Sysadministrivia

Linux, Lagers, and Late Nights

S2E0: "I Think There's a Delay"

Posted 2017-02-13 04:45
Modified 2017-02-13 15:50
Comments 0

Navigation

Previous Episode	Next Episode
S1E22: "Shitshow II: the Re-Shittening"	S2E1: "Like Files Caught in a Web"

Log

Recorded (UTC)	Aired (UTC)	Editor
2017-02-02 03:31:01	2017-02-13 04:45:00	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`7b436e079c975675c9696d67c23fc734279723e86dea4301d3cd36111fc8581b`	click	click
OGG	`d646aa2308aec6893912c689a067326d442a0b55fc27900424e44682d10993a5`	click	click

Quicklisten:

We talk about GitLab having an infra meltdown, some tools for enterprise fleet management, and a bird's-eye-view of BIOS/UEFI.

And Jthan wasn't HIGH-ENERGY enough. It must have been all the "cranberra vodkys".

- News
- Notes
- Sysbadministration Award
- Errata
- Music

News

- Delta Airlines has a pretty nasty snafu with their reservation system.
- Supposedly a hotel was 'held ransom' by ransomware, affecting their door locking system and leaving guests locked in/out of their rooms.
  - But this is bullshit and seems to have originated by a "news" source that was described by BuzzFeed as "the King of Bullshit News". Yes, you read that correctly. When BuzzFeed of all media calls you bullshit, you know you're in trouble.
- The Guardian reported WhatsApp as backdoored ...
  - But this also is complete and utter bullshit.
- A Los Angeles college paid off a ransomware. Gorram it, **stop doing this**. Keep a good backup system instead, knuckleheads.
- There's a pretty hilarious cryptkeeper bug
  - Upstream is dead, though, and it's been removed for Debian 9 so it's not such a big deal...
  - But if you're using it, stop.
- There are multiple tcpdump vulnerabilities (most having to do with separate functions suffering from similar flaws).

Notes

Starts at **19m53s**.

I was drinking Northcoast Brewing's Old Rasputin, Jthan was drinking an herbal infusion because he wasn't HIGH-ENERGY enough, and Paden was drinking Glenlivet 12 years.

- Enterprise fleet management
  - We have mentioned config management in S0E15
  - We talk about rConfig for managing net kit
  - And Augeas for accessing config files in an "object-oriented" sort of approach
  - NeDI is handy for an overview of your fleet...
  - But I like Observium better because it feels more "polished".
  - And handy for managing other information into visual presentation is Cacti.
  - Also, neti pots.

- We also talk about BIOS/UEFI **(39m08s)**
  - **BIOS** (Basic Input/Output System) has been around a *very long time*

    - It runs on the motherboard, and initializes the hardware sequentially
- **UEFI** (Unified Extensible Firmware Interface) has been around for less time (2005, but first developed in the mid-90's for IA-64), but is much more robust
    - It runs on a dedicated subsystem and initializes devices as-needed/in parallel, which greatly speeds up boot time
- UEFI lets you run things like memtest86+, various kernels, etc. **directly** – meaning without even needing to boot an initrd or memdisk!
- Bruce Schneier talks about the "Evil Maid" attack here
- We talk about the rm -rf bug with UEFI variables in S1E0
    - We didn't mention it in the show, but there was also a UEFI exploit on Thinkpad devices that we mention in S1E11.

Sysbadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(49m32s)**

GitLab killed a prod server with what was a literal wrong `rm -rf`. AND THEIR BACKUPS- ALL OF THEM- WERE BAD. They ended up recovering from a live copy (so props for redundancy). *However*, their write-up is top-notch (original issue) and they even livestreamed the recovery effort.

Bonus points, I reference this meme.

Errata

- Edita counted for me; the times I tell Jthan to be "high-energy" is 5 times throughout the episode. hahaha
- We talk about how hard it was to kill Rasputin. He actually survived one. He was a pretty tough bastard and people really wanted him dead.
- Juniper kit actually uses 'JunOS', not "JuniperOS", and it's FreeBSD-based, not GNU/Linux-based.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Shapeshift	Bio Dread	click	CC-BY-NC-SA 3.0
Outro	her's	Graffiti Mechanism	click	CC-BY-NC-SA 4.0

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

Author r00t^2
Categories Season Two

Comments

There are currently no comments on this article.

Published with Textpattern CMS