



TUNKU ABDUL RAHMAN UNIVERSITY OF MANAGEMENT AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATION TECHNOLOGY

BACHELOR OF INFORMATION TECHNOLOGY (HONOURS) IN INFORMATION SECURITY



Academic Year 2024/25

RIS 3 Semester 1 (Tutorial Group 3)

Assignment

BAIT3113 Systems Administration

2024/2025 (session 202405)

| Declaration | | | |
|---|------------------|---|---------------------------------|
| I declare that this assignment is free from all forms of plagiarism and for all intents and purposes is my own properly derived work. | | | |
| Student Name (Block Capital) | Registration No. | Signature | Marks (Lecturer / Tutor use) |
| WHELAN YAP BOON HONG | 23WMR02180 |  | |
| PANG JIN SIANG | 23WMR11552 |  | |

Tutor's Name: Ms. Chin Chai Lim

Date of Submission: 17 September 2024

BAIT3113 Systems Administration – Assignment Assessment Rubric (session 202405)Student Name: Whelan Yap Boon Hong Pang Jin SiangProgramme / Tutorial Group: RIS 3 Sem 1 Group 3Student Registration ID: 23WMR02180 23WMR11552**CLO2: Propose a basic system security to secure user accounts in the practise of professionalism. (A3, PLO11) – 100 marks**

| Category | Excellent | Good | Average | Poor | Points |
|---|--|---|--|---|--------|
| a. Introductory (CLO2) | Strong and well introduction of topic with well structure. (8-10) | Clear introduction of topic with acceptable explanation. (6-7) | Brief Introduction of topic with poor structure. (3-5) | Unclear or no introduction of topic. (0-2) | |
| b. Comparison of selected research topics between 2 platforms: Windows and Linux (CLO2) | Excellent comparisons of the selected research topics content between 2 platforms with well integrated effort to support finding. (16-20) | Show good comparisons of the selected research topics content between 2 platforms with some supports for the main finding. (11-15) | Show some comparisons of the selected research topics content between 2 platforms with minor integrated effort to support the finding. (6-10) | Show minor or no comparisons of the selected research topics content between 2 platforms with poor support or no support on the finding. (0-5) | |
| c. Selection & Justification on selected platforms (according to your chosen research topic). (CLO2) | Information clearly relates to the main topic. Points are clearly made. Analysis is sophisticated. (16-20) | Information clearly relates to the main topic. Points are made, but analysis is weak. (11-15) | Information clearly relates to the main topic. Points are insufficiently developed. Analysis is minimal. (6-10) | Information has little or nothing to do with the main topic. There is no critical analysis. (0-5) | |
| d. Conclusion (CLO2) | Conclusion is a concise, well-written summary of the argument. (8-10) | Conclusion is somewhat related to the research and argument. (6-7) | There is a conclusion but it is not obviously related to the research or argument. (3-5) | Poor conclusion with no argument. (0-2) | |
| e. Independence (CLO2 - Professionalism) | Always demonstrate a self-reliant attitude in all | Demonstrate a self-reliant attitude in most situations in | Sometimes demonstrate a self-reliant attitude in | Demonstrate dependency on other's guidance in | |

| | situations in performing the assigned task. (4-5) | performing the assigned task. (3) | general in performing the assigned task. (2) | performing the assigned task. (0-1) | |
|---|---|---|--|---|--|
| f. Understanding on Research Topic (CLO2 -Professionalism) | Excellent preparation and delivery of work. Excellent in explain the research topic finding in detail and well justify the thought / assumption made with proper reasoning. (8-10) | Adequate preparation and delivery of work. Able to explain the research topic finding and sometimes fair in justify the thought / assumption made. (6-7) | Lack of preparation of work and work delivered at average to below average standard. Able to explain and justify some parts / partial finding of the research topic or thought / assumption made. (3-5) | No preparation of work and work delivered in extremely low standard. Unable to explain and justify the finding of the research topic or thought / assumption made. (0-2) | |
| g. Work Originality (CLO2 - Ethics) | Product shows a large amount of original thought. Ideas are creative and inventive. Very minimal reference and citation used. All reference and citation are correctly written and present. (8-10) | Product shows some original thought. Some works show new ideas and insights with some other part of works use other people's idea / finding to support it. All reference and citation are correctly written and present. (6-7) | Product shows little original thought. Uses other people's ideas (giving them credit) and little evidence of original thinking. All reference and citation are included but sometimes one or two references / citation are incorrectly written. (3-5) | Product shows no original thought. Uses other people's ideas but does not give them credit (no reference/citation attached). (0-2) | |
| h. Work Responsibility (CLO2 - Professionalism) | Performed assigned tasks within the scope of work and beyond the scope of work with very little/no supervision and exceeds expectation. (8-10) | Performed assigned tasks within the scope of work with little supervision and overall meet expectation. (6-7) | Performed assigned tasks within the scope of work with close supervision and sometimes not meet expectation. (3-5) | Does not performed assigned tasks within the scope of work even with close supervision and not meet expectation. (0-2) | |
| i. Content Presentation (CLO2) | No grammatical, spelling or punctuation errors. & Information is very organized with well-constructed paragraphs and subheadings. (4-5) | Almost no grammatical, spelling or punctuation errors. & Information is organized with well-constructed paragraphs. (3) | A few grammatical spelling, or punctuation errors. & Information is organized, but paragraphs are not well-constructed. (2) | Many grammatical, spelling, or punctuation errors. & The information appears to be disorganized. (0-1) | |
| Total Marks: | | | | | |



