Lab Setup Instructions

These setup instructions contain everything you'll need to get ready for your upcoming SANS class. These can take some time to complete, and may involve downloading large files. So please allow ample time to complete them before you arrive at class - especially if you have limited Internet bandwidth.

If you require assistance with the instructions contained within this document, please contact support@sans.org. Be sure to include the name of your course, and if possible, your order number.

We're looking forward to having you in class!

Lab 0: Getting Started (Complete Prior to Class)

Objectives

The objective of this lab is to open the class virtual machines in VMware and confirm you can access the internet.

Lab Description

In this lab you will prepare your system for SEC573. To be ready for class, you only need one thing. You need your course Virtual Machines are connected to the internet. Import your course virtual machines into a virtualization product. If you can do that and reach the Internet from within the course virtual machines, you have everything you need for the course.

Full Walk Through

Before you Arrive in Class or Travel

Several steps must be accomplished before you start class. For those students attending a live class event, this means completing the setup process before you arrive at the venue. Some steps may require significant download bandwidth and hotel/venue Internet is not suitable for these downloads.

Before the start of class you should perform all of the following steps:

1. Download the course materials from your SANS Portal. Follow the guidance at https://sansurl.com/downloading-course-materials for accessing and downloading your course materials. Be sure to download the following:
   - A Linux Virtual Machine in a compressed 7ZIP file that you will use in the next two steps (step 2 and 3 below)
   - A mountable drive the form of a .ISO containing a Windows VM and other files that you will use in step 4 below
2. Extract and boot the Linux Virtual Machine in VMWare by following the instructions at https://sansurl.com/decompressing-booting-vms.
3. Follow the instructions in the "**Configuring your Linux Virtual Machine**" immediately below these instructions.
4. Extract and boot the Windows Virtual Machine that is stored on the mountable .ISO by following the instructions in the "**Mounting Course ISOs**" documentation at https://sansurl.com/mounting-isos and the "**Decompress and Boot the Virtual Machines**" documentation at https://sansurl.com/decompressing-booting-vms.

If you are pressed for time

Ideally each of these steps are performed before the start of class, but we don't always live in the ideal world. If you arrived in class without completing these steps you can start class after completing steps 1,2 and 3. Step 4 (The Windows VM) is not required until section 5 of this class.

When you are done you can pause each of your Virtual machines until the start of class.

Do NOT Perform Operating System Updates

Is is critical that you **do not** upgrade software within the virtual machine unless specifically directed to do so in the lab instructions. Your virtual machine has been extensively tested in the configuration which it was distributed. SANS cannot ensure your labs will function properly if the software is updated.

Configuring your Linux Virtual Machine

First, verify that your machine can access internet by resolving a DNS hostname such as sans.org.

Open a Terminal by double-clicking the Terminal icon on your desktop.

```
$ nslookup sans.org
Server:     127.0.0.53
Address:    127.0.0.53#53

Non-authoritative answer:
Name:   sans.org
Address: 45.60.103.34
Name:   sans.org
Address: 45.60.31.34
```


If you are unable to reach the internet from within the virtual machine, check your host firewall and network settings. If you require assistance with the instructions contained within this document, please contact support@sans.org. Be sure to include the name of your course, and if possible, your order number.

You will need port 10000 opened outbound on your firewall

To reach the lab environment you will need to be able to connect outbound through your firewall over port 10000. If you are attending SEC573 via OnDemand, Hybrid, a private on-site class or in some modality other than being in the live classroom at a SANS event please confirm that port is open before the class starts.

Activate your virtual environment by typing `573` and update your pywars client and lab software using `update-573` as shown below. The output below has been truncated to save space. Your output will contain additional information as updates are applied.

```
student@SEC573:~/Documents/pythonclass$ 573
(573) student@SEC573:~/Documents/pythonclass$ update-573
WARNING: Any changes you have made to python lab code in the 'pythonclass' folder will be lost.
Type uppercase YES to continue:YES
 Cloning https://github.com/markbaggett/pywars (to revision version5) to /tmp/pip-req-build-
mph1bpjs
  Resolved https://github.com/markbaggett/pywars to commit
2a602a5044ccc136e20d04d52988ef9ee0e5ca13
  Installing build dependencies: started
  Installing build dependencies: finished with status 'done'
Requirement already satisfied: pygments<3.0.0,>=2.6.0 in /home/student/python-envs/573/lib/
python3.10/site-packages (from rich>=9.1.0->pywars==5.0.3) (2.12.0)

Updating HOF - Fetching origin
HEAD is now at e50bd12 Update Robertos server
Already up to date.

Updating Labs - Fetching origin
HEAD is now at 584797d Force overwrite on update
Already up to date.

Installing new update script -
```

If the script prints a message indicating that a new update script was installed, then please run the script a second time.

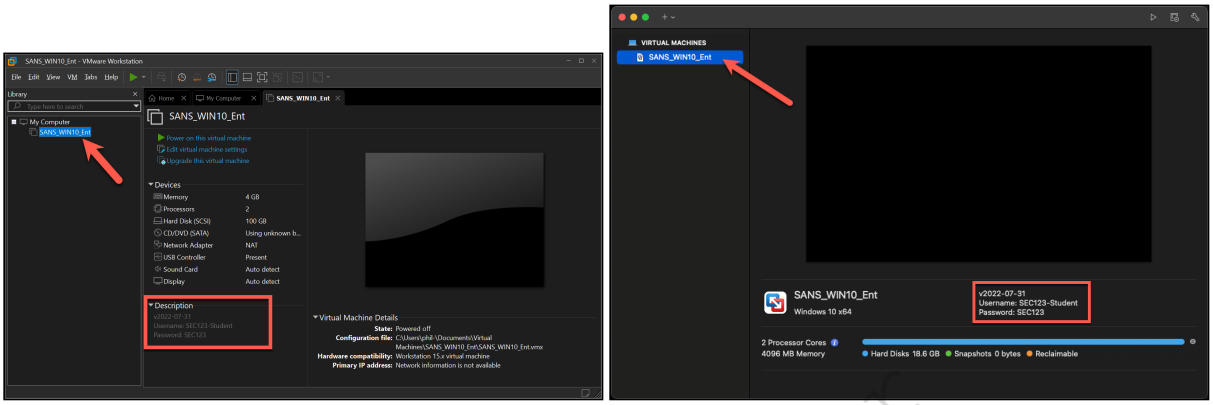
Banners, Version Numbers and Dates may not match

The banner that is printed when you start python includes a Python Version number as well as a date and time stamp associated with that version. The version numbers of software printed in banners (example 3.10.4 vs 3.8.5) may not match those in this workbook and other course material as we frequently apply updates to the VM. Additionally, as new updates are released the minor version numbers shown on your screen may not match those shown in this book either.

Virtual Machine Credentials

The login credentials for all virtual machines used in this class are listed below for quick reference.

All login credentials are also displayed in the respective virtual machine's information panel. Below are screenshots showing the login credentials under VMware Workstation and VMware Fusion, respectively.



1. SEC573 Linux Virtual Machine
   - Username: `student`
   - Password: `student`

   These credentials are used to automatically log into the graphical login. You can use this credential to perform administrative functions using `sudo`.
2. Optional SEC573 Windows Machine
   - Username: `student`
   - Password: `student`

   These credentials have administrative permissions and should be used to log into the graphical user interface.