


# The (potential) Art of the Hackathon

A blend of ideas, code, documentation, GUI, UX to **happy infosec communities**



 @circl\_lu - *TLP:WHITE*

[info@hack.lu](mailto:info@hack.lu)

March 26, 2018

# Objective

---

The objective of this hackathon is to have an interactive session in order to exchange, **enhance** and discover new **Open Source Security Software** and tools. The aim is not to be fully exhaustive or have a nicely packaged software at the end of the day, but to either bootstrap a new project, bootstrap enhancements on existing projects or improve **interoperability**.

As we are all learning together, don't hesitate to ask questions to each other and **interact during the session(s)**.

## What a hackathon is not (in our view) ...

---

- ...CTF (Capture The Flag)
- ...Game of Code (code competition)
- ...place to measure skills or be condescending if someone does not know something
- ...place to work (Fun takes priority and everything is informal and the Hacker Ethic<sup>1</sup> prevails)
- ...sprint, Hackathons like Marathons, is not conquered by going as fast as possible early-stage, **being constant and persevering is key**

---

<sup>1</sup><http://www.acrewoods.net/free-culture/the-hacker-ethic-and-meaningful-work>

## A hackathon is (in our view) a...

---

- ... place to learn from each other
- ...great opportunity to connect with like-minded people in real life
- ...constant discovery of new stuff, tools, techniques, recipes, concepts, thoughts
- ...bringing **communities together<sup>2</sup> and improving interoperability between Open Source Security Software**

---

<sup>2</sup>Social Architecture, Pieter Hintjens <http://www.foo.be/docs-free/social-architecture/main.pdf>

## What are requirements? Do I need to know the latest programming language?

---

- Good news everyone! **NO** special Ninja, Samurai or other 31337 Hax0r skillz needed.
- Hackathons have produced amazing: documentation, examples on software use-cases, graphic designs, etc...without any magical powers ;)
- One requirement is: be curious, adventurous, challenging in your ideas and respectful

# HELP, I am overwhelmed & not sure how to start

---

- Relax, you are not alone, we are also overwhelmed how awesome the group is :)
- Look around you, amazing people are present who help each other to get started
- Set yourselves goals, make a quick evaluation on how realistic it is
- Ask and share your ideas, questions and requests
  - **5 minutes introduction per project (at the beginning of the hackathon)**
  - **5 minutes presentation interrupt (when ever you like)**

# What have been done in previous OSSS hackathons?

## 1/3

---

- MISP<sup>3</sup> & Cortex<sup>4</sup> integration to allow the information sharing platform MISP to connect & use Cortex intelligence services.  
Cortex 1.1.1: 2-way MISP integration now a reality
- cve-search performed a new major release & reorganised the contribution aspect to ease the external contribution & test suite improvements
- shotovuln<sup>5</sup> - an offensive bash script for pentesters to find generic privesc issue on Unix boxes

---

<sup>3</sup> <https://www.misp-project/>

<sup>4</sup> <https://github.com/TheHive-Project/Cortex>

<sup>5</sup> <https://github.com/444xxk/shotovuln>

# What have been done in previous OSSS hackathons?

## 2/3

---

- Viper<sup>6</sup> made significant progress towards Python 3 support, including work on Python 3 port of PEfile & the creation of an open test suite for PEfile
- A new project has been evaluated for the exchange of software vulnerability information within open source projects supporting software evaluation, or security assessment. The idea is to share a common format between cve-search<sup>7</sup>, aboutcode to share software vulnerabilities within open source projects
- Updates in JSMF-Android<sup>8</sup> - Analysis of Inter-Component Communication links (ICC) & source code of Android applications (AST)

---

<sup>6</sup> <https://github.com/viper-framework/viper>

<sup>7</sup> <https://www.cve-search.org/>

<sup>8</sup> <https://github.com/ICC-analysis/JSMF-Android>



# What have been done in previous OSSS hackathons?

3/3

---

- The Seeker of IoC - CERTitude<sup>9</sup> is a Python-based tool, which aims at assessing the compromised perimeter during incident response assignments
- Improvement of mail\_to\_misp<sup>10</sup> with support for Thunderbird was added
- MISP taxonomy<sup>11</sup> improvement with assessment of the analysts
- MISP galaxy<sup>12</sup> improved with an extended ransomware cluster

---

<sup>9</sup> <https://github.com/CERT-W/certitude>

<sup>10</sup> [https://github.com/MISP/mail\\_to\\_misp/](https://github.com/MISP/mail_to_misp/)

<sup>11</sup> <https://github.com/MISP/misp-taxonomies>

<sup>12</sup> <https://github.com/MISP/misp-galaxy>

すごい  
凄い！ What's next?

---

- Open discussion on what ideas people already have and want to hack on
- Do we want to group together on certain ideas?
- Panic, I still do not feel comfortable on what to do...→ No worries, projects have idea lists<sup>13</sup>.

---

<sup>13</sup><https://github.com/MISP/MISP/wiki/Hackathon>

# Flexitime-line in Luxembourg & Japan - 26 March 2018

---

10:15 - Hackathon intro

10:30 - Project 5 minutes round table

12:30 - Lunch (while hacking)

18:00 - Conclusions, what have we learned

19:00 - The end? Next hackathon?

anytime - 5 minutes break presentation