Sysadministrivia

Linux, Lagers, and Late Nights

S1E18: "Pr0n and Nigerian Princes"

Posted 2016-10-24 04:42
Modified 2017-02-11 20:13
Comments 0

Navigation

Previous Episode	Next Episode
S1E17: "Is that Your Gun (or Are You Just Happy to See Me?)"	S1E19: "I Died but This Department Won't"

Log

Recorded (UTC)	Aired (UTC)	Editor
2016-10-13 03:04:21	2016-10-24 04:42:00	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`818261220a3b8b6078c1030fec6ef856ae0c538dd55697781a253ecf52939496`	click	click
OGG	`2f12093459bc1150c98a61ea4c74e1a070c48f791040c730db40596471a269ad`	click	click

Quicklisten:

Using VPNs in a corporate use case and surface discussion on running your own email server.

The birth of Jthan’s “VPN noise”.

- News
- Notes
- Sysbadministration Award
- Errata
- Music

News

Starts at **5m42s**.

- A story of quitting a one-man IT department
  - This probably should have been a discussion topic…
- Snowden designed a phone case that “detects/prevents monitoring”
  - > *inb4 snakeoil*
- Adding a shebang to files in Vim automatically
  - This also probably should have been a discussion topic…
- Samsung has requested the cessation of sales for Galaxy Note 7
- EFF fights against the Rule 41 changes

Notes

Starts at **16m40s**.

Jthan was drinking Chai High from Avery Brewing Company. Paden was drinking Grant’s Family Reserve Whisky. I was drinking Knob Creek (once again).

- We shortly recap BSides DE 2016.
- VPNs (Virtual Private Networks) can be a HUGE asset to your company.
  - The Microsoft VPN, or PPTP, has been around for a looong time, and has some major security issues.
  - macOS and iOS10 don’t support PPTP (source).
  - The Linux version of PPTP server is called Poptop, and the client is (aptly-named) PPTP Client.
  - IPSec is pretty popular. Windows has native L2TP / IPSec support, as does Mac OS X/macOS, iOS, Android, etc.- just about everything supports L2TP/IPSec. The Cisco “variant” is IPSec IKEv1 with XAuth extensions. Linux has several different projects that support IPSec and various iterations of it (FreeS/WAN (now defunct), Openswan, IPSec-Tools (including e.g. racoon)- which is what Android uses, and Strongswan. I recommend Strongswan).
  - Windows users (and Linux users…) can use ShrewSoft for IPSec if they need drop-in support for Cisco-style IPSec.
  - Microsoft’s PPTP replacement is SSTP, and if you want to run an SSTP server on Linux you’ll need to use SoftEther. Thankfully, the standalone SSTP Client for Linux feels a lot cleaner.
  - But OpenVPN is, by far, my personal favourite. (The community/opensource version also has a pretty fantastic HOWTO.)
  - USE SELECTIVE ROUTING WHENEVER POSSIBLE, don’t push a full default route to your clients!
  - Jthan also mentions Tinc. However, it is not viable for a company VPN.

- Email is omnipresent and messy as hell. **(39m24)**
  - Email has been around for a LONG. TIME. But is starting to show its age.
  - Email has a TON of RFCs.
  - I mention POP1 (RFC918).
  - MISCONFIGURED EMAIL SERVERS CAUSE SPAM. DO **NOT** RUN YOUR OWN MAIL SERVER IF YOU HAVEN'T DONE A TON OF STUDY AND TESTING FIRST.
  - If you choose to, use Postfix and Dovecot.
  - Learn the ins and outs of, and set up:
    - SPF
    - OpenDKIM
    - DMARC
    - Make sure your PTR/rDNS records are correct
    - SpamAssassin…
    - and the ClamAV plugin
    - and ALWAYS AND REPEATEDLY TEST TO MAKE SURE that you are NOT an open relay!
  - ArchWiki's Postfix article and Dovecot articles (and the suggested articles on the right sidebar) are immensely useful, as are the Gentoo articles.
  - This thread has some useful information as well (but be forewarned- it has a LARGE amount of noise/signal).
  - The SwiftOnSecurity thread on Twitter is here.

Sysbadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(56m18s)**

A bank is enforcing 8-digit passwords. Yes, you read that correctly – DIGITS, not characters.

Errata

- Jthan fixed his mumble… :P
- Paden refers to "Rule 43" when we're discussing the EFF rule 41 thing. He meant Rule 34. (Obligatory.)
- **srg** from our IRC channel has pinged us as let us know that he wrote an article for postfix/dovecot as well. And he totally reminded me of Sieve, which is super handy for giving users the power to perform their own filtering.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	White Eagles	Simon Mathewson	click	CC-BY-NC-SA 4.0
Outro	Wife (Johnny_Ripper Remix)	strangerfamiliar	click	CC-BY-NC-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.