Sysadministrivia

Linux, Lagers, and Late Nights

S1E2: "hunter2"

Posted 2016-03-14 04:08
Modified 2017-01-28 14:10
Comments 0

Navigation

Previous Episode	Next Episode
S1E1: "GHOSTv2: The Re-Hauntening"	S1E3: "Fuzzy-Wuzzy Was a Bugbear (Was He?)"

Log

Recorded (UTC)	Aired (UTC)	Editor
2016-03-03 03:37:15	2016-03-14 04:08:56	aaron k.

Verification

Format	SHA256	GPG	Audio File
MP3	a6eef2246118b6a85c54d2cbce95df318c1f0c501a38e5f649d8ff75fd8f144b	click	click
OGG	228917afbd033bcf5d1849f37396ae902e4c4f12ee60bed70d5c7dbfcb796455	click	click

Quicklisten:

Journalctl, lftp, passwords, WINE (yes, again), and acoustic/sidechannel crypto attacks.

- News
- Notes
- Errata
- Music

News

Starts at **3m23s**.

- The FTC is hitting Asus for making shitty router firmware, software, etc.
  - (Though it's more like just a slap on the wrist.)
- Linux Mint got fucked – hard and without lube.
- We talk more about this in the show notes.
  - This is why you don't use wordpress. lolz
- And ANOTHER ssl vuln, DROWN.
  - Affects/targets SSLv2, and yet again exists because of government-mandated weaker export encryption laws.
  - You can check for vulnerability here.
- Not really "news", but still hilarious: MSFT released .NET for GNU/Linux- as F/LOSS.

Notes

Starts at **8m49s**.

- DROWN is stupid and overhyped. But we sort of recap over various SSL-related vulnerabilities anyways.
  - DROWN is an acronym for **Decrypting RSA with Obsolete and Weakened eNcryption**
    - I told you it was stupid.
  - Their broken-ass piece of shit python scanner is here.
- We talk about some neat little features of journalctl and mention lftp. **(11m18s)**
  - The wget option I was thinking of is `--no-parent`. (e.g. For mirroring a specific directory, I would use `wget -e robots=off -r -N --no-parent -nH domain.tld/dir1/dir2/`.) Note that it does, however, traverse symlinks (this can be disabled by the `--retr-symlinks=no` flag, but ONLY if fetching via FTP. But it still won't get parent dirs (../).
- I didn't get a chance to talk about passwords because the co-hosts pull me down a tangent. **(15m56s)**
  - I really wanted to mention this and this. I'll keep bringing passwords up in the show until we get to talk about them, gorram it.
  - The "XKCD Algorithm" I mention is here, but I consider it bad advice. And Schenier agrees with me.
  - And Jthan actually defeated a (mild) on-air social engineering attack from me!
  - I also mention oclHashCat and JohntheRipper's MPI functionality (if you're using john, you'll probably also want to use the jumbo patchset).
  - And for password managers (I shared this link and their response), I like pass.
  - For generating passwords, I'm particularly fond of pwgen, and invoked usually via something like `pwgen -sy 64 1`. You might want to leave the -y off if you're generating MySQL passwords.

    - I talk about the cracking rig in S0E12.
    - Browsers are in general just terrible.
    - The title comes from this. Thanks, Kyle!

- WINE is (still) *Not* an Emulator! **(32m30s)**
    - I mention Cygwin briefly, which is sort of the WINE analog for Windows.
    - Recursive acronyms are fun!
    - As useful as it is, it needs to cut out that default file association bullshit.
    - WINE actually has a pretty robust CLI that emulates cmd.exe (e.g. `wine cmd.exe program.exe`). Need MS-DOS? Calling with `command.com` instead of cmd.exe will start DOSBox. (If that *still* isn't satisfactory, try giving FreeDOS a spin in a VM!)
    - The WINE compatibility database is here.
    - It also has regedit. (If you want to access Windows registry blogs without installing WINE, you have a lot of great options. You can even edit them!
    - Winetricks is awesome. You need to give it a look. Seriously.
        - Seriously.
    - And you can use native Microsoft-written libraries with WINE.
    - There's also PlayOnLinux, which has a limited (but still rather extensive) "pre-configured" library of programs with specialized tweaks implemented.

- "Acoustic Keyloggers" **(46m03s)**
    - The article Paden sent me is on Vice...
    - But this is nothing new.
    - Seriously, we've known about this stuff for a while already.
    - There's even a PoC!
    - I also mention Van Eck phreaking.
    - You can make your own laser microphone!
    - I suggest possible circumvention/prevention/negation against the various attacks would be a Faraday cage, "jamming" with junk RF signal on the same frequency, lead-lined... everything.
        - We're interested in hearing your creative ideas of circumventing these attacks! Let us know on Twitter or our Contact page!
        - By the way, I mention projection keyboards. Which are super cool! Unfortunately they're not very accurate.

Errata

- Our editor Aaron picked the music out for this episode!
- Aaron also makes a special appearance at **36m36s** to confirm an unexpected result- in a twist of the-butler-did-it proportions, the culprit of typing was *both Jthan **and** Paden*! (insert dramatic music sting here)
- Rainbow yelled at me because I neglected to mention that WINE works on FreeBSD (and presumably other BSDs) too! FreeBSD also has a Linux compatibility layer.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Glass Android	Lee Rosevere	click	CC-BY-SA 4.0
Outro	Glass Android	Lee Rosevere	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 One

Comments

There are currently no comments on this article.