Sysadministrivia

Linux, Lagers, and Late Nights

S0E14: "A Failed Experiment"

Posted 2015-09-14 04:18
Modified 2018-02-21 20:38
Comments 0

Navigation

Previous Episode	Next Episode
S0E13: "Better Late than Never"	S0E15: "I Spy with My Little Eye"

Log

Recorded (UTC)	Aired (UTC)	Editor
2015-08-15 16:39:15	2015-09-14 04:18:48	brent s.

Verification

Format	SHA256	GPG	Audio File
MP3	ce6b007337c67a5f604be4aff1d74c31e5478241f68beba2a4d786c2d054dc8c	click	click
OGG	31d51ecef2f424b0bec5e4e3e576fe54e27d925cf086706aa3e9028df4ddcb69	click	click

Quicklisten:

In this episode, we talk about Certifigate (an Android vulnerability), another Lenovo oopsies, more Windows 10 privacy issues, the UNIX Rosetta Stone (by request of *MOQ* in our IRC channel), key management (by request of ‘‘chthnous‘‘ in our IRC channel), making everyday crypto easier, and data recovery.

- Notes
- Errata
- Music

Notes

- I mention that we’ve talked about Stagefright before (in S0E13).
  - We also suggest flashing a non-carrier-provided firmware for your Android device. We’ve talked about this in more detail in S0E3.
  - You can read more about Certifigate here and the TechRepublic article here.
- We didn’t actually cover Superfish before, though I thought we had.
  - Uninstall instructions for Superfish are here.
  - The Ars Technica forum post is here.
  - Apparently there is a (risky) removal process for Lenovo-replaced autochk here.
- Windows 10’s privacy policy is horrible. PLEASE SEE THE ERRATA, this affects Windows 7 and 8/8.1 as well. Sorry, Jthan.
  - We talk about Wi-Fi Sense before.
  - We also mention the Debian (Package) Popularity Contest. It dates back to 01.24.2004, and Ubuntu had their first release on 10.20.2014.
- We mention the UNIX Rosetta Stone
  - And there’s also the UNIX Toolbox
- I mention Tripwire (which has since gone commercial), AIDE, and the bootloader-integrity-checker I mention that I couldn’t remember the name of is afick. Alternatively, if you’re using a Secure Boot-compatible UEFI machine, you can use that. Yes, even on GNU/Linux.
  - A common “Evil Maid Attack” tool is the USB Rubber Ducky. More information is here. Mostly used by skids and amateur pentesters, but it is at least rather extensible.
  - And yes, there are ways to protect yourself from NSA’s SSH attacks, see here.
- Crypto Might Not Suck
  - I should do an entire segment on Tor, but suffice to say: do not trust it. At all. And if your OpSec sucks, Tor isn’t going to help. And yes, tor does in fact have commits from Navy staff, and the NSA has actively performed MitM attacks on Tor exit nodes. Plus who knows how many exit nodes are under NSA control/access?
  - Tails is also bullshit. It’s primary selling point is Tor, which as shown above is pointless- thus negating all their claims. It’s not even useful, it’s missing an actually usable environment.
  - They make absolutely laughable claims, like Tor is better than a private VPN.
  - You might want to use GRML instead, if you’re a Debian advocate.
  - Or you can build your own (better) alternative to Tails by using BDisk.
- When doing data recovery, be sure you’re using GNU ddrescue, **not** dd_rescue. There are some corner cases in which dd_rescue may be better for your use, but ddrescue is a lot easier to use (and sees more stability).
  - Also, don’t use dcfldd either.
  - I also mention TestDisk
  - and PhotoRec
  - The Arch wiki has some excellent resources/documentation as well.
  - We’ll probably do a segment on forensics and post-incident response/audits, but the Forensics Wiki is a great start. Just keep in mind that

Forensics != Data Recovery.
    - But we mention TCT. See also: Scalpel, Foremost, and the SleuthKit.

- I talk about FOSSCON. You should check it out!

Errata

- I **totally** was able to edit out the weird sound on Jthan's track. Boo-yah!
- Windows 10's privacy-infringing stuff is now backported into Windows 7 and 8. We weren't aware of this at the time of recording.
- **ssh-keyscan** is awesome. Usage is simple: `ssh-keyscan <Host/IP address of server> >> ~/.ssh/known_hosts`
    - I don't mention it, but also handy is **ssh-copy-id**. It allows you to set up pubkey authentication for a user on a remote server in one step. Usage: `ssh-copy-id <Host/IP address of server>`. You'll be prompted for your password, and subsequent connections will not use password auth.
- I said "sfldd". I meant "dcfldd".
- We forgot to talk about terminal servers and password cracking in S0E15 (should be released 09.27.2015), sorry! I've pushed them back into the topic list.
- Jthan, Macs definitely supports their own variant of PXE/BOOTP called Netboot. You can also use iPXE and can also bootstrap via DHCP.
- I couldn't remember the name of the protocol when talking about Tor. It's I2P. Something like Hyperboria should work (a lot better than Tor) as well.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Blip Stream	Kevin MacLeod	click	CC-BY 3.0
Outro	Kawai Kitsune	Kevin MacLeod	click	CC-BY 3.0

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

Author r00t^2
Categories (Pilot Season)

Comments

There are currently no comments on this article.
