Sysadministrivia

Linux, Lagers, and Late Nights

S2E20: "The Shell Game"

Posted 2017-11-20 04:23
Modified 2018-01-14 19:01
Comments 2

Navigation

Previous Episode	Next Episode
S2E19: "Patching the KRACKs in the (Fire)Wall"	S2E21: "Barenaked Boxen"

Log

Recorded (UTC)	Aired (UTC)	Editor
2017-11-09 03:44:06	2017-11-19 18:00:35	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`681ccb72099c3ef0089871be9fe9c7874f92c2d314a70011594c643df9231edc`	click	click
OGG	`89f217eea296af8016b2e4eaeab42e18203699aa7c6bb4a874254b65322f8631`	click	click

Quicklisten:

We talk about clever deployment options for SSH, both for auth and for hostkeys. We also yammer a bit about the embedded Minix system discovered in Intel chips and the concept of a city-run ISP.

- News
- Notes
- Sysbadministration Award
- Errata
- Music

News

(Not mentioned on the show)

- We are running a contest!
- Our Shitshow for Season 2 will be on December 6, 2017. See here and here for more info. We'd love to have you join us!

- Military court bars forced unlocking of smartphones as evidence
  - The full ruling can be found here.
- There is a Minix system running on Intel Management Engine chips (see here, here, etc.)
- Linux USB subsystems are vulnerable to a slew of new attacks.
- Marissa Mayer, former CEO of Yahoo!, was grilled in a Senate Commerce Committee
  - See S2E18 for more discussion on the "Golden Parachute" policy we mention
- A keylogger was found in a keyboard's driver/management software
  - As Jthan mentioned, we talk more about outbound firewall rules in S2E19.
- Tor browser flaw leaks users' real IP address (yes, again). This one is called "Tormoil". (sigh)
- A Webroot bug keeps file handles open
  - Additional source
- Half of Colorado counties have rejected a Comcast-backed law restricting city-run Internet service

Notes

Starts at **25m08s**.

I was drinking (and FINALLY finished) the Bulleit 10-year bourbon. Paden was drinking a screwdriver. Jthan was drinking Tullamore Dew.

- SSH key management
  - Pubkey distribution
    - Jthan mentions using GitHub to fetch pubkeys.
      - Note that you can also use e.g. `https://github.com/<USERNAME>.keys` to get the raw pubkeys themselves (i.e. non-JSONified).
    - It can be done via LDAP
    - I think you can also use FreeIPA, which we talk about in S2E10

        - And of course, things like Ansible, Puppet, Chef, etc.
        - There are also things like ssh-keydb and SKM
        - You can use Kerberos too, but it requires password auth
    - Hostkey installation/Management
        - You can use Monkeysphere to “GPG-sign” your hosts
        - System-level known_hosts is also possible
        - ssh-keyscan (the wrapper script I wrote around it can be found here)
            - `ssh-keygen -R <host>` lets you remove a host form your known_hosts file (even if it’s hashed!)
            - `ssh-keygen -r <host>` will let you print the hostkey.
        - And there’s also host-based authentication which is great for cluster environments if you have many shared users across different boxes.

- Jthan petitions our listeners **(56m44s)**
    - He wants your feedback on if you like hearing about our current personal projects we’re working on. If so, we can have a dedicated segment or periodic episode dedicated to talking about it.
    - We also want to hear from you if you want to be or have a suggestion for a guest! (Contact Jthan directly for this.)
    - And make sure you send us any topic suggestions too!
    - We have contact information on our contact page.

Sysbadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(1h01m45s)**

A regular ol’ user, apparently accidentally, froze 150-280 million dollars in Ethereum cryptocurrency.

Errata

- Jthan did indeed mention “wild weenie” in S2E19, but not a “weenie in the wild”. I’d imagine those things are different. If they were actual things.
- Sorry for the weird mixing, especially on Jthan’s track. He wouldn’t stop doing that stupid voice, which made it impossible to mix into the rest of our balance. You should write to him and tell him to never do it ever again.
- At the time of publication, €50 is approximately 58.96USD
- I mention Podloader
- I was wrong about the naming “inconsistency” with /etc/ssh/ssh_known_hosts. e.g. Your private SSH config is ~/.ssh/config, the system-wide one is /etc/ssh/ssh_config. D’oh.
- As mentioned during the Baddie, if you’d like to donate, you can find out how to do so here.
- Jacob Evans let us know that you CAN use Active Directory to manage SSH keys by tweeting at us and said “Listening to your @SysAdm_Podcast and all versions of Active Directory support public keys. And you can change where they are stored with a custom SSSD value. But I like #freeipa views which can append those keys.”

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Mermaid Tank	Computer Music All-Stars	click	CC-BY 4.0
Outro	Tentou Morrer Com Facas & Estiletes	Madame Rrose Sélavy	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 Two

Comments

1. ## Ivan

   2017-11-24 11:02 (1499 days ago)

   Jthan mentioned that he’s typing password for key multiple times at work. Why? Why not use something like ssh-agent in order to cache private key?

2. 2017-11-24 15:40 (1498 days ago)

   Ivan-

   Good question! I’ll pass it along.

   For those reading that don’t know how:

   1.) ssh-agent -s (if you don’t have an ssh agent running already)
   2.) ssh-add path/to/ssh/privatekey