Sysadministrivia

Linux, Lagers, and Late Nights

S4E12: "It's Getting Routey in Here"

Posted 2019-08-05 02:59
Modified 2019-08-03 04:17
Comments 5

Navigation

Previous Episode	Next Episode
S4E11: "SCADA isn't an STI"	S4E13: "Xmas in July"

Log

Recorded (UTC)	Aired (UTC)	Editor
2019-07-24 02:33:11	2019-08-03 02:44:55	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`955908bd5abfefdf0d13bba36073a2ad05d80814776fb4455027eb6f1a4af3fc`	click	click
OGG	`c4eb89a31d4638b051a44ddfcdf865a610be2d4236bcd429236f9c9930ec5062`	click	click

Quicklisten:

We dig into ways to deal with terrible consumer routers.

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

Just the Tip

- Paden talks about the Parallel Dancer's/Distributed Shell. Similar to the Dancer's/Distributed Shell except it runs in parallel instead of sequentially (which means its runs go a LOT faster).
  - Originally it was on Google Code.

Notes

Starts at **11m26s**.

I was drinking another Victory Dirt Wolf. Paden was drinking Buckey Vodka. Jthan was drinking Miller Hi-Life.

Way back on June 16, 2019 we got an email from a listener, Ari Hamami:

> Would love if you guys could discuss routers and security regarding routers in an episode.
> Just had a bit of a hard time with spectrum because the routers that they hand out to people are shit.
>
> Anywho, good routers from a security perspective and how to secure oneself if they are with a router like the aforementioned.
>
> Cheers!

So here you go, Ari! As promised!

- Securing consumer routers
  - ISP-provided kit is bullshit. Pure bullshit.
  - The majority of consumer routers, regardless of reviews and quality of hardware, have terrible **firmware**.

- OpenWRT will mitigate a ton of your issues.
  - Don’t bother with DD-WRT and/or Tomato. They don’t offer anything OpenWRT doesn’t have, and OpenWRT offers more.
  - They support a lot of different hardware.
  - LEDE has merged back in with OpenWRT.
- “Leasing” the hardware from your ISP is a scam. Avoid it if at all possible.
- Alternatively, you can build your own router. We talk a bit about it initially in S0E11.
- UBIQUITI HARDWARE IS ASTOUNDING.
  - Their “Unifi” WAPs are **fantastic**.
  - Seriously, I cannot recommend them enough.
- Jthan is in the process of creating his router box.
- Paden mentions pfSense, which is almost as limiting as consumer firmware but on an x86_64 box. What’s the point at that point? You learn nothing and your control over the machine is crippled.
- We didn’t mention this on the air, but DON’T use a Raspberry Pi for this. They only have one NIC and all the connections share a bus.

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 **47m27s**.

What extremes have we gone to for operations?

Errata

- Well, no, Paden, any PoE injector works for Unifi because the **output**, that connects to the Unifi, is PoE (either CAT5e or CAT6), which is a common and have a standard.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	The River	Rolemusic	click	CC-BY 4.0
Outro	Sweet Spot	Scanglobe	click	CC-BY-NC-SA 4.0

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

Author r00t^2
Categories Season Four

Comments

1. ## Ari

   2019-08-07 05:27 (716 days ago)

   Hey guys,

   Quick thank you for covering this episode.

   Turns out of all the routers OpenWRT supports, my Spectrum/Time Warner provided router isn’t supported.
   Might need to just switch to my own. (Plus, considering a mesh topology. Definitely can help with range and haven’t had particularly good luck with regular extenders.)

   Jthan.. looking forward to seeing your build and it’s potentially something I’d follow along with.
   Unfortunately, I am a (relatively) broke college student, so this was more up my alley:
   https://blog.tjll.net/building-my-perfect-router/

   Lastly, an idea for another episode, where you all discuss different technical certifications and applications as a result of it. Or if it is simply a piece of paper to wave around. Certifications could include the CISSP, CEH, Security+, Network+,etc… Perhaps how it relates to gov’t and something like DoD Directive 8750.01.
   …Or you could do an episode on Defcon/Blackhat.

   Regards,
   Ari

2.

2019-08-07 10:55 (716 days ago)

Ari-

Oh man. That sucks! Sorry to hear that.

