Sysadministrivia

Linux, Lagers, and Late Nights

S1E6: "I Tour My ACL"

Posted 2016-05-09 02:48
Modified 2017-01-28 23:25
Comments 0

Navigation

Previous Episode	Next Episode
S1E5: "Jthan + Sysbot = 4evr"	S1E7: "Wake Up Call"

Log

Recorded (UTC)	Aired (UTC)	Editor
2016-04-28 04:34:35	2016-05-09 02:48:05	aaron k.

Verification

Format	SHA256	GPG	Audio File
MP3	`536e8b69c9b9a1b963daeddd22e48e4fe0b88ec8355322db6b308cadfe72f53f`	click	click
OGG	`36a1a18b30df7937a376e54fffa0833318bb7fb652a70e28c4a7509cf0dd2eaf`	click	click

Quicklisten:

Various security mechanisms such as ACL, SElinux, etc.

This is also the episode where the “cockulator” joke was born.

- News
- Notes
- Sysbadministration Award
- Errata
- Music

News

Starts at **4m36s**.

- The entire San Bernardino debacle was pointless.
- FBI contractor hired to implant Tor malware
- A Spotify “Compromise”
  - Which is most likely not actually a Spotify compromise. Per an anonymous infosec professional source on twitter PM, “Couple of hundred account dumps is not a data breach. It can be obtained from a public terminal or a network.”
  - And it’s a valid point.
- Nuclear power plant gets infected by malware on the 30th anniversary of the Chernobyl incident.
  - One of the found infections was Conficker. Let me say that again- **conficker**. In a power plant. Lovely.

Notes

Starts at **14m31s**.

I was drinking Different Drum Rum from La Colombe Distillery (yet again), Paden was drinking his Buckeye vodka also again, and Jthan was drinking Princess Yum Yum (lolz) from Denver Beer Co..

- There are a lot of interesting things you need to take into consideration when using Tor.
  - I mention CJDNS in particular, as well as OpenVPN as proper alternatives.
  - I reference this Radiolab episode regarding Timothy McVeigh.
  - If you **really** want a liveCD that has better anonymity options, either spin your own (which is easy using BDisk!) or use Qubes OS, which is basically meh.
- We finally (try to) put the San Bernardino thing to rest. (**32m12s**)
  - tl;dr: it was more about the precedent and being a power play by the FBI rather than the case, which is a clear and distinct abuse of power by the FBI.
  - Jthan also brings up the Philadelphia cop who is being jailed indefinitely due to his encrypted harddrive.
  - Which is bullshit.

- GNU/Linux security mechanisms (**56m40s**)
  - PAM is pretty cool.
    - Including Duo and Google Authenticator.
    - I also mention (though it's unrelated) SPDY. I also mention WiKID (see errata).
    - This is a good example of TTY login limitations. For more fine-grained control, you should also look into the options for */etc/security/access.conf*.
  - GRsecurity PaX.
    - You can hear Jim (TheTechStewart) on S0E18.
  - SElinux isn't all too hard to learn.
  - This is a good resource to learn it.
  - Aaron chopped some of this discussion out. :| You can find the link to the uncut/unedited mix in the Errata section.
  - The NSA security guide can be found here. Mysteriously, the original link is broken. Also worth a look is this.
  - Octal modes and Ownerships
    - Cheatsheet
    - Permissions calculator
    - But there's other ones here
    - The Pink Book
  - XATTRs (extended attributes) are pretty handy. The pink book goes into more detail for this, which is why I highly recommend it.
    - To use it, though, you need to use the "xattr" mount option.
  - There's also normal attributes.

Sysbadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(1h44m00s)**

This episode's winner of the Baddies was the unnamed sysadmin/netadmin responsible for this. Way to go.

Errata

- Jthan and Paden kept playing Slither during the pre-recording meeting.
- I refer to Chelsea Manning as Bradley Manning because at the time of incident, Manning still identified as male- or at the least was known as Bradley.
- Aaron has stated he wants to come on the show to discuss documentaries more in-depth, but it's already pretty irrelevant. I already know what he's going to say, though, since we're good friends and have talked about it in-length before- he doesn't believe there's such a thing as objective facts, and especially that humans aren't capable of objectivity even if it exists.
- I reference the Ballmer Peak.
- I mistakenly referred to WiKID as "Twistid"- I have no idea why, but I do it all the time.
- Aaron cut chunks out of conversation, and some context was missed. Please feel free to grab the FLAC XZ-compressed (and the signature).

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Sauronator (ft. Jthan)	GovLove	click	CC-BY-SA 4.0
Outro	Sauronator (ft. Jthan)	GovLove	click	CC-BY-SA 4.0

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

Author r00t^2
Categories Season One

Comments

There are currently no comments on this article.