Sysadministrivia

Linux, Lagers, and Late Nights

S4E11: "SCADA isn't an STI"

Posted 2019-07-22 03:59
Modified 2019-07-22 00:37
Comments 0

Navigation

Previous Episode	Next Episode
S4E10: "Unavailable"	S4E12: "It's Getting Routey in Here"

Log

Recorded (UTC)	Aired (UTC)	Editor
2019-07-11 02:51:24	2019-07-21 19:05:24	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`404d15208ad241c468deec64606f9b560a2074453bcdfc6fa2886252afda4d54`	click	click
OGG	`bfb33b2f986a4d8345c658b93eada946ba4ee2323fc647223ef6d1c319619d21`	click	click

Quicklisten:

Subtitle: “But it is an ICS”.

In this episode, we have Kate (from S3 shitshow) on to introduce us to ICS/SCADA systems.

We also have a “Jthan typing noise” at 1h02m41s.

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

Just the Tip

- Community involvement
  - You may want to give S0E15 a listen, where Jthan and I talk about this extensively.
  - Jthan hates PLUG. But you definitely can go if you want, it’s one of the larger LUGs.
    - He’s just mad.
    - But he doesn’t even live in PA, so.

Notes

Starts at **16m04s**.

I was drinking Dirt Wolf. Paden was drinking vodka and apple juice. Jthan was drinking a Jack and Coke. Kate was drinking vodka and Red Bull.

- We have Kate, a Senior Vulnerability Analyst at Dragos, Inc., on to talk about ICS/SCADA systems (and interesting ways they’re vulnerable that most computer networks wouldn’t be). You might remember her from the season 3 shitshow.
  - The guest we had that would be more familiar with SAP would probably be Phil, who we had on in S4E3.
  - Kate mentions FUD. If you’re unfamiliar with the term, it’s an acronym for “Fear, Uncertainty, and Doubt”.
    - Squirrels take down a lot of power plants.
    - See also this.
    - (You can see a recording of the actual webinar here.)
  - Kate shamed me for mentioning Stuxnet.
  - Just remember:
    - “If they don’t have a PIN, don’t let them in!”
    - “If they don’t have a card, punch them hard!”
    - “Empathy is the enemy of security.”
    - Kate prefers “complacency is the enemy of security”, which is perhaps a nicer way of saying it, but the most successful social engineering attacks focus on exploiting empathy rather than complacency. Just be careful and be aware, and remember that security procedures exist for a reason.
  - ICS/SCADA systems, due to inherent trust, are inherently insecure and are insecure by design.
    - And it’s more or less unfixable.

        - Tunneling doesn't fix it because they inter-communicate, so only one point is needed to compromise.
        - Encryption adds too much of a delay to these systems, because they are **highly** timing-sensitive and overhead introduces severe complications.

- ICS/SCADA vuln analysis vs. more common red team things…
    - Much more investigative – less necessary planning, more research, more contact with vendors, etc.
    - One device vs. one "topography" – physical, network, etc.
    - Kate likes this more because she can actually have effective change (and a much larger scope of improvement) by working with vendors.
    - She also likes it more because it's a new challenge each time.
- Per Kate, "segmentation is a **big** deal". Even MORE important with ICS/SCADA than it is in "normal" TCP/IP security!
    - The casino fishtank issue that Jthan mentions (it was actually a News item, not a Baddie) is in S3E5.

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 **59m38s**.

After Jthan's "Pissadministrivia" excursion…

Jthan's roommate's cat is nice and fat. His girlfriend's cat is a newcomer and he wanted to introduce the two so they'd get along. He doesn't have enough rooms in his apartment to do it right.

ANYWAYS, he thinks a lot of sysadmins have cats and he wants us to think about the cat situation in relation to the people situation.

Errata

- We ended up not editing the accidental death threat out. inb4 legal threat, IT IS NOT TO BE TAKEN SERIOUSLY.
- Jthan introduces us to abutments.
    - Kate has provided us an in-depth look.
- A Jim Beam warehouse did indeed burn down.
- And Jthan is indeed wrong again. Knob Creek does indeed come in multiple bottle sizes. Here are some.
- Jthan's ice failure can be found here.
- I absolutely missed an opportunity for a "It's a UNIX system; I know this!" joke at 19m25s. Darn it.
- RIP, Adam West.
- Kate's recording quality got a little dodgy from 41m54s to 42m13s because we-don't-know-why, but you should be able to hear her.
- There is, in fact, an RFC to reading IPsec RFCs.
- Paden mentions Jason Scott at HOPE; we had him on the show on S3E13. We recommend you give it a listen; he's pretty entertaining!
- Kate also linked us to this but I'm not sure why.
    - It's totally worth it though.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Habu	Silicon Transmitter	click	CC-BY-NC-SA 4.0
Outro	Apex	Bio Unit	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

There are currently no comments on this article.