Activity) Deploying MISP

In this lesson, we will be walking you through how to setup MISP within a virtual machine, so you can get a feel for the platform and build some practical experience with setting it up, and its many features. Please note this guide **does not** show how to setup a production-ready version of MISP. When using MISP in a production environment, appropriate hardening measures should be taken to ensure the MISP server itself is secure. This activity is to ensure students can get hands-on with MISP to learn more about threat intelligence platforms in general.

REQUIREMENTS

- Download the latest MISP .ova file here – https://www.circl.lu/misp-images/latest/
- If you don't already have VirtualBox installed, download it here – https://www.virtualbox.org/wiki/Downloads

DEPLOYING MISP

Transcript

> *In this video, we'll show you how to set up a MISP test environment, so you can get some experience with a threat intelligence platform*
>
> *Here we have the latest .ova file for MISP, and we're going to import this to virtualbox. If we click file, import appliance, and then select our .ova file, click next, leave these settings as they are, agree to the terms, and then start the import.*
>
> *Once the import has finished, we can run the virtual machine. We can login with the*

username misp and password Password1234. If we try to run ifconfig, the command isn't found, so we install it with sudo apt install net-tools. The next thing we need to do is put our VM in bridged mode, so it has its own unqiue IP. Now lets close the VM, and reopen it.

Now that the VM is in bridged mode, when we run ifconfig we can see it has its own IP address, 192.168.1.248! We needed to do this to ensure we can connect to the web interface from a remote system, in this case our host. To prevent any issues with the site trying to load resources with a url of "localhost" we need to set the baseurl to the IP address.

Run the command "sudo /var/www/MISP/app/console/cake baseurl https://192.168.1.248"

We can now visit this URL in a web browser on our host system, to connect to our virtual machine running MISP. To log in, use the username admin@admin.test, and the password "admin".

We will be prompted to change our password. And now we can start to explore MISP!

First, let's ensure the baseurl command has worked. Head to Administration, server settings and maintenance, then click the MISP settings tab and see if MISP.baseurl is set to the IP address. If it is not, double click it to change it.

Lets list all users by clicking the link on the left-hand side. We can see we're the only user. If we click on user settings we can see our permissions. Now lets add a new user so we're not super lonely. We need to input a username, select an organization, and then add them.

Click administration -> list organisations. Currently there is only one, with the name ORGNAME. Click edit on the right-hand side, and we can change the org name, nationality, and sector – we can see these when we list organisations. Let's also create a new organisation for security red team. If we list the orgs now we can see both of these. Let's move our new users over to Security Red Team by editing the profile. All done!

The next thing we're going to show you is the dashboard. We can place useful widgets here to monitor certain aspects of the platform. First, lets add a widget for MISP workers. This shows us the running processes for the backend, with workers designed for different tasks. Let's also add a widget for trending tags, which will be automatically populated when we pull in intelligence later.

Next we want to bring intelligence into our platform. Here we can see a lot of default threat feeds, and on the right we can see all of them except number 3 are disabled. Let's select the first 5 and enable them. Now, we can pull all events using the down arrow icon on the right. Let's do this for the first 3.

Going back to the dashboard we can see we have three pending jobs, but 0 of the workers are alive, so we need to initialise them from the virtual machine. Use the command "sudo -u www-data bash /var/www/misp/app/console/workers/start.sh.

Now back on the dashboard we can see that one of them is alive, and working on the events.

If we view the event list, we can see we now have intelligence in our platform! Let's take a look at this ransomware event. Click on the eye icon to view it, and we can see it was published by CIRCL, the developers behind MISP. We can see tags that have been assigned, and at the bottom we have some IOCs and even a virus total link. Clicking on the virustotal link shows this is a nasty piece of ransomware, and is widely detected.

Let's view another event. This one here has lots of MITRE ATTACK tactics, lets take a deeper look! At the bottom we have tons of IOCs, and if we click on the attack matrix, we can clearly see which tactics have been mapped to this event, tracking a threat actors activity!

We can also create our own events, by clicking add event. We need to give it a name, let's call it APT28 NCSC Report, assign a threat level of undefined, and set the privacy to our organisation only.

To add IOCs, lets find a report that includes some. We'll be using this NCSC report on apt28. We can copy the list of IOCs shown here, domain names and command and control

server IP addresses, and add them using the freetext import tool. We can neaten the input a little bit, then hit submit.

We can see all of the IOCs have been correctly assigned to a category and type. Click submit. The workers will begin importing these for us. Heading back to the dashboard we can see the trending tags widget is now populated based on our stored events. Going back to the events list, we can see our custom event, let's view it again. Now we can see all of the IOCs have been imported and stored within MISP!

We can also set our own tags, there's no tag for APT28 because we haven't created it, so lets use some existing ones, such as APT and OSINT to better define the information in this event.

In this video we have covered installing the test version of MISP, creating users and organisations, a basic dashboard, pulling intelligence into MISP, and creating our own event.

Previous Topic

Mark Complete

Back to Lesson