Sysadministrivia

Linux, Lagers, and Late Nights

S2E3: "Ass-Backwards Passwords"

Posted 2017-03-27 03:59
Modified 2017-04-26 01:44
Comments 0

Navigation

Previous Episode	Next Episode
S2E2: "Ayyy, I Took Your Job"	S2E4: "From TCP to Shining UDP"

Log

Recorded (UTC)	Aired (UTC)	Editor
2017-03-16 03:02:35	2017-03-27 03:59:00	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`9df3b5cfd3c552d167341368000b0df6894e6dc8d5d4309f1b8f5695adbe1c43`	click	click
OGG	`4afd5e540ed5bf8f38690efec0eb9d42480248407c688d27fd8352c35ef3e285`	click	click

Quicklisten:

In this episode we talk more about password policy, and we talk about a listener's technical issue he contacted us for help with (and, more to the point, general steps to take for troubleshooting/diagnosing).

- News
- Notes
- Sysbadministration Award
- Errata
- Music

News

- Show-related announcements!
  - I have an rsync mirror up! You can fetch the audio for ALL of our episodes (both OGG and MP3 formats), as well as the associated GPG signatures. It also contains HTML, Markdown (.md), and PDF-formatted copies of our shownotes. In addition to THAT, it also contains a mirror for PoC||GTFO, a hacker e-zine. (If you like Phrack, you'll like this.) If you find browsing via the rsync protocol clumsy (I don't blame you), there's also an HTTP interface to it. (Note that the audio files are not accessible there, as you can reach them at /media.)
  - Jthan **finally** got a website up. After 2 years.
    - Uses Lektor and Bootstrap
  - Jthan's hackathon site is up.
  - We'll be talking in detail about BDisk in S2E5!
- Microsoft websites apparently are 7 of the top 100 websites.
- 24% of official Docker images have high priority vulnerabilities (no surprise).
- Despite reports otherwise, apparently Munich sees no reason to switch back to Windows.
  - They run a custom Ubuntu derivative called LiMux.
- Gitlab is staying in the cloud.
- There have been some cases of pre-installed malware on Android.
- The British ISP TalkTalk is blocking TeamViewer.
- Microsoft is now pushing ads Windows 10 File Explorer.

Notes

Starts at **18m47s**.

I was drinking Bulleit 10. Paden was drinking Walsh's Irishman whiskey. Jthan was drinking Breckenridge's Avalanche Ale.

- Are password rules bullshit?
  - We have talked about password **policy** a lot in the similarly-titled S1E15: Backwards Passwords. This discussion was moreso public-facing websites.
  - I reference this Dilbert strip.
  - The takeaway is that password rules aren't bullshit as long as you have sensible and "good" restrictions in place.
  - We also discuss why education is **not** "The Answer" for security.
  - But also, seriously, use 2FA/MFA.

- A listener Matthew wrote in needing some help! **(35m46s)**

He wrote:

> Running a server at home as well as many for my small business (mainly VM's). Everything is running CentOS right now, either 6 or 7 based on when I spun up the server.
>
> I keep having my primary business server overloading and crashing. Log files aren't helping me one bit, as the system seems to be crashing journalctl first thing.
>
> I've got 4GB of memory, and a 4GB swap file, neither of which seem to be filling up before the panic.
>
> Any advice for diagnosing this problem? Would I be better off moving most functionality to my other servers while trying to figure out what's wrong? Backups are still happening on time, and security updates are applied whenever they are released.

And I replied with:

> Based on your explicit mentioning of running CentOS across your ecosystem **and** mentioning journalctl in the problem case, I'll assume the target system is CentOS 7.
>
> Before we go into anything else, I should note that the default CentOS 7 behaviour for journald is "auto" storage, meaning: log to volatile memory (RAM) if the directory /var/log/journal does NOT exist (and it doesn't, in default cases). If you want persistent logging (and it sounds like you do), you can either:
>
> - uncomment "#Storage=auto" in /etc/systemd/journald.conf and change to "Storage=persistent" (in which case it will force-create the directory if it doesn't exist), OR
>
> - simply just mkdir -p /var/log/journal
>
> However, CentOS' journald is by default configured to forward to rsyslog as well. Do you have any messages in /var/log/messages ?
>
> First, are you running any sort of custom partitioning/mounting scheme? I've had issues with journalctl crashing (albeit on Arch, and with previous versions of systemd, but CentOS isn't a rolling distro so they may have "freezed" at a version of systemd/journald that's affected) if I had- I think it was /var mounted on a different filesystem than /usr (or the rest of /… apologies, my memory's a bit fuzzy on the details). If it IS on a partitioning scheme that deviates in layout from the default the installer presents you with, do all the other CentOS 7 systems exhibit the same behaviour? Or is it only isolated to this one?

> (Also, the issue I was having wasn't overloading and crashing- it was simply that journald simply didn't log so it may not be the same issue.)
>
> If not, and you haven't run one yet, you might want to run memtest86+ on the box. It's on a plethora of rescue liveCDs, but we generally recommend SysRescCD if you don't have a preferred one. You can boot it by booting to the CD/USB that contains SystemRescueCD, and when prompted by the boot menu (teal background), go to "Run system tools from floppy disk image…", and then MEMTEST is the first option. (Note that I believe you have to be running in BIOS mode, as I don't think SystemRescueCD supports UEFI?). You'll also be able to (and I recommend doing so) running a badblocks test on the disks on the system to check for any abnormalities/defects. Make sure you do non-destructive tests. You might also want to run a S.M.A.R.T. test on each disk.
>
> ANYWAYS, if the memory tests OK, then you might want to at the very least set up remote logging. CentOS 7's systemd version doesn't provide a native remote journald logging implementation, but because it forwards to rsyslog you can use its remote logging capabilities. This should help with that. (Heads-up, it has an invalid HTTPS cert).

- But we use this opportunity to talk about the debugging process in general, and talk about steps you can take when encountering unknown root causes.
- I've mentioned it many times, but this should be required reading for anyone submitting support requests.
- We talked about how important uniformity is (and why 100% uniformity is impossible) in S2E1.
- The thread for the ZFS issue/interaction Jthan mentions can be found here.

(And yes, Matthew's issue was resolved – as turns out, it was actually a DDoS on php-fcgi against a published vulnerability. No access was granted, however, as the system was fully patched. Whew! Glad we could help, Matthew! And, as always, we're glad you keep your shit patched! You can read about it from his end in his blog post)

Sysbadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(54m49s)**

We officially award Amazon the Baddie for their fuck-up that we covered last episode.

Errata

- Jthan's still an insufferable dick.
  - But that's just, like, my opinion, man.
- It was confirmed later that my suspicions regarding Paden's ability to access VPN-locked resources without being connected to the VPN were correct – shortly thereafter, he was unable to access the resources without being connected. :)

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Face ONE	1up Collectif	click	CC-BY-NC-SA 4.0
Outro	Broken Hill	Nic Bommarito w. Santoré	click	CC-BY-NC-SA 3.0

(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.