| | |
|--|--|
| | |
|--|--|

Comment: _____



Acknowledgement

I would like to express my deepest gratitude to the individuals and the authors of the online resources that have provided invaluable assistance and knowledge throughout the preparation of this report. I would also like to acknowledge the support of my fellow students, tutors, & lecturers at Tunku Abdul Rahman University of Management and Technology (TAR UMT). Their knowledge & suggestions have been invaluable throughout this process. Thank you all for your support and assistance.

| Student Name (Block Capital) | Registration No. | Signature |
|---------------------------------|------------------|---|
| WHELAN YAP BOON HONG | 23WMR02180 |  |
| PANG JIN SIANG | 23WMR11552 |  |

Programme & Tutorial Group : RIS 3 Sem 1 Group 3

Date : 16 September 2024

Table of Contents

| | |
|--|-----------|
| Introduction | 1 |
| Comparison | 2 |
| Secure File Sharing Methods | 2 |
| Secure File Transfer Methods | 4 |
| Selection & Justification of OS Platforms | 6 |
| Windows | 6 |
| Linux | 8 |
| Conclusion | 10 |
| References | 11 |
| Appendix | 13 |

Introduction

As technology advances rapidly, the way to handle information securely is becoming increasingly important, especially when it comes to highly sensitive information. Advanced security measures become more crucial than ever before due to the fact that most businesses nowadays use digital platforms to share & exchange data. In order to create a secure environment for data movement & management, *Secure File Sharing* & *Secure File Transfer* methods are utilized to fulfill the requirements.

Secure File Sharing & *Secure File Transfer* are two distinct but related concepts that involve prioritizing file security. As their name suggests, *Secure File Sharing* refers to sharing digital files in a secure way with other entities while also protecting it from being accessed by unauthorized users. It typically involves the implementation of various security protocols such as data encryption & access controls before an entity is allowed to access the shared files (**Lindstrum, 2020**). Some of the service providers that provide secure file sharing include Google Drive & Dropbox.

Features of Secure File Sharing

| Features | Description |
|-------------------------------|---|
| Data Encryption | <ul style="list-style-type: none">• Uses algorithm to render the information into unreadable text• Only authorized entities can decode the information |
| 2-Factor Authentication (2FA) | <ul style="list-style-type: none">• Additional steps are needed to further verify identity• Access is only granted if the additional step is completed |
| Permission-based User Role | <ul style="list-style-type: none">• Admin can assign the actions allowed for different roles• Easier to manage information access |
| Watermarking | <ul style="list-style-type: none">• Can be visible or hidden on a document• Act as a deterrence for sharing of information without consent• Contain personally identifiable information for easier tracing in case information got leaked |
| Audit Logs | <ul style="list-style-type: none">• Record all activities in detail• Provide visibility of what is done to the document or file |

Secure File Transfer refers to the transmission or movement of digital files from one point to another through a secure & private channel, so that the data would not be intercepted, altered, or eavesdropped. The term “Secure” is highlighted as it uses encryption & other security measures to protect the data during transmission, unlike other regular file transfer methods which might send data plainly over networks (**Kiteworks, n.d.**). Some of the commonly used protocols that can fulfill the job are Secure File Transfer Protocol (SFTP), Secure Hypertext Transfer Protocol (HTTPS), etc.

