Sysadministrivia

Linux, Lagers, and Late Nights

S6E1: "A FreSSH View"

Posted 2021-02-28 23:59
Modified 2021-02-28 14:10
Comments 0

Navigation

Previous Episode	Next Episode
S6E0: "Fat Access"	S6E2: "Environmental Protection"

Log

Recorded (UTC)	Aired (UTC)	Editor
2021-02-18 03:36:40	2021-02-28 06:22:44	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`526c185a3c4d1b0a65715d8f6e3238281571f583bedeb98ddcc9e48f8c08a7ee`	click	click
OGG	`b05ee65fdb2ab2319535242647d2dfa672335cc952346301f0b0e851b1a7c9d5`	click	click

Quicklisten:

In this episode, we talk about how to identify some of the most common SSH issues (and how to debug less common ones).

- Just the Tip
- Notes
- 15 Clams
- Errata
- Music

Just the Tip

- How do you wake up a TTY without causing potential damage to any commands sitting at the prompt?

Notes

Starts at **16m13s**.

I was drinking a Guinness Baltimore Blonde. Paden was drinking Miller Lite. Jthan was drinking Michelob Ultra.

- Troubleshooting (Open)SSH
  - Common client-side issues, especially with pubkey auth, depends on permissions and ownership of `~/.ssh` and `~/.ssh/id_*` files.
  - SSH supports up to three levels of verbosity(`-v`) but usually you can get a good idea of what's wrong with just two (`-vv`).
  - For server-side issues, errors are usually printed to `/var/log/secure` or `journalctl -u sshd -e`.
  - `Connection reset by peer` is usually either DDoS filtering or denyhosts.
  - Key exchange ("kex") issues typically occur when your client requires a certain cipher suite that isn't compatible with what the server supports (or vice versa).
    - If you increase verbosity, you can see exactly what authentication methods and ciphers you are sending, whether the server rejects your auth method, and what ciphers the server accepts.
  - SELinux contexts/labels must be set properly on your keypairs (client) and authorized pubkeys (server)! The ssh_selinux man page has some good documentation on this.
  - You may get hostkey accepting/matching issues. Those are gone into detail in our new HOWTO.
    - For hosts you haven't connected to yet, you just need to accept the new key.
    - For hosts that have a different host key than what you have saved locally (in your ~/.ssh/known_hosts, or – if you keep a system-wide known_hosts, /etc/ssh/known_hosts), you'll need to confirm the reasons for the hostkey changing and verify the new hostkey.
      - Before resolving this, **confirm** that the host key should in fact be different than what you have!
  - If your **user** is **expired** you'll get something similar to the following: `Your account has expired; please contact your system administrator` (and yes, you manually need to edit the shadow file to remove **acount** expirations)
    - THIS IS DIFFERENT FROM PASSWORD EXPIRATIONS!
  - If you're using NFS-backed home dirs and the NFS drops out, you'll see an extended delay and an authentication error (most likely a permission denied).

15 Clams

In this segment, Jthan shares with you a little slice of life. The title is a reference to this video. (2m16s in)

Starts at **46m46s**.

Jthan asks about AIDE (see also RHEL docs, Arch docs). He essentially wants to know how if someone is making unathorized changes. I suggest mtree (and the AUR version I package, nmtree).

We also mention Tripwire, and some alternatives. A good product is Samhain for this. I mention I wish Osiris was still maintained.

NOTE: Whatever solution you use, it is important you set it up/get a snapshot/etc. **before** giving them access! There is no way to validate integrity afterwards otherwise!

Errata

- My explanation of kbdinteractive is… not very accurate, but it's a bit hard to concisely represent RFC 4256, where it's defined. You technically **could** use pexpect with it, but the entire point of kbdinteractive is the prompts may change over time and it's intended to be a user-interactive login. I **was** incorrect about it requiring heuristics on the input though.
- lol. If you set a password to a single-character and you have passwd strength checking enabled, you'll get `BAD PASSWORD: The password is a palindrome`.
  - I mean… Technically, they're not **wrong**…
- If you want to add timestamps to your bash history, add `export HISTTIMEFORMAT="%F %T "` to your `~/.bashrc` or your global bash config (sometimes `/etc/bash.bashrc`, sometimes `/etc/bashrc`, etc.)
- When I say "you can't add methods to types (in Golang)", I mean **built-in AND IMPORTED** types.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Opening	Noi2er	click	CC-BY-NC-ND 4.0
Outro	Emptiness5	Information Ghetto	click	CC-BY-ND 4.0

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

Author r00t^2
Categories Season Six

Comments

There are currently no comments on this article.