

Sysadministrivia

Linux, Lagers, and Late Nights

S2E15: "Playing HopskotSSH"

Posted 2017-09-11 03:59

Modified 2017-09-11 02:21

Comments 0

Navigation

Previous Episode	Next Episode
S2E14: "Short-Term Memory"	S2E16: "Playin' Cornhole"

Log

Recorded (UTC)	Aired (UTC)	Editor
2017-08-31 03:06:42	2017-09-10 22:11:59	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	5c2649c882b2d59ab4d2bba423e25e16fd83223c998cb587b92621983acf0e4a	click	click
OGG	0dbe4c50086770395aaef53ff6b3f593e7cbbd7cf6c3843919c343466055feb3	click	click

Quicklisten:

In this episode we talk about FOSSCON NE 2017, we briefly talk about a server configuration primer (and argue how "primer" is pronounced). We also talk about some fancy tricks to do with SSH in regards to a connection/jump chain and process masking (hiding processes one user owns from another). We also talk about our next conference/convention appearances and current projects. "We're all going down together."

- News
- Notes
- Sysbadadministration Award
- Errata
- Music

News

- There's been a spam dump of 711 million addresses
- Intel's IME (mentioned in S2E7) can be disabled (alternate link). Yay!
- The Supreme Judicial Court of Massachusetts has sort of declared that digital phones can't be searched without a warrant.
- Sonos speakers may cease to function without accepting the new privacy policy.
- Apple's SEP (Secure Enclave Processor) chip may have been cracked.

Notes

Starts at **9m07s**.

I was drinking Bulleit Bourbon 10-year. Paden was drinking Glenlivet's 12-year Founder's Reserve. Jthan was drinking Crown Royal's Northern Harvest rye.

- Paden and I give a recap of FOSSCON NE 2017! (If you haven't yet, you should read our write-up on it! It includes links to my talks and some other goodies.)
- Server primer (**13m36s**)
 - "Yak-shaving" can be referenced here.
 - The software I'm (still) writing is called KANT - Keysigning and Notification Tool. You'll be able to find it in my OpTools repository when done.
 - I ended up running a public SKS pool keyserver as well because deploying it was kind of fun! (Oh, yeah. I also deployed a couple other services.)
 - It also has some general hints and tips for setting up a private home network.
- Jumpbox/chaining SSH (**16m34s**)
 - There is a huge amount of really awesome SSH tricks.
- Process masking in Nix *(**19m05s**)
 - FreeBSD offers on installation if you want to hide processes between users
 - Do note that this doesn't, of course, apply to the root user.
 - I point out that SELinux and GrSecurity can do this and it can even be done with mount options.
- We talk about future conventions/conferences we'll be at and current projects (**24m56s**)
 - Myself and Paden will be at BSides Philly (Dec. 8, 2017)

- Jthan has started a Flask-framework-based CMS called whisky.
- All three of us will be at HOPE XII well! (July 20-22, 2018)
- Myself (and maybe Paden) will be at BSides DE (November 10-11, 2017)

Sysadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(36m38s)**

In 2013, attackers accessed the internal database of Scottrade, a securities brokerage firm based in St. Louis, MO (and got they asses straight-up caught). Thanks to Skip for passing this along to us!

Errata

- Jthan says he wants to know how to “route” his traffic over SSH. He actually means “tunnel”. They’re different. :)

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Amazing Grace - Dilbrent's All-Cowbell Rendition	Dilbrent	click	CC0 1.0
Outro	Scuba	simun_mathewson	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 Two

Comments

There are currently no comments on this article.