Benefits of Secure File Transfer

Secure File Transfer ensures that the information is rendered unreadable even if it is intercepted by a hacker. It also helps the entity to comply with law, standards, & regulations as data protection is often set as the base requirements of information handling. Lastly, it protects the privacy of data by preventing information disclosure to unwanted entities.

Essential Features of Secure File Transfer

| Features | Description |
|---------------------------------------|--|
| Data Encryption (In Motion & Rest) | <ul style="list-style-type: none"> File is encrypted during transmission File is encrypted during storage while the decryption key is also placed at a separate location |
| Automated Virus Scanning | <ul style="list-style-type: none"> Virus scanning mechanism is triggered during each file uploads Ensure that the uploaded file does not affect other files Infected or suspicious files will be quarantined or deleted |
| Strong Password Enforcement | <ul style="list-style-type: none"> Admin can assign the actions allowed for different roles Easier to manage information access |
| Event Logging | <ul style="list-style-type: none"> Provides detailed information about all the activities Make it easier to trace the cause of an event |
| Strong Authentication | <ul style="list-style-type: none"> Not limited to username & password authentication Authenticate through other means, such as SSL FTP that authenticates certification (<i>Villanueva, 2022</i>) |

Comparison

The OS platforms that are chosen for comparison are Windows & Linux due to their wide usage while also offering a range of tools & protocols to facilitate secure file sharing & secure file transfer. However, both systems have different methods & approaches to perform the tasks mentioned above due to their different nature.

Secure File Sharing Methods

File Server Resource Manager (FSRM)

FSRM is a Windows Server feature that is available **exclusively in Windows**. It provides role-service for administrators to manage & secure files in the server's data storage. It classifies the files & performs tasks automatically based on the classifications, such as defining the quota for different folders & creating reports regarding the storage usage (*Microsoft, 2023*).

The main features of FSRM are its quota management, file classification, file management, file screening, & reporting mechanism. FSRM allows the administrator to define the limit allowed for folder & volumes and will be automatically applied to the new folders created on the volume to ensure fair resource allocation. File classification rules can be set to classify the files automatically while also applying policies based on the classification. For file management, policies can be set & applied to trigger actions such as expiring files, encrypting files, or other custom commands. The administrator is able to manage file screening by controlling what types of files are allowed to be stored in the file server to prevent storage of unauthorized file types. Lastly, FSRM provides detailed reports on the file for better monitoring to the administrators, which works similarly like a log (*Microsoft, 2023*).

Network File System (NFS)

NFS is a file sharing protocol that is available on ***both Windows & Linux***. It allows the system to share directories & files over a network, allowing file access on remote systems as if the file is a local file (*Ubuntu, n.d.*). Although both Windows & Linux support NFS implementation, it was originally developed as a protocol for the Unix environment & best suited for Linux-based network architectures for network file sharing purposes (*AWS, n.d.*). Windows on the other hand, NFS is added by Microsoft later on to enable interoperability with Unix & Linux systems. NFSv4 is recommended as it enforces file

locking, which refers to only one process or user having exclusive access to a file at a time to prevent simultaneous file modifications, resulting in potential inconsistent results. The lock will be released once the process or user is done with the file (**Steiner, 2023**).

By default, NFS is not that secure due to not providing any form of encryption, which may result in data storing (**Synology, 2023**). In order to achieve a more secure file sharing, Kerberos can be set up in NFSv4 as a security mechanism that provides user authentication, data encryption & removes UID/GID matching requirements to simplify user management & access control. NFSv3 is usable too, however it does not provide full coverage of the Kerberos functionality (**ArchLinux, 2024**). It has 3 commands that provide data protection as shown below (**Steiner, 2023**).

