Threat Intelligence: MISP Lab Setup

hackingarticles.in/threat-intelligence-misp-lab-setup

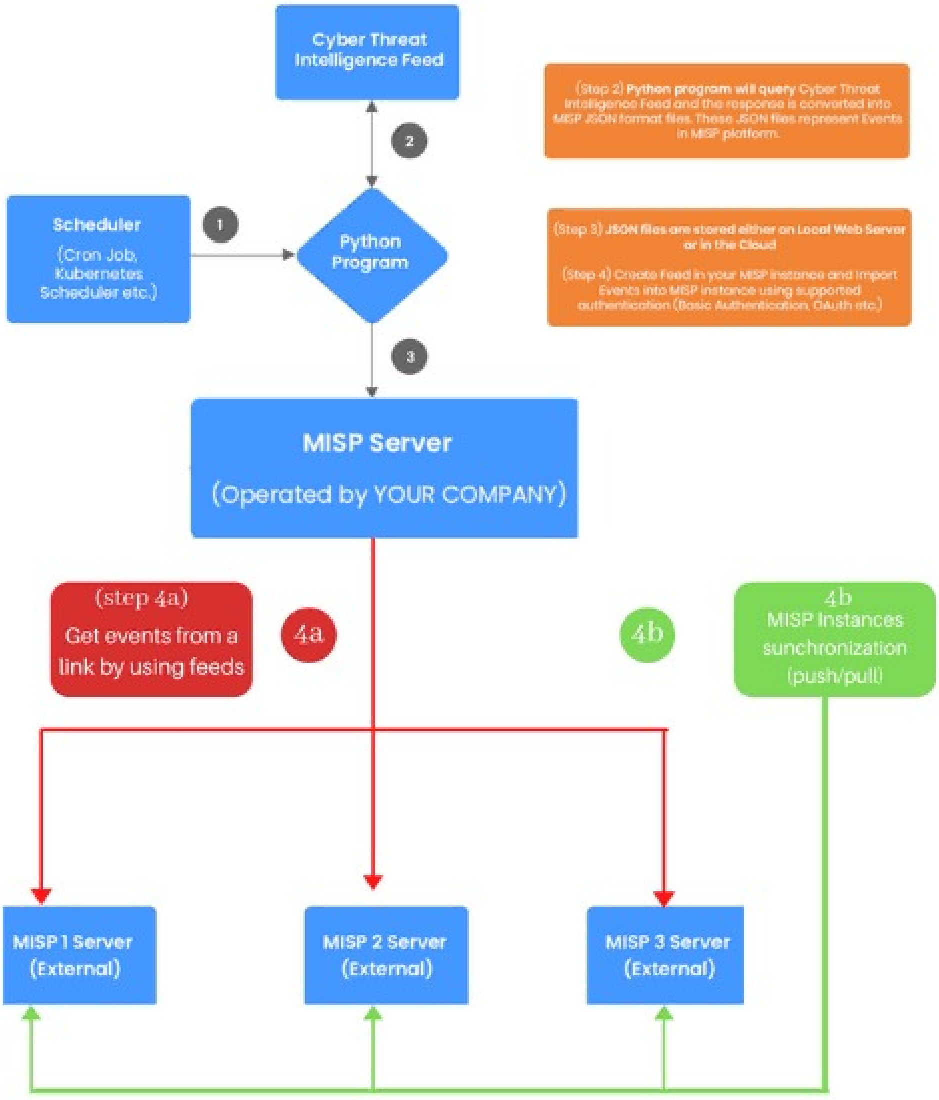
Raj

August 19, 2020

MISP is an open-source Threat intelligence and sharing platform (formerly known as Malware Information Sharing Platform) that is used for collecting, storing distributing and sharing cybersecurity indicators and threats about cybersecurity incidents & malware analysis.

MISP provides facilities to support the exchange of information but also the consumption of information by network intrusion detection systems (NIDS), a Log-based intrusion detection system (LIDS), but also by log analysis tools, SIEMs.

- MISP provides storage of technical and non-technical information about seen malware and attacks.
- Creates automatically relations between malware and their attributes.
- It Stores all of the intelligence and threat attributes data in a structured format.
- It Shares threat attributes & malware data by default with other trust-groups.
- MISP able to Improve malware detection and reversing to promote information exchange among organizations (e.g. avoiding duplicate works).
- MISP Stores all information from other instances locally (ensuring confidentiality on queries).


Cyber Threat Intelligence Feed
2
(Step 2) Python program will query Cyber Threat Intelligence Feed and the response is converted into MISP JSON format files. These JSON files represent Events in MISP platform.
Scheduler
(Cron Job, Kubernetes Scheduler etc.)
1
Python Program
(Step 3) JSON files are stored either on Local Web Server or in the Cloud
(Step 4) Create Feed in your MISP instance and import Events into MISP instance using supported authentication (Basic Authentication, OAuth etc.)
3
MISP Server
(Operated by YOUR COMPANY)
(step 4a)
Get events from a link by using feeds
4a
4b
4b
MISP Instances sunchronization (push/pull)
MISP 1 Server (External)
MISP 2 Server (External)
MISP 3 Server (External)

To configure MISP in your Ubuntu platform, there are some prerequisites required for installation.

Ubuntu 20.04.1

Mysql

Non-root user

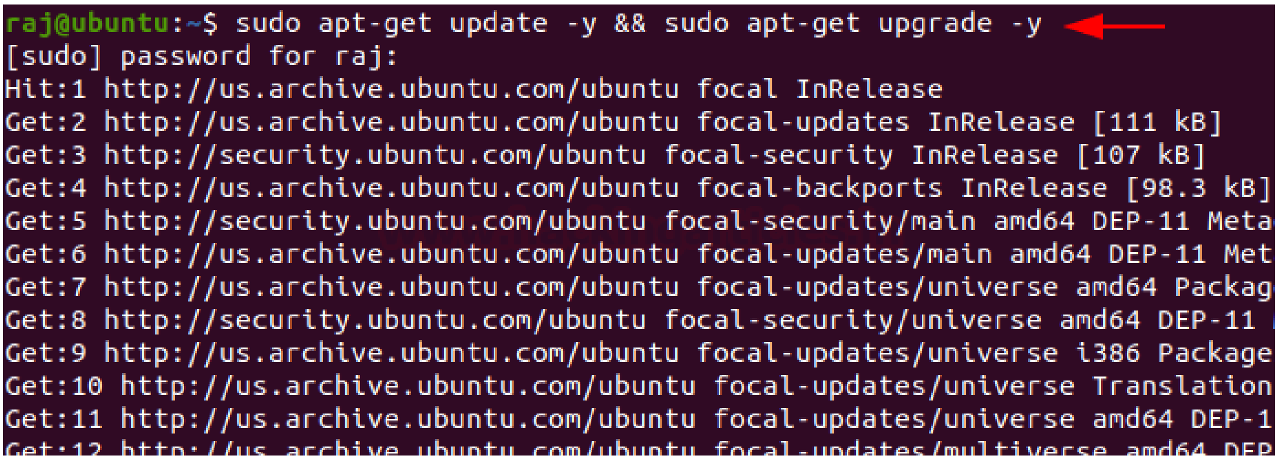
Table of Content

- Create a MISP event
- Addition of object to MISP event
- Search MISP for IOC
- Threat monitoring
- Updation of MISP in future for latest versions

Install MISP and All Dependencies

Let’s begin installation with system update and upgrade.

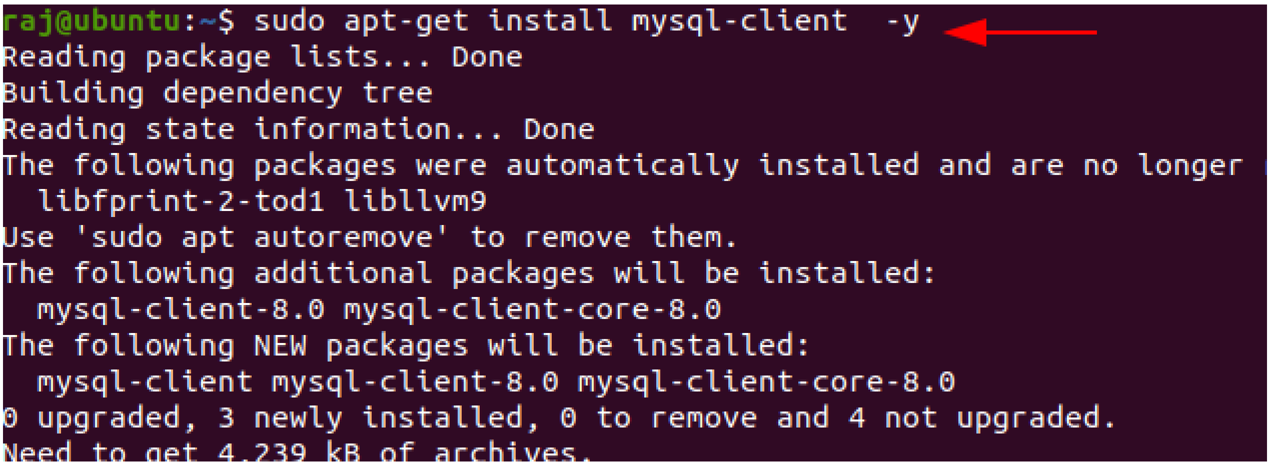
```
sudo apt-get update -y && sudo apt-get upgrade -y
```



```
raj@ubuntu:~$ sudo apt-get update -y && sudo apt-get upgrade -y
[sudo] password for raj:
Hit:1 http://us.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease [111 kB]
Get:3 http://security.ubuntu.com/ubuntu focal-security InRelease [107 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease [98.3 kB]
Get:5 http://security.ubuntu.com/ubuntu focal-security/main amd64 DEP-11 Meta
Get:6 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Met
Get:7 http://us.archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packag
Get:8 http://security.ubuntu.com/ubuntu focal-security/universe amd64 DEP-11
Get:9 http://us.archive.ubuntu.com/ubuntu focal-updates/universe i386 Package
Get:10 http://us.archive.ubuntu.com/ubuntu focal-updates/universe Translation
Get:11 http://us.archive.ubuntu.com/ubuntu focal-updates/universe amd64 DEP-1
Get:12 http://us.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 DEP
```

MISP requires Mysql-client available in our machine. Install Mysql-client using the below command.

```
sudo apt-get install mysql-client -y
```

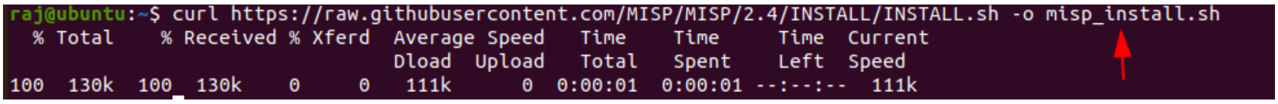


```
raj@ubuntu:~$ sudo apt-get install mysql-client  -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer
  libfprint-2-tod1 libllvm9
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  mysql-client-8.0 mysql-client-core-8.0
The following NEW packages will be installed:
  mysql-client mysql-client-8.0 mysql-client-core-8.0
0 upgraded, 3 newly installed, 0 to remove and 4 not upgraded.
Need to get 4,239 kB of archives.
```

To install MISP on fresh ubuntu 20.04.1, all you need to do is the following. Just remember one thing this is an automated bash script that can’t run with Root privileges run this script with Non-root users.

Install MISP with install.sh

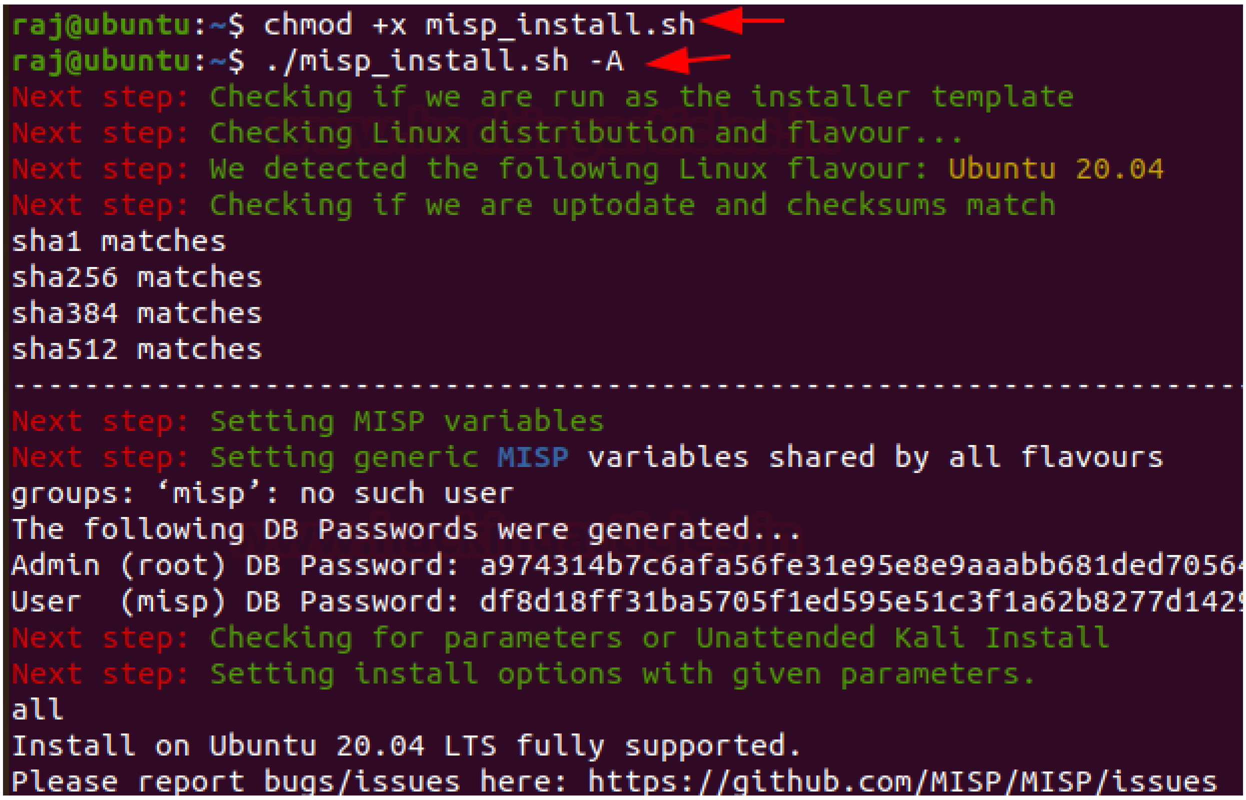
```
curl https://raw.githubusercontent.com/MISP/MISP/2.4/INSTALL/INSTALL.sh -o
misp_install.sh
```



```
raj@ubuntu:~$ curl https://raw.githubusercontent.com/MISP/MISP/2.4/INSTALL/INSTALL.sh -o misp_install.sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  130k  100  130k    0     0   111k      0  0:00:01  0:00:01 --:--:--  111k
```

