Sysadministrivia

Linux, Lagers, and Late Nights

S4E9: "Great Walls of Fire"

Posted 2019-06-24 03:59
Modified 2019-06-24 02:05
Comments 0

Navigation

Previous Episode	Next Episode
S4E8: "I Am Such a Git"	S4E10: "Unavailable"

Log

Recorded (UTC)	Aired (UTC)	Editor
2019-06-13 02:09:51	2019-06-23 19:07:59	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`aa00253905043ef4e5cecb76009ffdbe582399f2983f3b305c4c5deafc52023d`	click	click
OGG	`fbac1129f6e431992a05ed0ee11ecb56291f0b1b2878ad89df129a7349e35ca9`	click	click

Quicklisten:

In this episode, we have a weird spliced-in Jthan and we talk about some neat firewall tricks you can do to make firewalling a little easier.

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

Just the Tip

- Fail2Ban is a useful tool to dynamically blacklist or greylist IP addresses based on logged attempts.
  - In addition to the presentations and documentation found on Fail2Ban's wiki, the Arch wiki article and Gentoo wiki article, as usual, have some quick reference.

Notes

Starts at **7m51s**.

I was drinking water. Paden was drinking Coors Light and "plenty of vodka". Jthan was drinking an Alaskan Amber ale.

- Advanced firewalling tips/tricks
  - IPset
    - Arch wiki article
    - pyroute2's interface
  - Policy design
    - Always remember: **policies** control the *general traffic behaviour*, and **rules** control the *overrides/exceptions to the policy*.
    - **ALWAYS** implement outbound rules with a restrictive policy **whenever** possible! You really, really, really want to implement an outbound drop policy if you can, and take the time to craft your rules well. Your security auditors will swoon and fawn over you.
    - Policies + rules are useful for your company VPN as well! It prevents abuse of the VPN for nefarious purposes, which would possibly implicate your company. By implementing a default drop policy with several whitelisting rules (plus selective/specific pushed routes), you can ensure that they can **only** access certain Sysadministrivia resource (e.g. target IP and port/protocol).
  - Rate-limiting is immensely useful. Other people have covered this in some detail.
  - Remember to segregate your VPN traffic to its own VLAN, so you can easily apply access controls to it and treat it as a "kind-of-but-not-really DMZ". It helps if you run multiple VPNs with their own subnets as well, which allows you to further control access to those VPNs.
  - Also, make sure you check out the LART!
  - Just having a firewall isn't enough. You need to have a **good** firewall policy, **good** firewall rules, and it needs to be regularly audited for rules that can be cleaned up.
  - You can see my "ponies page" here. The configs and presentation notes (which are almost assuredly out of date) from that talk can be found in my notes dump. The upside-down internet HOWTO is here.

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 **49m49s**.

Jthan does a dramatic man page reading for sleep.

Errata

- Jthan was unable to join Paden and I for the recording itself, and instead recorded his 15 Clams segment and sign-off later and we spliced it in.
- IPset support was added in 2.6.16 (for the 2.6 kernel branch) and 2.4.36 (for the 2.4 branch). A new branch of IPset was created (I think a rewrite?), and that requres kernel version 2.6.32 or above.
- Martian packets and smurf packets are actual things.
- The blinkenlights ASCII-over-telnet “movie” is still up (and even has some special features if you have IPv6 available)! You can connect via the command `telnet towel.blinkenlights.nl` (and hit enter to get past the credits at the beginning).
- I forgot to mention it, but another handy tool in your firewalling toolkit is SYNPROXY.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Mount Fuji	Bio Unit	click	CC-BY-NC-SA 4.0
Outro	Bellwether	Manwomanchild	click	CC-BY-NC 4.0

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

Author r00t^2
Categories Season Four

Comments

There are currently no comments on this article.