ASSIGNMENT COVER PAGE

Programme	Course Code and Title
UCSEW	COS3023/N Operating System & Concurrency

Student's name / student's id	Lecturer's name
0204677 Lim Zhe Yuan **0207738 Mrigesh A/L Perbakaran** **0207778 Saw Keat Loon** **0207737 Tan He Xiu**	Siti Shafrah Shahawai

Date issued	Submission Deadline	Indicative Weighting
03.07.2023	01.08.2023	30%

Assignment [2] title	Memory Management and Security in Operating Systems - Case Study Problem Solution

This assessment assesses the following course learning outcomes

# as in Course Guide	UOWM KDU Penang University College Learning Outcome
CLO3	Analyse principal concepts and methods of memory management and file system implementation. (C4,PLO7)
CLO4	Evaluate variety of security threats and propose appropriate OS mechanisms to protect against them. (C6,PLO7)

# as in Course Guide	University of Lincoln Learning Outcome

Student's declaration

I certify that the work submitted for this assignment is my own and research sources are fully acknowledged.

Student's signature:

Zhe yuan   SAW

Mrigesh   HX

Submission Date: 1/8/2023

TurnItIn Similarity Report

OSasgn2

Table of Contents

Group task distribution

Name	Group task
Lim Zhe Yuan	Memory management challenges
Saw Keat Loon	Security issues
Mrigesh	Memory management recommendations
Tan He Xiu	Security recommendation

Main Report

Group Task

- ### Memory management challenges

As a company maintaining an operating system, OxTech Corporation may face memory management challenges in terms of memory allocation, particularly in dynamic memory allocation. To give a bit of context, memory allocation can be differentiated into two types: static and dynamic memory allocation. Static memory allocation is the allocation of memory which is performed at compile time, while dynamic memory allocation is the allocation of memory during execution time (Neha, 2019). Static memory allocations are more efficient than dynamic memory allocations as the former know the exact dimensions of process resources required before execution and is able to organize them more effectively whereas the latter do not (Neha, 2019). In this case, most memory management challenges appear in the form of the flexibility of dynamic memory allocation in deciding the exact memory spaces required by the programs running on OxTech's OS, not the OS itself.
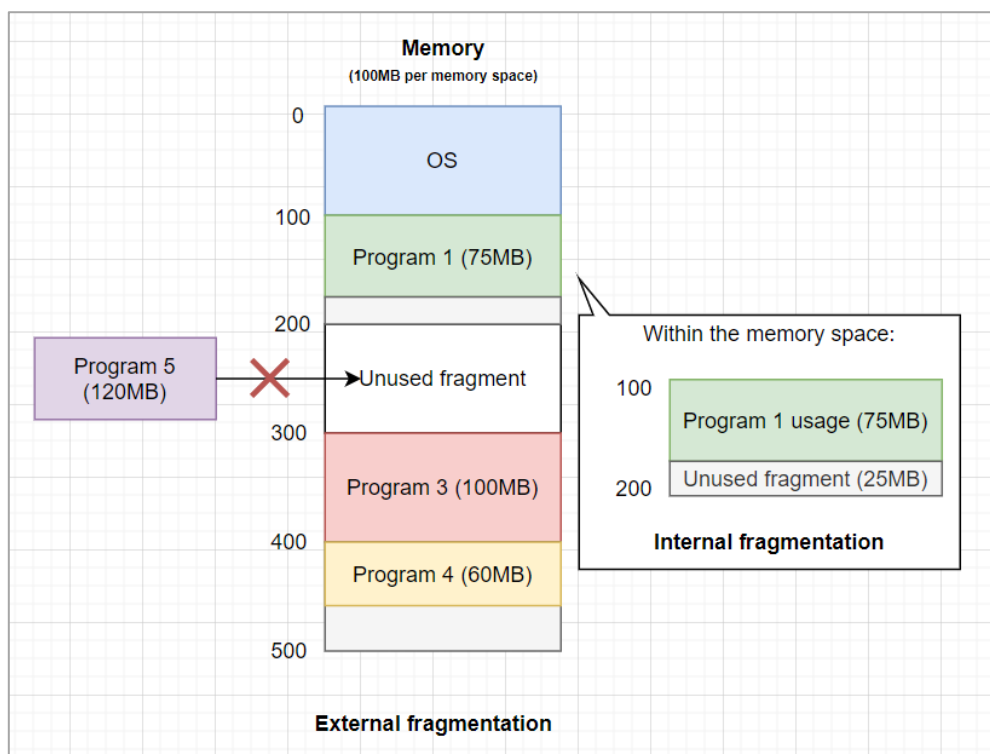

Figure 1: *External fragmentation vs. internal fragmentation*

In dynamic memory allocation, fragmentation, the main memory allocation problem, may be introduced to the system. Fragmentation is an unwanted problem where the memory blocks cannot be allocated to new processes after deallocating a completed process due to their small size, and the blocks remain unused (AfterAcademy, 2020). Fragmentation can again be divided into two distinct types: internal and external fragmentation. Internal fragmentation occurs when a process is allocated to a memory block that has a size bigger than its own, and the extra space remains unused (AfterAcademy, 2020). On another hand, external fragmentation occurs when there are unused spaces left between the fragments of non-contiguous memory, which are too tiny to fit in new processes (Panigrahi, 2023). Both fragmentation types expose the issue of leaving empty holes in memory, which makes allocation inefficient and increases process turnaround times. As Thakur (2022) mentioned, the fundamental goal of memory management is to make optimal use of memory by minimizing internal and external fragmentation.

1

The problem of fragmentation also causes poor locality of object references. The inaccessible holes left by external fragmentation may increase the distance between communicating processes in memory. This problematic layout of fragmented blocks, where the memory manager places the blocks that a program will use together far apart, will cause performance problems. It is more optimal if memory accesses are performed successively as locators can be faster if required data are placed in nearby memory locations (Ravenbrook, 2023).
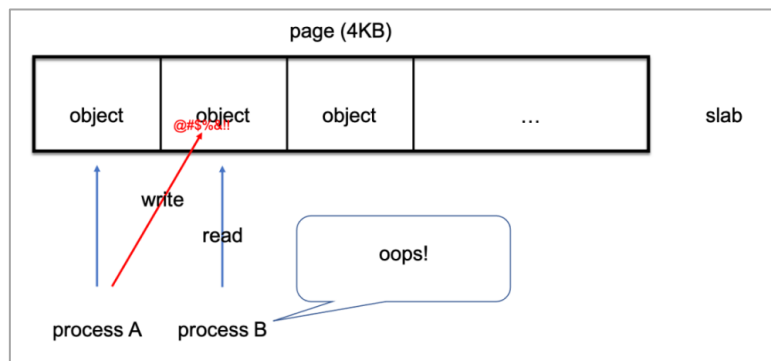

Figure 2: Memory corruption (Kernel SIG, 2022)

Another problem that may be faced by OxTech is memory deallocation issues. Problems such as memory leaks and corruption may infest within the OS if unnecessary memory allocations are not deallocated properly and appropriately. Memory leaks are situations when memory fails to free up segments that they no longer need that happen due to poorly designed or programmed applications (Kay, 2000). This causes programs to eventually run out of memory. It may also cascade the problem into memory corruption instead, which is the contamination of other memory blocks that do not belong to a process. This occurs because some OS, like Linux, performs no monitoring and constraints on specific memory usages after their allocation, is completely open and shared (Kernel SIG, 2022). When a program no longer needs the memory space that has been allocated to its resources, a mechanism is required to release that memory for other reassignments (Sheldon, 2022).