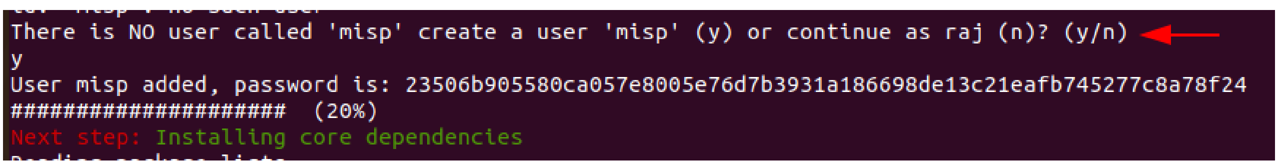
Change the permission of file misp_install.sh and make it executable. To do this run the following command. The script will need some time to install MISP on your Ubuntu platform.

```
chmod +x misp_install.sh
./misp_install.sh -A
```



```
raj@ubuntu:~$ chmod +x misp_install.sh
raj@ubuntu:~$ ./misp_install.sh -A
Next step: Checking if we are run as the installer template
Next step: Checking Linux distribution and flavour...
Next step: We detected the following Linux flavour: Ubuntu 20.04
Next step: Checking if we are uptodate and checksums match
sha1 matches
sha256 matches
sha384 matches
sha512 matches
---------------------------------------------------------------
Next step: Setting MISP variables
Next step: Setting generic MISP variables shared by all flavours
groups: ‘misp’: no such user
The following DB Passwords were generated...
Admin (root) DB Password: a974314b7c6afa56fe31e95e8e9aaabb681ded7056
User  (misp) DB Password: df8d18ff31ba5705f1ed595e51c3f1a62b8277d142
Next step: Checking for parameters or Unattended Kali Install
Next step: Setting install options with given parameters.
all
Install on Ubuntu 20.04 LTS fully supported.
Please report bugs/issues here: https://github.com/MISP/MISP/issues
```

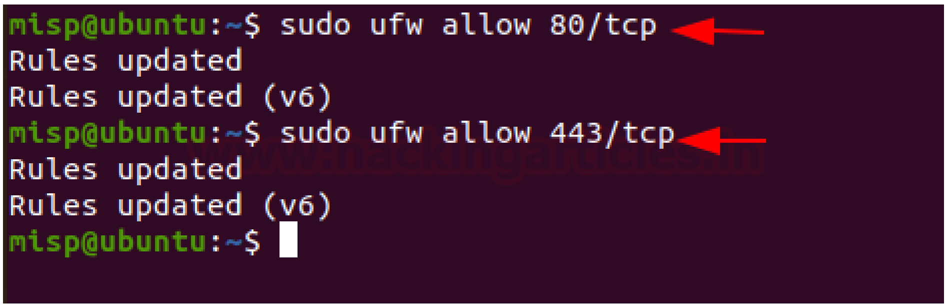
In the middle of installation Enter “Y” to create MISP user



```
There is NO user called 'misp' create a user 'misp' (y) or continue as raj (n)? (y/n)
y
User misp added, password is: 23506b905580ca057e8005e76d7b3931a186698de13c21eafb745277c8a78f24
######################  (20%)
Next step: Installing core dependencies
```

Now, we are going to add a rule to firewall this will allow port 80/tcp and 443/tcp

```
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp
```

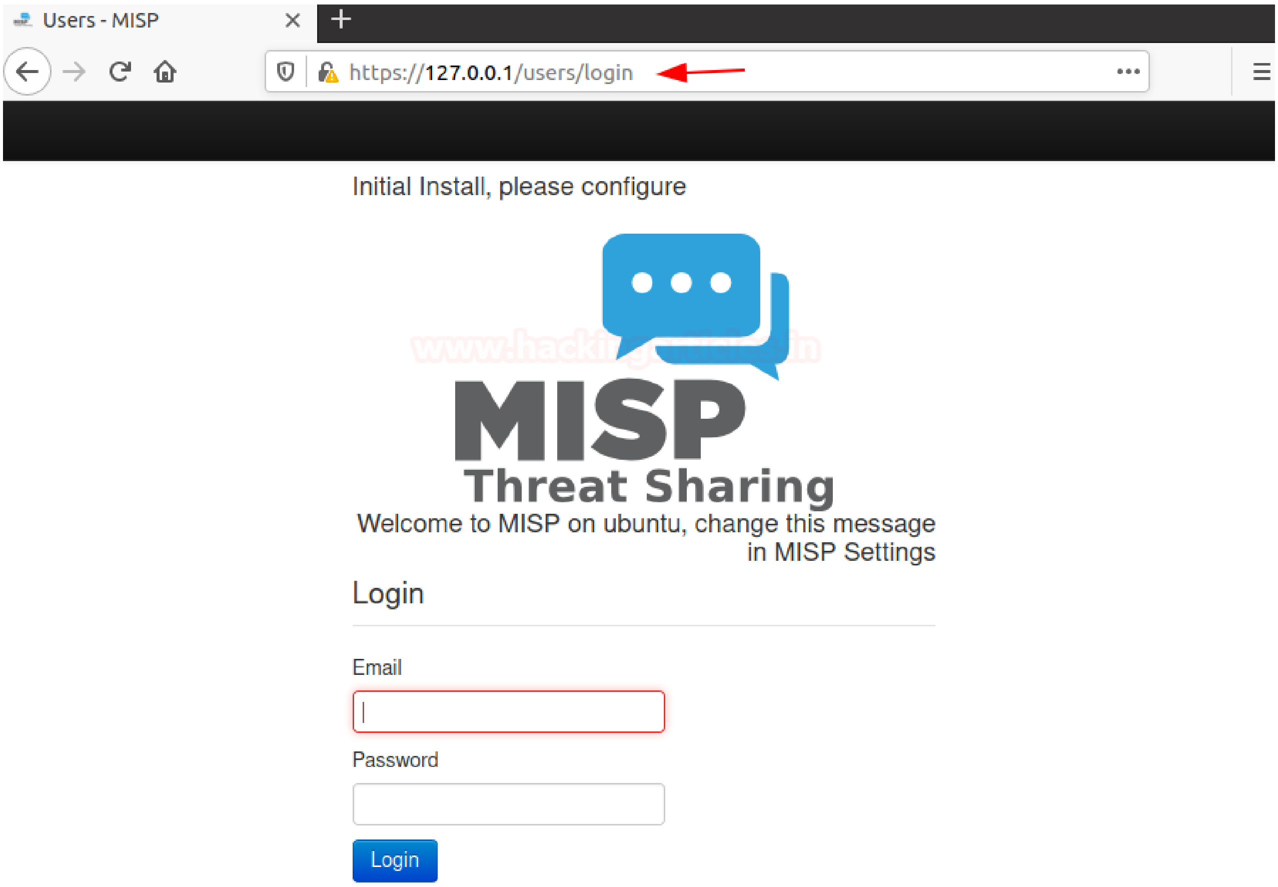


```
misp@ubuntu:~$ sudo ufw allow 80/tcp
Rules updated
Rules updated (v6)
misp@ubuntu:~$ sudo ufw allow 443/tcp
Rules updated
Rules updated (v6)
misp@ubuntu:~$
```

After, the installation of MISP we can use a browser to connect to MISP.

By Default, MISP is listening on loopback address or Base URL To access MISP on your Browser browse the following URL

```
https://127.0.0.1/users/login
```