As someone who has **extensive** experience with mesh networking, I can guarantee it's not the solution it seems to be. It's more ideal for cases where running a cabling backbone throughout the building is infeasible/impractical. You're always going to want to prefer a cable backbone supporting each of those WAPs. This ensures a lower congestion on the radios in the WAPs for client traffic instead of backhaul traffic, AND it ensures you don't suffer any degradations from speed. It's also faster handoff when switching between WAPs when walking through the house.

But as we mentioned in the show, you can absolutely just set your ISP router to bridged mode or, if it's separate from the modem/ONT/etc., replace it entirely with your own device that DOES support OpenWRT!

I hadn't heard of espressobin boards but they definitely look like a nice compromise between small devices like what OpenWRT targets vs. an x86(_64) platform! And multiple NICs, which is absolutely what you want for a device like this.

As far as certifications go, we make our **opinions** on them pretty clear! Jthan and I talk about them briefly in https://sysadministrivia.com/episodes/S0E3#notes and the three of us (plus a guest) a lot more extensively in https://sysadministrivia.com/episodes/S1E13#notes. Generally speaking, we aren't fans of them – they tend to make HR lazy and get people jobs they shouldn't have.
We don't really have much to say on InfoSec certs specifically – the three of us are Operations before we're InfoSec in our primary roles. But as luck would have it we have a guest on in S4E13 coming up that actually DOES touch upon InfoSec-specific certs!

For the same reason (Operations more than InfoSec), we don't do a lot of focus on hacker cons (e.g. DefCon/Blackhat). 2/3 of us are on the opposite coast and the word seems to be that it isn't worth it these days to make the trek, much less the cost of expenses and the ticket itself.

3. 2019-08-08 02:58 (715 days ago)

Hey guys,

Really entertaining and informative stuff, I'm really interested in the router box.
I'm in the middle of creating a home network of our old house which consist of around 10 rooms and additional 2 connected apartments. using cat 6a cables wired internally.

I got fiber coming from ISP and with provided router (Huawei HG8245Q) which as you guys mention in the episode is basically a spyware. sadly no openwrt for it but I figured out the telnet admin (defaults to root:admin)

I'm a recent CS graduate so got plenty of time and not much of experience.
This episode is giving me plenty of good information so thank you. and looking forward for Jthan results.

cheers

4. 2019-08-08 12:22 (714 days ago)

Mouath-

Thanks! Jthan's still working on his build but I'm sure he's going to talk about it on-air.

I just recently bought an old house myself (1906)! The cabling has definitely been a challenge. What I ended up working out with my electrician is for the majority we just drill up through the basement (he's upgrading it to 200A at the same time) and running it under floorboards where we can for the first floor, and running external conduit for the second floor. I'm also going to be running CAT6a. Have you run your cabling yet? Have you had much difficulty with any corners/bends running that CAT6a since it has that really stiff plastic core?

As for the Huawei, unfortunately, yeah… not a brand to trust these days. But I did find a little bit of information on that telnet interface, including access to administrative commands:

https://jalalsela.com/accessing-hg8245q-shell/

And it SHOULD support switching to bridged mode even through the web UI: https://forum.huawei.com/enterprise/en/how-to-use-hg8245q-as-a-bridge-for-a-second-router/thread/467425-100181

(provided, of course, your ISP doesn't arbitrarily feel like changing it back.)

5. 2019-08-19 08:01 (704 days ago)

oh wow our house is only 29 years old, I got a bit lucky in the ground floor where we have the old telephone lines and dish coaxial cables. all of these are no longer in use so I replaced them and it was a pain, some renovations work destroyed the conduits so I had to remove some of the cemented tiles to get to the conduits.

The fiber ran from the street to the inside throw an underground conduit that goes to a cable chamber. So I terminated it there and brought all my cat cables to the same chamber
network rack going to be hanged just above it.

The cable I got is UTP and was still a pain to fish it through old bent pvc conduits. TIP: if you are going to run 2 cables in the same conduit fish them BOTH at same time because if you don't the 2nd one will just rub on the 1st.

most of my challenges was figuring out where this conduit go. not a single person here follows basic NEC
so I spent some time fixing extremely dangerous stuff and halting my progress. (the breaker panel is spaghetti mess and the frame shocks you if you touch it lol)

Nice thing about the cable that it's not easily damaged, just use some lube

Thank you for the link lucky mine doesn't seem to be protect when invoking su.

sorry for the messy response, I haven't slept for a while.

cheers