Henry Post

ITMS 428

Applying access controls to a MySQL database

Contents

[In general 2](#_Toc524708259)

[Users 2](#_Toc524708260)

[local-system-admin 2](#_Toc524708261)

[data-entry 2](#_Toc524708262)

[data-view 2](#_Toc524708263)

[data-backup 3](#_Toc524708264)

[Notes 3](#_Toc524708265)

[References and citations 4](#_Toc524708266)

# In general

All passwords shall be rotated **periodically**.

All passwords shall be stored in a **hashed format**, never in plaintext.

Any user shall be disabled if a **sufficient amount** of failed logins are attempted on that user.

# Users

## local-system-admin

* Login shall be allowed from `127.0.0.1` only.
* Only one session shall ever be allowed to connect to this account.
* All global priviledges.
* All priviledges on all tables.
* Password shall be a random string of **sufficient length**, stored offline on paper or a USB key.

Rationale: The use of this account shall be limited to short periods of maintenance, or emergencies.

## data-entry

* Login shall be allowed ONLY from the local network, hosts matching `192.168.1.\*`.
* User shall be allowed ONLY to `INSERT,UPDATE` to database `terrorismdb`.

Rationale: This user is meant to only enter new entries should such an automatically-updating system be devised.

## data-view

* Login shall be allowed ONLY from the local network, hosts matching `192.168.1.\*`.
* User shall be allowed ONLY to `EXECUTE,SELECT,SHOW VIEW` from `terrorismdb`.

Rationale: This user is meant to retrieve and display data. It can also make reports and summarize data.

## data-backup

* Login shall be allowed from `127.0.0.1` only.
* They have the following global priviledges: `EVENT,LOCK TABLES,SELECT,SHOW DATABASES`
* User shall be allowed ONLY to `SELECT` from `terrorismdb`.
* Backup tasks shall be automated.
* Human login shall be limited to emergencies.
* Backups shall be performed to a hardware-controlled cold storage array that maintains a **time period** worth of backups before they overwrite the other media.
* Password shall be a random string of **sufficient length**, stored offline on paper or a USB key.

Rationale: This user is meant to backup the database **periodically**, and nothing more.

# Notes

* Bolded words are standards of time, security, or other quantitative things that are up to you, the implementer of these recommendations, to decide.

# References and citations

“NVD - Control - AC-5 - SEPARATION OF DUTIES.” *NVD - CVE-2017-5638*, nvd.nist.gov/800-53/Rev4/control/AC-5.