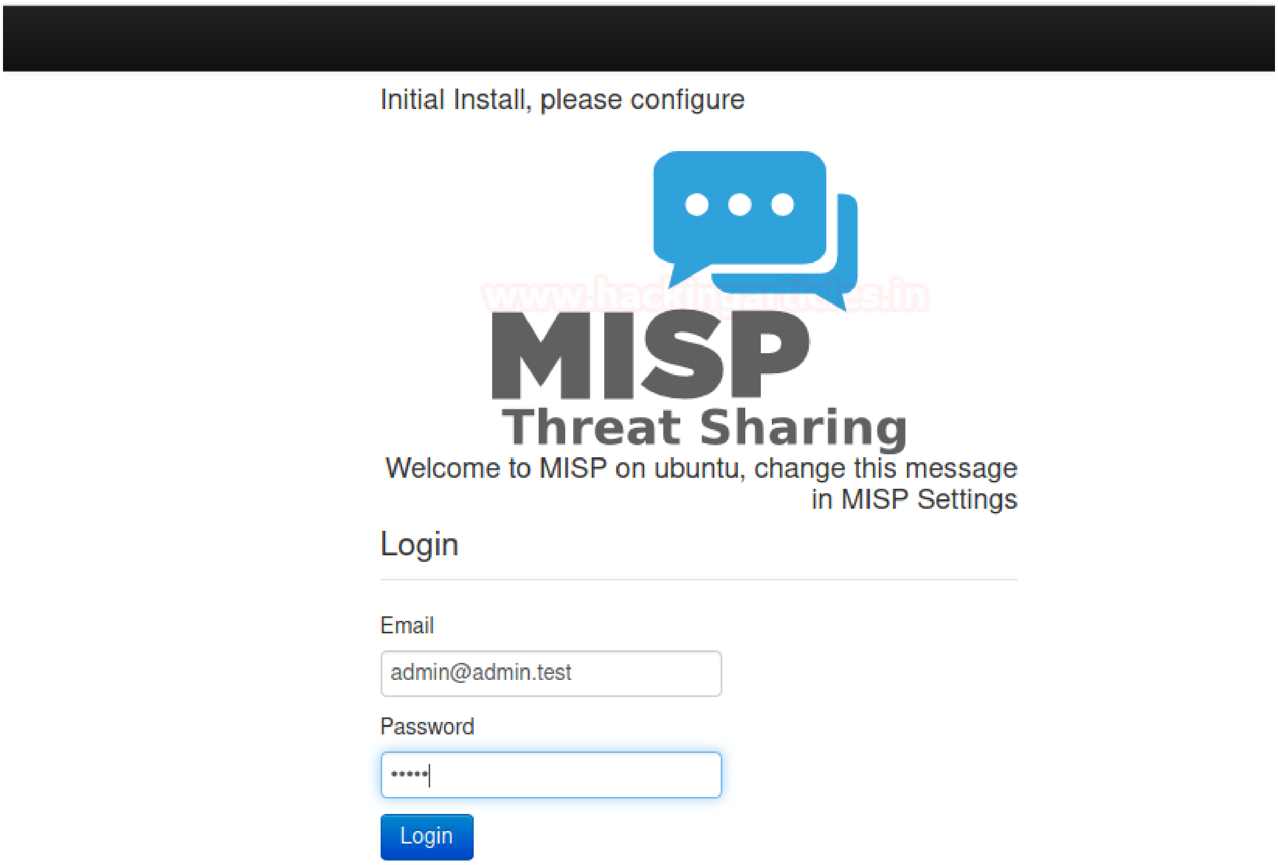
Initial Install, please configure

Welcome to MISP on ubuntu, change this message in MISP Settings

Default Credentials

For the MISP web interface -> admin@admin.test:admin

For the system -> misp:Password1234



Initial Install, please configure

Welcome to MISP on ubuntu, change this message in MISP Settings

Login

Email

admin@admin.test

Password

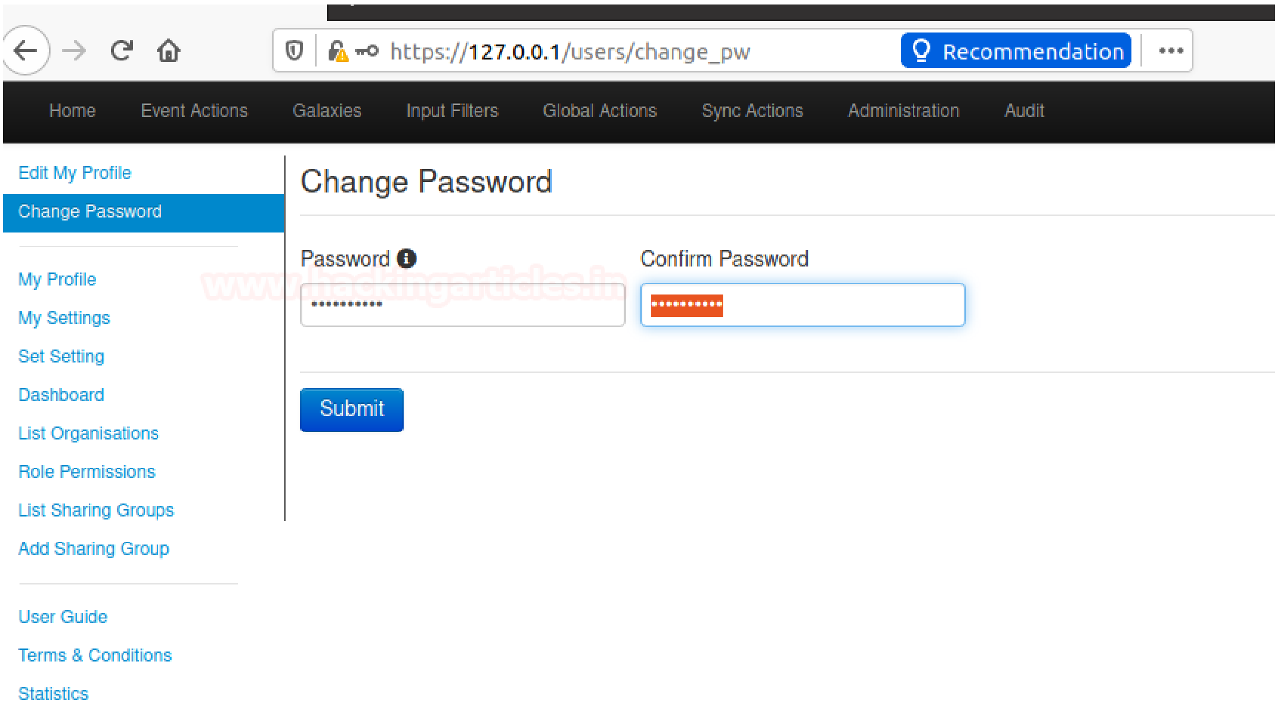
•••••

Change Admin Password

Enter new Password

The password must be in standard form. Minimum Length of password is at least 12 words that contain upper case & lowercase alphabet, special character and a numerical value

For example – Ignite@12345



Change Password

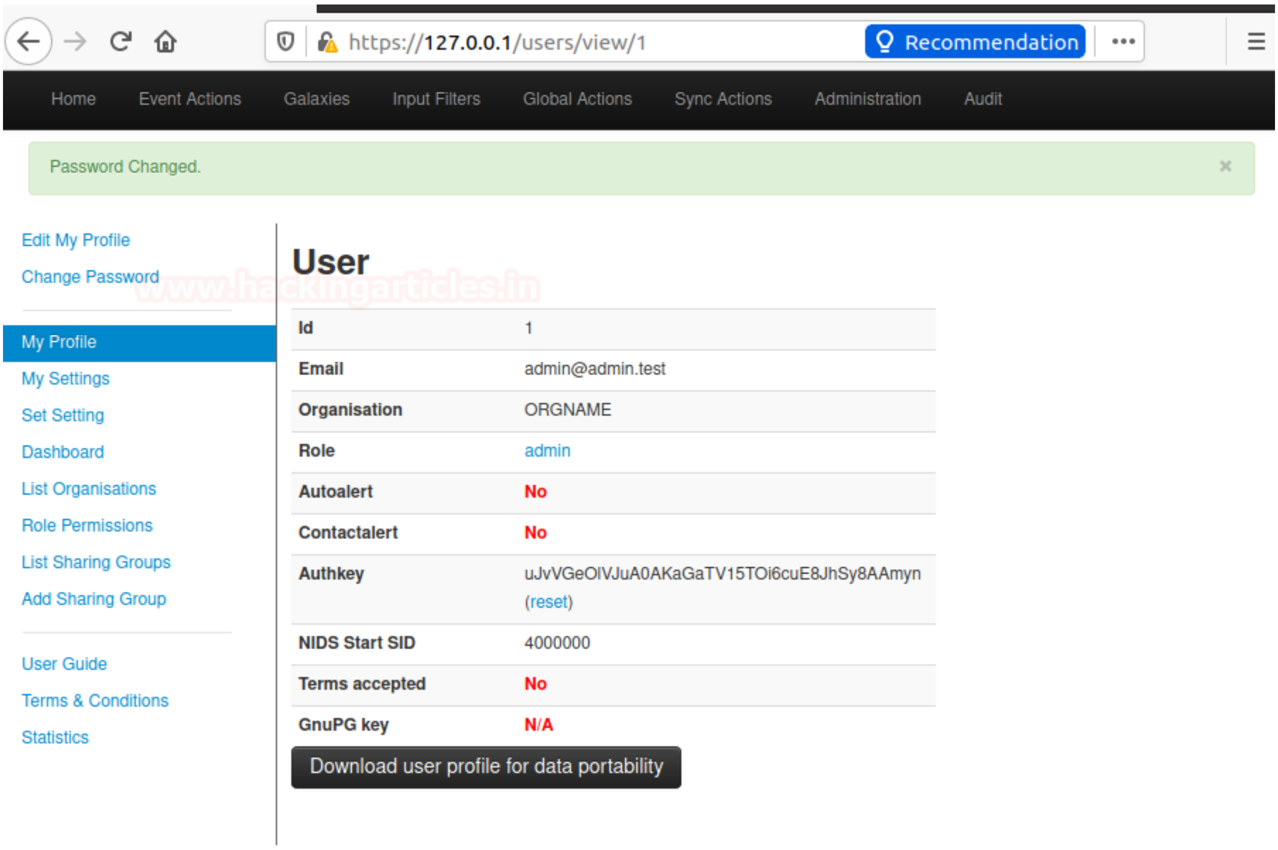
Password: ••••••••••

Confirm Password: ••••••••••

You can verify your credentials by a head over to

```
https://127.0.0.1/users/view/1
```

or also by going in my profile section of MISP Administration panel



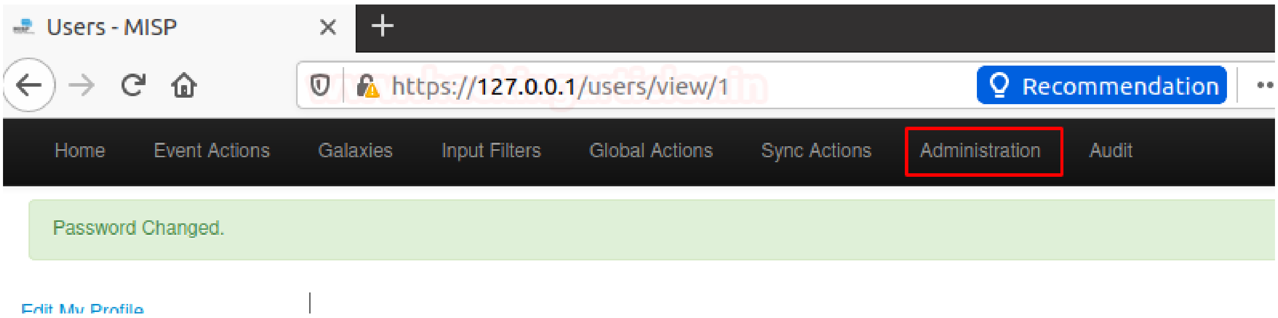
Password Changed.

User

Id	1
Email	admin@admin.test
Organisation	ORGNAME
Role	admin
Autoalert	No
Contactalert	No
Authkey	uJvVGeOIVJuA0AKaGaTV15TOi6cuE8JhSy8AAmyn (reset)
NIDS Start SID	4000000
Terms accepted	No
GnuPG key	N/A

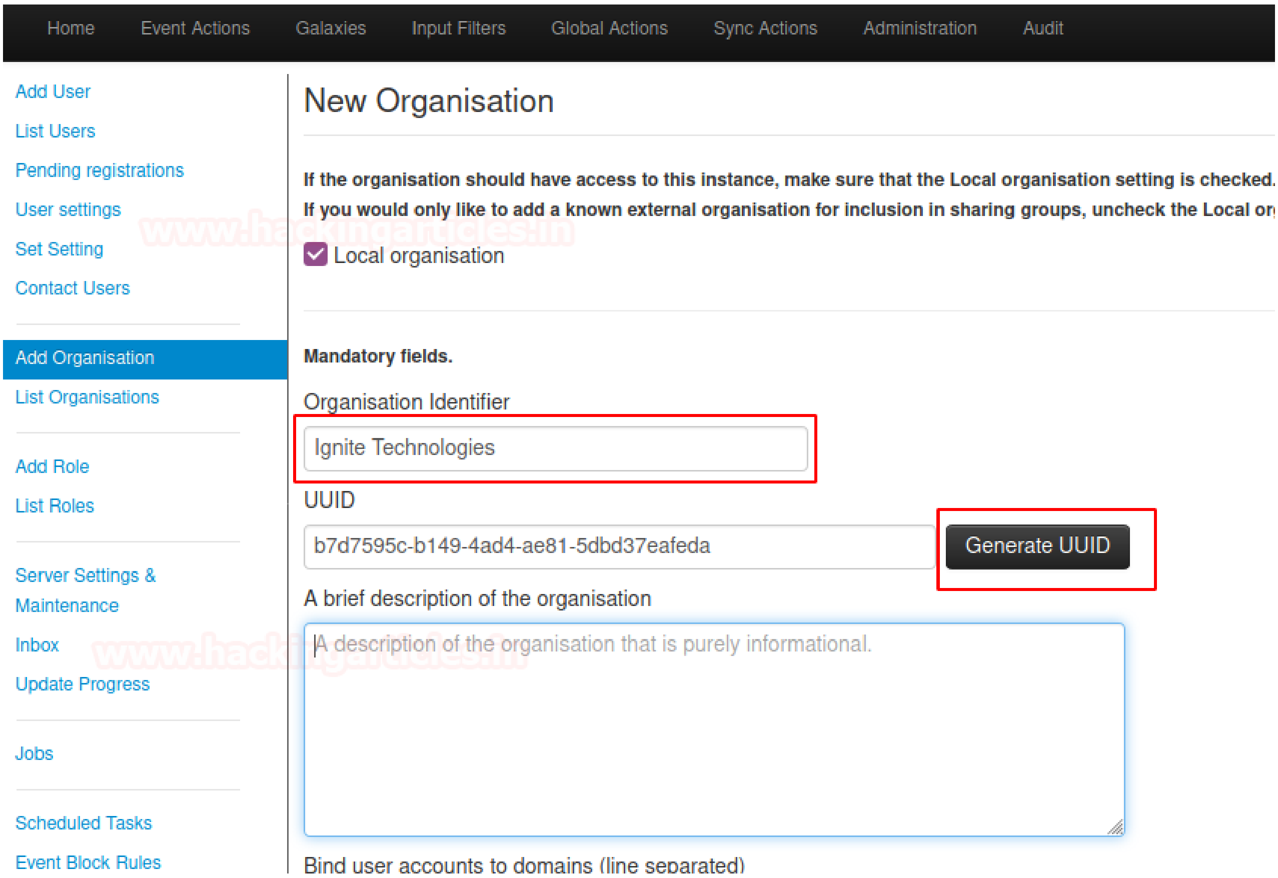
Create an organization

GO to Administration section head over to Add Organisations



Password Changed.

- Select Administration > add Organisations
- Enter "< organization name >" into organization identifier
- Select "Generate UUID"
- Select "submit" button at the bottom



New Organisation

If the organisation should have access to this instance, make sure that the Local organisation setting is checked.
If you would only like to add a known external organisation for inclusion in sharing groups, uncheck the Local or

☑ Local organisation

Mandatory fields.

