Sysadministrivia

Linux, Lagers, and Late Nights

S2E4: "From TCP to Shining UDP"

Posted 2017-04-10 03:59
Modified 2017-04-26 01:45
Comments 0

Navigation

Previous Episode	Next Episode
S2E3: "Ass-Backwards Passwords"	S2E5: "Suck my Disk"

Log

Recorded (UTC)	Aired (UTC)	Editor
2017-03-30 02:52:55	2017-04-10 03:59:00	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	411b89785b42a4ca6b428c7f8d1c9bda0b88cb1024d52db564ae99b78b8093db	click	click
OGG	862e0cb31cf7b7d3e8d39206758065863e5a4a614bf1051100a708d0e906581e	click	click

Quicklisten:

In which we talk about Caddyserver, some practical applications of QoS, and respond to an email we received.

- News
- Notes
- Sysbadministration Award
- Errata
- Music

News

- Lastpass has yet another vulnerability
  - I mention pass (and Jthan mentions GoPass, one of the compatible GUI clients).
- HP Bromium runs self-destroying VMs
  - We mention Qubes OS.
- Skype is now serving malware as advertisements
  - Remember how I said that adblockers are a necessity? This is why.
- Google has called Symantec out for mis-issuing 30k certs.
- Senate Joint Resolution 34 has passed, nullifying 81 Federal Regulation 87274
  - In other words, “yer digital privacy’s **officially** fucked now, lel”
- Reminder that Jthan still needs some people with programming experience (and biologists!) to sign up for his hackathon.

Notes

Starts at **13m45s**.

I was drinking Bulleit 10 again. Paden was drinking Old Tankard Ale from Pabst. Jthan was drinking Hot to Trot by 14Hands Winery.

- Caddyserver
  - I was not impressed. It felt like “Fisher-Price Nginx” – and I inherently don’t trust “automagic” things because they dumb down complex mechanisms/configuration, and something’s bound to be missed when you do that.
  - I mention mcTLS which is a very silly thing and should be shunned. SHUN THE NON-BELIEVER. SHUNNNNNNNNN-UH.
  - Our general takeaway/consensus is “It’s probably easier to use for beginners, but there isn’t a ‘good’ use case for it.”

- QoS/Traffic Shaping **(25m10s)**
  - I mention tc (which is part of the iproute2 suite)
  - (I do it with Shorewall’s traffic shaping, which can get pretty advanced.)
  - I mention Layer 7 filtering, for example Nginx’s limit_req module.
  - We joke about Layer 8, a sort of joke layer of the OSI model.

- A defense of “the cloud”/DevOps **(37m28s)**

- We mention S2E2.
- I mention (and highly recommend using) mtree – there’s a Linux port here.
- Paden mentions the Phoenix Project.
- His original message:

> Hi Guys,
>
> OK, no essay or chastisement like I sent last time :)
>
> I just wanted to weigh in a bit on the whole “cloud” thing after S2E3. For me, it’s a question of these providers allowing a user to communicate with the VM-based infrastructure via an API. This allows you to programatically bring up and tear down infrastructure just by writing code to do so. Hashicorp’s Terraform is a great tool for this.
>
> Most, if not all cloud providers are not without their issues, but I think that’s normal in this topsy-turvy threat-addled world in which we operate :) They’re also by-and-large big megacorps, so that can’t be good. Maybe the answer is an open-source specification for such a thing, but I guess then we have Openstack – though that seems mega-complex. If we could have a simplified thing like Digital Ocean, that would probably be better, in that it lowers the barrier for entry.
>
> I’ve currently just started a gig using AWS, Terraform, Kubernetes (my first real use of containers) so I’ve gone a bit devops-y, but I still self-identify as a sysadmin, don’t worry :) Currently looking at filebeat / logstash for log aggregation and parsing – perhaps a future topic?
>
> Thanks!
>
> Jerry (Admin Admin)

Sysbadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(55m15s)**

- A Redhat engineer pushed creds to GitHub.

Errata

- The episode in which we kept having to restart/have outtakes at the end is S1E5.
- If Jthan’s Solaris-esque endpoint was running in a VM, Solaris has flowadm as part of its Crossbow suite.
- It turns out filtering traffic per UID is indeed pretty easy with iptables.
- Jthan mentioned something about getting a Baddie for rm -rf’ing /bin. Turns out, that’s not what he got a baddie for.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Ace of Clubs	RoccoW	click	CC-BY-SA 4.0
Outro	PENicillin (Produced By JBlanked)	DRVN	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 Two

Comments

There are currently no comments on this article.