Additionally, another problem that may be faced by OxTech's OS may be the insufficiency of memory. There may be cases where there is not enough physical memory space for running a large batch of processes. This happens when there may not be an alternative device to increase available memory spaces to run more programs. Therefore, this issue only persists if OxTech's OS relies on systems from earlier years as these systems mainly use the RAM and secondary memory separately. There is a need to increase the capacity of memory without relying only on physical memory spaces, as programs in recent years are designed and built to consume large amount of memory to run an abundance of features (Kanade, 2023; Sheldon, 2022).

Finally, inflexible design in memory managers can also pose as a problem to OxTech's OS in memory management. It can cause severe performance problems if they have been designed mainly with one use in mind but are used differently. These problems occur because assumptions may be made about the way the program is going to use memory, such as typical block sizes, reference patterns, or lifetimes of objects. If these assumptions are wrong, then the memory manager may spend a lot more time doing checkups and recalibration work to keep up with current memory usages (Ravenbrook, 2023).

- **Security issues**

To prevent any future security breaches or attacks to the operating system, it is important to find and understand what is harming the system. As OxTech Corporation is a leading technology company, they will be one of the main targets from attackers to steal data from them.

There are multiple security threats that could be found attacking OxTech's operating system that cause them to lose data. One of them is malware attack. Cyberark (n.d.) stated that malware attacks usually are caused by malicious software that attacks the users without them noticing. Malware attacks are usually caused by weak or outdated system security that are unable to detect and destroy any virus that is hiding in a software. Cyberark (n.d.) also mentioned that malware is usually used by cyber attackers for personal reasons such as stealing financial or personal information illegally.

Worm is a type of malware attack that could be causing data loss from OxTech's operating system. Cisco (n.d.) stated that although worms are not a virus, worms are able to harm IT activities and bring data loss. Cyber attackers use worms to enable them to access infected computers from the spreading of worms through the shared network.
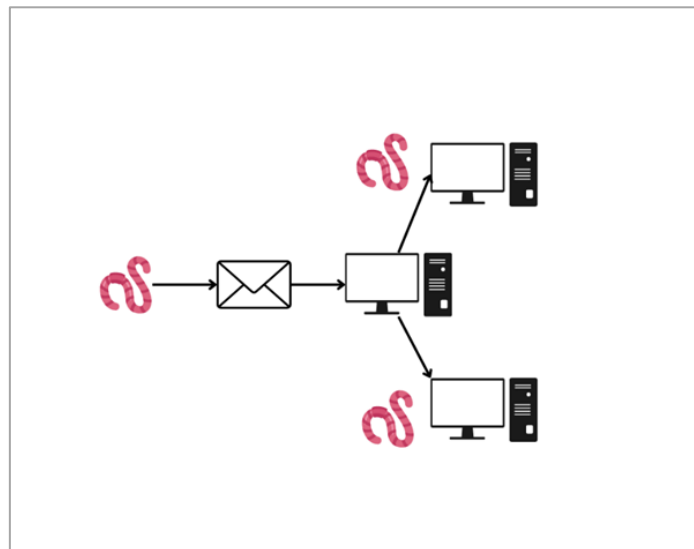

Figure 3: Worm attack illustration

Figure 1 illustrates how a worm spread to other computers. Worms are attached to an email that is sent by the cyber attacker. The email is opened by a computer within an organization. Upon opening, the worm infects the computer and later spreads to other computers within the same organization network either via file transferring or internet connection. All the infected computers are vulnerable to cyber attackers to get access to them to steal data.

Virus attack could be another type of malware that is attacking OxTech's operating system. Malwarebytes (n.d.) stated that a computer virus is malware that requires the user to activate it so that it can duplicate and infect the computer. Although viruses and worms might behave the same, there are differences between them both. Malwarebytes (n.d.) mentioned that worm does not need any action from the user to activate it while computer virus requires a specified action such as opening a file.
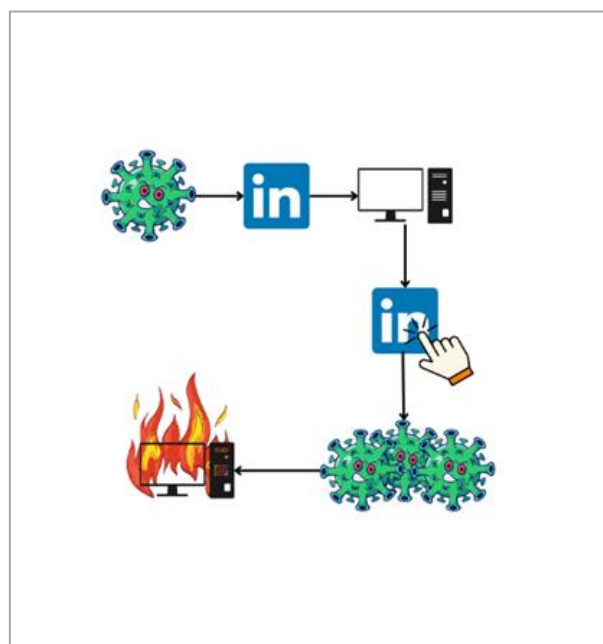
Figure 4*: Virus attack illustration*

Figure 2 illustrates how a virus destroys or attacks the infected computer. Cyber attackers embedded viruses into an application. The application is then installed onto the computer. The computer virus is in their hibernation phase where they are not doing anything. When the application is clicked or opened by the computer user, then the computer virus starts to duplicate themselves. Upon duplicating, the virus can either modify or steal data from the infected computer. Latto (2022) stated that some of the effects of computer viruses could bring are, failing of programs and crashing operating system. Computer viruses could be the threat that is causing constant crashes in OxTech's operating system.

Denial of Service

Denial of service or DoS is a well-known situation where users are unable to access their favorite website or internet platform due to limited access or too busy servers. Meanwhile, paloaltonetworks (n.d.) explained that DoS are used to take down a network or a machine to prevent intended users to access it. Paloaltonetworks (n.d.) also explained that DoS attacks crashes servers and machines by engulfing them with traffic or data. Servers and computers have limited bandwidth and computational power to handle any incoming request from the users. DoS happens when a massive number of requests is being thrown at a server and at a constant rate crashes the server due to its inability to handle all the requests. Denial of service could be one of the causes of system crashing and performance degradation by OxTech's operating system and computers.