Organisation Identifier

Ignite Technologies

UUID

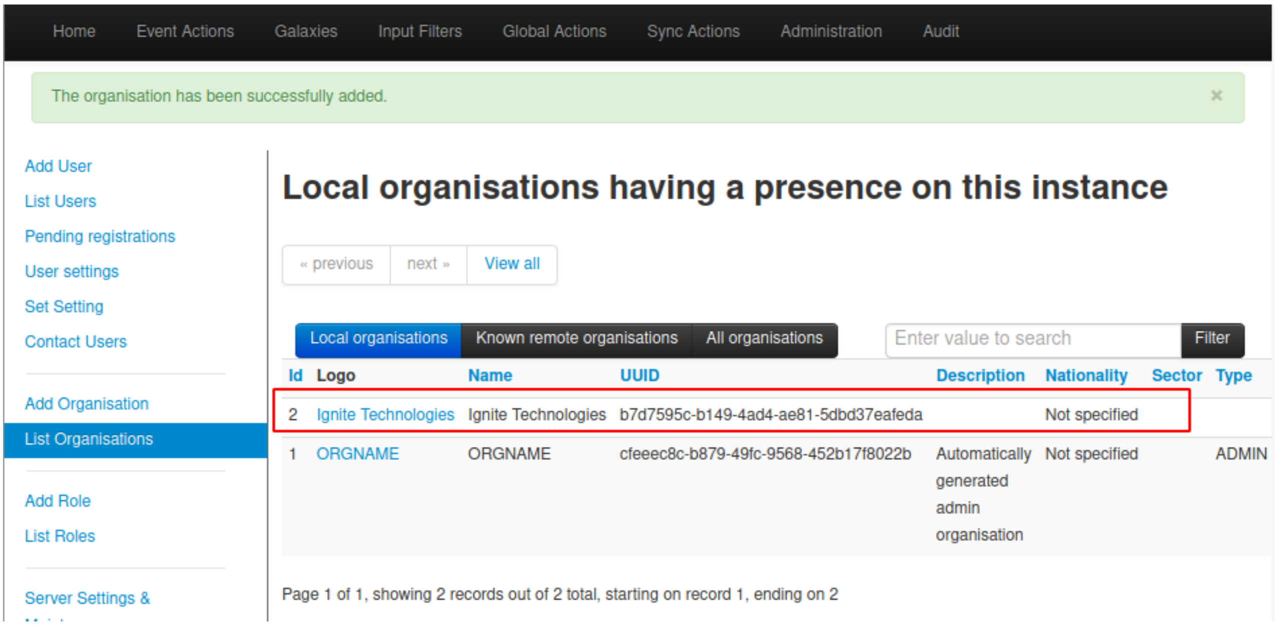
b7d7595c-b149-4ad4-ae81-5dbd37eafeda

A brief description of the organisation

A description of the organisation that is purely informational.

Bind user accounts to domains (line separated)

You can also check the instance presence of your local organizations by heading over to List organizations under the section of Administration



The organisation has been successfully added.

Local organisations having a presence on this instance

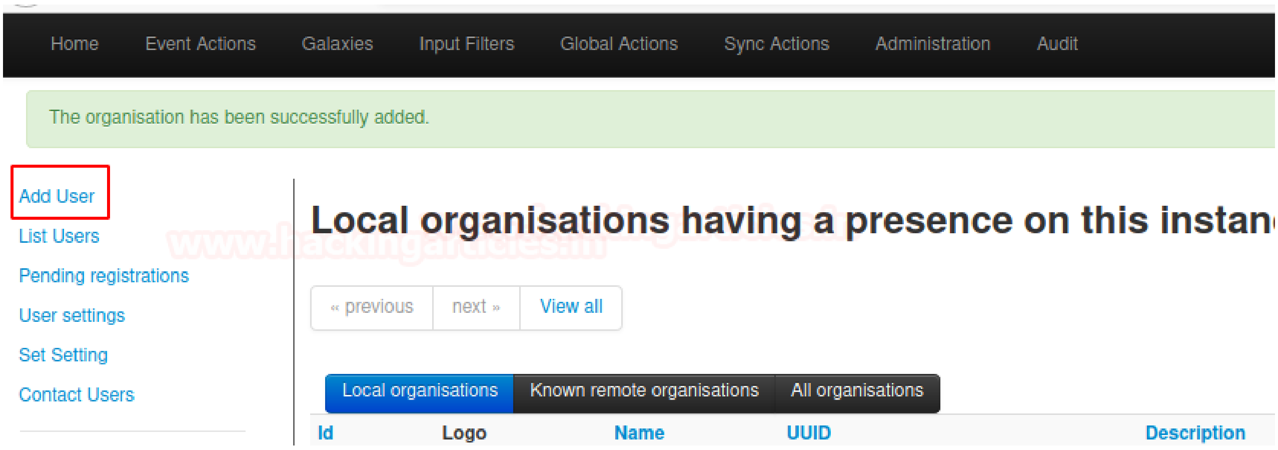
Id	Logo	Name	UUID	Description	Nationality	Sector	Type
2	Ignite Technologies	Ignite Technologies	b7d7595c-b149-4ad4-ae81-5dbd37eafeda		Not specified		
1	ORGNAME	ORGNAME	cfeeec8c-b879-49fc-9568-452b17f8022b	Automatically generated admin organisation	Not specified		ADMIN

Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2

Create Admin for New Organisation

we have successfully created an organization let’s assign an Admin role to the organization all you need to do is head over to “Add User” under the section of “Administration”

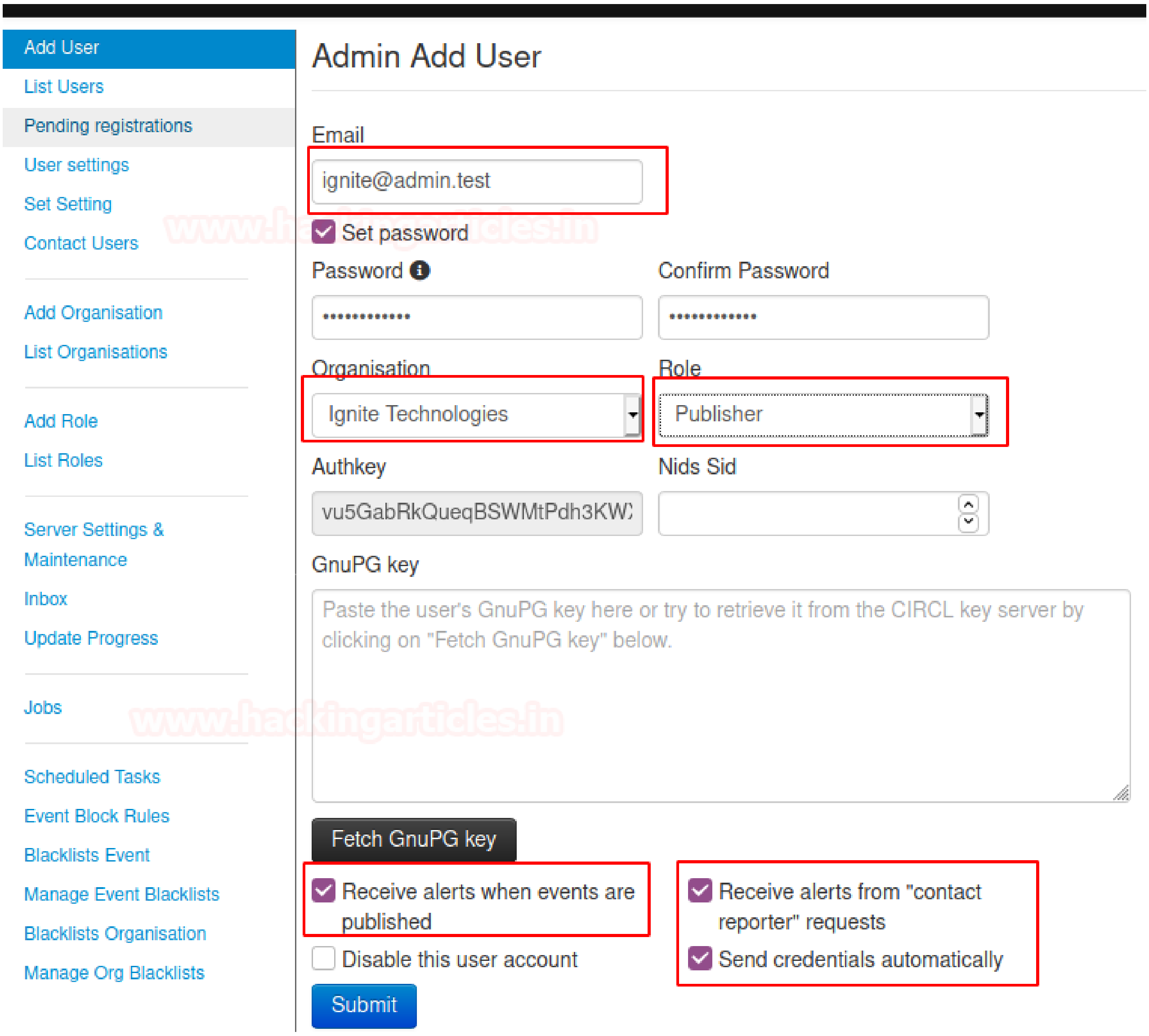
Administration > Add user



The organisation has been successfully added.

Local organisations having a presence on this instan

- Enter “ignite@<fqdn>” for email
- Check the “set password” password should be in a standard form that satisfies the minimum requirements.
- Select “<new org name>” for organization
- Select “Role” for the new organization
- Select “submit” button at the bottom



Add User
List Users
Pending registrations
User settings
Set Setting
Contact Users

Add Organisation
List Organisations

Add Role
List Roles

Server Settings & Maintenance
Inbox
Update Progress

Jobs

Scheduled Tasks
Event Block Rules
Blacklists Event
Manage Event Blacklists
Blacklists Organisation
Manage Org Blacklists

Admin Add User

Email: ignite@admin.test

☑ Set password

Password: ••••••••••••

Confirm Password: ••••••••••••

Organisation: Ignite Technologies

Role: Publisher

Authkey: vu5GabRkQueqBSWMtPdh3KW

Nids Sid:

GnuPG key: Paste the user's GnuPG key here or try to retrieve it from the CIRCL key server by clicking on "Fetch GnuPG key" below.

Fetch GnuPG key

☑ Receive alerts when events are published

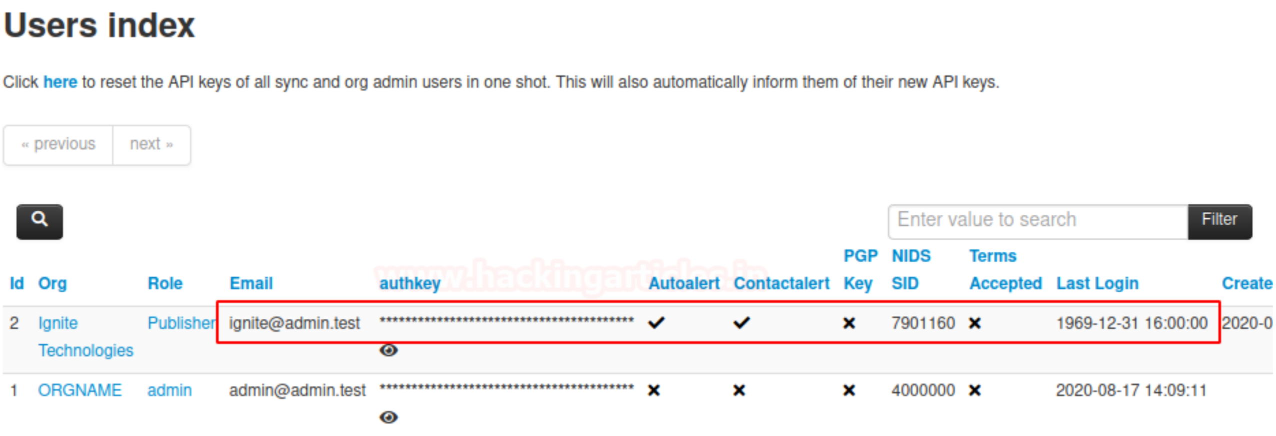
☑ Receive alerts from "contact reporter" requests

☐ Disable this user account

☑ Send credentials automatically

Submit

You can also check the instance Rights of your local organizations by heading over to List organizations under the section of Administration



Users index

Click **here** to reset the API keys of all sync and org admin users in one shot. This will also automatically inform them of their new API keys.

« previous next »

Enter value to search Filter

Id	Org	Role	Email	authkey	Autoalert	Contactalert	PGP Key	NIDS SID	Terms Accepted	Last Login	Create
2	Ignite Technologies	Publisher	ignite@admin.test	**	✓	✓	✗	7901160	✗	1969-12-31 16:00:00	2020-0
1	ORGNAME	admin	admin@admin.test	**	✗	✗	✗	4000000	✗	2020-08-17 14:09:11	