| Command | Function |
|---------|--|
| krb5 | <ul style="list-style-type: none"> Used to secure authentication Encryption is not used however Kerberos ticket is used for identity verification Only legitimate entities can request & access the shared files |
| krb5i | <ul style="list-style-type: none"> Used to ensure data integrity An extension of krb5 by adding a validation layer to ensure that data is unaltered during transmission between client & server Secure checksums is used for integrity checking (Microsoft, 2024) Does not encrypt data |
| krb5p | <ul style="list-style-type: none"> Used to ensure data privacy Offers the highest level of security by using both authentication & encryption Data is encrypted during transmission to prevent eavesdropping or interception |

| | Windows | Linux |
|-------------------------------------|--|--|
| Reporting | <ul style="list-style-type: none"> - Has built-in reporting capabilities such as Event Viewer & Server Manager - The report only provides a basic overview, 3rd party tools are needed for more advanced reporting needs | <ul style="list-style-type: none"> - Highly customizable due to existing command-line utilities (nfsstat) - Can be integrated with system logs for customized reporting - Provide in-depth performance metrics related to file systems & NFS (iostat) |
| Convenience & Complexity | <ul style="list-style-type: none"> - Requires additional steps for setting up Windows Server as KDC as it is not native - More user-friendly due to GUI | <ul style="list-style-type: none"> - Configuration is straightforward as it is supported natively - Configuration is done via CLI, making it less user-friendly - Provide better flexibility in terms of security configuration but require deep understanding of the environment |

Secure File Transfer Methods

Secure File Transfer Protocol (SFTP)

SFTP, also known as SSH File Transfer Protocol, allows the users to transfer files remotely in a secure way via encrypted SSH data stream. It is a protocol that is natively supported in the Linux environment initially. The characteristics of SFTP are as shown below (**Cohen, 2023**).

| Characteristic | Description |
|------------------------------|---|
| Encrypted Connection | <ul style="list-style-type: none"> Data are encrypted during transmission via an SSH tunnel to protect the confidentiality & integrity of files |
| Standard SSH Port | <ul style="list-style-type: none"> Port 22 is the default SSH port used to make secure connections to remote devices Root login can be disabled or use strong passwords for authentication to make the port more secure |
| Cross-Platform Compatibility | <ul style="list-style-type: none"> File can be transferred cross-platform as it is supported on widely used OS, such as Windows, Unix, & macOS |
| Speed | <ul style="list-style-type: none"> Can transfer smaller files faster due to less protocol overhead compared to other file transfer methods |

Both **Windows & Linux support SFTP**, however, the way that it is being implemented & set up is different in terms of complexity & convenience.

On the Linux side, SFTP is natively supported & enabled by default when OpenSSH is being installed and configured. UNIX-based file permissions & Access Control Lists (ACLs) are used to manage access control, such as using `chmod` or `chroot` to restrict access. The setup of SFTP is also more convenient as it is bundled with OpenSSH. Linux is also more efficient in terms of handling network services, which results in better performance in high-demand server environments (**Lee, 2024**). The “downside” for using Linux is that it is often managed through CLI, which makes it not be that user-friendly for inexperienced users.

On the Windows side, SFTP is only natively supported starting from Windows 10 & Windows Server 2019. OpenSSH must be installed in order to perform encryption during file transfer (**Young, 2024**). However, for the earlier version of Windows, 3rd party software must be installed in order to allow the machine to be used as a SFTP server. Although OpenSSH has been built-in since Windows 10, setting up SFTP still needs additional steps, such as using PowerShell. The upside of using Windows for SFTP is that it provides both GUI & CLI controls, allowing users to choose how they operate. However, GUI comes with the price of being more resource consuming.

Applicability Statement 2 (AS2)

AS2 is a HTTP-based protocol that is used to transmit messages over the Internet that are supported by **both Windows & Linux**. It is commonly used for Electronic Data Interchange (EDI) in the industry, which refers to the document exchange between computers (**EDI Basics, n.d.**). This protocol builds messages in MIME format & sends it over HTTP(S) via SSL tunnel (**Informatica, 2022**). The security features of AS2 are shown below (**SeeBurger, n.d.**).

| Security Feature | Description |
|--------------------|---|
| Encryption | <ul style="list-style-type: none">Commonly used encryption algorithms are utilized (AES, 3DES) to secure data confidentiality |
| Digital Signatures | <ul style="list-style-type: none">Verifies the data is untampered during transmission to ensure integrityAuthenticate the sender to confirm that the data comes from a trusted source |
| SSL/TLS | <ul style="list-style-type: none">Establish encrypted communications between client & serverEnsure that data cannot be intercepted or tampered by unauthorized entities while ensuring the confidentiality |

Although the security it provides is strong, the configuration for AS2 can be troublesome & requires careful consideration while also needing personnel with specialized knowledge towards the topic. First of all, AS2 utilizes HTTPS that has the ability to sign & encrypt data with known certificates. It is crucial for the organizations to have their web server certificate signed by a known certificate authority to reduce the risks of disruption as the certificates are exchanged with their partners (**SeeBurger, n.d.**). Besides that, the organization must also communicate to ensure that their AS2 systems agree on the protocols, encryption standard, & other settings to ensure secure & smooth data transmission.

