Hardening Linux : A Triple-Threat Approach with SELinux, Fapolicyd, and Auditd

- **Speaker**: Joshua Loscar
- **Room**: CC 202
- **Time**: Sun 2:00 pm – 3:30 pm

- **Format**: Hands-on Lab (90 min)
- **Difficulty**: Introductory
- **Track**: Security / Privacy
- **Additional Tags**: DevOps, Self-Hosting
- **Presenter Location**: In-person
- **Experience**: first time speaking / several-th time speaking
- **At**: anywhere / at lfnw

Description:

In an era of increasingly sophisticated cyber threats, securing Linux systems is more important than ever. This hands-on lab introduces a **triple-threat approach** to Linux hardening using three foundational security tools:

- **SELinux** — Implements Mandatory Access Control (MAC) to enforce strict policy-based access
- **Fapolicyd** — A user-space daemon that enhances file access control and prevents unauthorized execution
- **Auditd** — Logs and monitors system calls and user activity for visibility and compliance

Participants will learn how these tools complement each other to form a comprehensive security strategy. The lab covers installation, configuration, and practical usage, showing how to:

- Build a strong security foundation for Linux infrastructure
- Meet compliance requirements (C