There are a large number of variations for DoS attack to happen. Among them, buffer overflow attacks are the most common among them. Imperva (n.d.) stated that buffer overflow happens when the volume of memory buffer could not store the size of data hence leads to overwriting of nearby memory location. Although buffer overflow is a normal thing in the world of computing, attackers exploit it by overwriting an application's memory (Imperva, n.d.). Attackers could add additional lines of code into an application via the buffer overflow and causes the application to leak private information. Stack-based buffer overflow is a method that is used by cyber attackers to take down a server. Watters (2019) wrote that stack-based buffer is the most frequently used and flashy way to control processes of codes while being unnotified. Rouse (2016) wrote that buffer is a non-permanent storage area for data while it is waiting to be moved to another place in a computer.
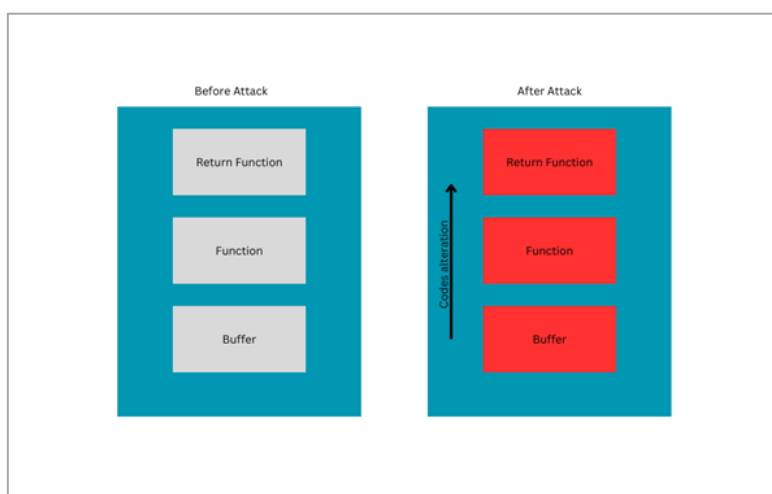
Figure 5: Stack-based buffer example

The figure above shows how a stack-based buffer overflow attack takes place in an application. Before the attack, the buffer, codes in the main function and return function are unaltered. During the attack, cyber attackers flood the application or server by sending it massive amounts of data or traffic at the same time causing the buffer to be unable to store them. As more and more data are being sent, the extra data overflows. As it overflows, cyber attackers could change or hack the server by altering the original codes through the overflow data. If there is no hacking taking place, servers usually will slow down and eventually crash as it is unable to handle the incoming request.

The second type of DoS attack is called ICMP flood or ping flood. Imperva (n.d.) explained that cyber attackers use ping flood to take down their victim's computer by flooding it with pings or ICMP echo requests.
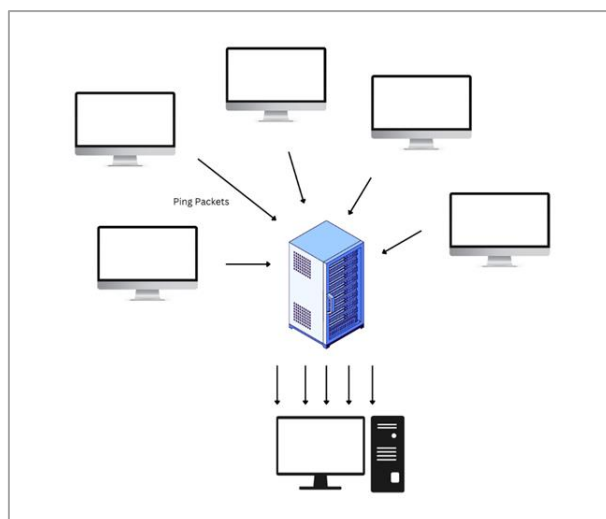
Figure 6: Ping flood

The diagram above illustrates how a ping flood could occur in OxTech's cooperation. Cyber attackers use multiple computers or bots to send ping packets to OxTech's server. Depending on their motive, cyber attackers could send the pings only to the server or to a targeted victim based on their IP address. Attacking based on IP address could cause the server to redirect all the ping towards the victim's computer and cause it to slow down or even crash it.

- **Memory management recommendations**

a. Paging and Segmentation Techniques (Fragmentation Recommendation)

Fragmentation is a typical issue in memory management that can prompt wasteful memory use and execution debasement. By carrying out paging and segmentation techniques, OxTech can resolve this issue.

Paging

Paging partitions the actual memory into fixed-sized blocks called pages and partitions the coherent memory into equivalent estimated blocks called page outlines. This approach helps in diminishing outer fragmentation. At the point when a cycle needs memory, the working framework can distribute touching page outlines, which could not really be bordering in actual memory. This diminishes fragmentation, as more modest lumps of memory can be allotted on a case-by-case basis, decreasing the possibilities of huge holes between distributed blocks.

Segmentation

Segmentation separates the intelligent memory into variable-sized fragments that compare to the coherent units of a program, like code, information, and stack. Each section can be dispensed dynamically, and when a portion is not generally needed, the memory can be deallocated, opening space. This aides in diminishing inside fragmentation, as memory blocks can be better matched to the genuine size of the information being put away.

Legitimization: Paging and segmentation are broadly involved memory management techniques in present day working frameworks because of their viability in overseeing memory fragmentation. These techniques further develop memory allocation as well as upgrade framework solidness and execution by decreasing the gamble of accidents and further developing memory usage.

b. Garbage Collection (Memory Deallocation Recommendation)

Garbage collection is critical for successful memory management, particularly in undeniable level programming dialects where manual memory deallocation isn't possible. OxTech ought to carry out a garbage collection system to consequently recognize and deliver memory that is at this point not being used by programs.

Garbage Collection Calculations

There are different garbage collection calculations, for example, Imprint Clear, Reference Counting, and Generational Garbage Collection. The decision of the calculation relies upon the necessities of OxTech's working framework.

Legitimization: Manual memory deallocation can be blunder inclined, prompting memory spills or getting to liberated memory, causing accidents and security weaknesses. Garbage collection computerizes the memory deallocation process, guaranteeing that memory is delivered when it is not generally required, in this manner forestalling memory spills and upgrading framework security.

c. VRAM (Lacking Memory Recommendation)

Video Smash (VRAM) is devoted memory utilized for putting away designs related information, and lacking VRAM can prompt execution issues, graphical errors, and even framework crashes. OxTech ought to resolve the issue of deficient VRAM in its working framework.

Dynamic VRAM Allocation

Executing a dynamic VRAM allocation instrument permits the working framework to designate VRAM considering the necessities of uses or cycles. It can guarantee that each interaction gets the vital VRAM for smooth illustrations delivering, and when the VRAM is not generally needed, it tends to be recovered and allotted to different cycles.

VRAM Swap

OxTech can likewise present a VRAM trading instrument, like conventional memory trading, where less often-utilized illustrations, information can be briefly moved to framework Slam or capacity to let loose VRAM space for additional basic errands.

Legitimization: In present day figuring conditions, graphical connection points and sight and sound applications request critical VRAM. Deficient VRAM can prompt execution bottlenecks, diminished client experience, and even framework crashes. By carrying out dynamic VRAM allocation and VRAM trading, OxTech can upgrade the general exhibition and soundness of its working framework.

