Sysadministrivia

Linux, Lagers, and Late Nights

S3E19: "Byte Sudo Sys Jail Privilege"

Posted 2018-11-19 04:59
Modified 2018-11-19 16:50
Comments 0

Navigation

Previous Episode	Next Episode
S3E18: "Arousal (pt. 1)"	S3E20: "Clockulators"

Log

Recorded (UTC)	Aired (UTC)	Editor
2018-11-08 03:29:35	2018-11-18 15:26:13	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`d7602916a23e766ef557b689600c6f5e200c9100d7c4e24953ff9932c34f8bfd`	click	click
OGG	`3be1b22e527e9ddc5004e97c79bd5103ede0b8717241b61e432a4587d332689a`	click	click

Quicklisten:

Just Jthan and myself again. We talk about ways of separating privileges on a GNU/Linux (and some UNIX/BSD) systems based on a listener writing in. Jthan saw a furry on Halloween.

I also spend a weirdly large amount of time talking about Nagasaki and Hiroshima.

- News
- Notes
- Sysbadministration Award
- Errata
- Music

News

- Many electronic/digital voting machines were likely configured with weak passwords.
  - We talk about the password complexity… complexities here as well.
- The Snowden-recommended (and pricey) IronChat app had messages massively decrypted.
  - So no, Moxie (and others), **this** is why GnuPG/PGP/gpg has precisely **not** run its course. Because it still works, and it isn't in the hands of one company, country, or individual.
  - The Baddie Jthan mentions that we gave to GnuPG can be found here.
- Some SSD hardware encryption was severely broken.
  - You can read the actual paper here.
- IBM has indeed bought Red Hat.
  - For 33.4 billion USD.

Notes

Starts at **20m58s**.

I was drinking chai (again) and a Porterhouse's An Brain Blásta again (same as S3E18). Jthan was drinking Michter's American Whiskey. (Paden wasn't with us again.)

- We reply to this comment.
  - One can configure the wheel group (or any specific group, really; tradition just dictates it's "wheel") to facilitate checks for su (and found in BSDs and other unices as well).
    - **Please see the Errata! We fucked this up, just *s/sudo/su/g* in this discussion topic.** It's been a while since I used the wheel group. :)
  - We'll, at some point in the future, do an entire episode on sudo. :) Until then, though, I **highly** recommend watching this talk.
    - I still say you don't need augeas to manage sudo users – just add/remove files, one per user, under /etc/sudoers.d/. :P
  - Another way of segregating software can be via virtual environments, which we dicuss the pros/cons of **at (heated) length**, in S3E3.
  - You technically can use containers for this, but I wouldn't. The entire reason the topic came up is because of one of the many weaknesses in containers we were discussing. ;)
    - We'll probably be talking about Vagrant in the future, so you can manage full VMs as if they were containers.

- Chroots are tried-and-true for separating out software, but you have to be careful. There are a lot of ways of escaping chroots, and even scripted ways. Basically, make sure nobody has shell in a chroot and never EVER gets root user access **inside** that chroot, and you should be okay. Though at that point, it does sort of render chroots useless from a segregation functionality.
- BSD jails are indeed just as easily escaped, and don't let any fanboy tell you differently. The difference is they also can run different bincompats. A rough analog of this would be, for instance, a 32-bit chroot on a 64-bit (non-multilib) host, and how it has to be entered via the **linux32/setarch** utility. Alternatively, a more direct analog would be LXC (Linux containers) – though it's Linux-only. You cannot run a BSD container on a Linux host (but why would you ever need to?) — a VM is still the recommended course anyways.
- We do also mention briefly the WSL.
- The most guaranteed sort of privilege separation is probably going to be hardware separation.
- We talk about SELinux (and grsecurity/PAX) in S1E6 and AppArmor in S2E6.

Sysbadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(50m10s)**

There was a public 0day in VirtualBox. The Baddie goes to both Oracle for the severity/ease of escalation of the vulnerability, and to the researcher for not following an ethical disclosure policy (as far as I know).

Errata

- Yes, Jthan, sneezing is indeed quite traumatic to the human body. It's not surprising; the air that leaves your head from the sudden contractions is traveling around 100mph (that's about 161kph, or 45m/s).
- I think I mentioned Toyko when talking about bombing… They **benefited** economically and developmentally from the renovation, but the bombs themselves were dropped on Hiroshima and Nagasaki (duh).
- I did indeed do this while typing up the notes, as I predicted during the episode:

```
13:10:11 < r00t^2> sysbot: r00t^2 is also an unzen bitch
13:10:12 <@sysbot> r00t^2: yeah, let me get RIGHT fucking on that for you, fucker.
13:10:16 < r00t^2> jthan: ^ 4 u
```

- Jthan talks about wheel in the context of ***sudo*** rather than ***su***, and I forget to correct him because **seriously, who the fuck uses *su* anymore when you can use sudo?**
  - He also wasn't using 'requited' correctly.
  - And I say *sudo -u*, I actually meant *sudo -i*. Talking about the terminal vs. sitting in front of it is a lot different and harder. :(
  - I confirmed – SUSE (OpenSUSE, at the very least) does **not** use wheel group membership. It doesn't even have a wheel group upon initial install.
- RIP, Foresight Linux.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Breathing Out	Mid-Air Machine	click	CC-BY-SA 4.0
Outro	Fake Protest Song(feat. Ema Grace)	Ryoma Maeda	click	CC-BY 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.