Create an API user for the new organization

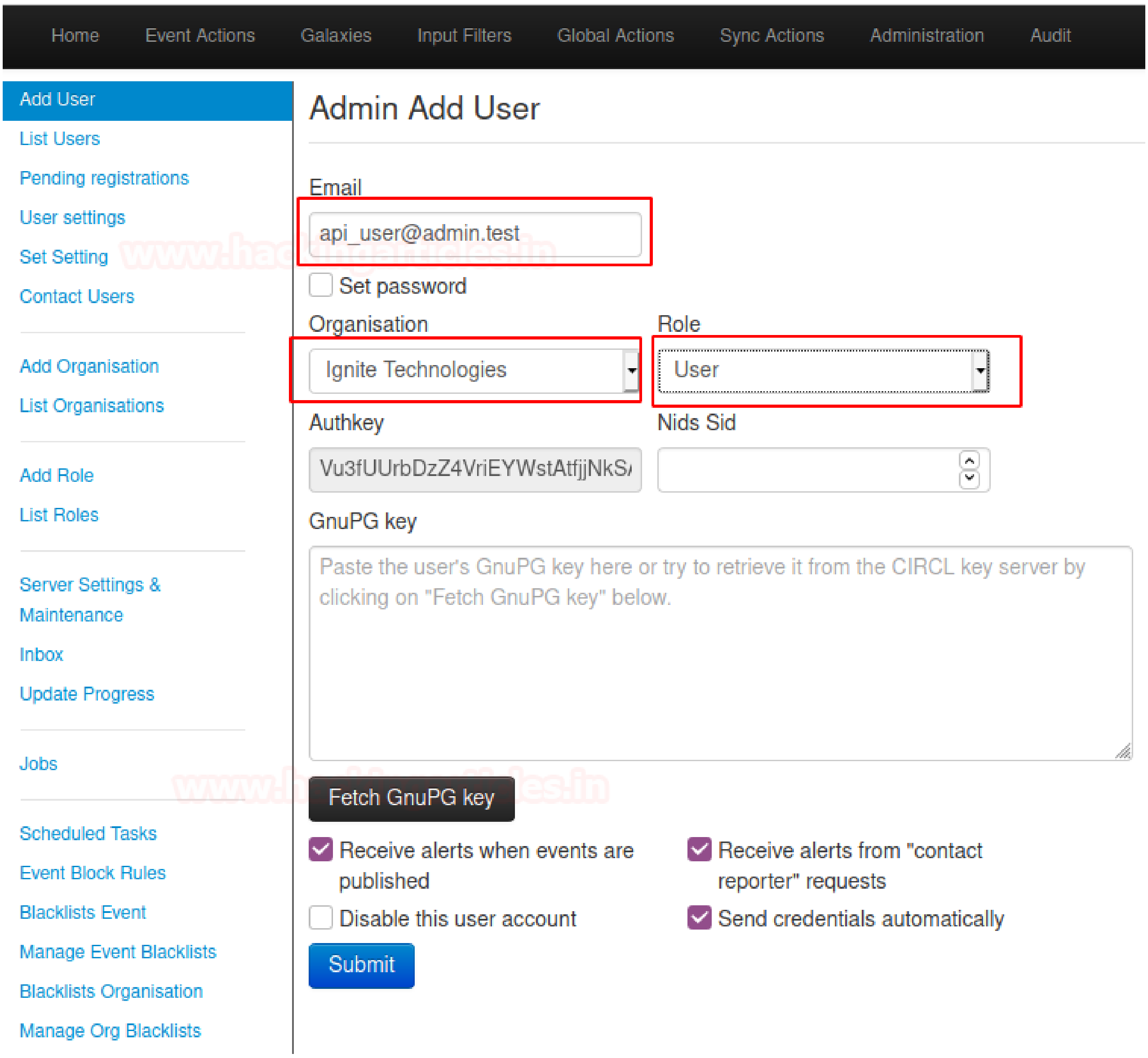
Administration > Add user

Enter “api_user@<fqdn>” for email

Select “<new organization name >” for organization

Select the “user” role for the new organization

Select “submit” button at the bottom



Admin Add User

Email: api_user@admin.test

□ Set password

Organisation: Ignite Technologies

Role: User

Authkey: Vu3fUUrbDzZ4VriEYWstAtfjjNkS/

Nids Sid:

GnuPG key: Paste the user's GnuPG key here or try to retrieve it from the CIRCL key server by clicking on "Fetch GnuPG key" below.

☑ Receive alerts when events are published

☑ Receive alerts from "contact reporter" requests

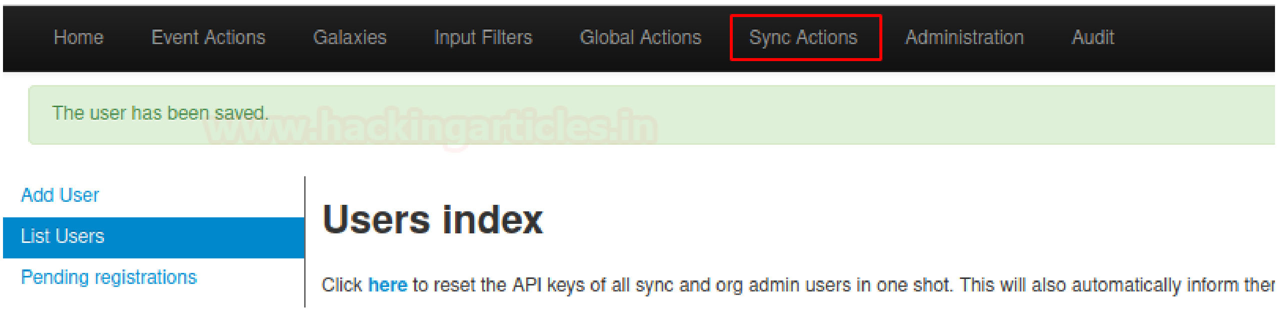
□ Disable this user account

☑ Send credentials automatically

Enable Threat intel feeds

To enable feeds you will need to login to MISP console with the superuser account which is admin@admin.test account.

This one is a little bit special, as we can go into the “Sync actions” tab to build our panel.



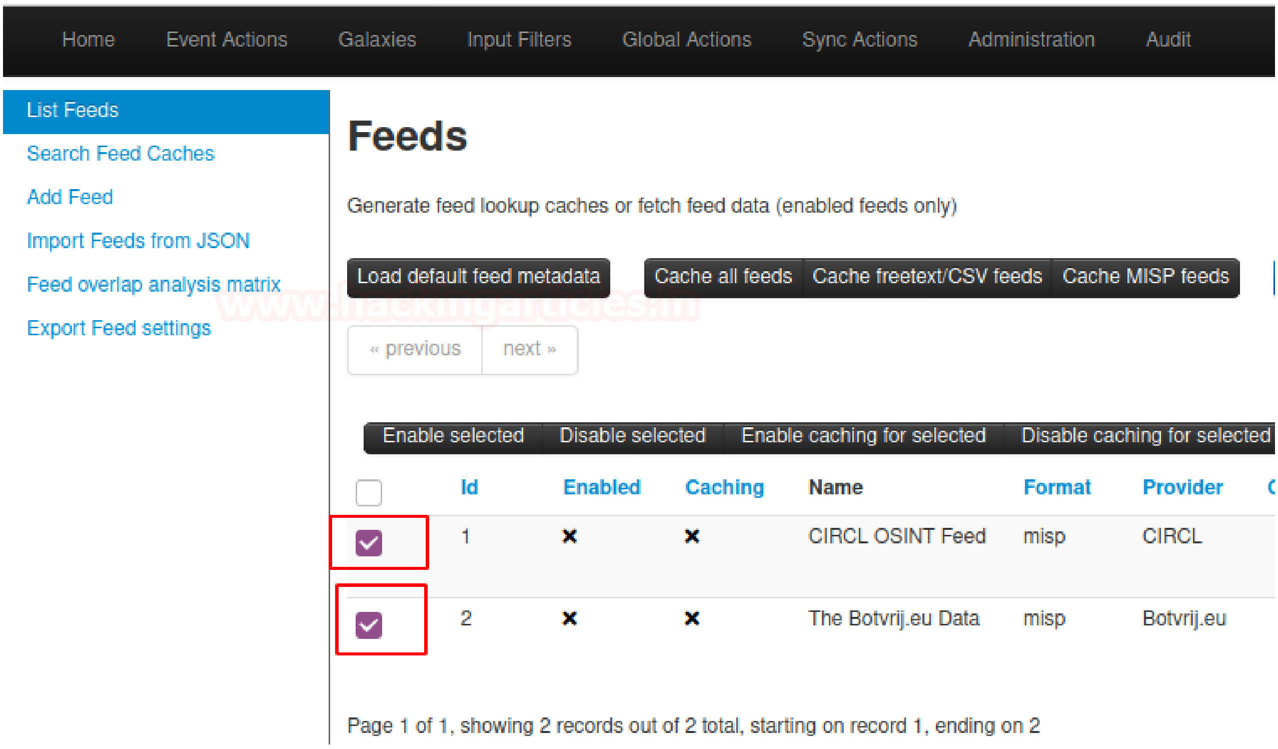
The user has been saved.

Users index

Click here to reset the API keys of all sync and org admin users in one shot. This will also automatically inform ther

When entering the Sync actions tab, select the list feeds tab.

From there find feeds such as CIRCL osint and check feeds tab



Feeds

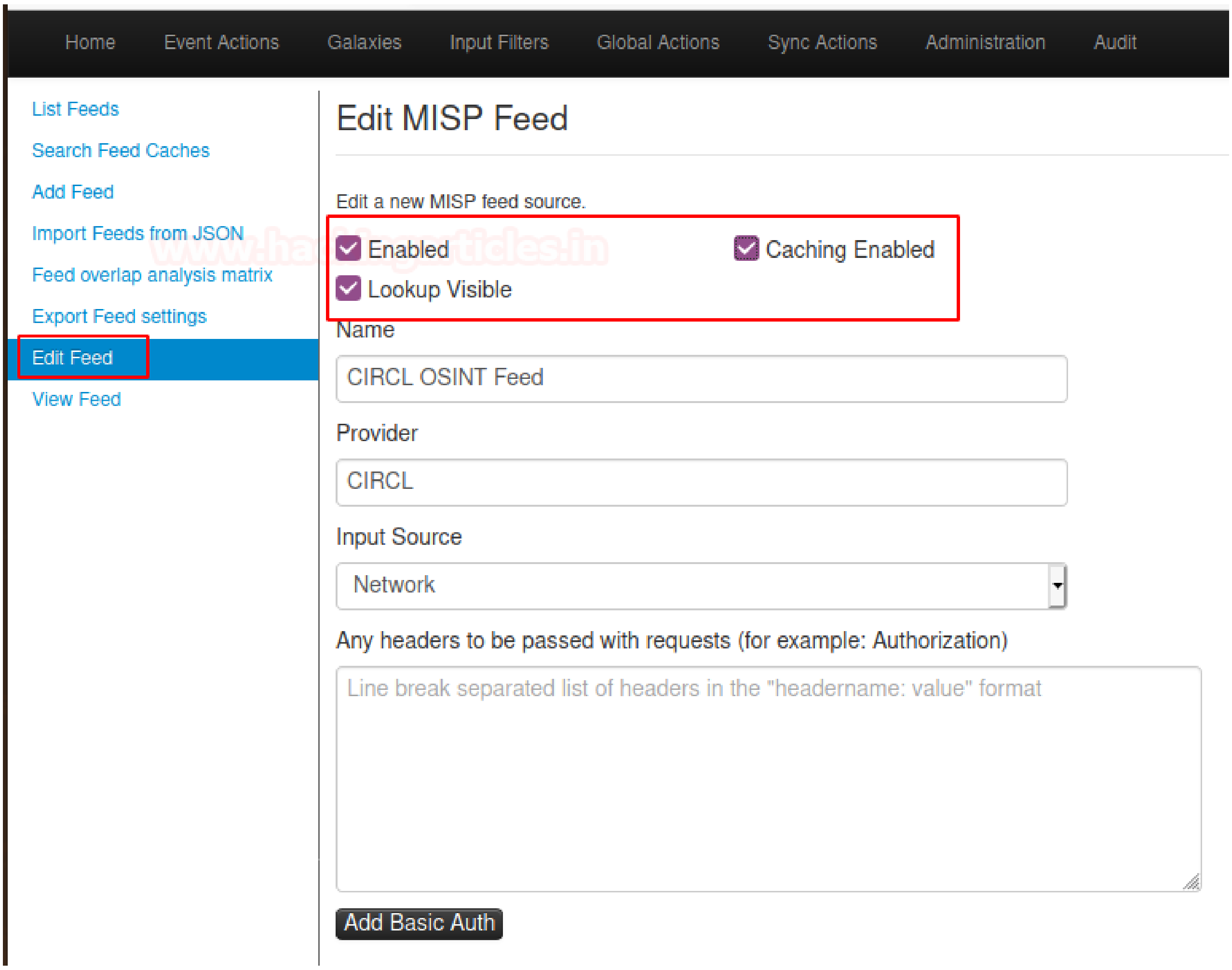
Generate feed lookup caches or fetch feed data (enabled feeds only)

☐	Id	Enabled	Caching	Name	Format	Provider
☑	1	✗	✗	CIRCL OSINT Feed	misp	CIRCL
☑	2	✗	✗	The Botvrij.eu Data	misp	Botvrij.eu

Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2

And then head over to the “Edit” icon

- Check “Enabled”
- Check “Lookup Visible”
- Check “Caching Enabled”
- Select “Edit” at the bottom



Edit MISP Feed

Edit a new MISP feed source.

