Sysadministrivia

Linux, Lagers, and Late Nights

S1E15: "Backwards Passwords"

Posted 2016-09-12 03:45
Modified 2017-01-31 06:16
Comments 0

Navigation

Previous Episode	Next Episode
S1E14: "The HOPE Campaign"	S1E16: "Takes One to GNOME One"

Log

Recorded (UTC)	Aired (UTC)	Editor
2016-09-01 02:44:01	2016-09-12 03:45:00	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	39745f71e836f9c83eeb9577468d02e03bd4f55dcf11fc99a44fb804df302077	click	click
OGG	51f63b5ea03de77bf4d8cbe326bdebd9b4b238f495634b569b7e324d3f404dfd	click	click

Quicklisten:

A LOT about passwords (and we revisit the topic of HTTPS and general SSL/TLS auditing).

We mention it a lot during the intro- if you aren't familiar with what The Game is, you should. (If you are, we both just lost.)

- News
- Notes
- Sysbadministration Award
- Errata
- Music

News

Starts at **5m41s**.

- I totally forgot to mention it, but I was on an episode of the Radio Statler podcast!
- Hillary Clinton (well, her IT) used bleachbit to wipe her server. (Presumably.)
    - In addition to BleachBit, we mention DBAN and nwipe (which is included in the default package list for BDisk).
- An activist is compromised, and Apple patches three 0days as a result.
- Dropbox is telling users to reset their passwords, despite "no compromise"…
    - Except lol there totally was.
- FINALLY, a hospital that got slammed with ransomware is actually smart about it.
- Mozilla releases an alternative to Qualys' SSL Labs (though I think it's either bugged or their scoring is totally whack).
    - It's F/OSS and it even has a CLI utility.
    - The XMPP security scanner Jthan mentions is indeed XMPP.net.
- According to the FTC, password changes are bad security
    - And we talk about why that's wrong in the segment.

Notes

Starts at **19m58s**.

I was drinking water, but I mention Killian's Red. Jthan was drinking Telluride's Whacked Out Wheat. Paden was drinking Grant's Family Reserve whisky.

- Qualys has a Github repo full of awesome docs. **(14m46s)**

- Passwords are terrible. Let's get that out of the way. **(19m58s)**
    - But we don't really have anything "better" that can do what passwords do.
    - You need something: you can store in your brain instead of physical, you can change, can't be stolen physically, isn't biometrics (because lel).
    - It was also found that the department in question had no complexity requirements, just a rotation/expiration policy.
    - We also go on a tangent of how "previous password" detection might work- how many are authentication mechanisms storing it in plaintext, are there alternate ways besides a generated regex pattern or a simplified permutation being hashed, etc. If you've implemented this, please contact us!
    - The "luggage" reference is from Space Balls.

- And as a kicker, we didn't mention it in the show but I'm not convinced we should follow FTC's concepts of 'security'.

Sysbadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(50m42s)**

So funny. Despite being changed, I've redacted out his old password to avoid wide exposure of his generation schema.

```
10:20:49< jedijf> paden: good luck
10:50:25< jthan> KyleYankan: I'm not actually. Been awhile.
11:28:17< jthan> [REDACTED]
11:28:24< jthan> that
11:28:25< jthan> is
11:29:36< r00t^2> your password
11:29:49< jthan> well
11:29:50< jthan> for one thing
11:29:54< jthan> OBVIOUSLY NOT ANYMORE
```

Errata

- I said Jthan brought the Game back. I was wrong, after checking my logs- it was Paden. Oops.
- The story Paden references during the intro is here.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Plumy Tale	Dumbo Gets Mad	click	CC-BY-NC-SA 3.0
Outro	Bollywood Blades	Professor Kliq	click	CC-BY-NC-SA 3.0

(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.