Sysadministrivia

Linux, Lagers, and Late Nights

S4E3: "Insane in the Mainframe"

Posted 2019-04-01 03:59
Modified 2019-04-02 14:15
Comments 4

Navigation

Previous Episode	Next Episode
S4E2: "Repo, Man!"	S4E4: "Special Delivery"

Log

Recorded (UTC)	Aired (UTC)	Editor
2019-03-21 02:57:44	2019-03-31 19:27:30	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`aef620f7e80481a26010b9c39c8dfcc6d5e75669fa6c8241e17e1ef4d82cde8a`	click	click
OGG	`2e30eb7f18551e4d1e71ed71a0ad059f1b5c7d7d89ea8c681cd2f60a17d0fd2a`	click	click

Quicklisten:

We have Phil (@mainframed767) on to talk about mainframes. Yes, they're still being used and yes, they're modern implementations.

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

Just the Tip

- An introduction to LXC (Linux Containers)
  - He mentions haveged (pronounced "have G-E-D" or, if I'm in a rush, I say "have ged")
    - The SuperUser question I answered (I said StackOverflow, oops; same network) is here. Why it was downvoted, I'll never know.
  - He also mentions an optional dependency is dnsmasq, which we've mentioned more than once on the show before.
  - LXC is basically a cross between a virtualization (VM) and a chroot.
    - Know what OpenVZ/Virtuozzo is? Yeah, basically that.
  - LXC used to be the driving technology behind Docker (but as of Docker 0.9, Docker replaced LXC with libcontainer).
  - The kernel capabilities I mention can be found here.
    - You can find documentation on how to grant these capabilities in a Systemd unit here.

Notes

Starts at **8m56s**.

I was drinking a Guinness Extra Stout. Paden was drinking Absolut and Glenmorangie again. Jthan was drinking a lime Spindrift. Phil was drinking Highland Park 18-Year.

- Mainframes in the modern era!
  - Mainframes are not only still used, they are modern and **integral to modern global/enterprise business**.
  - Phil mentions Connor buying a used mainframe. You can find his talk here.
  - You can find access to the DISA STIGs here.
    - And mainframe-specific STIGs are here.
  - DES is a really bad idea, but many mainframe logins still use it...
    - The Baddie that was mentioned is S1E18. The solution was given in S1E21.
  - Patching in mainframes is typically pretty obfuscated/obtuse.
- You can find more about Phil (Soldier of Fortran) and mainframes here:
  - His talks
  - The talk I've seen and referenced (Mainframe hacking)
  - The IMP (Internet Mainframes Project) is here.

- His PoC||GTFO contributions (we have a mirror here):
  - #12, **A JCL Adventure with Network Job Entries**
  - #17, **Murder on the USS Table**
- His blog is here.
- Another mainframe hacker mentioned a lot, Chad, has a mainframe-hacking blog here.
- He and Chad also offer mainframe pentesting classes, which you can find here.
  - Mainframe pentesting is still pretty niche; they need all the passionate pentesters they can get!
- He mentioned the Logica breach…
  - and the IBM Websphere CVE and corresponding exploit.
- The z/OS emulator he mentions is here…
  - and an opensource full-stack (running an older mainframe OS), called Hercules, is here.
- He also recommends this z/OS on Hercules guide.

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 **1h12m35s**.

Jthan ponders whether it's "better", in terms of what you learn/experience, to work for a big enterprise or small business.

Interestingly, shortly after we talked about it, I found a nice summation/thread on Twitter of why the question may not have a direct answer.

Errata

- Contrary to what Paden said about LXC, you do NOT need to run/start libvirtd to use LXC – this is only necessary if you're using LXC as a backend for libvirtd.
- To give some context, this episode was recorded roughly a week after Facebook had a severe outage.
- Sure enough, on March 28 and March 31, new PoC||GTFO issues **are** in digital format and have made it to our mirror. :)
- The CIA sabotage manual is indeed still available.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Truckin	Bio Unit/Metre	click	CC-BY-NC-SA 4.0
Outro	The Opening Closing	P C III	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 Four

Comments

1. ## mouath

   2019-04-06 10:01 (1001 days ago)

   Awesome episode!

2. 2019-04-06 10:05 (1001 days ago)

   mouath- thanks! glad to have you listening!

3. 2019-04-07 05:44 (1000 days ago)

   Great episode. A small portion of my daily life is supporting zPDT (the emulated development environment for z/OS) and your guest gave a lot of great information about the attack surface of these systems. Also good to know that there are people dedicated to breaking into them; it's easy to assume that mainframe security doesn't need care and feeding because "none of the bad guys would even know where to start with them."

4. 2019-04-07 06:09 (1000 days ago)

   tim- thanks! i'm sure Phil would be glad to hear your support!