STAMUS NETWORKS

Suricata Landlock Support

How in-person conference can improve software.

About Me

Stamus Networks

- Co Founder
- CTO

Social Media

- @regiteric on Twitte (#jesors)
- https://www.linkedi m/in/ericleblond/

Mickaël Salaün at Pass the Salt Conference

- Sandboxing your application with Landlock, illustration with the p7zip case
  - By Mickaël Salaün
    - Author of Landlock
    - Linux kernel developer at Microsoft
- Video: https://passthesalt.ubicast.tv/videos/sandboxing-your-application-with-landlock-illustration-with-the-p7zip-case/
- A practical introduction on adding landlock support to software
- Info on the project: https://landlock.io/
  - Added in Linux 5.13
  - After 3 years of fight

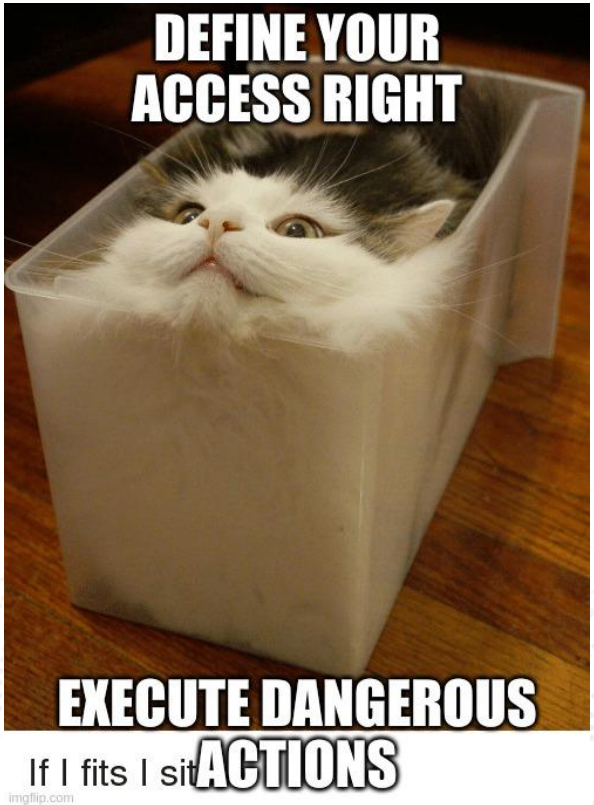
Linux Kernel Developer at Microsoft

- We come from far
- One of my first open source t-shirt (from 2004)

Landlock concept

- Restrict ambient rights (e.g. global filesystem access)
- Per process
- Declaration of access rights done by process
  - Process start
  - Declare what access it needs
    - In which directories it will write
    - In which directories it will read
    - … more access settings
    - Enforce the policy
  - Run active code
    - On unsecure data

Landlock in one image



Risk assessment of Suricata

- Suricata in sniffing mode
  - Read configuration file
  - Overwrite files (running as privileged user)
- Suricata in pcap reading mode
  - File modifications as user
  - Parsing untrusted data
    - Pcap with potential active attacks

Configuration

https://suricata.readthedocs.io/en/latest/configuration/landlock.html

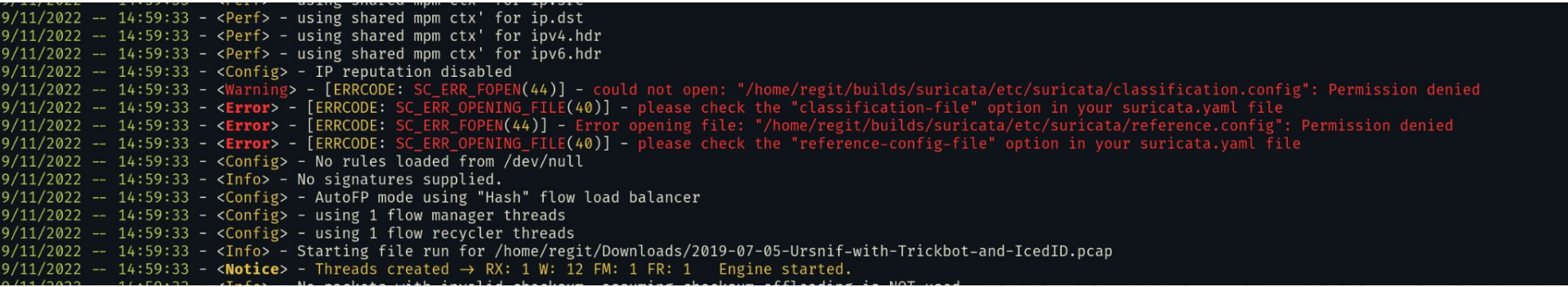
```
1108
1109 security:
1110   # if true, prevents process creation from Suricata by calling
1111   # setrlimit(RLIMIT_NPROC, 0)
1112   limit-noproc: true
1113   # Use landlock security module under Linux
1114   landlock:
1115     enabled: yes
1116     directories:
1117       #write:
1118       #  - /home/regit/builds/suricata/var/run/
1119       # /usr and /etc folders are added to read list to allow
1120       # file magic to be used.
1121       read:
1122         - /usr/
1123         - /etc/
1124         - /etc/suricata/
1125
```

Suricata case

- Easy determined interactions with file systems:
  - Read signatures & configuration
  - Write log files
- Specific values can be analysed from:
  - Configuration files
  - Command line option

Demo

- From command line
- Custom build



Conclusion

- Available from Suricata 7.0
- Need at least Linux 5.13
- Easy to setup
- Feedback welcome

Questions ?

Thank You

Eric Leblond
CTO
el@Stamus-Networks.com

STAMUS NETWORKS