

Sysadministrivia

Linux, Lagers, and Late Nights

S0E12: "It Hurts when IP"

Posted 2015-07-27 05:11

Modified 2017-01-28 10:49

Comments 0

Navigation

Previous Episode	Next Episode
S0E11: "Proto-Router"	S0E13: "Better Late than Never"

Log

Recorded (UTC)	Aired (UTC)	Editor
2015-07-17 03:01:56	2015-07-27 05:11:23	jonathan d.

Verification

Format	SHA256	GPG	Audio File
MP3	544273c8afb0cb2969fdf8a1d2cefa0c79b4a81971856667adf495e9d8197dc2	click	click
OGG	8c6b637017a61da1f372630a27017a9c848411efdbdb327bc92d81f1f00990ce	click	click

Quicklisten:

Firewalls, presenting proposals for (change) management, git/gitolite (and blast on third-party git hosting), ethernet media classifications, DIY cracking rigs, pentesting tools, and more regular expressions.

- Notes
- Errata
- Music

Notes

- The thread where the guy clearly doesn't understand DROP vs. REJECT is, *I think*, here (it might be a closed group). I know that was ONE of the threads I got into an argument with an idiot on... WAIT, wait. Nope, it was this one. Turns out the same guy is in my LUG. We haven't killed each other yet. (Trust me. It's about 2/3 into the entire comment section. If you're feeling lazy, find-in-page for "iptables is your friend".)
- I wonder what happens when jthan's openvpn fails to start and he can't SSH in to fix it.
- Git is awesome.
 - Seriously, read the book
 - and read Git Magic too.
 - Seriously.
 - It'll stop you from making stupid mistakes.
 - Or asking stupid questions. (Like jthan does, because he never reads documentation.)
- GitLab has their software available. But it's bullshit.
 - And so is GitHub.
- So in steps Gitolite!
 - Its documentation is great.
- Jthan and I once tried to port NetBSD to the first release of the SheevaPlug.
- If you know nothing about ethernet cable classifications/categories, this might help.
 - but I recommend these.
- I usually get my cables and heads from Sewell Direct. No, they didn't paid us. I just really like their prices and service.
- I mention the 'Hacker Arsenal'.
 - You should get the Nmap book, because it's written by the same guy that wrote nmap.
- There's also a HOWTO for DIY cracking rig
 - You can use Hashcat with that.
 - or specifically, oclHashcat, which uses CUDA / NUMA.
- There are some pretty interesting 3DES/DES papers out there
 - There's even a hardware cracking rig for it, via Pico FPGA.
 - One could assemble a 3DES rig by combining pipelines across multiple FPGA's, is my guess.
 - You'll also want to check out NSA@home. For SHA-1/MD5, but a good example of why FPGA's are awesome.
- RegEx Crossword - Thanks, Lyz!
 - You can learn regexes here, here, or here (among many others).

Errata

Jthan tried to edit this one too. I tried to clean it up.

- Jthan, a web + VPN + SSH-only-on-VPN server != a “simple server”. A simple server runs one dedicated service.
- Turns out in modern GNU/Linux + iptables (at least with shorewall), opening a port with no service behind it will list the status as “closed” in nmap, which is the same result from a DROP. I could have sworn, at least on early 3.x kernels, that the behavior I described occurs instead.
- The kernel actually has a SHIT-ton of lines of code.
- FPGA's are **Field Programmable Gate Arrays**
- Thanks to Forge in our IRC channel, he points out:

```
< Forge> NUMA = NonUniform Memory Architecture, unrelated.  
< Forge> [AMD] and Intel both back OpenCL.  
< Forge> CUDA is Nvidia proprietary.
```

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Black Vortex	Kevin MacLeod	click	CC-BY 3.0
Outro	Ouroboros	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.