System and Web Security
System Security VM Instructions

University of Stuttgart
Germany

Institute of Information Security
Prof. Dr. Ralf Küsters

Last update: April 11, 2017

How to Install the System Security Virtual Machine

This document tells you how to set up the *system security virtual machine (VM)* that will be used in the course *system and web security*. The System Security VM is used as a reference system for all homework assignments of the part *system security*. The VM contains a very old installation of *Ubuntu Linux 8.04* with several security features disabled. This setup allows you to test several attacks, such as *buffer overflows*, without having to circumvent defense mechanisms of the operating system.

Warning:

The System Security VM is a very insecure system. You should never connect it to a public network. Please pay special attention to the network setup section below!

To set up the VM, you first need to install and configure the software *VirtualBox* (Sections 1 and 2). After this, you can import the VM into your VirtualBox installation (Section 3). Instructions on how to use the VM are given in Section 4.

1 Preparation of Your Host System

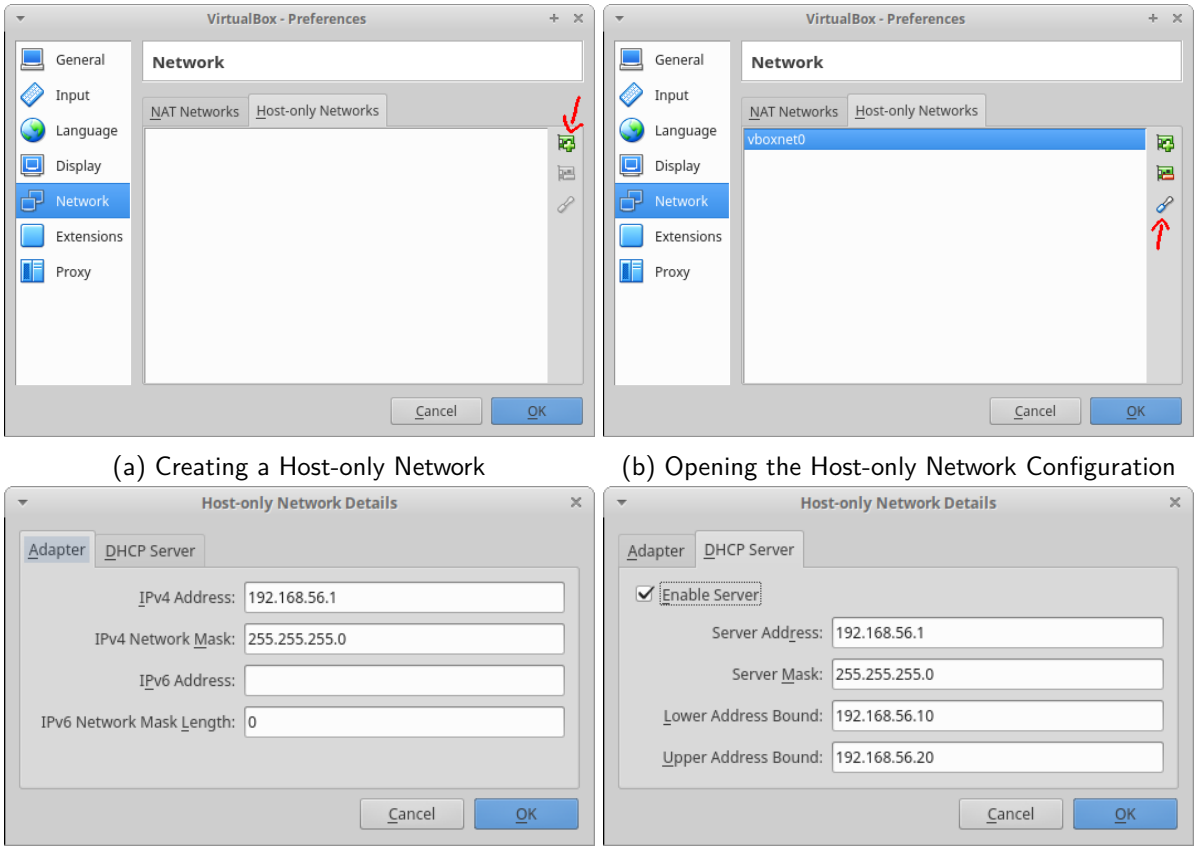
First, you need to install a hypervisor software that allows you to run virtual machines on your host computer. We recommend you to use *Oracle VirtualBox*. You can download VirtualBox at `https://www.virtualbox.org/` or—if you are running a Linux system—you can install it using your package manager (VirtualBox is usually included in the default software repositories).