By carrying out these memory management recommendations, OxTech Company can address the difficulties connected with memory allocation, deallocation, fragmentation, and VRAM deficiency in its working framework. This will prompt better framework steadiness, improved execution, and expanded client fulfilment while limiting the gamble of safety breaks and information misfortune.

d. Memory Compression

Memory compression is a strategy that can fundamentally further develop memory proficiency by compacting data in memory, subsequently diminishing the general memory impression of the working framework and its running cycles.

How Memory Compression Functions

At the point when an interaction or the working framework distinguishes that specific pages of memory contain repetitive or compressible data, rather than putting away them with no guarantees, memory compression calculations are utilized to pack the data. The packed data occupies less room in memory, permitting more data to be put away in a similar measure of actual memory.

Advantages of Memory Compression

- **Expanded Memory Capacity**
  By packing data in memory, more data can squeeze into the accessible actual memory, really expanding the powerful memory capacity of the framework.

- **Decreased Memory Pressure**
  Memory compression can assist with mitigating memory pressure during top use times, forestalling the requirement for successive trading to plate and further developing generally framework execution.

- **Quicker Data Access**
  Accessing packed data in memory is quicker than accessing data from circle, bringing about better reaction times for applications and the working framework.

Legitimization: Memory compression is a strong strategy that can be especially valuable for frameworks confronting memory constraints or unreasonable paging to plate. It can prompt a

critical decrease in memory-related execution issues, like stoppages and accidents, while additionally further developing the general client experience.

- **Security recommendations**

Due to the company's problems which is the security breaches, data loss and compromised user privacy, OxTech Corporation must take action as soon as possible to solve the current problems. We as the consultants of the company need to provide some recommendation of security to improve company's security and improve customer loyalty. Below is the recommendation for security improvement.

Access Control

Accessing to an area, a building, a room or another place that can be allowed or denied is defined as the access control system. It takes controls who has the access to a certain area at a specific moment using an electronic type or physical type (Morefieldcommunications, 2022). Other than that, access control also a technique for limiting access to some confidential or sensitive content. An access control gateway will allow only those personal or individual whose identity have been validated to access corporate data (Abi, 2023). Access control is very important to the improvement of security to prevent more company's data loss or user privacy leakage. Below will explain the importance of access control.

- **Stronger Security**
    - o It allows the expertise of security to have more effectively control who can access to a structure or property. Next, operator is way easier to limit by just asking users to provide the credentials when they wish to enter a certain area or building that is fully restricted for security reason.
- **Simple access management**
    - o It also normal to applied access control in security management because the expertise will not be facing the problems or recall key about the user join or leave. With just some simple steps or auto sync with the software that provided will keeps the database real time update and secure.
- **More Data**
    - o Through the access control, it also helps to record OxTech Corporation's employees all the entry activity as well as the identification and credential types. When it comes to a problem, security expert can track back to find the possible issues. It also can help OxTech Corporation in compiling and comprehensive of all the buildings.

Encryption

Encryption basically is the encoded data that using encryption method to stay hidden from the unavailable to unauthorised users (GENETEC, n.d.). All the information that is private, confidential data and some communication between clients and server in OxTech Corporation will be protected if the encryption is done properly. In basic terms, if the data that is encrypted and get stolen by other people, they still need the owner permission to read the information or else it cannot be able to read it. The encryption word like a plain text turn into unreadable text which we can called ciphertext. This helps to improve the security in preserving the privacy of electronic information that is either transported across the network.

When the people that receive the encrypted message, they need a secret key to turn the text to original form and the process called decryption. For the encryption, there are 2 types of encryptions which is Symmetric encryption and Asymmetric encryption.

- Symmetric Encryption
    - Symmetric encryption does encrypt and decrypt the data using the same secret key or password that is provided by the software randomly. This is the most popular type and often use by many companies of the encryption because of its simplicity. It has 2 forms in symmetric which are block algorithms and stream algorithms. The only difference between these 2 forms is it encrypt a bunch of text as one block in block algorithms and it convert a symbol of text directly into ciphertext in stream algorithm.
- Asymmetric Encryption
    - Asymmetric Encryption can be known as the cryptography of public key that is needed two keys for the process of encryption and decryption. Talking about the key, there are 2 types of keys which is public key and private key. For public key, even the information has been hacked during transit, it also assures that only the receiver may use the specific key to decrypt the text message. For private key, it allows the recipient of the information to make sure the identity of sender, since they cannot be able to decrypt the data by someone random.

With the help of the encryption, we can ensure that the security of OxTech Corporation will have a big improvement.

Intrusion Detection System

Intrusion detection system or we can write in short form IDS is a software that helps to keep an eye out for hostile activities or policy breaches on a network. This could help in OxTech Corporation security information and event management system. This will notify the risk or violations and helps to gather them centrally. Other than that, IDS also call for the response team to look for the problems before taking any necessary action to remove the danger (RiskXchange, 2023). With the help of the system software, the number and variety of incidents might be analysed with the function of IDS. OxTech Corporation can use this opportunity to modify the security protocols or try to set in the place for a better security measurement (Lutkevich, B., 2021). Other than that, OxTech Corporation also may find the defects or the issues with the configuration of their device related to the network with the use of the IDS which is intrusion detection system. IDS also play a vital role in security because it brings a lot of benefits towards the network security. Below points are the benefit that will bring to OxTech Corporation.

- Detect malicious activity
    - Before any significant damage is done by other harmful link or website, intrusion detection system will identify unusual behaviour and notify the network administrator.
- Improves network performance
    - IDS also can be able to make sure the performance issues on network are smooth and always be ready at any time.
- Complaisance need
    - To create the reports and monitoring the network activity, IDS is a must because it assists OxTech Corporation firm in meeting its regulatory needs.
- Insights will be provided
    - To get uncover flaws in network security, IDS provide critical insights into the network traffic to enhance the overall network security.

Firewall

In a company, firewall is a tool that cannot be lack in security because it can guard the OxTech Corporation network against the unauthorised use of confidential information. Firewall also helps to protect the systems against harmful malware and separate the trusted network of internal and the unauthorised external network (Datto, n.d.). This is to prevent they mix together and viruses get into the company server. Moreover, company's customer is depending on the security requirements and firewall is good to provide a varying level if protection and increase customer trust. Improve the firewall of OxTech Corporation is a very good idea because firewall have served for over 25 years as the first line of defence in network security. There are some benefits of the firewall and the first one is preventing hacking from outsider. Firewalls are becoming even more essential as the hacker and criminals have increased since they can access company data, information, emails, servers and other things without any permission. With the firewall assists, it can fully block the hacker from stealing all information of a company. Other than that, firewall also can stop virus attacks. If a company server has virus, it has a possibility to shut the business down within a few hours. To prevent this happen, firewall is needed because it can maintain the server or system healthy and prevent the virus attack. Lastly, firewall also promotes privacy (Fortinet, n.d.). This is to keep company and customer personal data safe. This also helps to build the environment that the company's customer can trust. There is nobody like their personal data get stolen or leak to outside particularly when it is obvious that measures might stop the infiltration.