For Windows, the implementation of SSL/TLS is more straightforward & is also more user-friendly due to GUI. The setup process is also easier with the guidance of wizard & GUI. However, the licensing fees for Windows platform are often expensive, which can be a burden for smaller organizations. The GUI nature of Windows also tends to consume more resources.

For Linux, the implementation of SSL/TLS requires manual configuration with other tools, such as OpenSSL, but ACLs can be used to further configure the access control involved in AS2 data transfer. As Linux is open source, the costs for licensing can be waived. Besides that, Linux typically performs better in terms of resources utilization & speed (**Shining International, n.d.**), allowing it to shine at high-demand environments. The downside of the Linux platform is its CLI that can grant greater controls for familiar users but can be challenging for unfamiliar users.

Selection & Justification of OS Platforms

It is important when we are selecting the protocols or methods to be used for secure file sharing & secure file transfer in different platforms. This is because we need to consider the specific needs of the environment in which OS the methods will be deployed. Both Windows & Linux offer different advantages and disadvantages that make them suitable for different use cases.

Windows

Advantages

One of the key advantages that make Windows dominant in its industry market (more than 68% of the market share) is the **user-friendly interface** that it offers. The interface provided has high learnability & is intuitive, making it accessible to users with varying levels of technical knowledge, ranging from unfamiliar new users to users that are familiar with the technical aspect of things. This also contributes to the ease of use of the OS, which is beneficial for businesses as it reduces the training time needed for the staff who are responsible for managing the system but not that familiar with technical controls. As training time is reduced, the same also goes for the training costs, helping the company or enterprise to save money for other expenses.

As Windows is developed by Microsoft, it also allows **integration with the Microsoft Ecosystem**, such as OneDrive for cloud storage, Bitlocker for encryption services, File Explorer for efficient file management, and Active Directory for user & group management. By combining these tools together into the platform, it greatly simplifies the process of administrative tasks. If the organization has already adopted services provided by Microsoft, it may greatly benefit them as it streamlines the processes of encryption, file sharing, & user management, which is crucial for secure file sharing & secure file transfer that highlights security for protecting sensitive information. In short, the advantage of being able to integrate various Microsoft tools make Windows a solid choice for organizations that emphasize on file security.

Microsoft **provides extensive documentation, support resources, & regular updates** for its developed OS, Windows. This is especially important for maintaining a secure file sharing & transfer environment. All these supports given are helpful for companies or enterprises to maintain a secure business operation continuity. The documentation provided includes the guidelines & instructions on how to configure & manage the features provided by Windows, allowing the responsible personnel to learn & resolve any issues that surface. Support services for Windows given by Microsoft include help desks & forums that allows them to get assistance on troubleshooting or resolve any complex technical issues in case the documentation provided is not understood. Regular security patches & updates are also constantly provided by Microsoft to help the Windows users to protect against newly discovered vulnerabilities.

Disadvantages

One of the downsides that Windows has is its **pricing**. Although it does not directly impact personal or business operations by using the platform, it may become a factor that the entity needs to consider in terms of financial aspect. Windows is known for its expensive pricing, hence it is not strange that most people use the pirated version of Windows. As a matter of fact, most of the devices that come with a pre-installed Windows are most probably the pirated version (***FP Explainers, 2022***). For instance, the legitimate Windows 11 Home costs RM 919 per licence, which is nearly the price of a cheap laptop for work use or $\frac{1}{3}$ of an average Malaysian monthly salary. As for business use, Windows 11 Pro costs nearly RM1300 per license, which can accumulate to a huge amount of money for enterprises that adopt large usage of computers due to 1 license being limited to 1 device only. Microsoft, the developer of Windows, allows pirated use of Windows if it is limited to personal private use only, however that is not the case for businesses or corporations. Microsoft takes the piracy of Windows for business uses very seriously, notices will be sent to the respective businesses if they found out that

business use computers are not using the legitimate Windows license (**FP Explainers, 2022**). If the notices sent are ignored, the businesses may face legal actions taken against them. In short, Windows license's expensive pricing acts as a barrier for entities that want to adopt Windows as their operating system, leading them to consider using other cheaper alternatives.

