**Week 8 Assignment**

**Case Study: Linux Server Best Practices**

Prof. Kristen Macdonald

Group No. 4

* **STRONG PASSWORD MANAGEMENT**
* **Avoid unnecessary software**
* **UPDATE SOFTWARE REGULARLY**

**STRONG PASSWORD MANAGEMENT**

**Unique and Complex Passwords**

At MOJOINC, it is essential to enforce the usage of distinct and complicated passwords for user accounts on the Ubuntu server. Both administrative and standard user accounts are affected by this. MOJOINC guarantees that unauthorized access attempts are reduced by employing passwords that are distinctive and challenging to guess.

**Length and Complexity**

Stress the importance of using passwords that adhere to our specified length and complexity specifications on our Ubuntu systems. We increase password complexity and make them more resistant to hacking attempts by promoting the use of a mix of uppercase and lowercase letters, digits, and special characters.

**Do not Use Common Passwords**

Encourage our server users at MOJOINC not to use widely used passwords. These passwords are easier to crack using automated hacking tools or dictionary assaults. Encourage choosing one-of-a-kind passwords that reflect your personality and are difficult to find in password databases. (Choosing and Protecting Passwords | CISA, 2009)

**Using two factors to authenticate (2FA)**

Consider using two-factor authentication on our Ubuntu servers where it is practical to do so. By requiring a second form of verification in addition to the password, such as an OTP app or a hardware token, this additional layer of security offers an additional layer of protection. (NIST Special Publication 800-63B)

**Password Managers**

We may advise our administrators to use trusted password manager software to simplify password management for our Ubuntu systems. This makes managing many passwords easier while generating strong, unique passwords and securely storing them.

**Regular Password Updates**

On our Ubuntu servers at MOJOINC, impose a rule requiring regular password updates. To maintain a better level of security, remind users, particularly administrators, to update their passwords frequently with new, secure ones.

**Reliable Storage**

We must take care to properly encrypt and securely store passwords on our Ubuntu servers. Passwords should not be kept in files with easy access or in plain text. Use effective encryption techniques and follow the suggested password storage security procedures.

**User Access Control**

Implement robust user access control mechanisms on our Ubuntu servers. Assign appropriate permissions and privileges based on the principle of least privilege, ensuring that only authorized personnel have administrative access to critical resources.

**Monitoring and Auditing**

Implement auditing and monitoring tools on our Ubuntu servers to track and report user login actions, including password-related events. Review and examine logs frequently to spot any unusual activity, investigate security breaches right away, and keep a proactive security posture.

**Learning and Training**

At MOJOINC, regularly educate and teach our server admins and users on the best practices for password security. Emphasize the need of keeping excellent password hygiene while teaching people how to generate strong passwords, identify and prevent social engineering attempts, and construct strong passwords.

**Avoid unnecessary software**

**Reduced Attack Surface**

MOJOINC limits potential entry points for cyber threats by decreasing the installation of unused software. Software that is not required frequently adds new security risks and vulnerabilities that can be abused by bad actors. We reduce the overall risk to our systems and data by maintaining a lean and focused software inventory.

**Enhanced System Performance**

Software that is not required uses up system resources such as the CPU, memory, and storage. MOJOINC promotes optimum system efficiency by preventing the installation of software that is not directly relevant to our business demands. As a result, our employees' response times are quicker, their productivity is higher, and their workflow is more effective. (National Cybersecurity Alliance, 2023)

**Simplified IT Management**

MOJOINC lowers the complexity and work needed for IT management by maintaining an optimized software environment. Software that is not required frequently needs additional patches, updates, and maintenance, which puts a load on our IT infrastructure. We optimize our IT operations and free up key resources for more important activities by concentrating on fundamental software programs and technologies.

**Cost Savings**

The budget for MOJOINC may be impacted by unnecessary software licenses, subscriptions, and maintenance costs as they accumulate over time. We would drastically cut unnecessary costs and more efficiently manage resources by refraining from buying software that is either redundant or does not support our company's goals.