Individual Task

1. 0204677 Lim Zhe Yuan

In retrospect after examining the group work, it has come to my realization that building an operating system is an impressive and sophisticated feat which requires a meticulous approach to the management and solution of unseen issues. As a consumer, one would rarely pay any mind into the technicality of a computer device's operating system. However, one will definitely be amazed by the countless amount of effort that have been contributed by the brightest of minds into designing an operating system's architectures and methodologies if they took a step further into investigating the wonders of computers. The fact that initially unknown computing issues are able to be captured, identified, and handled by machinists expertly without foreseeing them at all is also mind-boggling, because these issues were undocumented, and the occurrence of these issues most likely came with a disruptive effect and caused huge losses. It is fortunate that people can now be aware and steer clear of these issues after they are documented with detailed descriptions so that they do not experience similar hardships again.

As a group member tasked with writing about memory management challenges, I do think that I worked efficiently and effectively because I made as much research as I can online and had gathered a variety of sources that claimed to hold explanations and evidence of memory management issues, so that key takeaways are cross-checked and can be clearly, sufficiently highlighted in my work. These challenges were mainly identified based on concepts and descriptions that indirectly reference memory management issues in articles and online tutorials. This way, the content written for memory management challenges is backed with indisputable facts stated and proven true by professionals. The method used for writing memory management challenges also provided more obvious content choices for the group member who is tasked with writing memory management recommendations to choose from as some points are applicable to be used as their main points as well.

Although I mostly performed above average levels, I did find some of my areas for improvement in the assignment. One of them is that I should have been more active and become the conversation initiator in the assignment group. While I did converse with my group members moderately, it is still usually a type of communication that is unorganized and unfruitful, which does not help the group achieve the level of clarity for assignment progresses. To correct my mistakes, I should have shown more leadership in the group and make clear of assignment objectives and roles, so group members have full awareness of their responsibilities and consequences of forfeit.

Moreover, the diagrams and graphics I used to provide more context in my work in memory management challenges can be improved as well. Instead of using the original diagrams used in my references, I can also choose to draw them out myself using my knowledge of the issues. This increases the originality of my work and simplifies complex ideas of the challenges. Unfortunately, I did not think I had enough time to do it at the time of writing about my tasked topic. Besides these improvements, I feel that my performance is satisfactory and conforms to general expectations.

All in all, I felt that I have personally grown as an individual after working in the group assignment. Working in a group have re-emphasized my perception on the importance of teamwork and cooperation with different individuals to get work done as efficiently as it is perfectly. It has allowed me to build on my character in terms of attitude and social personality, which were aspects of my life that were slightly lacking. It also gave me more ideas on ways to improve my overall performance in upcoming groupworks. This experience definitely helped me realize that making peace with group members also help relieve stress as academic work starts piling up, and that they are very willing to help one another to distribute workloads so that one does not have to shoulder all the burdens by themselves.

2. 0207778 Saw Keat Loon

There are a few concepts and contents that are discussed in the group task. One of the concepts is the relationship between security threats and security recommendations. Although there are various kinds of security threats such as malware and DoS attacks, there are solutions to solve and prevent them. Security software acts as a firewall to incoming attacks and even assists users in scanning and removing any detected threats in the computer. Memory management also plays an important role in securing and managing local data on a computer. With proper memory management such as managing fragmentation, allocation and deallocation of memory will greatly increase the performance of the computer by reducing memory and performance wastage.

Some of my personal contributions towards the completion of the group task is by completing the security threats. There are various kinds of security threats that are available on the Internet. Thus, it is important to select the kinds that suit for the case study such as malware attack and denial of service (DoS).

When completing the given task, there are a few strengths and room for improvement shown. One of the strengths is effective time management. I have planned out my days ahead in completing the group task by making a timetable and following it. Doing so enables me to not be in a rush and have some spare time if there are corrections. Besides that, creativity is shown throughout the report. I have decided to include some diagrams and figures in the report to make it much more enjoyable to read. The diagrams and figures are also created by own hands to avoid copyrights.

Although there are quite a number of strengths shown when doing the group task, areas of improvement should not be ignored. Content management is an area where things could be improved. I have the tendency to write things more than needed in case of insufficient or incorrect points. That habit increases my chance of going over the page limit that is placed in the group task. The second area of improvement is communication skills. In the early phase of giving out tasks, there were a few misunderstandings between the members. Misunderstanding occurs because of the lack of context when telling something to the other person and causes confusion.

To complete the given group task, critical thinking, analysis and research are required. Some good amount of effort is given into researching due to the huge amount of content that is available on the Internet. I have filtered and determined what is needed and what is not when doing my research so that I can save some time and energy. Analyzing the gathered information is a crucial step in completing the group task. Instead of having only text, I have decided to have figures and diagrams. Figures and diagrams make the report to be more enjoyable to read and might ease people to understand some concepts. Critical thinking is also applied when determining if the gathered data matches with the case study. Critical thinking comes in naturally when gathered data are being analyzed to determine what is best for the group task.

Upon completion of the report, I learned a better way to manage my time. Initially I will just place priority in each assignment based on their submission date. However, I have changed my approach by doing the simplest first. Completing the easiest will enable me to not spend too much time on the hard assignment. Communication and critical thinking skills also are improved. To complete the task given, I am required to do tons of research on the Internet. Analyzing and applying critical thinking on the gathered data to finalize them. I am able to finish the report by going a different route such as including various kinds of diagrams and figures.

3. 0207737 Tan He Xiu

Since this assignment is a group task, we have been hired as a consultant by the company called OxTech Corporation and I am in charge in security recommendation. This company is a leading technology that creates and supports the operating system used by millions of users from worldwide. Recently, OxTech Corporation facing some extreme problem and challenge that related to managing memory and maintaining security. The problems and challenges which are the data loss and harming user privacy have outcome the system failure, performance degradation and security breaches are suffered by the company OxTech Corporation. Me as the consultant who in charge of security recommendation must analyse and suggest some possible solution to deal with the problems that company has faced.

With the task given by leader, which is in charge of security recommendation, I have to recommend additional or make some improvement for security mechanisms such as, access control, encryption, intrusion detection systems and firewalls. This is to reduce the previously mentioned security risks. I strongly show my research skill that I have gather all the information that I can found in google that related to security recommendation. All the sources that I have found is strongly reliable and can helps with the company OxTech Corporation to solve the issues that they have faced. All the points such as access control, encryption, intrusion detection systems and firewalls, I have clearly explained how they work and help to the company and provide some relevant examples to strengthen the points.

Even though I have suggested 4 elements of security recommendation, personally I still think there is a lot of improvement to make. For example, I can give more recommendation up to 8 elements, provide more relevant examples to make the elements look clearer and so on. Due to the time and other personal work, I also show my professional skill on handling this assignment and manage to complete on time. Through this group work, I manage to find out teamwork and team communication is the key point on this group task. Teammates also explain their task to me such as case analysis, memory management recommendation and security threats to make me more clearly on this assignment. All the information they have given me, I can provide more clearly in security recommendation.

