

SECURITY WORKSHOP: **THREAT INTEL SHARING** **WITH MISP** **SETUP INSTRUCTIONS**

LIVIU VÂLSAN

SPRING 2017 HEPIX, BUDAPEST

INTRODUCTION

- ▶ You will learn how to deploy, configure and use MISP inside a virtualized environment
- ▶ Screenshots provided in this document are for macOS, steps should be very similar for all other operating systems
- ▶ To speed up the hands on part of the workshop it's highly recommended that you follow the following steps before the start of the workshop

1. DOWNLOAD AND INSTALL VIRTUALBOX

- ▶ In case you don't have VirtualBox already installed download it from the official website:
<https://www.virtualbox.org/wiki/Downloads>
- ▶ Follow the instructions for you operating system to get it installed

2. DOWNLOAD THE VM IMAGE

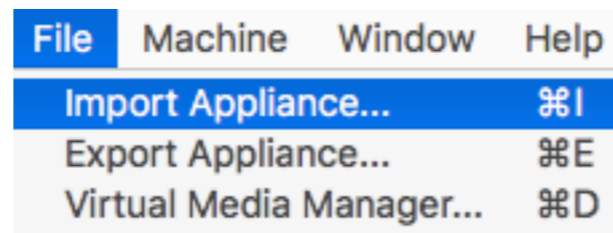
- ▶ The VM image that will be used during the workshop has been made available for download on the local WiFi network. It has a size of 492 MB and it can be downloaded via HTTP from one of the following two URLs:

[http://172.16.104.249/workshop/
hepix_misp_training_centos-7.x86_64.ova](http://172.16.104.249/workshop/hepix_misp_training_centos-7.x86_64.ova)

[https://lvalsan.web.cern.ch/lvalsan/trainings/hepix/
2017_spring/misp/
hepix_misp_training_centos-7.x86_64.ova](https://lvalsan.web.cern.ch/lvalsan/trainings/hepix/2017_spring/misp/hepix_misp_training_centos-7.x86_64.ova)

3. IMPORT THE VM IMAGE IN VIRTUALBOX

- ▶ Use the “Import appliance...” option from the “File...” menu



- ▶ Select the ova VM export file from the location where you downloaded the image
- ▶ If needed adjust the location of the virtual disk image after the export and ensure that you have sufficient free space on the target partition (~2GB of total space will be needed)
- ▶ Click import
- ▶ The import process may take a few minutes, depending on the speed of your local drive