The instructions in this document are based on VirtualBox 5.1 (the latest version at the time of writing).

2 Network Setup

VirtualBox allows you to set up a dedicated virtual network between your host computer and a VM. This feature is called *host-only network*. Such a network does not allow internet access to the VM, which is exactly what you want when dealing with an insecure system.

A host-only network must first be created in your VirtualBox setup before connecting it to any VM. To do so, open the *preferences* (from the *file* menu of VirtualBox). There select *network* in the list on the left and then the tab *host-only networks* on the top. Click on the small icon button with a plus (on the right) to create a new host-only network (see Figure 1a). This network will (most likely) be named *vboxnet0*.



(a) Creating a Host-only Network

(b) Opening the Host-only Network Configuration

(c) Host-only Network Adapter Settings

(d) Host-only Network DHCP Server Settings

Figure 1: Network Preferences Dialogs

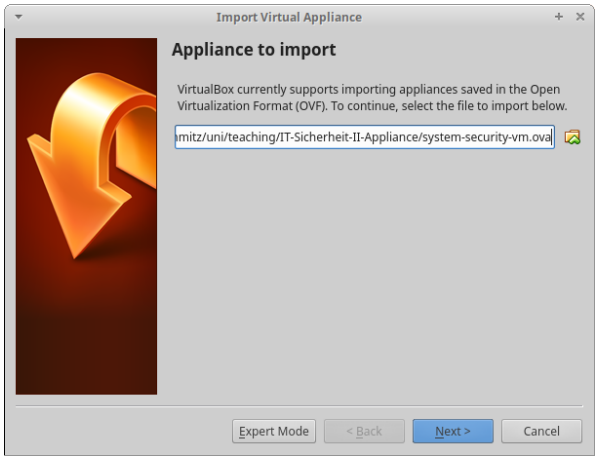
Below the previously used button, you also find a screw driver button (see Figure 1b). This opens the network configuration for the network selected in the list. In the *adapter* tab, VirtualBox automatically inserts a default IP configuration for a newly created network. For example, our host system will have the IPv4 address 192.168.56.1 and a network mask 255.255.255.0 (see Figure 1c). We will ignore the IPv6 configuration as we will not use it. In the *DHCP server* tab, you need to enable the server and insert the settings as shown in Figure 1d.

3 Import of the System Security VM

After completing the network setup, you are ready to import the system security VM. To do so, select *import appliance* in the *file* menu.

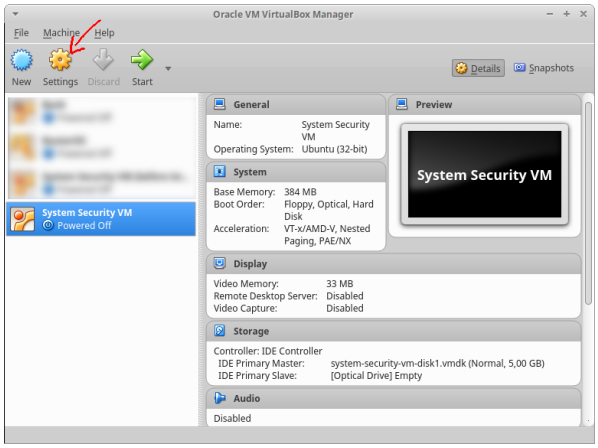
In the first dialog (shown in Figure 2a), select the file *system-security-vm.ova*, which you downloaded in ILIAS. In the next dialog (Figure 2b), you can see an overview of the VM's configuration. (You do not need to check the *reinitialize MAC address* checkbox.) Here, you just have to confirm the import.

Now, make sure that the network settings of the imported VM are correct. In VirtualBox' main window, first select the imported VM on the left (probably you just have only one VM at this point) and open the settings dialog with the button shown in Figure 2c. In the settings dialog, select *network* on the left (see Figure 2d to open the network settings of the VM. Here, make sure that the *adapter 1* is enabled and attached to the host-only adapter that you have created above (most likely *vboxnet0*). All other adapters should not be enabled.