In a nutshell, in this assignment I have learn about how to teamwork with teammates, communication with them, ability on research security for OxTech Corporation and self-thinking for the examples. Other than that, in future I will make more improvement for myself in future assignment and hope it smooth and successful.

4. 0207738 Mrigesh A/L Perbakaran

All through the OxTech Working Framework contextual analysis, I acquired significant experiences into the intricacies of memory the board and security challenges looked by innovation organizations in keeping up with and fostering a working framework. A thorough comprehension of these ideas and their real-world effects on system stability, performance, and user privacy was necessary for this task.

My personal contribution to the group task consisted of conducting extensive research on memory management recommendations. I effectively partook in meetings to generate new ideas with the group to distinguish possible answers for OxTech's difficulties and given my basic examination of each proposed arrangement. In addition, it was my responsibility to compile and arrange the data into a cohesive report, ensuring that our recommendations were effectively communicated and supported by solid evidence.

One of my assets during this gathering task was my capacity to combine complex specialized data and make sense of it in a reasonable and brief way. I had the option to get a handle on the subtleties of different memory the ideas, which permitted me to contribute significant thoughts during our conversations. Moreover, I effectively drew in with my members, empowering open correspondence and encouraging a cooperative climate.

Notwithstanding, I likewise perceived regions for development. I realized how crucial it is to keep up with the most recent developments and trends in technology and operating systems given their rapid evolution. There were minutes where I believed I might have dug further into specific subjects, particularly those connected with arising security dangers and state of the art memory advancement methods.

My singular exploration, examination, and decisive reasoning abilities were scrutinized during this contextual analysis. Based on the requirements of OxTech's operating system, I had to weigh the advantages and disadvantages of several potential solutions. By considering the ramifications of every decision, I could add to the advancement of balanced suggestions.

Generally, the OxTech Working Framework contextual investigation was a difficult and compensating experience. It permitted me to apply my insight, research abilities, and decisive abilities to reason in a functional setting. Going ahead, I expect to keep assembling my aptitude in memory the board, security, and arising advances to more readily address future difficulties in the field of working framework advancement and give significantly more hearty and creative arrangements.

References

AfterAcademy (2020) *What is Fragmentation and what are its types?* Available at: https://afteracademy.com/blog/what-is-fragmentation-and-what-are-its-types/ [Accessed 23 July 2023].

Cyberark (no date) *Malware Attacks.* Available at: https://www.cyberark.com/what-is/malware/#:~:text=Malware%20attacks%20are%20any%20type,infrastructure%20without%20end%2Duser%20knowledge (Accessed: 15 July 17, 2023).

Cisco (no date) *What Is a Worm.* Available at: https://www.cisco.com/c/en/us/products/security/what-is-a-worm.html#~steps-of-a-worm-attack (Accessed: 15 July 2023).

IAPP (no date) *Augmented Reality and Virtual Reality: Privacy and Autonomy Considerations.* Available at: https://iapp.org/resources/article/augmented-reality-and-virtual-reality-privacy-and-autonomy-considerations/.

Imperva (no date) *Buffer Overflow Attack.* Available at: https://www.imperva.com/learn/application-security/buffer-overflow/ (Accessed: 16 July 2023).

Imperva (no date) *Ping flood (ICMP flood).* Available at: https://www.imperva.com/learn/ddos/ping-icmp-flood/ (Accessed: 17 July 17, 2023).

Lampropoulos, G. *et al.* (2022) *Augmented reality and gamification in education: A systematic literature review of research, applications, and empirical studies*, *MDPI*. Available at: https://www.mdpi.com/2076-3417/12/13/6809.

Lee, H.-W., Kim, S. and Uhm, J.-P. (2021a) *Social Virtual Reality (VR) involvement affects depression when social connectedness and self-esteem are low: A moderated mediation on well-being*, *Frontiers*. Available at: https://www.frontiersin.org/articles/10.3389/fpsyg.2021.753019/full.

Lin, J. and Latoschik, M.E. (2022) *Digital Body, identity and privacy in Social Virtual reality: A systematic review*, *Frontiers*. Available at: https://www.frontiersin.org/articles/10.3389/frvir.2022.974652/full.

Kanade, V. (2023) *What Is Virtual Memory? Meaning, Architecture, Benefits and Challenges.* Spiceworks. Available at: https://www.spiceworks.com/tech/devops/articles/what-is-virtual-memory/ [Accessed 23 July 2023].

Kay, R. (2000) *Memory Leaks and Garbage Collection.* ComputerWorld. Available at: https://www.computerworld.com/article/2596992/memory-leaks-and-garbage-collection.html [Accessed 23 July 2023].

Kernel SIG (2022) *Solutions to Memory Corruption and Memory Leak.* Alibaba Cloud Blog. Available at: https://www.alibabacloud.com/blog/solutions-to-memory-corruption-and-memory-leak_599371 [Accessed 23 July 2023].

Malwarebytes (no date) *Computer Virus.* Available at: https://www.malwarebytes.com/computer-virus (Accessed: 15 July 2023).

Neha, T. (2019) *Memory Allocation.* BinaryTerms. Available at: https://binaryterms.com/static-and-dynamic-memory-allocation.html [Accessed 23 July 2023].

Paloaltonetworks (no date) *What is a denial of service attack (DoS) ?*. Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos#:~:text=There%20are%20two%20general%20methods,the%20most%20common%20DoS%20attack. (Accessed: 16 July 2023).

Panigrahi, K.K. (2023) *Difference between Internal Fragmentation and External Fragmentation*. Tutorialspoint. Available at: https://www.tutorialspoint.com/difference-between-internal-fragmentation-and-external-fragmentation [Accessed 23 July 2023].

Philips, K. (no date) *Why ethics must be at the heart of augmented reality*, *World Economic Forum*. Available at: https://www.weforum.org/agenda/2022/08/ethics-not-technological-limits-will-be-the-guiding-factor-for-an-augmented-age/.

Ravenbrook (2023) *Memory Management Reference*. Available at: https://www.memorymanagement.org/mmref/begin.html [Accessed 23 July 2023].

Rouse, M. (2016) *Buffer.* Available at: https://www.techopedia.com/definition/2759/buffer (Accessed: 17 July 17, 2023).

Sheldon, R. (2022) *DEFINITION – memory management.* TechTarget. Available at: https://www.techtarget.com/whatis/definition/memory-management#:~:text=The%20OS%20is%20also%20responsible,emulate%20the%20computer%27s%20main%20memory. [Accessed 23 July 2023].

Thakur, S. (2022) *Understanding Paging In Operating System In Detail*. Unstop. Available at: https://unstop.com/blog/what-is-paging-in-os [Accessed 23 July 2023].

Watter, B. (2019) *Stack-Based Buffer Overflow Attacks: Explained and Examples.* Available at: https://www.rapid7.com/blog/post/2019/02/19/stack-based-buffer-overflow-attacks-what-you-need-to-know/ (Accessed: 16 July 2023).

