

Sysadministrivia

Linux, Lagers, and Late Nights

S1E19: "I Died but This Department Won't"

Posted 2016-11-07 10:04
Modified 2017-01-29 01:23
Comments 0

Navigation

Previous Episode	Next Episode
S1E18: "Pr0n and Nigerian Princes"	S1E20: "My Markup Brings All the Parsers to the Yard"

Log

Recorded (UTC)	Aired (UTC)	Editor
2016-10-27 02:47:37	2016-11-07 10:04:35	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	284a5018bedd3a816c76e4ad42b7be82d6f77de229babe9489451f6be785e5dc	click	click
OGG	0596ed8eebaebf0e4c8cffa77b3f57b357ab2a3cadb62c1c9d112fb16e818b0e	click	click

Quicklisten:

Developing tools/resources/etc. in-house versus using third-party and the "hit by a bus" clause.

- News
- Notes
- Sysbadministration Award
- Errata
- Music

News

Starts at **5m44s**.

- British Court extradited Lauri Love
- Globalsign is broken
- CCleaner users are having some key mishaps
- The Locky variant Thor came online, and the Locky fix doesn't work
- There was a huge Linux kernel security flaw, and even Android phones are affected
- There's also a huge security vulnerability ripe for eavesdropping in 4G LTE
- Dyn (poor, poor Dyn) has released a statement on their Internet-crippling DDoS attack
- There was a discovered passive data leak at Verizon
- A PAC has leaked credit card numbers
- It is now a federal crime to bring a Note 7 onboard an aircraft
- A new "acoustic keylogger" method was released that uses VoIP as the vector
 - We mention Dvorak (and other alternative layouts) in S0E5

Notes

Starts at **14m44s**.

Jthan was drinking rum (he neglected to say what kind). Paden was drinking Heineken. I was drinking Knob Creek again.

- How do you decide between rolling your own solution as opposed to going with a third-party provider?
 - Jthan brought it up in a discussion- should use something like OpenVPN AS/OpenVPN on your own or something like Cisco's VPN?
 - Use libvirt and build out your own system or deploy a VMWare lab?
- The "hit by a bus" clause (**37m55s**)
 - In other words, "how to protect your company in the event of your death/capture/sudden and permanent/long-term unavailability"
 - Important things to consider preparing for your extended/permanent absence/leave:
 - Project mapping (TODO lists, processes, etc.)
 - Handling key escrow
 - Documentation

- Deliverables handoff
- Shared password is a bit tricky. We mention:
 - pass
 - Vaultier
 - I have no knowledge or experience with it, but there's also Teampass. It also supports file/image attachments as well, so you can attach binary keys.
- At the end of the day, you need to decide between the quality of the end product or the quality of your documentation.

Sysadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(57m00s)**

It took us forever to mention this one, but passwords were reset and delivered... over the compromised vector during the DNC leak.

Errata

- None!

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Creepy	Bensound	click	CC-BY-ND 4.0
Outro	Sonic Bloom	The Night Beats	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.