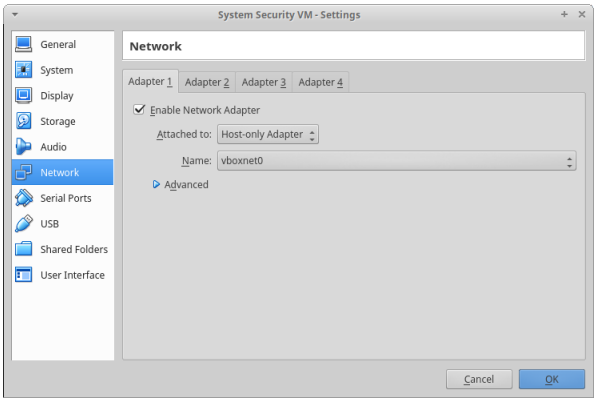


(a) Select the File system-security-vm.ova

(b) Confirm the Import



(c) Open the VM Settings



(d) Network Settings of the VM

Figure 2: Import and Configuration of the Virtual Appliance

4 Using the System Security VM

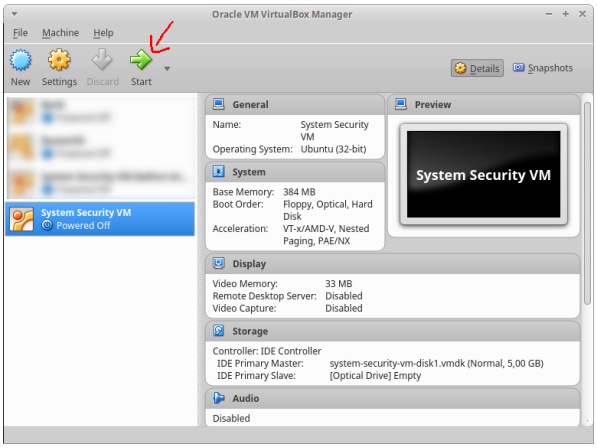
You can boot/start the VM by selecting the VM in the list on the left in the main window of VirtualBox and clicking on the *start* button on the top (see Figure 3a). The VM opens in a new window and boots into a Linux text terminal. After the boot process has finished, the VM welcomes you with its IP address and a command prompt of the user *isuser* (for *information security user*). As the VM contains a (more or less) standard Linux installation, you can now use the command prompt like on any other Linux machine.

Instead of just using this console, there are also other ways to interact with the VM (out of which *SSH* and *shared folders* are explained below).

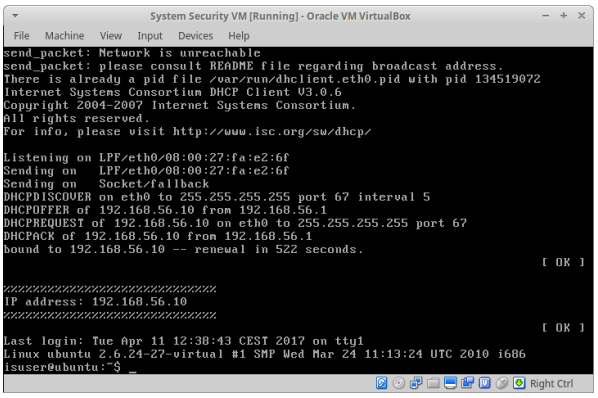
4.1 SSH

You can use *SSH* to log in to the VM from your host system, which gives you several advantages (e.g., a bigger terminal size), and SCP/SFTP to transfer files to and from the VM. (*Hint:* Good programming editors allow you to edit and compile files remotely.)

The IP address of the VM is displayed in the welcome message of your VM instance (see Figure 3b, note that the IP address may differ in your installation). The username is *isuser* and the password is *isuser*.