Webroot (no date) *Symptoms of Malware and How it Can Slow Your Computer Performance.* Available at: https://www.webroot.com/us/en/resources/tips-articles/malware-slow-pc (Accessed: 15 July 17, 2023).

COS3023/N OS & Concurrency
MARKING RUBRIC
ASSIGNMENT 1
Case Study Analysis Assessment (30%)

		Task A Group Task (70%) : CLO3 & CLO4							
LEARNING OUTCOME	**MARKING CRITERIA**	SCALE					YOUR MARKS/COMMENTS		
		Fail **(0-49)**	**3rd Class** **(50-59)**	**2nd Lower Class** **(60-69)**	**2nd Upper Class** **(70-79)**	**1st Class** **(80-100)**	**Marks**	**Weightage**	**Actual marks**
CLO3 : Analyse principal concepts and methods of memory management and file system implementation. (C4,PLO7) CLO4: Evaluate variety of security threats and	1.Case Analysis (7%)	The analysis of memory management challenges and security threats is insufficient or inaccurate. There is a lack of understanding of the issues faced by OxTech Corporation's operating system.	The analysis of memory management challenges and security threats is basic and provides some understanding of the issues faced by OxTech Corporation's operating system, but it lacks depth and critical analysis.	The analysis of memory management challenges and security threats demonstrates a satisfactory understanding of the issues faced by OxTech Corporation's operating system. The analysis provides some relevant information, but it may lack depth or critical analysis.	The analysis of memory management challenges and security threats is well-developed and demonstrates a good understanding of the issues faced by OxTech Corporation's operating system. The analysis provides relevant information and shows some critical thinking.	The analysis of memory management challenges and security threats is comprehensive, thorough, and demonstrates a deep understanding of the issues faced by OxTech Corporation's operating system. The analysis is insightful, supported by evidence, and shows critical thinking.	100	0.15	15

	2.Memory Management recommendations(7%)	The recommendations are incomplete or lack coherence. The student fails to address key concepts and techniques adequately, and the recommendations may contain significant errors or misunderstandings.	The recommendations are basic and partially address the given problem. The student demonstrates a basic understanding of memory management techniques but may have limitations in applying them effectively.	The recommendations are satisfactory and cover the essential aspects of the problem. The student demonstrates a good understanding of memory management techniques and their application but may lack depth or originality in the recommendations.	The recommendations are comprehensive and demonstrate a solid understanding of memory management concepts. The student provides well-reasoned and effective recommendations, considering different techniques and their advantages.	The recommendations are outstanding and reflect an exceptional understanding of memory management concepts. The student offers innovative and efficient recommendations, considers different techniques, and provides clear justifications for their choices.	100	0.2	20
	3.Security recommendations (15%)	The recommendations are insufficient or lack coherence. The student fails to address key security threats adequately, and the recommendations may contain significant errors or misunderstandings.	The recommendations are basic and partially address the given security threats. The student demonstrates a basic understanding of security mechanisms but may have limitations in applying them effectively.	The recommendations are satisfactory and cover the essential aspects of the security threats. The student demonstrates a good understanding of security mechanisms and their application but may lack depth or originality in the recommendations.	The recommendations are comprehensive and demonstrate a solid understanding of security concepts. The student provides well-reasoned and effective recommendations, considering different mechanisms and their effectiveness in mitigating threats.	The recommendations are outstanding and reflect an exceptional understanding of security concepts. The student offers innovative and robust solutions to address the identified security threats, considering various mechanisms and their effectiveness in mitigating threats.	100	0.2	20

4. Writing Style and Organization (10%):	The writing style and organization are poor. The student's work may contain numerous grammatical, spelling, or punctuation errors, and the structure and flow of the report may be unclear or confusing.	The writing style and organization are basic. The student's work demonstrates some attempt at clarity and coherence, but there may be frequent errors and inconsistencies in grammar, spelling, punctuation, or report structure.	The writing style and organization are satisfactory. The student's work generally communicates ideas effectively, with only occasional errors or inconsistencies in grammar, spelling, punctuation, or report structure.	The writing style and organization are good. The student's work is well-written and well-structured, with minimal errors or inconsistencies in grammar, spelling, punctuation, or report structure.	The writing style and organization are excellent. The student's work is polished and demonstrates exceptional clarity, coherence, and professionalism, with no grammatical, spelling, punctuation, or structural errors. The report is engaging, easy to follow, and effectively conveys ideas.	100	0.1	10
5. References (6%)	Inadequate inclusion of a list of high-quality references in the proper format; inconsistent or improper citations throughout the report.	Basic inclusion of a list of high-quality references in the proper format; some inconsistencies or improper citations throughout the report.	Adequate inclusion of a list of high-quality references in the proper format; generally consistent and proper citations throughout the report.	Well-presented inclusion of a list of high-quality references in the proper format; consistent and proper citations throughout the report.	Exceptional inclusion of a comprehensive list of high-quality references in the proper format; consistent and proper citations throughout the report.	100	0.05	5
					Total 70%:			70

Lim Zhe Yuan : MARKING RUBRIC

ASSIGNMENT 1
Case Study Analysis Assessment (30%)

LEARNING OUTCOME	MARKING CRITERIA	Task B Individual Task (30%) : CLO3 & CLO4							
		SCALE					YOUR MARKS/COMMENTS		
		Fail (0-49)	3rd Class (50-59)	2nd Lower Class (60-69)	2nd Upper Class (70-79)	1st Class (80-100)	Marks	Weightage	Actual marks
CLO3 : Analyse principal concepts and methods of memory management and file system implementation. (C4,PLO7) CLO4: Evaluate variety of security threats and propose appropriate OS mechanisms to protect against them. (C6,PLO7)	1.Self-Reflection(15%)	Demonstrates limited understanding of the concepts and content covered in the group task; lacks reflection on personal contribution and areas for improvement; does not evaluate individual research, analysis, and critical thinking skills; lacks insights into personal learning outcomes and growth.	Shows a basic understanding of the concepts and content covered in the group task; provides some reflection on personal contribution and areas for improvement; offers a limited evaluation of individual research, analysis, and critical thinking skills; provides some insights into personal learning outcomes and growth.	Demonstrates a clear understanding of the concepts and content covered in the group task; reflects on personal contribution and identifies some strengths and areas for improvement; evaluates individual research, analysis, and critical thinking skills to some extent; provides insights into personal learning outcomes and growth.	Exhibits a solid understanding of the concepts and content covered in the group task; reflects on personal contribution and assesses strengths and areas for improvement in a comprehensive manner; evaluates individual research, analysis, and critical thinking skills effectively; provides meaningful insights into personal learning outcomes and growth.	Demonstrates an exceptional understanding of the concepts and content covered in the group task; reflects on personal contribution with depth and precision, highlighting strengths and areas for improvement; evaluates individual research, analysis, and critical thinking skills comprehensively and critically; provides profound insights into personal learning outcomes and substantial growth.	100	0.15	15
	2.Peer Evaluation(15%)	Refer to the result in online peer evaluation form	Refer to the result in online peer evaluation form	Refer to the result in online peer evaluation form	Refer to the result in online peer evaluation form	Refer to the result in online peer evaluation form	100	0.15	15

