Sysadministrivia

Linux, Lagers, and Late Nights

S2E14: "Short-Term Memory"

Posted 2017-08-28 03:59
Modified 2017-09-01 12:24
Comments 0

Navigation

Previous Episode	Next Episode
S2E13: "This Server Ain't Big Enough for the Two of Us"	S2E15: "Playing HopskotSSH"

Log

Recorded (UTC)	Aired (UTC)	Editor
2017-08-17 02:30:25	2017-08-27 15:36:30	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	9fca13ba5ca300a64426a7886c5c400d42b4fae421b75eb7a2f8f82aee990788	click	click
OGG	4faca5e0d8faada57cb05cc86c79055f4555f77127c10e37a45d721c03db33ba	click	click

Quicklisten:

We talk about Bill Burr rescinding his recommended password complexity guidelines, ransomware victims and the apparent rise in malware infections, opensource tools to help the fight against phishing, and uses for ramdisks.

- News
- Notes
- Sysbadministration Award
- Errata
- Music

News

- Marcus Hutchins has been declared not guilty (because duh) after being detained post-DEF CON.
- FCC has been sued because they haven’t released details on their DDoS.
  - The FCC has also claimed that citizens “don’t need broadband/fast Internet access”…
  - and congress is getting sick of FCC’s shit.
- Bill Burr has officially denounced his password complexity recommendations (better non-Gizmodo source)
  - But he shouldn’t have. I explain why.
- US Army stops using Chinese drones
- Microsoft Icons being used to masquerade PE (“portable executable”) files with special icons
  - We discussed something similar to this (“Badtaste”) in S1E13.
- Fosscon was August 26th! (We’ll talk about it in detail in the next episode)
- BSidesPhilly is December 8, 2017.

Notes

Starts at **11m45s**.

I was drinking water again. Paden was drinking Stella Artois. Jthan was drinking Boulder Beer’s Bump ‘n Rind.

- We discuss the password complexity requirements in greater detail
  - We talk about passwords in general a LOT: S1E2, S1E15, S2E3
  - Jthan talks about the method he uses, which is still a good method.
  - My original comment on the (private) Facebook post is as follows:

> my take on this is this:
>
> 1.) you should have strong passwords, as laid out by bill burr originally. the better randomization behind it, the better; the wider the character selection space, the better. the longer, the better. no real words.
> 2.) you should be using a unique password for every authentication where possible.
> 3.) (and this ties 1 and 2 together) you should **use a non-cloud-based authentication/credentials manager**. THIS is where we, as IT, have failed. we have not failed by requiring complex and good-entropy passwords- we have failed in providing our users an easier way of doing things the right way.
>
> though, i imagine some of it may be a cultural issue as well.
>
> further, i hate the “correct horse battery stapler” method because the people that tout it as the end-all be-all don’t realize that **crackers are now, and have been for quite some time, able to bruteforce using wordspace instead of characterspace**. schneier agrees with me (find in-line for “This is why the oft-cited”)…

- 38% of ransomware victims pay the ransom **(27m15s)**

- Opensource tools to fight phishing **(38m47s)**
  - IsThisLegit
  - Phinn

- Ramdisk uses, etc. **(39m49s)**
  - I start off talking explicitly about initrds/initramfses
  - But Jthan was talking in a more general sense of memory-driven filesystems (such as tmpfs, overlayfs, etc.)
  - They help a lot for performance since it lets you perform I/O operations into RAM instead of storage
    - The Nagios resources he mentions can be found here and here
  - Handy for diskless/thin-client booting over NFS
  - ClamAV scanning attachments would be copied into memory-driven filesystems
  - Handy for making modifications when booted inside liveCD’s etc.
  - Package manager caches
  - Jthan used it for PhenVar for faster performance in SQLite

Sysbadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(54m13s)**

A smartlock company ended up locking all of their customers of a certain model out.

Errata

- BSidesDE 2017 tickets haven’t gone on sale yet, and the official dates haven’t actually been announced (the dates Paden gave were for 2016, not 2017). However, if you’re sneaky like me, finding their CFP for 2017 isn’t too difficult.
- The theory I was thinking of is called the Theory of Everything.
- The numbers I give on cracking stats are remarkably low. This should provide some insight, as does this.
- I said Btrfs in regards to snapshot pointing; I meant ZFS.
- DANG IT, I can’t believe we forgot to mention this but much thanks to Ivan Tomica (@IvanTomica on Twitter) who very helpfully pointed out that we forgot zram! It’s like a normal ramfs except it’s compressed.
- A bonus…

```
14:00:57 < r00t^2> drunk jthan is 100% best jthan
14:01:19 < r00t^2> fyi, he gets *gone* in S2E14, so keep an eye on your clients
14:01:29 < r00t^2> should publish at midnight
16:20:27 < jthan> I don't get gone
16:20:41 < jthan> fuck off
16:20:42 < jthan> ye wanker
16:29:04 < r00t^2> and i quote, somewhere around the mid-40's minute mark, "i am so drunk" -jthan
...
13:20:08 < jthan> r00t^2: dude I'm not even that drunk in this episode
13:22:03 < r00t^2> near the end? DUDE
13:22:06 < r00t^2> you're LIT
13:22:17 < r00t^2> after we have you chug
13:22:38 < r00t^2> 54 mins 30 seconds ish
13:26:03 < jthan> I am hearing it
```

```
13:26:51 < r00t^2> 57 MINUTES 44 SECONDS JTHAN. "wow, i'm actually drunk right now" -jthan
13:26:55 < jthan> meh.
13:27:00 < jthan> Anyone can just make shit up
13:27:06 < r00t^2> you...
13:27:10 < r00t^2> you said it yours-...
13:30:09 < r00t^2> also, 59m47s "i'm really drunk" -jthan
13:32:16 < r00t^2> 1h1m33s "omigodi'msodrunk" -jthan
13:32:44 < r00t^2> and then you just start laughing non-stop from 1h1m50s to the end of the episode
13:34:01 < r00t^2> and then your LAST little giggle got cut off but it sounded like an accordion bellow, which ties like perfectly into the outro
```

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	In Heaven	Decreek	click	CC-BY-SA 4.0
Outro	Dr Gears Dub	BANDRIS	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 Two

Comments

There are currently no comments on this article.

Published with Textpattern CMS