(a) Location of Start Button



(b) Welcome Screen of the VM

Figure 3: Booting the VM

4.2 Shared Folders

You can use VirtualBox' *shared folders* feature to mount a directory from your host computer into the VM: First, you need to create a shared folder in VirtualBox. Right click on the folder icon in the status bar of the VM (see Figure 4a) and select *shared folder settings*. This opens the configuration dialog for shared folders where you add a new folder by clicking on the icon with the plus on the right side (see Figure 4b). In the now opened *add share* dialog (see Figure 4c), you select a path you want to share from your host computer and select a folder name (filled out automatically). You should check the *mark permanent* checkbox. As the *auto-mount* feature does not work with the system security VM, we finally have to mount the shared folder manually within the VM using the following command (see also Figure 4d, you need to replace `mysharedfolder` with the name you have chosen for your folder):

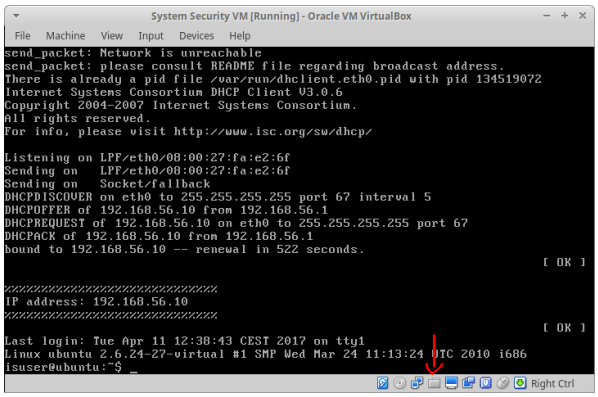
```
sudo mount -t vboxsf -o uid=1000 mysharedfolder /mnt
```

Now, the folder of your host system (as selected above) is available in the VM (as `/mnt`) and changes to the contents of this folder are instantly available on both systems, your host computer and the VM.

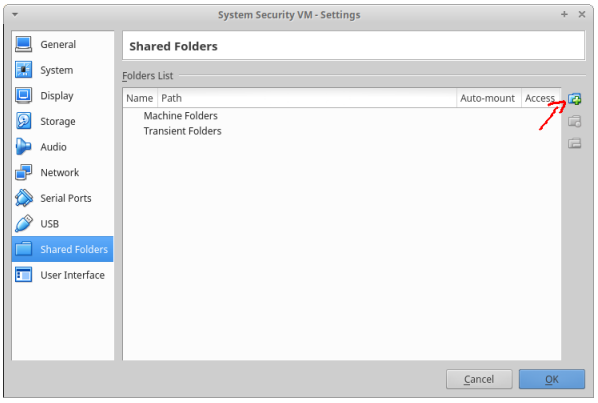
Note that the mount command above does not permanently make the folder available in the VM. After the next boot, the folder will not be mounted. If you want to execute the mount command above at each boot, you can, for example, add it to the file `/etc/rc.local` before the line that contains `exit 0`. You can edit this file, for example, with the command `sudo nano /etc/rc.local`.

4.3 Shutting Down the VM

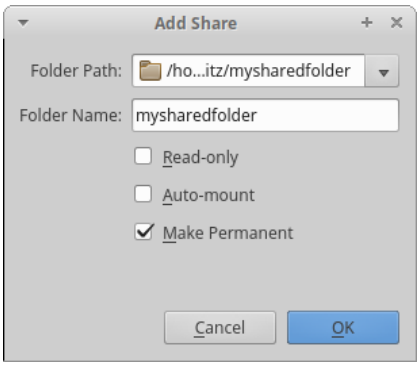
To shut down the VM, you just need to enter the command `sudo halt` into the console.



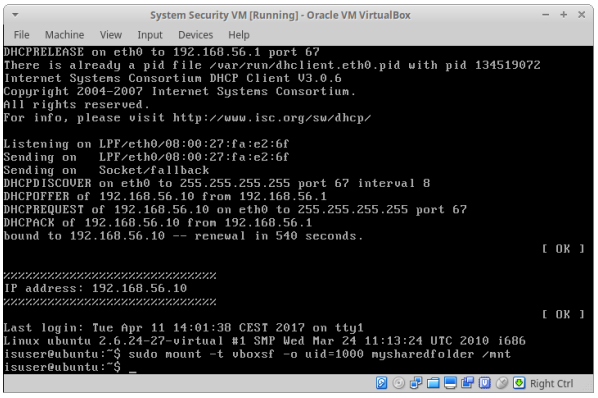
(a) Status Bar Icon for Shared Folders



(b) Shared Folder Settings Dialog



(c) Dialog for Adding a Shared Folder



(d) Mounting a Shared Folder

Figure 4: Setting Up a Shared Folder