Sysadministrivia

Linux, Lagers, and Late Nights

S2E17: "Garden of Deloittes"

Posted 2017-10-09 03:23
Modified 2017-10-08 18:42
Comments 2

Navigation

Previous Episode	Next Episode
S2E16: "Playin' Cornhole"	S2E18: "Dueling Banditos"

Log

Recorded (UTC)	Aired (UTC)	Editor
2017-09-28 02:27:58	2017-10-08 17:31:55	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`49b90e9a51ef18b327b6c27537b8ac52af20098bd3d7e16ffefb96fb0879b404`	click	click
OGG	`e58125e323dec7ab712422d07246c52cc15d6a5e2e543e09ab44976d4f1fd140`	click	click

Quicklisten:

We talk about Glances (which we mentioned in S2E16), Samba, and opensourcing company code.

- News
- Notes
- Sysbadministration Award
- Errata
- Music

News

- There’s a new bill out to strengthen IoT security
- macOS High Sierra’s keychain is FUUUUUCKED
- Ransomware is now demanding nudes instead of bitcoin
- Heathrow airport police demanded a prisoner rights’ activist’s passwords for his encrypted devices and he refused, landing him in custody and released on bail 9 hours later
- Equifax directed users to a spoofed site because they can’t even remember their own domains
- Equifax CEO resigned (and gets 90million USD out of it?)
- Adobe leaked their private PGP key. Blatantly. By their own DFIR team.
- Avast/Piriform’s ccleaner was trojaned for about a month
- Google Play’s new protection software failed to identify older malware

Notes

Starts at **18m02s**.

I was drinking 10-year Bulleit Bourbon. Paden was drinking Glenlivet Founder’s Reserve. Jthan was drinking Jameson.

- Paden talks about glances (which we mentioned in S2E16).
  - He runs through some of the features; you should be able to glean this from the documentation/trying it out
  - (He highly recommends it)

- Jthan talks about some woes with samba **(24m58s)**
  - TL;DR: Jthan turned up a new storage box with ZoL, Samba don’t play that way
  - He has an Active Directory-backed auth system that Samba on Illumos can map directly to…
  - And it can map Samba/AD accounts as local users
  - …Except GNU/Linux don’t play that way, holmes. It does the above in reverse.
  - Winbind? No apparent way (unless you deep-dive into PAM) to use it to circumvent this.
  - The fix? He had to join Samba to AD, join the box via Kerberos and Winbind, and **group** checking is done via LDAP.

- I talk about opensourcing company code **(34m33s)**
  - Firefox 57 is moving to Webextensions…
  - Which means all plugins need to be re-written.
  - So the plugin that my work releases was re-written…

- But because the storage engine changed and plugins are no longer allowed to use the filesystem directly, and the new config uses JSON instead of XML, I wrote a configuration converter…
- But these configuration files can have sensitive data, and I personally wouldn't want to provide that info to a third party.
- So I opensourced it but the question remains, *what is the best way to encourage other companies to do this?*
- The "you can't make money from opensource software" idea is dead; look at RedHat, for instance (a la RHEL/CentOS).
- Linksys did, indeed, have opensource firmware. And it wasn't Linus Torvalds that criticized TiVo but rather RMS (of course).
- Key tips/takeaways:
  - Keep your proprietary data stripped out from the project and/or included in a totally separate (private) repository.
  - Make it easy for people to contribute back to your software.

Sysbadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(43m40s)**

A major accountancy security/auditing firm (Deloitte) leaked information about its highest-profile clients.

Some highlights:

> ..The Guardian understands Deloitte discovered the hack in March this year, but it is believed the attackers may have had access to its systems since October or November 2016…

> …The hacker compromised the firm's global email server through an "administrator's account" that, in theory, gave them privileged, unrestricted "access to all areas"…

> …The account required only a single password and did not have "two-step" verification, sources said…

> …Emails to and from Deloitte's 244,000 staff were stored in the Azure cloud service, which was provided by Microsoft. This is Microsoft's equivalent to Amazon Web Service and Google's Cloud Platform…

Wow. Great. Job.

Errata

- I am still in a battle with my ISP. You're going to notice me become de-synced from time to time; sorry!
- Jthan and I were talking about augeas during the intro. (Not "aegis", Paden.)
- The Equifax spoof site no longer redirects to Google; it now resolves to localhost.
- I mentioned that Juicero shut down
- NSS is Name Service Switch
- When speaking about proprietary software, I said "you're lucky if they release a vulnerability at all" – I meant "you're lucky if they release a vulnerability *announcement* at all".

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Say It Anyway	P C III	click	CC-BY 4.0
Outro	Graveyard Shift	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 Season Two

Comments

1. **Anon**

   2017-10-16 03:55 (1538 days ago)

   re: your rant on samba -
   I use quite a bit of ZOL on fedora, and samba. Also EMC w/ AD & EMC's LDAP.
   In my opinion, the winbind layer may be unnecessary, but you stumbled in the right direction.

   Samba can do "pure ADS" auth. winbind was broken in samba 4.0-4.2:
   https://wiki.samba.org/index.php/Configuring_Winbindd_on_a_Samba_AD_DC

   I'm using samba 4.4 and I have no problems on fedora 24. If you had gone samba 3.6, it might have worked out of the box. shell account exists but **LK** is fairly common in local /etc/passwd, for many apps.

   Haven't checked up on illumos in a couple years, but the openSolaris 'idmap' was a one-off kind of beastie, and the 'smb' implementation can be in-kernel, or the more generic userspace smbd. I wonder if your choices/defaults lead you to such a two week ordeal.

2.

   2017-10-16 04:10 (1538 days ago)

   Anon-

   thanks for this! i've passed it along to jthan.
