



WORKSHOPS SCHEDULE

Monday 2nd July, 2018

- Afternoon (2h30, 25 attendees): **Introduction to Bro Network Security Monitor**
by **Eva Szilagy**i (CEO at Alzette Information Security) and **David Szili** (CTO at Alzette Information Security)

Tuesday 3rd July, 2018

- Morning (3h, 25 attendees): **AIL-Framework: A modular framework to analyse potential information leaks**
by **Sami Mokaddem** (CIRCL)
- Afternoon (2h, 25 attendees): **URL Analysis with Faup**
by **Sébastien Tricaud** (Open source and security pro and enthusiast, Splunk)

Wednesday 4th July, 2018

- Morning (2h, 25 attendees): **FreeIPA: Open Source Identity Management**
by **Florence Renaud** (Senior Software Engineer FreeIPA, Red Hat) and **Fraser Tweedale** (Software Engineer, Red Hat)
- Afternoon (3h, 20 attendees): **Suricata and SELKS workshop**
by **Éric Leblond** (Suricata core developer, Stamus Networks)



TALKS SCHEDULE

Monday 2nd July, 2018

- 14:00 - 14:15: **launching talk**

Linux Distribution Security

- 14:15 - 14:50: **Debian security team: behind the curtains**
by **Yves-Alexis Perez** (Security researcher and developer, Debian security team)

Reverse and Low-Level Session

- 14:50 - 15:25: **r2frida - Better Together**
by **Ole André V. Ravnås** (Frida developer) and **Sergi Alvarez** aka pancake (r2 developer)
- 15:25 - 16:00: **Static instrumentation based on executable file formats**
by **Romain Thomas** (LIEF developer, Quarkslab)

~~~ afternoon pause ~~~

- 16:20 - 16:55: **Machine-Code Analysis With Open-Source Decompiler RetDec**  
by **Jakub Kroustek** & **Peter Matula** (RetDec developers, Avast software)
- 16:55 - 17:30: **Are there Spectre-based malware on your Android smartphone?**  
by **Axelle Apvrille** (Senior researcher, Fortinet)
- 17:30 - 17:50: **A graphical user interface for radare2: Cutter**  
by **Antide Petit** (Cutter developer)

Tuesday 3<sup>rd</sup> July, 2018

## Network Security Session

- 09:00 - 09:35: **Traffic filtering at scale on Linux**  
by **François Serman** (OVH)
- 09:35 - 10:10: **Performance with a S like Security: the eBPF XDP case**  
by **Éric Leblond** (Suricata core developer, Stamus Networks)

~~~ morning pause ~~~

- 10:30 - 11:05: **KEYNOTE: a 10 years journey in Linux firewalling**
by **Pablo Neira Ayuso** (Head of Netfilter core team)
- 11:05 - 11:40: **Full packet capture for the masses**
by **Xavier Mertens** (Security consultant, ISC SANS handler)
- 11:40 - 12:15: **Rumps session**
by **you!**

~~~ MID DAY BREAK ~~~

## Web Security Session

- 14:15 - 14:50: **Security and Self-Driving Computers**  
by **Stefan Eissing** (Mod\_md developer (Let's Encrypt Apache module))
- 14:50 - 15:25: **Snuffleupagus: killing bug classes and virtual patching the rest**  
by **Julien Voisin, Thibault Koechlin, Simon Magnin-Feysot** (Snuffleupagus developers, NBS Systems)

- 15:25 - 15:45: **Preview of Vulture's upcoming web filtering engine**  
by **Jérémie Jourdin** and **Hugo Soszynski** (Vulture developers, aDvens)
- 15:45 - 16:05: **SecureDrop, for whistle-blowers**  
by **François Poulain & Loïc Darchary** (SecureDrop admin, developer)

~~~ afternoon pause ~~~

IAM Session

- 16:25 - 17:00: **Second factor authentication (2FA) in LemonLDAP::NG**
by **Clément Oudot & Xavier Guimard** (LemonLDAP::NG developers)
- 17:00 - 17:35: **No way JOSE! Lessons for authors and implementers of open standards**
by **Fraser Tweedale** (Software Engineer, Red Hat)
- 17:35 - 17:55: **Too bad... your password has just been stolen! Did you consider using 2FA?**
by **Florence Blanc-Renaud** (Senior Software Engineer FreeIPA, Red Hat)

Wednesday 4th July, 2018

Blue Team Session

- 09:00 - 09:35: **Fail frequently to avoid disaster, or how to organically build an open threat intelligence sharing standard to keep the intelligence community free and sane!**
by **Alexandre Dulaunoy** (CIRCL) & **Andras Iklody** (CIRCL)
- 09:35 - 10:10: **The story of Greendale**
by **Thomas Chopitea** (Forensics investigator and engineer, Google)

~~~ morning pause ~~~

### Secure Programming and Architecture Session

- 10:30 - 11:05: **Internals of Landlock: a new kind of Linux Security Module leveraging eBPF**  
by **Mickaël Salaün** (Security researcher, ANSSI)
- 11:05 - 11:40: **Secure programming is slow - really?**  
by **Pierre Chifflier** (Long time FLOSS developer, ANSSI)
- 11:40 - 12:15: **Immutable infrastructure and zero trust networking: designing your system for resilience**  
by **Geoffroy Couprie** (Security researcher and developer, Clever Cloud)

~~~ MID DAY BREAK ~~~

IoT Security Session

- 14:15 - 14:50: **IoT Honeypot, new types of attacks**
by **Sébastien Tricaud** (Open source and security pro and enthusiast, Splunk)
- 14:50 - 15:25: **Io(M)T Security: A year in review**
by **Rayna Stamboliyska** (Risk management and crisis mitigation expert)
- 15:25 - 16:00: **Expl-iot: IoT Security Testing Framework**
by **Aseem Jakhar** (R&D director and open source developer, Payatu software lab)

~~~ afternoon pause ~~~

### Red Team Session

- 16:20 - 16:40: **Freedom Fighting Mode - Open Source Hacking Harness**  
by **Ivan Kwiatkowski** (Pentester and malware analyst)
- 16:40 - 17:00: **Open Hardware for (software) offensive security**  
by **Antoine Cervoise** (IT security engineer, NTT Security)
- 17:00 - 17:20: **Shadow on the Wall - Risks and Flaws with Shadowsocks**  
by **Niklas Abel** (Pentester and security auditor, X41)
- 17:20 - 17:40: **Glassfish from (IN)Secure admin**  
by **Jérémy Mousset** (Pentester)