☑ Enabled ☑ Caching Enabled

☑ Lookup Visible

Name: CIRCL OSINT Feed

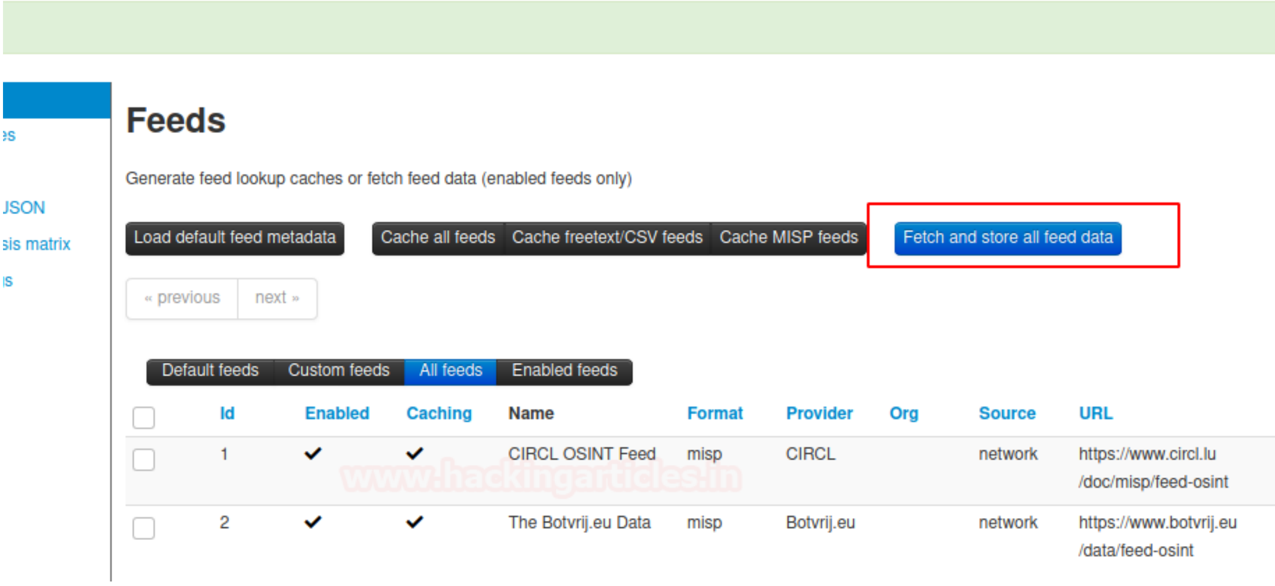
Provider: CIRCL

Input Source: Network

Any headers to be passed with requests (for example: Authorization)

Line break separated list of headers in the "headername: value" format

By Editing feeds head over to “fetch and store all feed data” tab



Feeds

Generate feed lookup caches or fetch feed data (enabled feeds only)

□	Id	Enabled	Caching	Name	Format	Provider	Org	Source	URL
□	1	✓	✓	CIRCL OSINT Feed	misp	CIRCL		network	https://www.circl.lu/doc/misp/feed-osint
□	2	✓	✓	The Botvrij.eu Data	misp	Botvrij.eu		network	https://www.botvrij.eu/data/feed-osint

Great! we have successfully Enabled threat intel feeds.

Setup Ipython+PyMISP

PyMISP is a python library to access MISP platforms via there REST API.

PyMISP allows you to fetch events, add or update events/attributes, add or update samples or search for attributes. PyMISP API is used to store indicators of compromise (IOCs) in MISP and query IOCs from MISP.

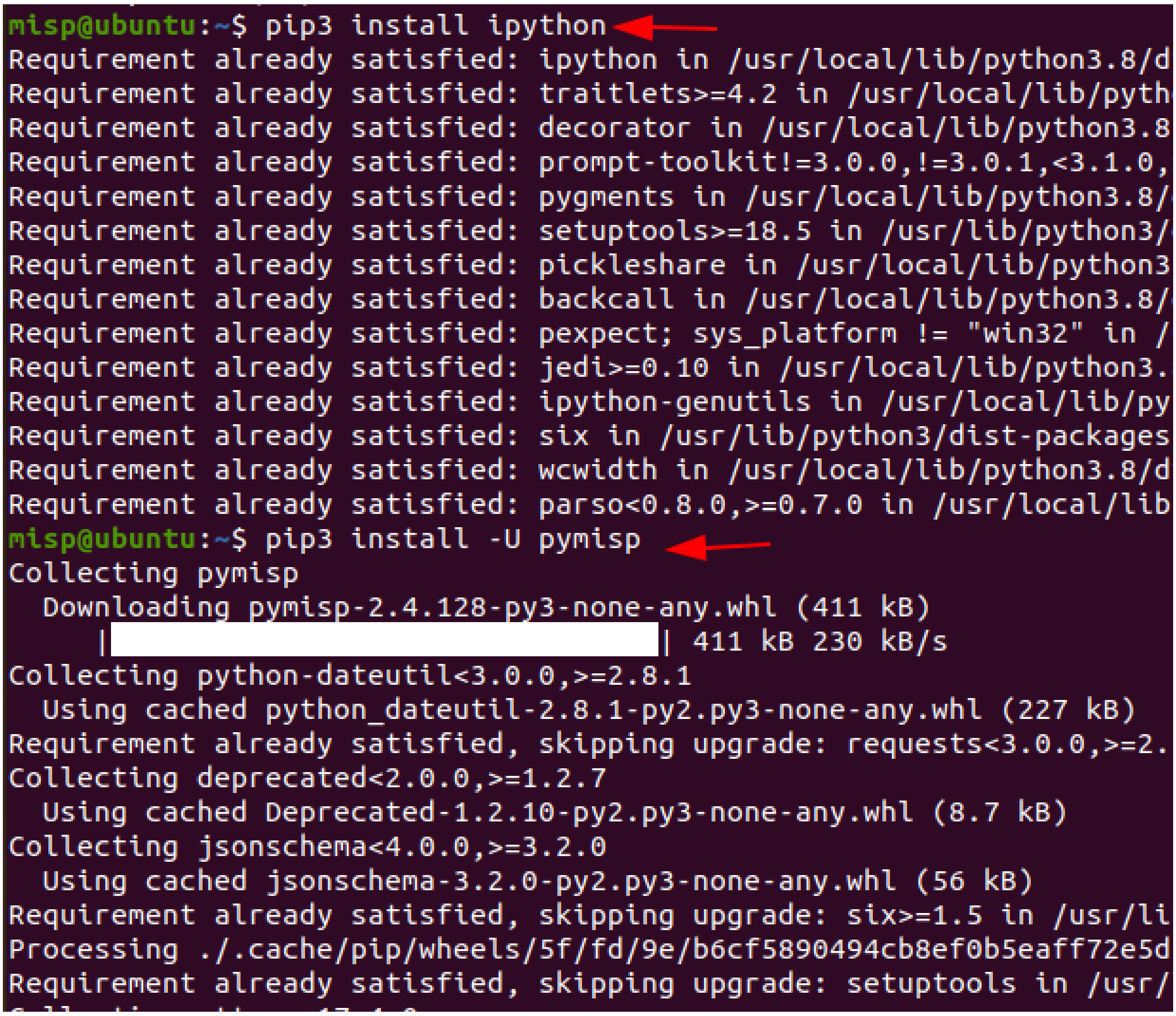
In the MISP console head over to Administration and select List Users

Look for “**api_user@<fqdn>**” and copy “**auth key**”

Let’s open the terminal and begin setup of Ipython & PyMISP

To do this run the following command

```
pip3 install ipython
pip3 install -U pymisp
```



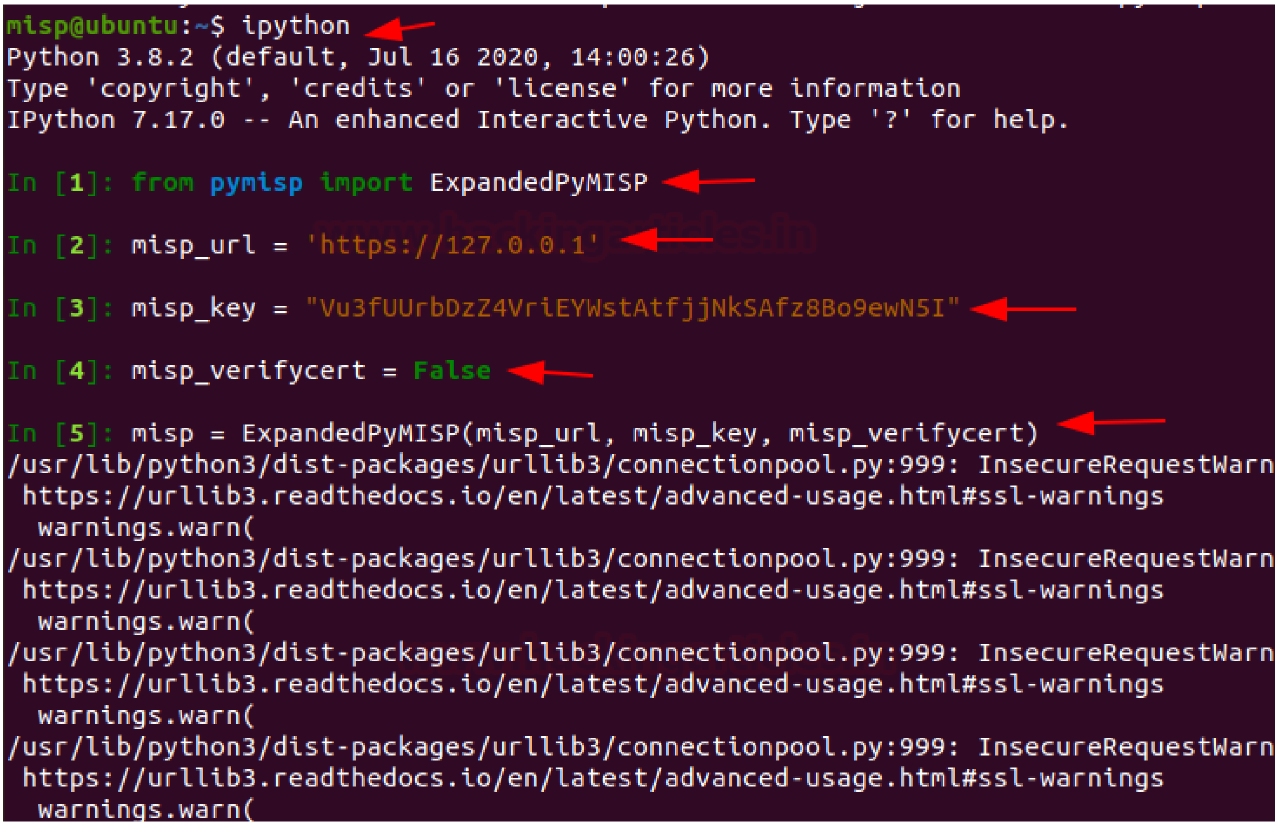
```
misp@ubuntu:~$ pip3 install ipython
Requirement already satisfied: ipython in /usr/local/lib/python3.8/d
Requirement already satisfied: traitlets>=4.2 in /usr/local/lib/pyth
Requirement already satisfied: decorator in /usr/local/lib/python3.8
Requirement already satisfied: prompt-toolkit!=3.0.0,!=3.0.1,<3.1.0,
Requirement already satisfied: pygments in /usr/local/lib/python3.8/
Requirement already satisfied: setuptools>=18.5 in /usr/lib/python3/
Requirement already satisfied: pickleshare in /usr/local/lib/python3
Requirement already satisfied: backcall in /usr/local/lib/python3.8/
Requirement already satisfied: pexpect; sys_platform != "win32" in /
Requirement already satisfied: jedi>=0.10 in /usr/local/lib/python3.
Requirement already satisfied: ipython-genutils in /usr/local/lib/py
Requirement already satisfied: six in /usr/lib/python3/dist-packages
Requirement already satisfied: wcwidth in /usr/local/lib/python3.8/d
Requirement already satisfied: parso<0.8.0,>=0.7.0 in /usr/local/lib
misp@ubuntu:~$ pip3 install -U pymisp
Collecting pymisp
  Downloading pymisp-2.4.128-py3-none-any.whl (411 kB)
     |████████████████████████████████| 411 kB 230 kB/s
Collecting python-dateutil<3.0.0,>=2.8.1
  Using cached python_dateutil-2.8.1-py2.py3-none-any.whl (227 kB)
Requirement already satisfied, skipping upgrade: requests<3.0.0,>=2.
Collecting deprecated<2.0.0,>=1.2.7
  Using cached Deprecated-1.2.10-py2.py3-none-any.whl (8.7 kB)
Collecting jsonschema<4.0.0,>=3.2.0
  Using cached jsonschema-3.2.0-py2.py3-none-any.whl (56 kB)
Requirement already satisfied, skipping upgrade: six>=1.5 in /usr/li
Processing ./.cache/pip/wheels/5f/fd/9e/b6cf5890494cb8ef0b5eaff72e5d
Requirement already satisfied, skipping upgrade: setuptools in /usr/
```

Connect MISP instance with PyMISP

Ipython

Ipython is an alterative python interpreter it is an interactive shell used for computing in python. Let’s load the Ipython interpreter and start scripting to do this follow the below commands. Just remind one thing don’t leave or exit from python interpreter till the end (e.g ipython).

```
ipython
from pymisp import ExpandedPyMISP
misp_url = 'https://<FQDN of MISP>'
misp_key = "<Enter MISP API key>"
misp_verifycert = False
misp = ExpandedPyMISP(misp_url, misp_key, misp_verifycert)
```