4.1. CONFIGURE NAT & PORT FORWARDING (1)

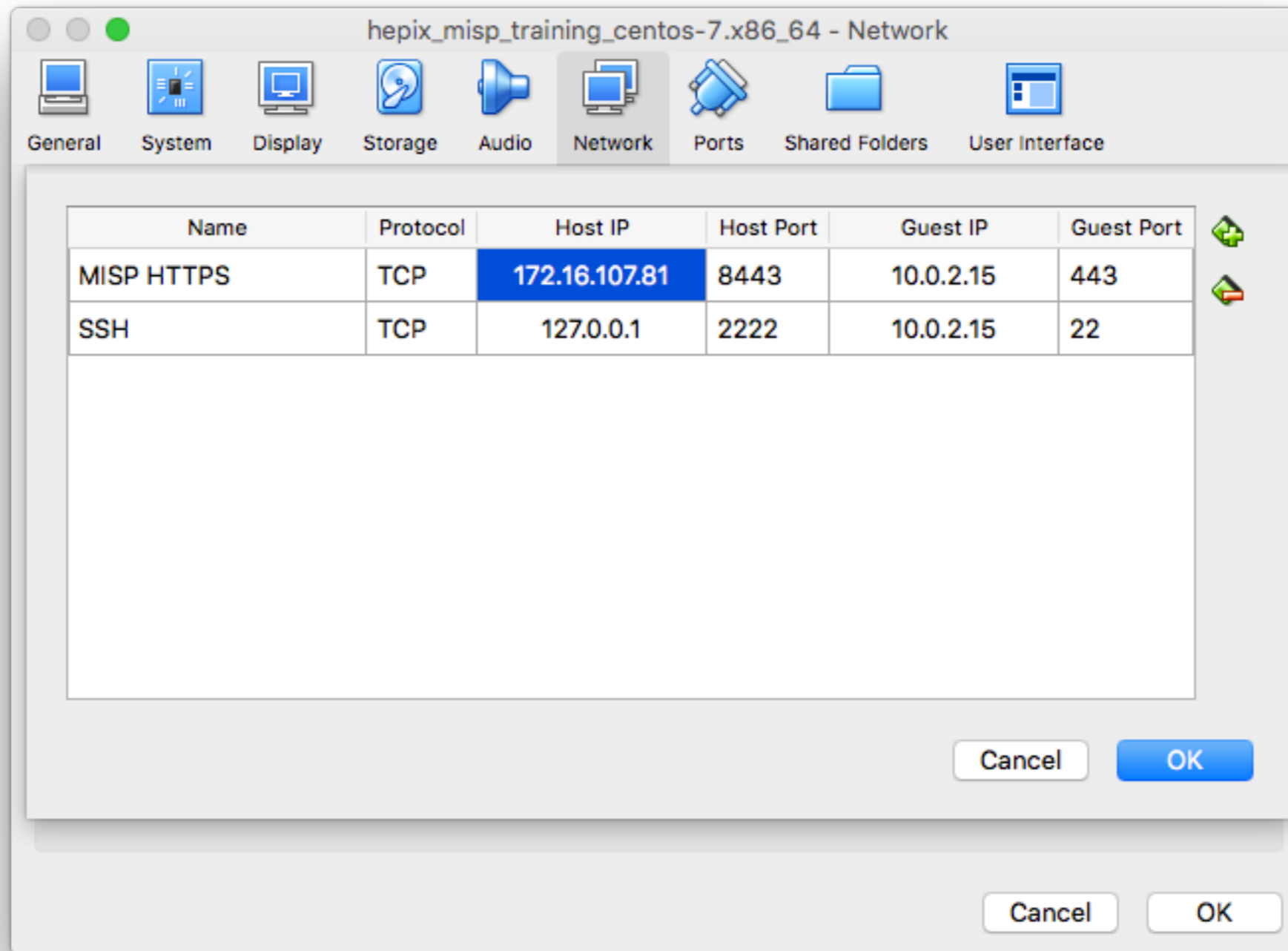
- ▶ Due to various constraints of the local HEPiX WiFi network the VM will need to be configured behind NAT with port forwarding
- ▶ Select the `hepixon_misp_training_centos-7.x86_64` VM in the list of VirtualBox VM instances
- ▶ Click the settings button (gear icon)
- ▶ Go to the network tab
- ▶ Select "Adapter 1"
- ▶ Ensure the following:
 - ▶ "Enable Network Adapter" is checked
 - ▶ "Attached to" is set to "NAT"
 - ▶ Click "Advanced"
 - ▶ Verify that the "Cable Connected" checkbox is checked
 - ▶ Click the "Port Forwarding" button

4.2. CONFIGURE NAT & PORT FORWARDING (2)

- ▶ There should be 2 NAT rules created
 1. A first rule named "MISP HTTPS":
 - ▶ Change the Host IP to the IP address of your laptop's wireless interface on the local HEPiX WiFi network. It will be in the form of "172.16.x.y"
 - ▶ Check that the Host Port is set to "8443", the Guest IP to "10.0.2.15" and the Guest port to "443"
 2. A second rule named "SSH":
 - ▶ Check that the Host IP is set to "127.0.0.1" and the Host Port to "2222"
 - ▶ Check that the Guest IP is set to "10.0.2.15" and the Guest port to "22"

4.3. CONFIGURE NAT & PORT FORWARDING (3)

- ▶ Your port forwarding rules should look like the following:



- ▶ Please ensure that you are using your current IP address for the "MISP HTTPS" rule. Do not use the IP address in the example above.

5. TEST ACCESS TO THE VM

- ▶ Power on the VM, it should boot up in less than a minute
- ▶ Try to login on it as root
 - ▶ From a Unix based system:

```
ssh -p 2222 root@localhost
```
 - ▶ The root password is (without the double quotes):
"centos"

THAT'S ALL

- ▶ Now you just need to wait for the start of the workshop 😊