Logo

Description automatically generated

**Access Controls**

**INFT 1203-03**

Abheyjeet Singh (100904911)

Kalyani Kamepally (100897552)

Sanyam Chopra (100897636)

Kamaljeet Kaur (100902546)

Shweta Ketswal (100900888)

Sanu Varghese (100898181)

Prof: Vigna, Thanikaslam

Date: 5th July 2023

This paper highlights our organization's plans for implementing three essential best practices on Ubuntu servers: using strong passwords, updating software often, and keeping an eye on log files. Each procedure is covered in depth, emphasizing its significance for the security and operational resilience of the firm.

1. **Strong password management strategy**

**Implementation Strategy**

* Create a password policy that enforces standards for complexity, such as minimum length, character kinds, and recurring password expiration.
* Inform staff members of the value of secure passwords and offer advice on keeping and establishing them.
* To create and securely store complicated passwords, encourage the usage of password managers.
* Where it is practical, use multi-factor authentication (MFA) to offer an extra degree of protection.

**Importance**

Strong password management is essential for protecting our company from unwanted access and data breaches, which is why it is important to the company. We lower the possibility of attackers guessing or breaking passwords by implementing strong password standards and training staff. Employers are encouraged to use strong passwords for all accounts, including Ubuntu servers, by using password managers, which also improves convenience. By requiring an additional verification step, MFA increases security by reducing the possibility of password compromise.

1. **Regular Software Updates**

**Implementation Strategy**

* Create a procedure for checking for updates and patches offered by Ubuntu and other software suppliers on a regular basis.
* To speed up the update procedure, use solutions like unattended upgrades or an automated patch management system.
* Set essential security upgrades as a priority and implement them right away.
* To find and fix any holes in the software update process, conduct routine vulnerability assessments.

**Importance**

Software updates are necessary for minimizing vulnerabilities and lowering the risk of exploitation. This includes the Ubuntu operating system and any installed packages. Our servers may be vulnerable to known security flaws due to outdated software, which attackers may exploit. We reduce the window of opportunity for possible threats and ensure a safe and reliable infrastructure by immediately implementing security upgrades.

1. **Monitor Log File**

**Implementation Strategy**

* Use a centralized logging system, such Splunk or the Elastic Stack (ELK stack), to gather and examine log information from Ubuntu servers.
* Create policies for log aggregation and retention to make sure that old logs are still available for auditing and analysis.
* Define alerts and notifications for particular log events that need to be addressed right away, including attempted unauthorized access or suspicious activity.
* Dedicate staff to reviewing log files on a regular basis, looking for abnormalities, and quickly responding to security problems.

**Importance**

Monitoring log files is important to the business because it enables us to promptly identify and address security issues, system failures, and policy breaches. We can spot indications of illegal access, odd activity, or attempted attacks by examining log data. The potential harm from such situations is minimized, data breaches are avoided, and the general integrity of our Ubuntu servers is ensured by prompt detection and action.

**Conclusion**

It is essential for upholding a safe and robust infrastructure to implement best practices on our Ubuntu servers for strong password management, routine software upgrades, and log file monitoring. Together, these procedures strengthen our defenses against unwanted access, reduce vulnerabilities, and provide quick identification and reaction to possible security events. By implementing these procedures, we give the security of the resources, information, and reputation of our company priority.

**References**

1. <https://www.thesslstore.com/blog/linux-server-security-linux-hardening-best-practices/>
2. <https://ubuntu.com/blog/linux-server-management-in-2022>
3. <https://serverfault.com/questions/850283/new-ubuntu-server-best-practice-for-setup>