input, with

database(s) located on server(s)

You will need to produce a security assessment scenario in the form of a professional technical report. In order to achieve this you should also:

* + Describe how data integrity could be implemented. Discuss any proposed solutions and/or

possible alternatives. How can data integrity be used to improve the company’s database

security so to protect their clients’ data in general and financial operations in particular?

* + Investigate certain malwares such as botnets and worms that are generating various security

threats to the company’s service applications and systems. In your answer, address the

following points:

1. Types and exploitation
2. Life cycle/Timeline
3. Suitability as a potential threat to the company’s information
4. Strengths and Weaknesses
5. Short and long term implications on the company’s network resources
6. Preventative and mitigation techniques
7. Use extensive examples to support your answer
   * Specify the major vulnerabilities and threats such as SQL injection and XSS attacks,

countermeasures and solutions which you think that are appropriate for such a scenario

* + Compare and contrast the different types and methods of intrusion detection systems that

can be used by Njemu Coffee Estate to monitor all network level and application level

communications and activities. This is to identify any possible malicious and unauthorised

activities and to minimise their effects.

* + Finally, you might think of any other security issues that need to be considered.

In a summary, your **report should propose appropriate security measures and cost-effective solutions, considering the company’s concerns and possible security threats and limitations.** Having analysed the network structure and how it accesses the Internet, identify the security protocols and mechanisms that should be implemented. The solution should be adequate enough to support this company. You should give a detailed explanation, any technical constraints, diagrams and comparison tables in terms of capabilities, performance, and strengths and limitations.

Typically, your report might be organized (but not necessarily to be) as follows:

1. abstract
2. introduction
3. background information, literature review, scope and limitations
4. main body including methods used
5. investigations and analysis
6. conclusion
7. recommendations, unsolved problems
8. references (books, conference papers, journal publications, WWW references)

You should clearly state any assumptions that you have made with justification in your report and discuss any alternatives to your proposed solutions.

The write up for this question should

* + Be between 4500 and 5500 words in length **maximum**, approximately 12-15 pages excluding diagrams
  + Be your own work - plagiarism will not be tolerated
  + Use relevant sources, properly referenced throughout
  + Include a bibliography of references

## Note:

The assignment will be marked according to the attached mark scheme and as such you should address each of the mark criteria within your assignment.

## Plagiarism will not be tolerated

**Hand in Date: 15:00 EAT 1ST MARCH 2022**

**Marking Criteria (for each question)**

**70% - 100%**

☺ A wide range of discussion points that reflect a strong understanding of the topic area

☺ Critical evaluation, reflection and process regarding concepts.

☺ Evidence of wide ranging and effective research.

☺ A very strong list of relevant references.

☺ Observations and points of discussion are sensible, relevant and supported with excellent examples.

☺ The assignment is well structured, with a high level of presentation and organisation.

**60% - 69%**

* A wide range of discussion points that reflect a significant understanding of the topic area
* Effective evaluation, reflection and process regarding concepts.
* Evidence of a range of effective research
* A strong list of relevant references.
* Observations and points of discussion are sensible, relevant and supported with good examples.
* The assignment is structured, with a high level of presentation and organisation.

**50% - 59%**

 A range of discussion points that reflect a good understanding of the topic area  Evaluation, reflection and process regarding concepts.

 Evidence of an effective research beyond the course materials  A good list of relevant references.

 Observations and points of discussion will generally be sensible, relevant and supported with examples.  The assignment has some structure with a good level of presentation and organisation.

**20% - 49%**

 A range of discussion points that reflect a reasonable understanding of the topic area but not at Masters level  Insufficient evaluation, reflection and process regarding concepts.

 Evidence of research beyond the course materials  A limited list of relevant references

 Observations and points of discussion are sensible but irrelevant and not supported with examples.  The assignment will not be completed to an acceptable standard of presentation and organisation.

**0% - 19%**

Work reflecting little or no effort

Njemu Coffee Estate Security Report

1. abstract

Security is a major concern in the modern world. With increased use of computers and connectivity to the internet more threats are very common. Every there are more cyber threats occuring than ever. Cybersecurity is a major concern to every business in the world right now. This is because most of the business has gone online.

There are a lot of attact vectors to an online business. And if a company is vulnerable to this attacks it can be crippled very fast and go out of the business. Cybersecurity is a continous process that requires companies to regularly keep their systems safe. The importance of security can not be argued with.

Attackers are regularly on the look out to attack any company systems. They use very sophisticated methods and tools to attack systems. Common attack vector are sql injection, xss vulnerabilities, api vulnerabilities, csrf vulnerabilities, remote code execution, weak passwords, server side request forgery, and many more others. This types of attacks are the most common and Njemu coffee estate should keep a look on them.

1. Introduction

Njemu coffee estate uses a distributed sytem on their servers side request. Distributed System’s are very recommended in any system because of their tolerate to failure, multiple points of usage,

1. background information, literature review, scope and limitations
2. main body including methods used
3. investigations and analysis
4. conclusion
5. recommendations, unsolved problems
6. references (books, conference papers, journal publications, WWW references)