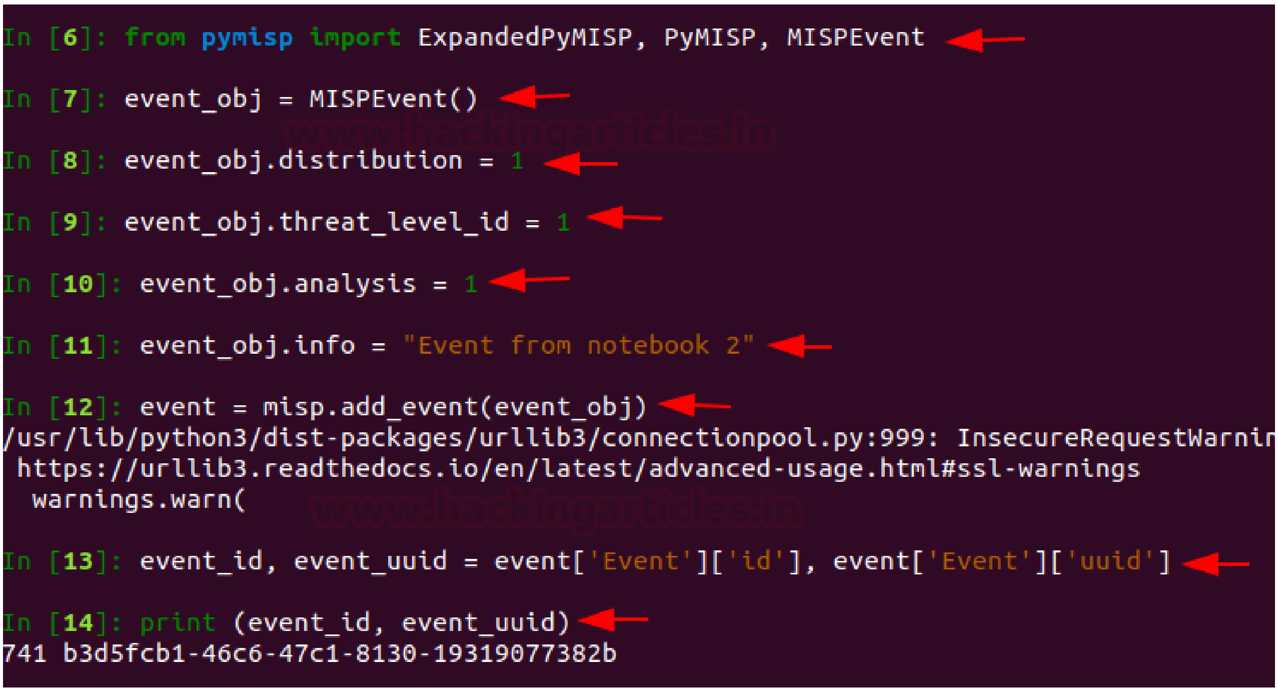


```
misp@ubuntu:~$ ipython
Python 3.8.2 (default, Jul 16 2020, 14:00:26)
Type 'copyright', 'credits' or 'license' for more information
IPython 7.17.0 -- An enhanced Interactive Python. Type '?' for help.

In [1]: from pymisp import ExpandedPyMISP

In [2]: misp_url = 'https://127.0.0.1'

In [3]: misp_key = "Vu3fUUrbDzZ4VriEYWstAtfjjNkSAfz8Bo9ewN5I"

In [4]: misp_verifycert = False

In [5]: misp = ExpandedPyMISP(misp_url, misp_key, misp_verifycert)
/usr/lib/python3/dist-packages/urllib3/connectionpool.py:999: InsecureRequestWarn
 https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
  warnings.warn(
/usr/lib/python3/dist-packages/urllib3/connectionpool.py:999: InsecureRequestWarn
 https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
  warnings.warn(
/usr/lib/python3/dist-packages/urllib3/connectionpool.py:999: InsecureRequestWarn
 https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
  warnings.warn(
/usr/lib/python3/dist-packages/urllib3/connectionpool.py:999: InsecureRequestWarn
 https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
  warnings.warn(
```

Create MISP Event

MISP events are encapsulation for contextually linked information. Linked information will include things such as domains, file hashes, IP addresses, Malicious binaries,. We are going to call an object named “Event from notebook 2” to do this run the following command.

```
from pymisp import ExpandedPyMISP, PyMISP, MISPEvent
event_obj = MISPEvent()
event_obj.distribution = 1
event_obj.threat_level_id = 1
event_obj.analysis = 1
event_obj.info = "Event from notebook 2"
# Add event to MISP
event = misp.add_event(event_obj)
event_id, event_uuid = event['Event']['id'], event['Event']['uuid']
print (event_id, event_uuid)
```



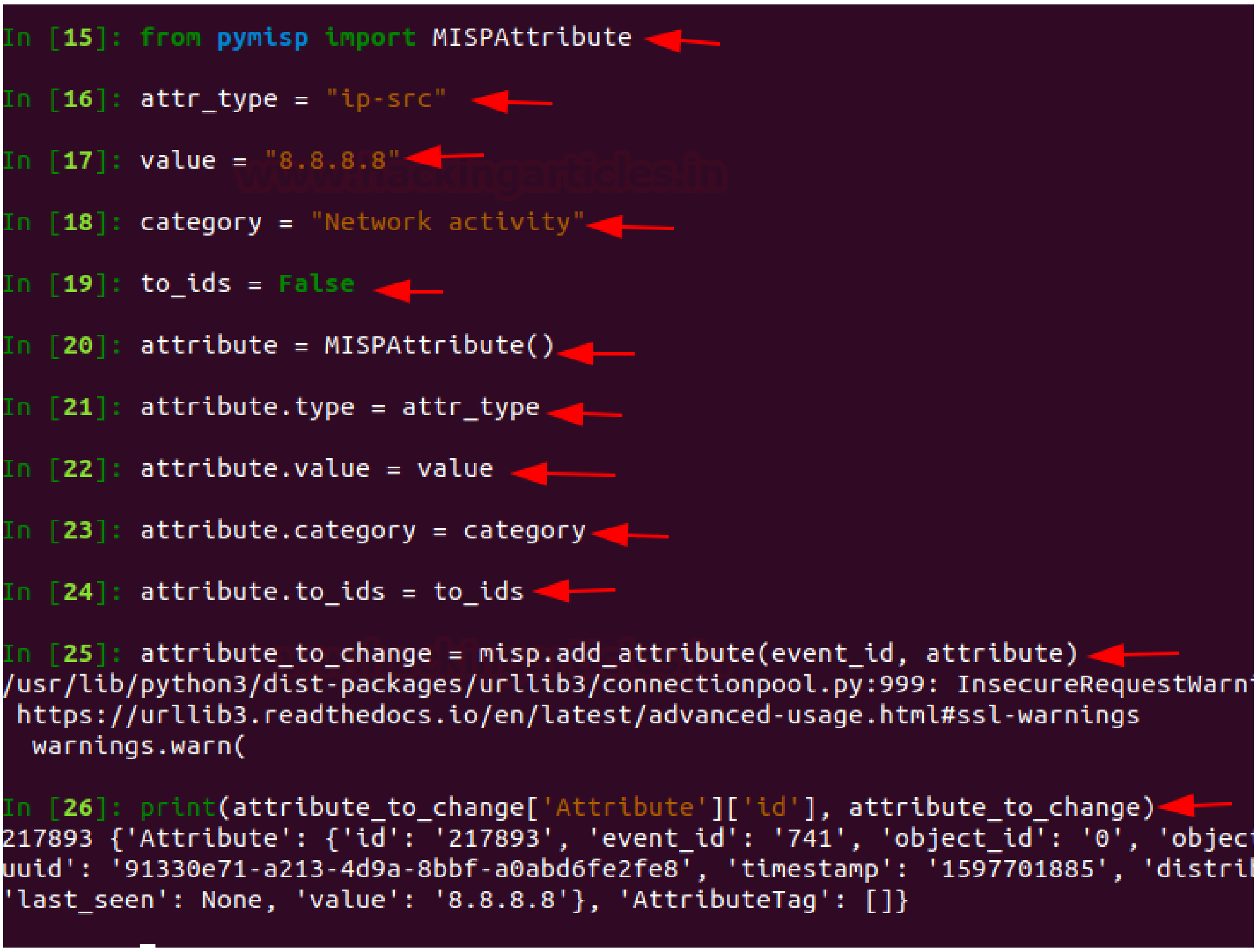
```
In [6]: from pymisp import ExpandedPyMISP, PyMISP, MISPEvent

In [7]: event_obj = MISPEvent()

In [8]: event_obj.distribution = 1

In [9]: event_obj.threat_level_id = 1

In [10]: event_obj.analysis = 1

In [11]: event_obj.info = "Event from notebook 2"

In [12]: event = misp.add_event(event_obj)
/usr/lib/python3/dist-packages/urllib3/connectionpool.py:999: InsecureRequestWarnin
 https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
  warnings.warn(

In [13]: event_id, event_uuid = event['Event']['id'], event['Event']['uuid']

In [14]: print (event_id, event_uuid)
741 b3d5fcb1-46c6-47c1-8130-19319077382b
```

Addition of object to MISP event

The creation of a new MISP object generator should be done using a pre-defined template and inheritance. Our new MISP generator needs to generate attributes, and add them as class properties using additional attributes. When the object is sent to MISP, all the class properties will be exported to JSON Export. Attributes in MISP can be network indicators such as IP address, System indicators (e.g a string in memory), or bank account details.

To do this run the following command.

```
from pymisp import MISPAttribute
# Define attributes
attr_type = "ip-src"
value = "8.8.8.8"
category = "Network activity"
to_ids = False
# Create attribute object
attribute = MISPAttribute()
attribute.type = attr_type
attribute.value = value
attribute.category = category
attribute.to_ids = to_ids
# Add attributes to event
attribute_to_change = misp.add_attribute(event_id, attribute)
# Print event
print(attribute_to_change['Attribute']['id'], attribute_to_change)
```

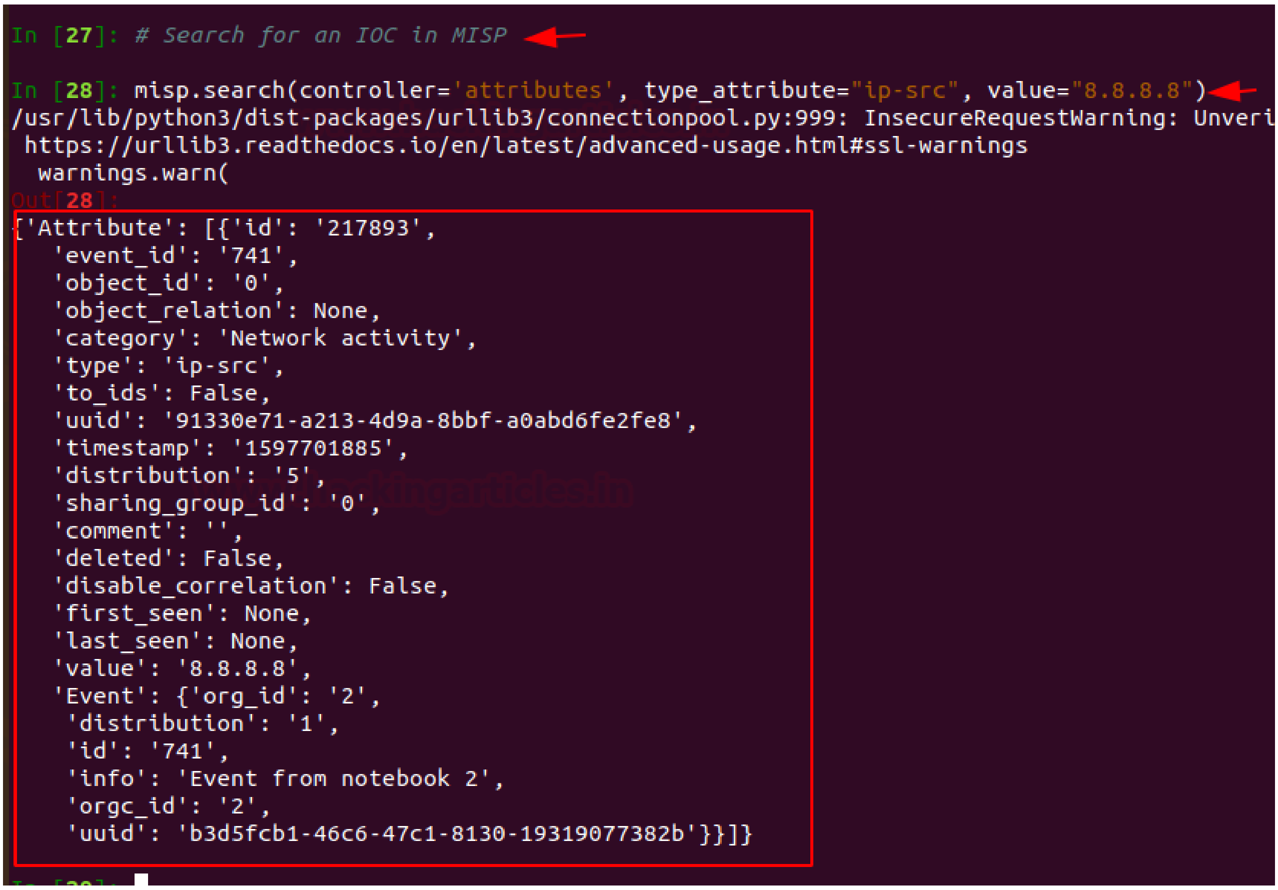


```
In [15]: from pymisp import MISPAttribute

In [16]: attr_type = "ip-src"

In [17]: value = "8.8.8.8"

In [18]: category = "Network activity"

In [19]: to_ids = False

In [20]: attribute = MISPAttribute()

In [21]: attribute.type = attr_type

In [22]: attribute.value = value

In [23]: attribute.category = category

In [24]: attribute.to_ids = to_ids

In [25]: attribute_to_change = misp.add_attribute(event_id, attribute)
/usr/lib/python3/dist-packages/urllib3/connectionpool.py:999: InsecureRequestWarn
 https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
  warnings.warn(

In [26]: print(attribute_to_change['Attribute']['id'], attribute_to_change)
217893 {'Attribute': {'id': '217893', 'event_id': '741', 'object_id': '0', 'objec
uuid': '91330e71-a213-4d9a-8bbf-a0abd6fe2fe8', 'timestamp': '1597701885', 'distri
'last_seen': None, 'value': '8.8.8.8'}, 'AttributeTag': []}
```

Search MISP for IOC

Let's search for an IOC in MISP ipython interpreter. Run the following command to perform the search.

misp.search(controller='attributes', type_attribute="ip-src", value="8.8.8.8″)



```
In [27]: # Search for an IOC in MISP

In [28]: misp.search(controller='attributes', type_attribute="ip-src", value="8.8.8.8")
/usr/lib/python3/dist-packages/urllib3/connectionpool.py:999: InsecureRequestWarning: Unveri
 https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
  warnings.warn(
Out[28]:
{'Attribute': [{'id': '217893',
   'event_id': '741',
   'object_id': '0',
   'object_relation': None,
   'category': 'Network activity',
   'type': 'ip-src',
   'to_ids': False,
   'uuid': '91330e71-a213-4d9a-8bbf-a0abd6fe2fe8',
   'timestamp': '1597701885',
   'distribution': '5',
   'sharing_group_id': '0',
   'comment': '',
   'deleted': False,
   'disable_correlation': False,
   'first_seen': None,
   'last_seen': None,
   'value': '8.8.8.8',
   'Event': {'org_id': '2',
    'distribution': '1',
    'id': '741',
    'info': 'Event from notebook 2',
    'orgc_id': '2',
    'uuid': 'b3d5fcb1-46c6-47c1-8130-1931907738 2b'}}]}

In [29]:
```

Awesome now you have completely setup MISP on your Ubuntu Platform.

