Sysadministrivia

Linux, Lagers, and Late Nights

S3E2: "Zen Administration"

Posted 2018-03-26 03:59
Modified 2018-04-22 20:54
Comments 0

Navigation

Previous Episode	Next Episode
S3E1: "Strike(r) In the New Season"	S3E3: "Ranting Lunatics"

Log

Recorded (UTC)	Aired (UTC)	Editor
2018-03-15 03:02:01	2018-03-25 17:04:23	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`5cc270b6810c3b4f766ef259036b7c282acad7e5ad3eb3b942228fa4c8b16bac`	click	click
OGG	`76d1459e7f99cfb06263f4c8ff2e4fb8491e32f1f2511e9856bc63e215d7fa52`	click	click

Quicklisten:

Where we talk about choosing which enterprise Linux distro to use (or, rather – how to choose which Linux distro you should use in your enterprise environment), being a valuable mentor, Let's Encrypt offering wildcard certs, and why people need to clam dwno about Net Neutrality (as important as it is!).

The origin of the "transvanporent" and "grunchy" inside jokes.

- News
- Notes
- Sysbadministration Award
- Errata
- Music

News

- Samba servers suffer from a vulnerability that can allow for an unauthorized password reset and DoS.
  - CVE-2018-1050 (DoS)
  - CVE-2018-1057 (unauthorized password change)
- Remember how smug and sure of themselves AMD was in the Spectre/Meltdown fiasco? They probably shouldn't have been.
  - As a grain of salt, there are some questions raised about this report…
  - But the "debunking" article never actually debunks any of it in a factual manner.
  - There's also this, in which the flaws themselves were confirmed by a separate security research firm.
  - This was released after we recorded, but AMD has confirmed the vulnerabilities.
- Hotspot Shield has failed again, along with PureVPN and Zenmate.
  - You may remember Hotspot Shield as the Baddie recipient from S3E0.
- China has infiltrated a UK government contractor and stole military intel.
- There was a hardcoded password found in Cisco devices.
- Memcrashed (which we talked briefly about in S3E1) was used to hit Gihub with a **1.35 Tbps** DDoS. (For those curious, that is 168.75 Giga**bytes** per second.)

Notes

Starts at **27m45s**.

I was drinking Jefferson's Reserve bourbon (again). Paden was drinking Absolut vodka. Jthan was drinking Auchentoshan's 12-year scotch.

- Choosing a Linux distro for your enterprise environment
  - We mention a /. article that seems to be heavily biased towards Clear Linux but we have our doubts, as the entire thing seems to be a puff piece.
  - Clear Linux is indeed Intel-backed.
    - And it should run **on Intel CPUs for the speed optimizations**.
  - Criteria for an Enterprise distro: stability and point-released
  - We probably talked about Gentoo in the enterprise environment/for HPC in S2E1 during the "bleeding edge" discussion.
  - Paden's point about the "Home Edition" is actually for *ClearOS*, **not** Clear Linux. See errata; we got ourselves confused here and there.

- Mentoring a padawan **(40m51s)**
  - One-to-one mentoring has a long legacy in the *nix world, going all the way back to VMS/VAX and UNIX greybeards.
  - You're going to have your **own** dynamic between guru/apprentice. What works for Jthan and I may not work for you and your guru/apprentice.
  - Corporate mentorship, depending on your mentoring style (or learning style), can feel too stifling.
  - Some people don't want to be mentored (autodidacts, etc.)!
  - Passion for the skills/trade/industry you're mentoring (whether you're the guru or the apprentice) is **very** important. Probably the most important component of mentorship.

- Let's Encrypt now offers wildcard certs (and/via ACMEv2) **(59m1s)**
  - You need to use DNS challenges via TXT records to take advantage of this.
  - It's still a little buggy, though, so be vigilant and make sure you report bugs.
  - I don't think you can (or should) use wildcard certs across multiple servers; it's more useful for virtualhosting one or more subdomains on a single server.
  - CA trust doesn't really mean much these days.
  - Jthan mentions an article saying it's possible to have multiple wildcard certs with multiple different keys. He however implied (or so I thought) that you could have **one** wildcard cert that works with **multiple** keys (you can't — at least not without some serious intermediate fuckery). However, while what the article asserts — that it is possible to have multiple certificates, wildcard certificates included, issued for the same CN across different keys — is technically possible, I don't know of a single CA offhand that will allow you to do this with a wildcard certificate in practice. It'd be much more practical to get a SAN'd certificate for the records that host will serve instead.

- Sensationalism sucks. **(1h6m40s)**
  - Net Neutrality is a **very important concept**. That being said…
  - You **do not** win battles by hyperbolizing and sensationalism. This is divisive and only furthers the ignorance of those involved in making actual legislation at best, and makes you a shitty and manipulative person at worst. It only hurts your cause and makes you appear unknowledgeable of the thing you claim to support.
  - Net Neutrality is not covered by a single bill or act, it's a concept that is **worked towards** by **many** – hundreds, potentially – of bills and acts and other legislative actions.
  - In closing: fuck clickbait, fuck hyperbole, fuck FUD, fuck the mainstream media, fuck people talking about things they don't understand, and fuck radicalization.

Sysbadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(1h15m6s)**

Trustico is absolute trash.

See also this and this.

Errata

- We didn't catch it at the time, but I was so tired that I apparently pronounced "transparent" as "transvanporent". See **18m51s**; it'll slip right by you if you aren't listening for it (neither myself nor the co-hosts noticed it!).
- When talking about Github's DDoS, I may have implied that the "reflector" – the server with the open memcached sending the responses to the forged destination – would be the one sending REJECT packets. That should instead be "the forged destination would be sending REJECT packets to the reflector while the reflector is sending memcached responses to the forged destination".
- We occasionally referred to Clear Linux as ClearOS. That is something different.
- Yes, Jthan, mentee is indeed a word.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Orion I	Pedro Santiago	click	CC-BY-NC-SA 4.0
Outro	Sea	Portrayal	click	CC-BY 4.0

(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.