Sysadministrivia

Linux, Lagers, and Late Nights

S3E10: "DNS Near"

Posted 2018-07-16 03:59
Modified 2018-07-15 05:19
Comments 0

Navigation

Previous Episode	Next Episode
S3E9: "Git Outta Here"	S3E11: "But First, Let Paden Take a SELFie"

Log

Recorded (UTC)	Aired (UTC)	Editor
2018-07-08 21:16:27	2018-07-15 01:08:36	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`8d27fc10fe57e92b0a0725ac003e81bb75a24faf7056711d80b8de2753ee345d`	click	click
OGG	`f9adce12098032fb0db2c6badeac88e34c0500952d9e790b3b1d956352abc1ba`	click	click

Quicklisten:

It was, in fact, DNS (this time!).

We talk about some basics of DNS via a bird's-eye-view of how it works.

- News
- Notes
- Sysbadministration Award
- Errata
- Music

News

- Data for mobile apps using the Firebase backend has been breached.
- Kazashkstan caught engaging in Internet censorship via speed throttling that targets political rivals.
- Two 0day exploits have been discovered in a PDF with a joint effort between Microsoft and ESET.
- A VA eBenefits account has been compromised.
- Marketing firm Exactis has leaked 340 million accounts (including contact/personally identifying information AND further habitual/lifestyle/etc. data correlated to those).
- It has been ruled by the Supreme Court that the Fourth Amendment applies to cell phone location data. (Hooray!)
- A man attempted to hijack a domain at gunpoint and is sent to prison for 20 years.
- Tapplock, the "smart padlock" (notorious by now for having a biometric auth via fingerprint scanning that is thwarted by… a jeweler's screwdriver) has another attack surface as well.
- Gentoo's GitHub repositories were found to be compromised (but it does not seem to be a serious issue per Gentoo).

Notes

Starts at **20m17s**.

I was drinking water. Paden was drinking a "diet soda" (he didn't specify which). Jthan was drinking a Miller Lite.

- DNS (Domain Name System)
  - (I mention in a throwaway comment nmap, which we've talked about before, and masscan.)
  - It serves primarily as a human-friendly directory for IP addresses.
  - There are Authoritative Nameservers, Resolvers, and Root (Name)Servers
    - Authoritative serve records and their contents (e.g. "foo.bar.com is an A record for 1.2.3.4")
    - Root servers operate with registrars and authoritative nameservers to "learn" the domains and develop a query path for resolvers to take. Resolvers (which usually cache the records they look up, and can either resolve for a specific domain or "recurse" to find other domains) then serve records to clients (browsers/workstations, etc.) — which may also perform caching of their own as well.
  - There are a multitude of DNS record types. You can find an extensive amount of RFCs for DNS here and here. It is highly recommended you read them.
  - We mention DNSSEC in passing, but there are some alternatives being discussed.
  - Jthan brings up DNS over HTTPS (currently in draft format). I mention that for one, Unbound can support DNS over TLS, which I argue is better.
  - We also talk about glue records. For an example of this, do a WHOIS (note the authoritative nameservers) and a DNS analysis on sysadministrivia.com. ;)

Sysbadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(44m10s)**

A betting/gambling site, BetVictor, leaked creds to its own infra … via a help article.

Errata

- Our audio was TOTALLY off for this episode, so sorry! Paden was totally blown out (I received the recording in that condition), and Jthan was peaking a couple times (and he almost never peaks). Sorry!
  - He also had a baby on his lap, so there’s some background noise we couldn’t remove. Apologies.
- The SRV record is no longer a draft, but is now a proposed standard.
- It appears that Unbound does not (yet) support DNS over HTTPS, but it DOES support DNS over TLS.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Say It Again, I'm Listening	Daniel Birch	click	CC-BY 4.0
Outro	Suddenly It Occurs To Me There's No Ocean Here	Artificial Intelligence in Texas	click	CC-BY-SA 4.0

(All music is royalty-free, properly licensed for use, used under fair use, or public domain.)

Author r00t^2
Categories Season Three

Comments

There are currently no comments on this article.