				Total 30%:		30

Saw Keat Loon: MARKING RUBRIC								
ASSIGNMENT 1 **Case Study Analysis Assessment (30%)**								
LEARNING OUTCOME	**MARKING CRITERIA**	**Task B Individual Task (20%) : CLO3 & CLO4**						
		SCALE						
		Fail **(0-49)**	**3rd Class** **(50-59)**	**2nd Lower Class** **(60-69)**	**2nd Upper Class** **(70-79)**	**1st Class** **(80-100)**	**YOUR MARKS/COMMENTS**		
							Marks	**Weightage**	**Actual marks**

		Demonstrates limited understanding of the concepts and content covered in the group task; lacks reflection on personal contribution and areas for improvement; does not evaluate individual research, analysis, and critical thinking skills; lacks insights into personal learning outcomes and growth.	Shows a basic understanding of the concepts and content covered in the group task; provides some reflection on personal contribution and areas for improvement; offers a limited evaluation of individual research, analysis, and critical thinking skills; provides some insights into personal learning outcomes and growth.	Demonstrates a clear understanding of the concepts and content covered in the group task; reflects on personal contribution and identifies some strengths and areas for improvement; evaluates individual research, analysis, and critical thinking skills to some extent; provides insights into personal learning outcomes and growth.	Exhibits a solid understanding of the concepts and content covered in the group task; reflects on personal contribution and assesses strengths and areas for improvement in a comprehensive manner; evaluates individual research, analysis, and critical thinking skills effectively; provides meaningful insights into personal learning outcomes and growth.	Demonstrates an exceptional understanding of the concepts and content covered in the group task; reflects on personal contribution with depth and precision, highlighting strengths and areas for improvement; evaluates individual research, analysis, and critical thinking skills comprehensively and critically; provides profound insights into personal learning outcomes and substantial growth.	100	0.15	15
CLO3 : Analyse principal concepts and methods of memory management and file system implementation. (C4,PLO7) / CLO4: Evaluate variety of security threats and propose appropriate OS mechanisms to protect against them. (C6,PLO7)	1.Self-Reflection(15%)								
	2.Peer Evaluation(15%)	Refer to the result in online peer evaluation form	Refer to the result in online peer evaluation form	Refer to the result in online peer evaluation form	Refer to the result in online peer evaluation form	Refer to the result in online peer evaluation form	100	0.15	15
						Total 30%:			30

ASSIGNMENT 1
Case Study Analysis Assessment (30%)

Task B Individual Task (20%) : CLO3 & CLO4

LEARNING OUTCOME	MARKING CRITERIA	SCALE					YOUR MARKS/COMMENTS		
		Fail (0-49)	3rd Class (50-59)	2nd Lower Class (60-69)	2nd Upper Class (70-79)	1st Class (80-100)	Marks	Weightage	Actual marks
CLO3 : Analyse principal concepts and methods of memory management and file system implementation. (C4,PLO7) CLO4: Evaluate variety of security threats and propose appropriate OS mechanisms to protect against them. (C6,PLO7)	1.Self-Reflection(15%)	Demonstrates limited understanding of the concepts and content covered in the group task; lacks reflection on personal contribution and areas for improvement; does not evaluate individual research, analysis, and critical thinking skills; lacks insights into personal learning outcomes and growth.	Shows a basic understanding of the concepts and content covered in the group task; provides some reflection on personal contribution and areas for improvement; offers a limited evaluation of individual research, analysis, and critical thinking skills; provides some insights into personal learning outcomes and growth.	Demonstrates a clear understanding of the concepts and content covered in the group task; reflects on personal contribution and identifies some strengths and areas for improvement; evaluates individual research, analysis, and critical thinking skills to some extent; provides insights into personal learning outcomes and growth.	Exhibits a solid understanding of the concepts and content covered in the group task; reflects on personal contribution and assesses strengths and areas for improvement in a comprehensive manner; evaluates individual research, analysis, and critical thinking skills effectively; provides meaningful insights into personal learning outcomes and growth.	Demonstrates an exceptional understanding of the concepts and content covered in the group task; reflects on personal contribution with depth and precision, highlighting strengths and areas for improvement; evaluates individual research, analysis, and critical thinking skills comprehensively and critically; provides profound insights into personal learning outcomes and substantial growth.	100	0.15	15

	2.Peer Evaluation(15%)	Refer to the result in online peer evaluation form	Refer to the result in online peer evaluation form	Refer to the result in online peer evaluation form	Refer to the result in online peer evaluation form	Refer to the result in online peer evaluation form	100	0.15	15
					Total 30%:				**30**

		Mrigesh A/L Perbakaran: MARKING RUBRIC							
		ASSIGNMENT 1 **Case Study Analysis Assessment (30%)**							
		Task B Individual Task (20%) : CLO3 & CLO4							
LEARNING OUTCOME	**MARKING CRITERIA**	**SCALE**							
		Fail **(0-49)**	**3rd Class** **(50-59)**	**2nd Lower Class** **(60-69)**	**2nd Upper Class** **(70-79)**	**1st Class** **(80-100)**	**YOUR MARKS/COMMENTS**		
							Marks	**Weightage**	**Actual marks**
CLO3 : Analyse principal concepts and methods of memory management and file system implementation. (C4,PLO7) **CLO4: Evaluate variety of security threats and**	**1.Self-Reflection(15%)**	Demonstrates limited understanding of the concepts and content covered in the group task; lacks reflection on personal contribution and areas for improvement; does not evaluate individual research, analysis, and critical thinking skills; lacks insights into personal learning	Shows a basic understanding of the concepts and content covered in the group task; provides some reflection on personal contribution and areas for improvement; offers a limited evaluation of individual research, analysis, and critical thinking skills; provides	Demonstrates a clear understanding of the concepts and content covered in the group task; reflects on personal contribution and identifies some strengths and areas for improvement; evaluates individual research, analysis, and critical thinking skills to some extent; provides insights into personal learning	Exhibits a solid understanding of the concepts and content covered in the group task; reflects on personal contribution and assesses strengths and areas for improvement in a comprehensive manner; evaluates individual research, analysis, and critical thinking skills effectively; provides meaningful insights	Demonstrates an exceptional understanding of the concepts and content covered in the group task; reflects on personal contribution with depth and precision, highlighting strengths and areas for improvement; evaluates individual research, analysis, and critical thinking skills comprehensively	100	0.15	15

		outcomes and growth.	some insights into personal learning outcomes and growth.	outcomes and growth.	into personal learning outcomes and growth.	and critically; provides profound insights into personal learning outcomes and substantial growth.			
	2.Peer Evaluation(15%)	Refer to the result in online peer evaluation form	Refer to the result in online peer evaluation form	Refer to the result in online peer evaluation form	Refer to the result in online peer evaluation form	Refer to the result in online peer evaluation form	100	0.15	15
						Total 30%:			30