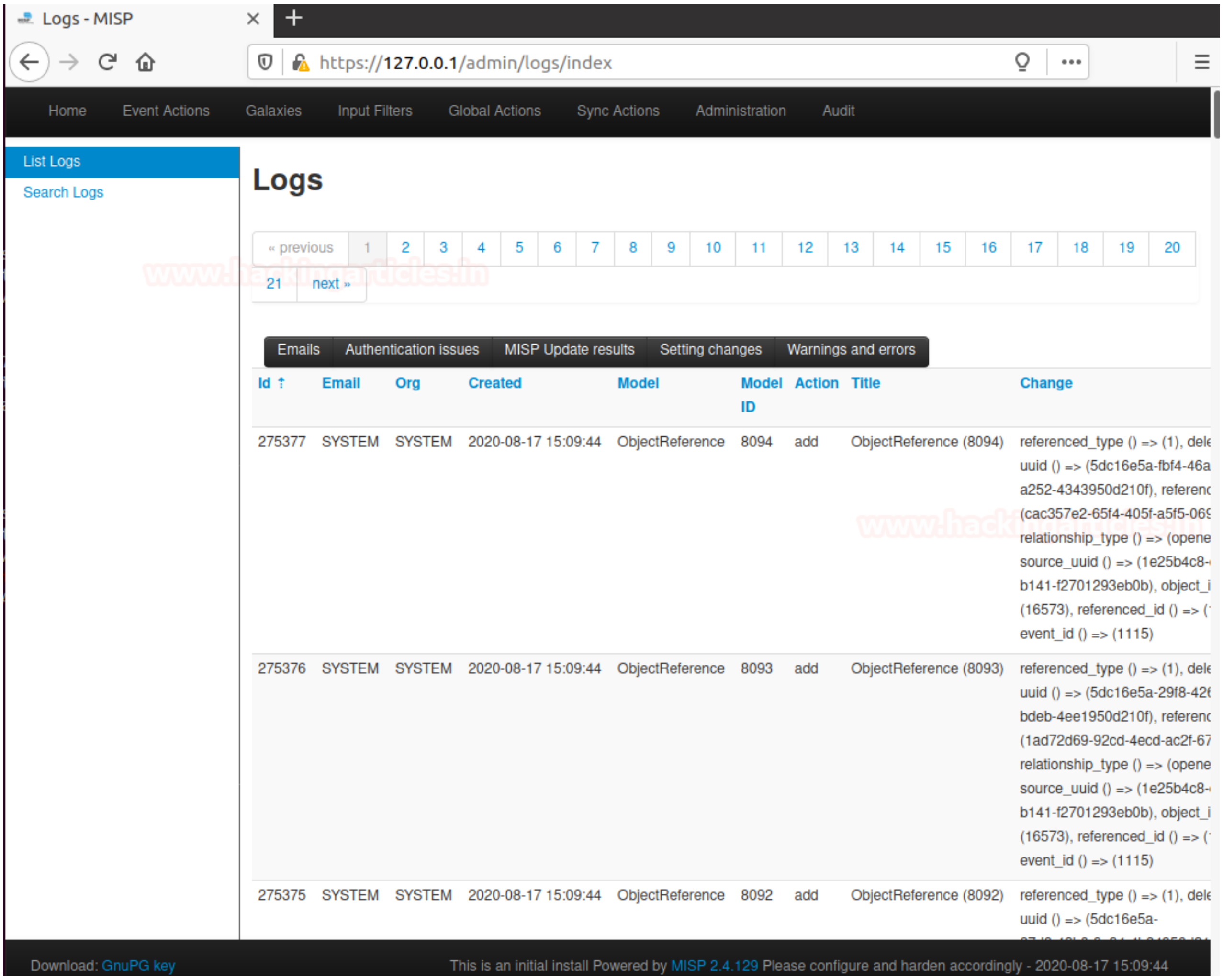
Great!

Threat Monitoring

Let’s check what happens on the MISP dashboard.

This one is gonna very special as we can go into the “**Audit**” tab to build our panel.

When entering the **Audit** tab select “**List Logs**” tab



Logs

Id ↑	Email	Org	Created	Model	Model ID	Action	Title	Change
275377	SYSTEM	SYSTEM	2020-08-17 15:09:44	ObjectReference	8094	add	ObjectReference (8094)	referenced_type () => (1), dele uuid () => (5dc16e5a-fbf4-46a a252-4343950d210f), referenc (cac357e2-65f4-405f-a5f5-069 relationship_type () => (opene source_uuid () => (1e25b4c8- b141-f2701293eb0b), object_i (16573), referenced_id () => (' event_id () => (1115)
275376	SYSTEM	SYSTEM	2020-08-17 15:09:44	ObjectReference	8093	add	ObjectReference (8093)	referenced_type () => (1), dele uuid () => (5dc16e5a-29f8-42 bdeb-4ee1950d210f), referenc (1ad72d69-92cd-4ecd-ac2f-67 relationship_type () => (opene source_uuid () => (1e25b4c8- b141-f2701293eb0b), object_i (16573), referenced_id () => (' event_id () => (1115)
275375	SYSTEM	SYSTEM	2020-08-17 15:09:44	ObjectReference	8092	add	ObjectReference (8092)	referenced_type () => (1), dele uuid () => (5dc16e5a-

Download: GnuPG key   This is an initial install Powered by MISP 2.4.129 Please configure and harden accordingly - 2020-08-17 15:09:44

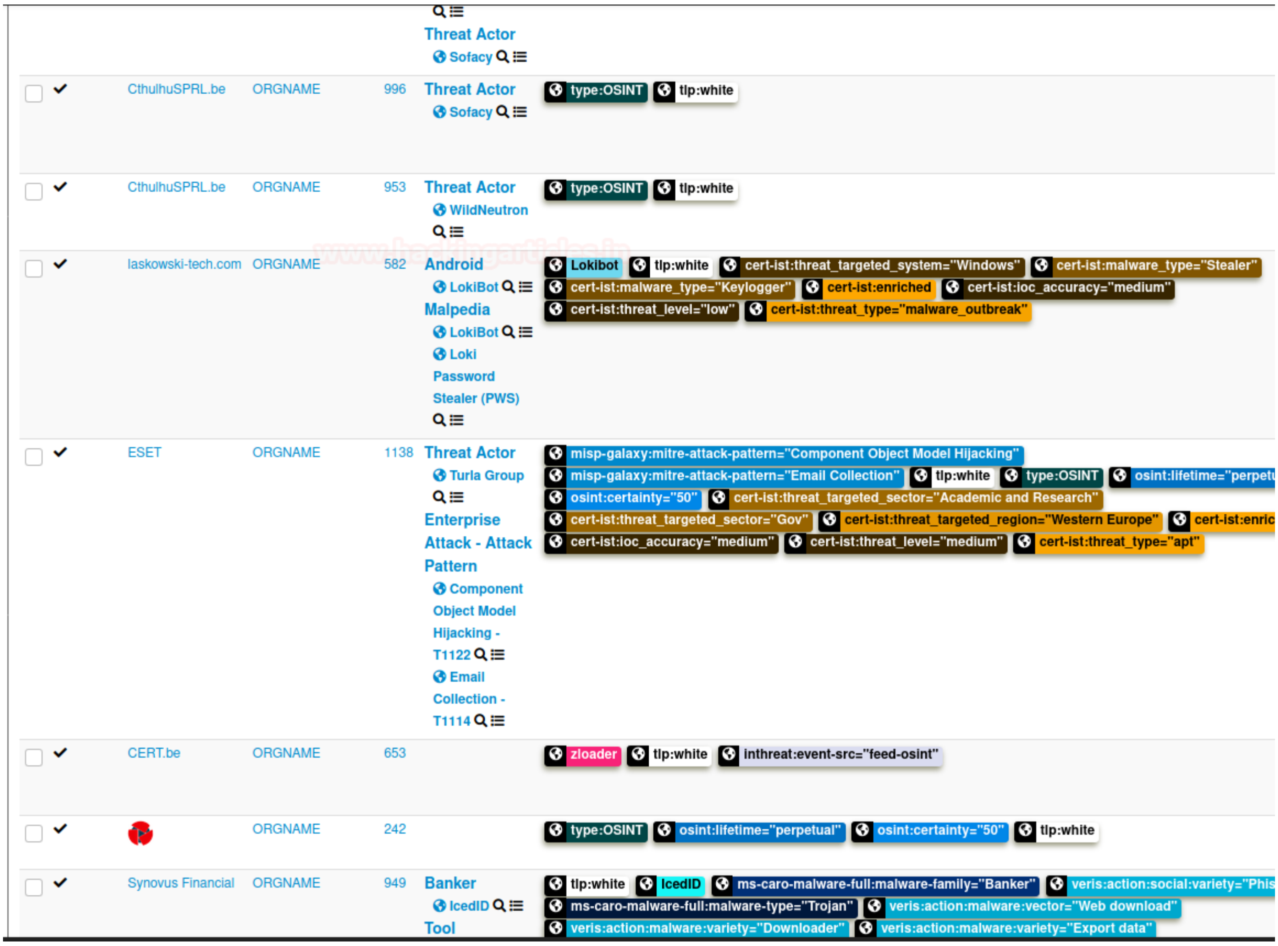
Wait this is not enough

Hold tight!

As we can see, Now we have direct access to every log related to Threat Intelligence.

We can for Example track illegal attacks.

Similarly, we can do Malware analysis from various servers also we can see logs of (NIDS) Network intrusion detection system, (LIDS), Log analysis Tools, SIEMs.



					Threat Actor Sofacy	
□	✓	CthulhuSPRL.be	ORGNAME	996	Threat Actor Sofacy	type:OSINT tlp:white
□	✓	CthulhuSPRL.be	ORGNAME	953	Threat Actor WildNeutron	type:OSINT tlp:white
□	✓	laskowski-tech.com	ORGNAME	582	Android LokiBot Malpedia LokiBot Loki Password Stealer (PWS)	Lokibot tlp:white cert-ist:threat_targeted_system="Windows" cert-ist:malware_type="Stealer" cert-ist:malware_type="Keylogger" cert-ist:enriched cert-ist:ioc_accuracy="medium" cert-ist:threat_level="low" cert-ist:threat_type="malware_outbreak"
□	✓	ESET	ORGNAME	1138	Threat Actor Turla Group Enterprise Attack - Attack Pattern Component Object Model Hijacking - T1122 Email Collection - T1114	misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking" misp-galaxy:mitre-attack-pattern="Email Collection" tlp:white type:OSINT osint:lifetime="perpetu osint:certainty="50" cert-ist:threat_targeted_sector="Academic and Research" cert-ist:threat_targeted_sector="Gov" cert-ist:threat_targeted_region="Western Europe" cert-ist:enric cert-ist:ioc_accuracy="medium" cert-ist:threat_level="medium" cert-ist:threat_type="apt"
□	✓	CERT.be	ORGNAME	653		zloader tlp:white inthreat:event-src="feed-osint"
□	✓		ORGNAME	242		type:OSINT osint:lifetime="perpetual" osint:certainty="50" tlp:white
□	✓	Synovus Financial	ORGNAME	949	Banker IcedID Tool	tlp:white IcedID ms-caro-malware-full:malware-family="Banker" veris:action:social:variety="Phis ms-caro-malware-full:malware-type="Trojan" veris:action:malware:vector="Web download" veris:action:malware:variety="Downloader" veris:action:malware:variety="Export data"

Nice! Now your Panel is included in your dashboard.

Updation of MISP in Future for Latest Versions

It is strongly recommended to upgrade MISP via the Web interface. This Blog may not always be up-to-date and will require you to fix permissions.

In general, updating MISP between point releases for example 2.4.50 -> 2.4.53 happens with the following command are to be executed to be as root.

To update the latest commit from 2.4 branches simply pull the latest commit.

Enter the following command

```
cd /var/www/MISP
sudo -u www-data git pull origin 2.4
sudo -u www-data git submodule update –init –recursive
```

Author – Vijay is a Certified Ethical Hacker, Technical writer and Penetration Tester at Hacking Articles. Technology and Gadget freak. Contact **Here**