Windows, an OS that is being widely used, is known for being **resource-intensive**. As time advances, the software that we use will slowly but surely evolve over time. In other words, the size of the software will increase due to the new updates for more functionality & support to the platform. Usually, an OS that has been updated will consume slightly more resources (RAM & CPU) than its previous version. However, the additional minor resource consumption from the continuous updates will definitely stack up, eventually adding up into an amount of additional resources consumption that cannot be overlooked, which can be easily noticeable if the device is slowing down or acting badly in terms of performance. In order to resolve the performance issue, additional costs are required to upgrade the hardware so that the device can run smoothly & efficiently such as adding RAM or replacing a better CPU for processing. However, the solution above can only serve as a temporary measure because Windows are being updated constantly, meaning that the upgraded hardware will still reach its limit in the future, demanding for further upgrades. Although the utilities can be turned off from the startup list in Windows to ensure that the device uses fewer resources, it can be quite tricky & difficult to know which utilities can be disabled so that it would not disrupt the usage & operation (**Notenboom, 2019**). If the above situation is being related to a business, whether it to be a small-sized company or a large enterprise, the additional incurring costs can be quite significant, not to mention the already expensive costs that had to be paid for the Windows license. The company or enterprise cannot afford to avoid this issue either as it is directly related to their business operation, which performance is critical, hence they have no choice but to pay for the additional costs.

As Windows is an OS that is being widely used, it is natural that it offers robust security features to guard against various cyber attacks. However, its reputation also comes with the concern of needing to frequently be aware of new forms of cyber attacks as new Windows vulnerabilities will be exploited by cyber criminals due to its widespread use, making **Windows users a frequent target**. Windows users are required to keep their OS configured properly & updated regularly to protect against newly discovered vulnerabilities. Updating concerns can be resolved by enabling auto updates for new security patches, but there are companies that prefer to control their update timing just in case that the new updates may bring in new problems for the business operation. Configuration issues on the other hand, require personnel with specialized knowledge in the security settings provided by Windows as the configurations are done manually, some of the configurations include managing firewalls, setting access controls, enabling encryption, etc. Managing all the configurations can be challenging as it can be complex & time-consuming sometimes.

Linux

Advantages

Linux is an open-source platform, which means that it shares the advantages that other open-source platforms offer, including the aspects of securing file sharing & file transfer. First of all, Linux offers the **flexibility** of allowing personnel to set up custom security measures or make changes to the open-source code according to their specific needs to adapt the platform to the organization's needs (**Cemazar, 2022**). For instance, if an organization wants to block access to or from a specific address, custom rules can be created manually by using *iptables*. This command allows the organization to set which connections are allowed or denied, thus providing a security measure that is tailored to the organization's requirement, which is also applicable in securing file share & file transfer by customizing encryption algorithms & access permissions.

Unlike Windows, which requires their license to be purchased for legitimate use in a company or enterprise, Linux is a free open-source OS, meaning that it **saves the costs of licensing** by eliminating the purchasing fees associated with the use of proprietary operating systems like Windows. Additionally, Linux is known for being more efficient in terms of performance & resources usage as it runs fewer processes in the background, which is quite the opposite compared to Windows that runs a lot of processes in the background that consumes a considerable amount of the device's resources. This also relates back to the advantage of Linux being cost effective as it is lighter on the device's RAM, CPU, & storage (**Keegan, 2024**), not requiring the personnel or organization to have a costly set-up to adopt Linux, which also includes the need of upgrading a device's hardware to have an acceptable level of performance, making it a cost-effective solution for organizations looking to minimize their expenses.

Asides from being able to minimize expenses, Linux also offers **strong security** due to its nature of being open-source, allowing the community to look over the code for bugs identification & bug fixing. Besides that, Linux also requires full system access through password input in order to make any system changes or software installations, acting as a security barrier to prevent malicious programs from making damage to the system without the user knowing. Its design inherently minimizes vulnerabilities, and the availability of a wide range of open-source security tools allows users to enhance the platform's security further. Protocols like SFTP provide robust options for secure file transfer, ensuring data protection during file transmission. One of the factors that Linux is more secure than Windows is that its reputation is more obscure compared to Windows. Cybercriminal tends to design more malware targeting Windows systems but less for Linux as it is unusual for cybercriminal to target such a small group of Linux users (**Keegan, 2024**).