**Minimized Software Conflicts**

Software conflicts and compatibility problems are more likely to arise when redundant software is installed. Conflicts like these can cause system instability, crashes, or even data loss. MOJOINC reduces the danger of these conflicts by thoroughly examining the requirement and compatibility of software programs, resulting in a more stable and dependable computing environment.

**Improved User Experience**

MOJOINC makes sure that our staff has access to the equipment and software they require to complete their jobs successfully by concentrating on the essential software. The user experience is improved by a simplified software environment that reduces complexity and complexity and makes it simpler for users to find, navigate, and use the software they rely on.

**Compliance and Licensing**

MOJOINC can manage software licenses and ensure adherence to software usage agreements by minimizing unused software. It becomes easier to keep correct software license records, lowering the risk of non-compliance and related legal penalties.

**System Stability and Security**

Software that is not required can compromise security or work against already-in-place security measures. To improve system stability and fortify our overall security posture, MOJOINC carefully assesses and restricts software installations. For this reason, there is a lower chance of security lapses, data leaks, and unwanted access to our systems and sensitive data.

**UPDATE SOFTWARE REGULARLY**

**Fixing security flaws**

We aggressively address any known vulnerabilities and flaws by maintaining the most recent version of our software. The risk of unauthorized access, data breaches, or malicious attacks is decreased thanks to regular updates that contain crucial security patches that shield MOJOINC against various risks.

**Bug Fixes and Stability**

The overall stability and performance of our programs and operating systems are improved via software updates, which also fix bugs and malfunctions. We reduce the likelihood of software-related difficulties that can have influence on our productivity and regular business operations by staying up to date with upgrades.

**Compatibility**

The most recent hardware, protocols, and technologies are compatible with software that is regularly updated. We can take advantage of new functionality, integrations, and technological improvements in the software ecosystem by keeping our software up to date, which enables us to work successfully and efficiently.( Archived NIST Technical Series Publication)

**Compliance and Legal Requirements**

It is crucial for a responsible business to adhere to statutory obligations and industry norms. In order to fulfill these commitments and keep our systems safe and compliant with the appropriate standards, we regularly upgrade our software.

**Protection Against Exploits**

Cybercriminals frequently target obsolete software that has known flaws. We minimize the window of opportunity for potential attacks by immediately implementing software upgrades, preventing the compromising of MOJOINC's systems and sensitive data.

**Vendor Support**

The most recent versions of software applications are usually supported and assisted by software suppliers. By maintaining the most recent version of our software, we reduce any downtime or interruptions by making sure we can contact vendor support, address any problems right away, and get help when we need it.

**Performance Optimization**

Performance enhancements and resource conservation are frequently included in software updates. By routinely updating our software, we can take advantage of improved performance, quicker response times, and better system resource use, all of which increase our productivity.

**Automated Updates and Patch Management**

MOJOINC can set up automated update methods and patch management systems to make the software update process more efficient. These programs automate the updating process, easing the administrative effort and guaranteeing that our software is always up to date.

**Risk Mitigation**

We reduce the risk of security incidents, system failures, and interruptions to our operations by routinely updating our software. It demonstrates MOJOINC's dedication to preserving a secure environment for our staff, clients, and partners.

**Stay Ahead of Threats**

With new vulnerabilities and attack methods regularly appearing, the threat environment is constantly changing. Since MOJOINC incorporates the most recent security precautions, defenses, and countermeasures offered by software suppliers, we are always one step ahead of potential threats.

**Reference:**

NIST Special Publication 800-63B. (n.d.-b). <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf>

*Choosing and Protecting Passwords | CISA*. (2009, May 21). Cybersecurity and Infrastructure Security Agency CISA. <https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords>

National Cybersecurity Alliance. (2023). Passwords. *National Cybersecurity Alliance*. <https://staysafeonline.org/online-safety-privacy-basics/passwords-securing-accounts/>

Archived NIST Technical Series Publication. (n.d.). <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-40.pdf>