Sysadministrivia

Linux, Lagers, and Late Nights

S3E21: "Sussudo"

Posted 2018-12-17 04:59
Modified 2019-08-18 16:45
Comments 0

Navigation

Previous Episode	Next Episode
S3E20: "Clockulators"	S3E22: "Shitshow IV: the Return of the Shitshow"

Log

Recorded (UTC)	Aired (UTC)	Editor
2018-12-10 03:10:54	2018-12-17 00:15:08	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`e1ecd4346cdb823c64b41f2dfcee87b6db119262bd119cfaebbb7a823fe8515f`	click	click
OGG	`57c99f2aec28384f3c67f7aad78667b6ecc1fbe7d354d52fa3303c28da99d2c7`	click	click

Quicklisten:

All about sudo (and su)!

- News
- Notes
- Sysbadministration Award
- Errata
- Music

News

- Bulgarian prosecutors detain 3 criminals involved in $5 million crypto theft.
- Billion dollar secret project nearly compromised by rogue employee.
- Someone found out that Google Translate can be used to execute a reverse shell.
- Australia is first western country to pass a bill forcing tech companies to hand over encrypted data.

Notes

Starts at **17m06s**.

I was drinking chamomile tea and a Shock Top Lemon Shandy. Paden was drinking a Coors Lite. Jthan was drinking Wasmund’s Rappahannock..

- Sudo in-depth
  - Resources:
    - The Pink Book, 5th Edition, middle of chapter 3.
      - The “pink book” nickname is shorter than the real title, and comes from the 2nd edition.
    - Sudo: You’re Doing it Wrong
      - The presenter also wrote a book on sudo.
    - And of course, the Arch Linux wiki entry.
  - When to su vs. sudo?
  - `sudo -i` vs `sudo su`
  - Auditing:
    - For interactive shells, see log_input and log_output.
    - For anything more handy, though, you’ll want to use auditd.
      - We’ll talk more about auditd next season!
  - **Use visudo.** It checks syntax and will prevent you from locking yourself out of sudo.
    - I did indeed file a feature request.
  - `sudo [-U <user>] -l` will list privileges you or another user has access to.
  - **Be sure** to use double double quotes (`""`) to disallow args to whitelisted commands!
  - Be VERY careful with e.g. `sudo less`, `sudo more`, `sudo vi`, etc.! These can spawn subcommands/subshells! Specify NOEXEC (or use groups-based permissions on e.g. log files instead, etc.)
    - Alternatively, write a specific script that ONLY spits out specific files to stdout.

- Sudoedit is a special command that uses the invoking user's `$EDITOR`, shell escapes, etc. and uses a temp file before writing to the (protected) destination file.
- MOST of the invoker's environment variables are stripped/sanitized.
- We didn't talk a lot about it, but Sudo supports LDAP.
- Sudo can also enforce checksumming for scripts!
- Sudo is useful in that it will let you "become" another user for debugging environments/perms/etc. via `sudo -i [-u <user>]` (leave -u off for a more proper `sudo su` replacement!)
  - For example, to debug Nginx issues, I will frequently open a shell as the nginx user: `chsh -s /bin/bash nginx; sudo -i -u nginx; chsh -s /sbin/nologin nginx`

Sysbadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(49m40s)**

Quora got they asses smacked, but it took them a week to announce it.

Errata

- True to Jthan's weird ability to reference episodes, it was indeed S3E13 where he had the Wasmund's Rappahannock.
- The thing I was thinking of is actually gksu.
- As I promised Jthan, this is the link to 'external anal sphincter'.
- Jthan could not stop giggling.
- The "genie thing" I was thinking of is indeed The Akinator.
- UPDATE: the feature request I filed for sudo will be in sudo 1.8.27! **Nice!**

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Take Your Time	Bio Unit	click	CC-BY-NC 4.0
Outro	Aimer, c'est ce qu'il y a de plus beau	Monplaisir	click	CC0 1.0

(All music is royalty-free, properly licensed for use, used under fair use, or public domain.)

Author r00t^2
Categories Season Three

Comments

There are currently no comments on this article.