Sysadministrivia

Linux, Lagers, and Late Nights

S3E4: "More Audits Than the IRS"

Posted 2018-04-23 03:59
Modified 2018-04-23 02:02
Comments 0

Navigation

Previous Episode	Next Episode
S3E3: "Ranting Lunatics"	S3E5: "Remotely Interested"

Log

Recorded (UTC)	Aired (UTC)	Editor
2018-04-13 02:23:54	2018-04-22 20:33:48	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`a7046035b029c9620dc1e0265ec11247422644a4fd00a6c13ed082ef522ca6e1`	click	click
OGG	`3b38fac9c5416c504c01d16a16cf9a9b2ff0eec49dd9831e8a78fbefa0db73ac`	click	click

Quicklisten:

In which we talk about conducting audits and why hardware vulns are such a big deal. We also mention a charity event we want to do at HOPE!

- News
- Notes
- Sysbadministration Award
- Errata
- Music

News

- We're *hoping* (see what I did there?) to do a charity event at HOPE!
  - You can find the twitter thread here.
- Saks, Lord & Taylor had a 5 million account breach.
- There's malware floating around that pretends to be Kaspersky Antivirus.
- Panera Bread has become something of a joke among security researchers lately (except the joke isn't funny).
- Google is ending its URL-shortening service.
- Intel is not going to be supporting older CPUs for Spectre/Meltdown fixes.
- Under Armour's MyFitnessPal has had 150 million user accounts leaked via a breach.
- VPN providers are in hot water for "leaking" IP addresses via WebRTC...
  - Except all it does is leak your private VPN IP. It just looks like a LAN IP. The reaction to this is entirely overblown and misunderstood by paranoid people who don't actually understand what it means.
- Phoronix explained a little better why Clear Linux had such good testing results (which we talk about in S3E2).
- The Linux utility **beep** had a vulnerability...
  - Which was made worse by the patch that the researcher provided.
  - More info here.

Notes

Starts at **36m25s**.

I was drinking Jefferson's Reserve bourbon. Paden was drinking water. Jthan was drinking the 'Bout Damn Time IPA from Four Noses Brewing Company.

- Paden passed the CompTIA LXO-103! He talks a bit about how he prepped for the exam.
- This is super cool: `telnet mapscii.me` (source is available!) **(39m45s)**
- Just why **are** the intel SME and amd vulns so bad if they require root/admin access to exploit? **(40m25s)**
  - **Persistence**. If you get a virus, you can just wipe a machine.
  - With a hardware-level vulnerability like these, wiping the OS won't do anything since malignant code could have been injected into the hardware/firmware itself.

- Conducting audits **(43m28s)**
  - Security audits
    - We recommend you hire an actual InfoSec firm to handle this (as we've talked about in the past) as they have specialized training (or have an in-house dedicated InfoSec team/department).
    - We talk more about providing (**cursory**) self-pentests in S0E6
    - For more in-depth discussion on incorporating infosec contractors/firms, you may want to check out S1E14 and S2E18.
  - Backups
    - The backup processes are completing properly.
    - The schedule should be correct.
    - All hosts that SHOULD be backed up ARE being backed up.
    - A backup isn't a backup if you can't restore from it. "An untested backup system is not a backup system." Avoid the "Schrödinger Backup".
  - Inventory
    - Nmap is useful for comparing network points.
    - Make sure your asset tags, etc. are up to date, your hardware components are properly updated, etc. (dmidecode and python's psutil and dmidecode module (dead?) are very valuable tools for this).
  - Access
    - MySQL users are username and host-specific, your GRANT statements are up to date.
    - Shell users are appropriately locked/unlocked, octal modes and ownership on files are correct, etc. (mtree is incredibly useful for this. I recommend NetBSD's mtree. Building example for Linux can be found here.)
    - SUID/GUID are locked down.
    - SSH is locked down.
    - VPN access is revoked for employees or contractors no longer in service.
    - LDAP/other centralized authentication/authorization mechanisms **immediately** make so much of this easier.

Sysbadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(55m30s)**

T-Mobile responds to a security risk completely flippantly.

Errata

- There are actually four levels of PCI compliance, and you can find more information on PCI compliance at the site itself.
- After we ended recording, I did indeed read Jthan a bedtime story (specifically, this one that I found at random).

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	amusement park.	Ryan Little	click	CC-BY-SA 4.0
Outro	Coastin'	Defy the Mall	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 Three

Comments

There are currently no comments on this article.
