

Sysadministrivia

Linux, Lagers, and Late Nights

S0E11: "Proto-Router"

Posted 2015-07-13 03:23

Modified 2018-12-03 03:56

Comments 0

Navigation

Previous Episode	Next Episode
S0E10: "Jthan Tries to Edit"	S0E12: "It Hurts when IP"

Log

Recorded (UTC)	Aired (UTC)	Editor
2015-07-03 04:42:42	2015-07-13 03:23:10	brent s.

Verification

Format	SHA256	GPG	Audio File
MP3	0034de006ef16710edf39a18ed62e6c7303f1cab0cc443682f5284e06d682c70	click	click
OGG	4592df6eae5b6a176d914cc85d062c07be39727598fc11ebf49a05f39ae8e334	click	click

Quicklisten:

"InfoSec Speaks!"- where I get some input from the InfoSec crowd via Twitter. We also talk about running your own router box, briefly talk about VPNs, IPv6, and a really stupid decision MSFT made with Windows 10.

- Notes
- Infosec Speaks
- Errata
- Music

Notes

- I don't see anything about individually shipped packages per RMA shipping policy Seagate's
- Jthan mentions the importance of a good toolkit for your cabs. I'd recommend the following:
 - Telescopic magnetic grabber
 - something like this
 - a good precision toolkit such as this or this
 - a beefier screwdriver set
 - and, if you maintain your own cage/cabs as well, these are pretty dang handy.
 - cable management is very important, so don't underestimate it
 - labeling your stuff is also SUPER important.
 - and don't forget your livecds! (We'll be doing an episode on this coming up, so get your USB sticks and optical drives ready!)
- I searched but couldn't find any purse that explodes into nanchaku. :(
- Windows 10's Wi-Fi Sense is stupid. And dangerous.
 - But hopefully it won't work with things like EAP-TLS.
 - And yeah Google's Wi-Fi mapping opt-out and MSFT's bullshit are, indeed, incompatible.
- iproute2 obsoletes net-tools
 - and ARIN is indeed out of IPv4 allocations
 - I freakin' love Shorewall
 - Shorewall has super awesome rate-limiting
 - And its documentation kicks ass
 - Internet routing protocols such as BGP, RIP, OSPF, and (E) IGRP are only needed if you need to be your own border/gateway router directly connected to a backbone provider.
 - Quagga is my recommended internet routing software (forked originally from zebra)
 - There's also BIRD
- As mentioned, a RIPv1 vulnerability recently announced
- For Wireless functionality, you can either:
 - Throw some WLAN cards in your routerbox and use hostapd (VERY limited range/coverage)
 - Get some old OpenWRT - compatible devices and run them in bridge mode, and run a cable backbone to the switch connected to your routerbox, or
 - (My personal recommendation- and no, I'm not being paid) Ubiquiti's Unifi-AP system, switched into a PoE switch (it doesn't *have* to be Ubiquiti, but they make good stuff at an affordable price), and connect that PoE switch into your normal backbone switch
 - the APs are even fully OpenWRT compatible themselves!
- I mention that PacketPushers published a list of free reference books
 - And my personal recommendations:

- The Pink Book (named after their 2nd edition)
 - NoStarch Press' TCP/IP Guide (and the author does indeed provide it online for free)
 - I fail to mention it specifically, but the LARTC HOWTO is free and a **great** resource as well.
 - Also failed to mention but a fantastic resource, the RUTE is great for Linux beginners (it seems the site no longer offers the book. It's under a distributable license, though, so we're hosting a copy).
- IPv6 has many of the same concepts as IPv4, but this is a good start to learn the difference.
 - You can test a website's IPv6 compatibility here, here, here, here, and many others
 - You can test your local connection here
 - And also check out HE's TunnelBroker.net for an IPv6 tunnel. They also offer IPv6 certification. It is, indeed, free.
 - Sixxs also offers free IPv6 tunnel brokering and education.
- Also, NIST has changed the requirements for Random Number Generation.
 - Shorewall's documentation talks about the 'Roadwarrior setup' (for those that aren't aware, this is what I mean by "roadwarrior"; not this.)
 - The OpenVPN HOWTO is super helpful, and you can use it to route through to the Internet by enabling packet forwarding.
 - PPTP sucks, even when running on GNU/Linux.
 - Not only is MS-CHAPv2/MPPE encryption and auth broken, it's broken hard. Like, really hard. And we've known this since 1998. STOP USING PPTP.
 - If you'd rather not use cloudcracker, while oclHashcat is *awesome*, it isn't presently supported. You'd need an FPGA-based cracker, something like this. Or, if you have some time, Asleep can be used perhaps. But really, it's super easy to break.
 - IPsec (The GNU/Linux implementation is StrongSwan / OpenSwan)
 - The "IPSec" part is (sort of) like PPTP's MPPE, whereas L2TP is kind of like the PPP/MS-CHAPv2 implementation, if comparing to PPTP
 - Except, you know. It doesn't suck.