Disadvantages

The first downside of using Linux is its **complexity & steep learning curve** due to its CLI nature. This makes it difficult for users that are unfamiliar with Linux to work with it, making the configuration of securing file sharing & file transfer to be challenging. Hence, additional time, training, or technical expertise on Linux are required. Although Linux does provide GUI, most of its configurations are done through CLI and it is natural for companies or enterprises to instead adopt CLI-based Linux to save resources & costs since configurations are typically done through CLI anyways. If GUI is used, the organization will most probably choose to use Windows instead due to its design of having an intuitive interface & easy navigation unless license costs are being considered.

Another disadvantage that Linux has is its **limited support for proprietary software** that are often used for managing day-to-day operations. Some of the proprietary softwares include Microsoft Office tools, Adobe Creative Suite, etc. The softwares mentioned above are well-known & widely used but will have limited or no compatibility with Linux, making it difficult for the organizations to manage their daily operation that rely on the tools previously, therefore having to find alternatives, which may not be the feasible way. Being a proprietary software means that software updates & security patches are constantly being provided, Linux being not able to support these proprietary softwares cannot benefit

from their approach of using alternatives. If an organization is trying to shift to Linux as their OS, they need to consider if the available alternatives can replace the proprietary softwares the organization is using without having many trade-offs.

| Platform | Advantage | Disadvantage |
|----------------|---|---|
| Windows | <ul style="list-style-type: none"> • Has a user-friendly GUI for ease of use & navigation • Able to integrate with the Microsoft Ecosystem that provides a range of security tools • Has extensive documentation, support resources, & regular updates to assist users | <ul style="list-style-type: none"> • Expensive license for both home use & office use • Resource intensive due to many processes running in the background • Its widespread use makes it a frequent target for cyber criminals |
| Linux | <ul style="list-style-type: none"> • Flexible in terms of configurations • Cost-effective due to being open-source • Offers strong security configurations & settings | <ul style="list-style-type: none"> • Can be complex • Has a steep learning curve for new or unfamiliar users • Limited support for proprietary software that are commonly used for business operations • Its obscurity makes it a rare target for cyber attacks |

With the advantages & disadvantages listed, we can effectively know which kind of environment where each platform shines. Being a user that uses OS for **personal use**, I will choose **Windows** as my choice as it has an excellent UI for navigation, eliminating the need for having to study how to use the OS. Due to its intuitivity, I can simply navigate freely & eventually be able to know how to use it after a short amount of time without needing any guidance. However, if it's regarding security configurations, documentation which is provided by Microsoft may be needed.

If it is for organization's **business usage**, **Linux** is the preferred platform as usually it requires high performance, robust security, and flexibility for file sharing and transfer. Linux's open-source nature allows for more precise control over configurations, making it ideal for organizations that need to tailor their systems to specific security requirements and performance demands. It also helps the organization to save additional costs on the license for each device, which can be a considerable amount of money depending on how many devices the organization has.

Conclusion

In conclusion, both Windows and Linux provide powerful tools for secure file sharing and file transfer. Each OS platform has its advantages, as well as disadvantages, to fulfill different use cases. Windows, with its exclusive File Server Resource Manager (FSRM), provides a user-friendly and integrated solution that works well in environments that utilize active directory. Its support for secure file transfer methods like SFTP and AS2 make it a solid choice for organizations seeking for ease of use and centralized management.

Linux is an open-source platform that allows extensive customization and configuration, making it the preferred choice for organizations that emphasize cost saving, such as small business or individuals while also prioritizing security, performance and adaptability. Linux's capability of being able to perform efficiently on older or less powerful hardware makes it a cost-effective choice by eliminating the need for expensive hardware upgrades, especially for companies & enterprises that have a lot of devices. With its strong support for SFTP and AS2, it offers flexibility, scalability, and superior performance in high-demand environments.

Finally, the selection of an operating system for secure file sharing and secure file transfer should align with the entity's specific requirement, existing infrastructure and long term goals. For entities that seek for a highly customizable, secure, limited resource and cost-effective solution, Linux is always the better option to consider & choose from. On the contrary, entities that want ease of use and integration with existing Windows environments while also being generous on their budget, Windows is the better option.

