MISP Training Cheat Sheet

Virtual Machine (MISP Training VM)

The MISP Training VM is available at the following location : https://www.circl.lu/misp-images/latest/.
The VM can be imported in VirtualBox or VMWare as an appliance (OVA).
The MISP training VM includes multiple applications and packages which are configured by default without production-ready secure settings. We strongly recommend to not use this VM for production and/or for storing sensitive information.

Default URL and (username/password)

- MISP web interface - http://127.0.0.1 (NAT: http://127.0.0.1:8080) (**admin@admin.test/admin**)
- MISP-modules - http://127.0.0.1:6666
- MISP-dashboard - http://127.0.0.1:8001
- Viper-web - http://127.0.0.1:8888 (admin/Password1234)
- jupyter-notebook - http://127.0.0.1:8889
- system credentials via ssh/terminal - (misp/Password1234)

How to get the API key of my user?

Go to the MISP web interface, and simply click your username in the right upper corner to see your user profile which includes your API key.

How to reset a password in MISP?

If you did any specific mistake while setting up your password at the first loging. You can reset the password by login on the system (via SSH or terminal) and type the following command:
`/var/www/MISP/app/Console/cake Password admin@admin.test YourTemporaryPasssword`

How to reset the bruteforce login protection?

While trying to log into MISP multiple times unsuccessfuly, the bruteforce protection might be triggered. You can reset the bruteforce login protection's state by loging into the system (via SSH or terminal) and typing the following command:
`/var/www/MISP/app/Console/cake Admin clearBruteforce`

How to upgrade MISP to the latest version?

Log in via SSH or terminal and type the following commands (your VM must have an Internet access):

1. `cd /var/www/MISP`
2. `git pull origin 2.4`
3. `git submodule update --init --recursive`

Getting OSINT information into your MISP

By default, a fresh installation of MISP is emtpy as we prefer to leave it up to the users to store, gather and share the information they need. If you would like to populate your MISP with some real-life data, simply enable the CIRCL OSINT feed, which contains cybersecurity threat-related information. In order to enable the OSINT feed, go to → `Sync Actions` then → `List Feeds`. Then select the first feed's (called `CIRCL OSINT Feed`) checkbox and click on top `Enable Selected`. Then on the right side of the `CIRCL OSINT Feed` row, simply click the icon depicting a downward pointing arrow in a circle. Once you go back to the event index, the events will start appearing gradually.

Training materials and documentation

The MISP training materials are available at the following location https://www.circl.lu/services/misp-training-materials/ and are freely licensed under CC-BY-SA. MISP book is available at the following location https://www.circl.lu/doc/misp/.