Infosec Speaks

Many thanks to all that contributed input! It was really great to hear from them!

NOTE: Some of the following have been modified from their original form to be more easily read in US English. I have included a link to the original tweet for your reference.

We asked:

If you could give one piece of advice to system/network administrators/engineers, what would it be? (12:49 AM – 2 Jun 2015)

These are the replies we got.

Learn to triage problems well, and learn it from people who do it day in and day out. – @hacks4pancakes, 12:57 AM – 2 Jun 2015

Nail down the fundamentals. – @fugueish, 12:59 AM – 2 Jun 2015]

RTFM, of course. :) – @CodedBe, 1:00 AM – 2 Jun 2015

Never accept 24x7x365 on-call duty. Rotate monthly with someone under Director of Operations. – @GeneticSequence, 1:07 AM – 2 Jun 2015

Vodka gives less of a hangover than whiskey. – @tobermatt, 1:07 AM – 2 Jun 2015

Make sure to take your vacation days throughout the year. – @GeneticSequence, 1:08 AM – 2 Jun 2015

Project work with Milestone Bonuses and get it in writing; they may not pay otherwise. – @GeneticSequence, 1:09 AM – 2 Jun 2015

Don't just learn what buttons to push and/or when. Learn the fundamentals of your technologies. – @t0x0pg, 1:24 AM – 2 Jun 2015

Make sure 20% of your time is spent not doing administration/engineering. Get an unrelated hobby. Stay off the forums. - @J0hnnnyXm4s, 1:53 AM - 2 Jun 2015

Learn to know when to listen, and when to be aggressive like bear. - @hacks4pancakes, 1:54 AM - 2 Jun 2015

If you are a lone admin: don't give up your holidays just because someone derped. - @chkconfig, 1:59 AM - 2 Jun 2015

Find a (third-party) IT support provider and get the business to buy rolling hours just in case. - @chkconfig, 2:00 AM - 2 Jun 2015

Compliance doesn't mean secure. - @IDSninja, 2:04 AM - 2 Jun 2015

Buy one of those purses that explodes into nunchucks. - @J0hnnnyXm4s, 2:11 AM - 2 Jun 2015

You gotta be crazy to beat crazy. - @PeterGanzevles, 4:32 AM - 2 Jun 2015

Always quote your regexps, because you just wrote a buncha pipelines and sub-shells! :-P - @Dave_Korn_, 4:34 AM - 2 Jun 2015

Get experience in non-tech areas too. Gives you new perspectives. - @unfo, 6:04 AM - 2 Jun 2015

Make sure your response plan is proactive rather than reactive. - [https://twitter.com/mzbat @mzbat], 7:16 AM - 2 Jun 2015

We can't do our job without you guys, and without your cooperation. We aren't the enemy. - @da_667, 7:18 AM - 2 Jun 2015

[REDACTED] - @porthunter, (redacted)

Learn how easy antivirus is to bypass, how weak passwords are, common social engineering attacks, ... try to understand the concept of credential theft and view rights from an attacker's perspective. ... e.g. "If I can control your box, I may as well have all your privileges." - @scriptjunkie1, 1:57 PM - 2 Jun 2015, 2:11 PM - 2 Jun 2015, 2:13 PM - 2 Jun 2015

Errata

- When discussing OpenVPN, I say it supports both tunneling and "peer-to-peer"; I actually meant **TAP and point-to-point** ("Bridged"-mode). Pretty similar concepts, but there are differences. See here and here.
- When discussing PPTP, I mention the weak security of MS-CHAPv2. That's actually the **authentication** method; the encryption is MPPE (but they're pretty closely intermingled, so potato/potato).

Music

Music Credits

music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Exit the Premises	Kevin MacLeod	click	CC-BY 3.0
Outro	Rhinoceros	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 (Pilot Season)

Comments

There are currently no comments on this article.