Sysadministrivia

Linux, Lagers, and Late Nights

S5E8: "Feeling Vulnerable"

Posted 2020-06-07 23:59
Modified 2020-06-11 15:58
Comments 0

Navigation

Previous Episode	Next Episode
S5E7: "SIT Tunnels? How Sixy!"	S5E9: "Chaotic Good"

Log

Recorded (UTC)	Aired (UTC)	Editor
2020-05-31 02:32:42	2020-06-07 13:00:51	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`ba67fe9ed0932b6dc9df36a447172f8ed377843c7e2c27fb9ab1310f0792d649`	click	click
OGG	`5dcc44ded774354d693d348d1cd065b722da1daf8327940f91a4d700d9bdd83e`	click	click

Quicklisten:

We talk about vulnerability scanners/virus scanners that run on, and for, Linux.

- Just the Tip
- Notes
- 15 Clams
- Errata
- Music

Just the Tip

- Paden talks about building a playhouse...(?)
  - He has pictures here and here.

Notes

Starts at **15m12s**.

I was drinking water. Paden was drinking Miller Lite. Jthan was also drinking Miller Lite.

- We talk about vulnerability scanners for Linux.
  - Lynis
    - Seems to be the best of the vuln scanners we cover (with maybe the exception of some aspects of commercial scanners, such as Nessus)
  - rkhunter
    - Second-best behind Lynis.
  - chkrootkit
    - Dated, but still maintained.
  - Extending/wrapping scanners
    - Tiger
    - skdet
  - IDS
    - Tripwire
    - afick
    - You can find a nice comparison (if not fairly outdated) of various IDS here.
    - I mention the (confirmed defunct) osiris project.
    - mtree is **fantastic**, which is why I have an AUR package for it.
  - NIDS
    - Snort

- Virus scanners that run on/for Linux **(37m44s)**.

- clamav (with the clamTK GUI)
- Sophos
- F-Prot
- There was an AVG version for Linux but it’s been discontinued.

15 Clams

In this segment, Jthan shares with you a little slice of life. The title is a reference to this video. (2m16s in)

Starts at **46m33s**.

Jthan talks about various service outages all tracing back to the AddTrust CA expiration. The blog post he references on-air is here and you can check your chain validation with this.

We talk a little about certificate chaining and cross-signing.

Errata

- We talk about Deloitte in S2E17.
- Paden hasn’t sent me pictures of the playhouse yet.
- Yes, Jthan, carpenter bees do (can) sting.
- Jthan mentions Bro, which has been renamed to Zeek.
- The Richard Stallman-esque copypasta I reference.
- Jthan doesn’t understand corner cases vs. edge cases.
- He also doesn’t understand the difference between a client certificate vs. a server certificate.
- Apple Safari indeed will not consider certs with expiry greater than one year as valid.
- By the way, Jthan, it’s erroneous to insinuate that most X509 certificates are cross-signed.
- All the solutions presented here are not guaranteed to work, Jthan and Paden. In Gnome 3, for instance, it seems that none of them work.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Rollin'in	Initial Master Kay	click	CC-BY-NC 4.0
Outro	Lost Futures	4t Thieves	click	CC-BY-NC 4.0

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

Author r00t^2
Categories Season Five

Comments

There are currently no comments on this article.