[4500 words]

References

- Lindstrum, C. (2020, July 7). Secure file sharing: How the best systems actually work. SecureDocs. <https://www.securedocs.com/blog/secure-file-sharing-how-the-best-systems-actually-work>
- What is secure file transfer?* (n.d.). Kiteworks. <https://www.kiteworks.com/risk-compliance-glossary/secure-file-transfer-definition/>
- Villanueva, J. C. (2022, October 24). *10 essential attributes of secure file transfer systems*. JSCAPE. <https://www.jscape.com/blog/10-essential-attributes-of-a-secure-file-transfer>
- Cohen, C. (2023, October 20). *What is Port 22?* CBT Nuggets. <https://www.cbtnuggets.com/common-ports/what-is-port-22>
- Lee, K. (2024, June 4). *Why use Linux for servers in enterprise environments? A D...* Open Source Solutions for Enterprise Servers & Cloud | SUSE. <https://www.suse.com/c/why-use-linux/>
- Young, T. (2024, March 7). *Best file transfer for Windows: Evaluating SFTP vs. FTPS pros and cons*. Cerberus FTP Server. <https://www.cerberusftp.com/blog/best-file-transfer-for-windows-evaluating-sftp-vs-ftp-pros-and-cons/>
- File server resource manager (FSRM) overview*. (2023, March 21). Microsoft. <https://learn.microsoft.com/en-us/windows-server/storage/fsrm/fsrm-overview>
- NFS vs SMB - Difference between file access storage protocols - AWS*. (n.d.). Amazon Web Services, Inc. <https://aws.amazon.com/compare/the-difference-between-nfs-smb/>
- Network file system (NFS)*. (n.d.). Ubuntu. <https://ubuntu.com/server/docs/network-file-system-nfs>
- What can I do to encrypt NFS data transfer? - Synology knowledge center*. (n.d.). Synology. https://kb.synology.com/en-ro/DSM/tutorial/what_can_i_do_to_encrypt_data_transmission_when_using_nfs
- Steiner. (2023, January 31). *NFSv3 and NFSv4: What's the difference?* NetApp Community. <https://community.netapp.com/t5/Tech-ONTAP-Blogs/NFSv3-and-NFSv4-What-s-the-difference/ba-p/441316#toc-hld-1705566247>
- NFS/Kerberos*. (2024, March 23). ArchWiki. Retrieved August 31, 2024, from <https://wiki.archlinux.org/title/NFS/Kerberos>
- Performance impact of Kerberos on Azure NetApp files NFSv4.1 volumes*. (2024, February 7). Microsoft. <https://learn.microsoft.com/en-us/azure/azure-netapp-files/performance-impact-kerberos>
- What is EDI (Electronic data interchange)?* (n.d.). EDI Basics. <https://www.edibasics.com/what-is-edi/>
- Seeburger: What is AS2? AS2 is a protocol for transmission of EDI messages*. (n.d.). SeeBurger. <https://www.seeburger.com/resources/good-to-know/what-is-as2>
- As2 (S/Mime over HTTP(S))*. (2022, September). Informatica. <https://docs.informatica.com/data-integration/b2b-data-exchange/10-4-0/user-guide/encryption/as2--s-mime-over-http-s--.html>
- Advantages and disadvantages of Linux compared with windows*. (n.d.). Shining International. <https://www.shiningltd.com/what-are-the-advantages-and-disadvantages-of-linux-compared-with-windows/>

Explained: Why Windows 11 failed to take off like Windows 7 and 10. (2022, April 18). Firstpost.
<https://www.firstpost.com/tech/news-analysis/explained-why-windows-11-failed-to-take-off-like-windows-7-and-10-10569611.html>

Notenboom, L. A. (2019, August 15). *Why is Windows 10 using more and more RAM?* Ask Leo!.
<https://askleo.com/why-is-windows-10-using-more-and-more-ram/>

Keegan, K. (2024, March 12). *Linux vs. Windows: Which is more secure?* PIA VPN Blog.
<https://www.privateinternetaccess.com/blog/linux-vs-windows/>

Appendix

Originality report

COURSE NAME

BAIT3113 SA (Practical Class)

STUDENT NAME

WHELAN YAP BOON HONG

FILE NAME

BAIT3113_System Administration Assignment_RIS3 S1 G3_ Whelan Yap Boon Hong_ Pang Jin Siang

REPORT CREATED

Sep 16, 2024

Summary

| | | |
|-----------------------|---|----|
| Flagged passages | 7 | 2% |
| Cited/quoted passages | 6 | 1% |