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)

Before You Arrive or Travel to Class

You must complete several steps before you arrive or travel to 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 access is not suitable for these downloads.

The following steps should be completed prior to the start of class:

Notice

The documents linked to in the steps below are purposely template content designed to be consistent across all SANS courses. As such, you will see screenshots that differ slightly from your course files. However, the file naming conventions and setup processes are the same by design.

1. Downloading Course Materials

- Follow the guidance at https://sansurl.com/downloading-course-materials for accessing and downloading your course materials.
- These files are large and may take a long time to download, depending on your Internet connection and many other factors. If you are attending a live class, you should not rely on Internet access at the event to download these files.

2. Mounting Course ISOs

- Follow the guidance at https://sansurl.com/mounting-isos for mounting and accessing the the data within the downloaded course ISO files.
- The course ISOs are archives that contain important files for your class. The course ISOs are not bootable operating systems.

3. Decompressing and Booting Virtual Machines

- Follow the guidance at https://sansurl.com/decompressing-booting-vms for decompressing and booting the course VMs.
- You must extract the Virtual Machines (VMs) for your course to your local storage and boot them for use in the class.
- Note that at the end of this Lab Setup Instructions document is a ***Virtual Machine Credentials*** page with the login credentials for the course VMs. The credentials can also be found in the VM notes area once opened in the VMware application.

4. Review/Complete Specific Course Notes Below

- The additional instructions below are unique to your course. Follow the remainder of this document once you are able to login to your course VMs.

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.

Time Zone and Region Settings Within Virtual Machines

Do not change your regional or time settings within your VMs. The system time zones in the VMs are set to Universal Coordinated Time (UTC). Many tools will output in the standard ISO 8601 format `YYYY-MM-DD HH:MM:SS` [1]. The labs are written specifically in this format to avoid any confusion across different regions. Changing your time settings may cause tools to fail as dealing with time zones and regional settings is complex[2].

Virtual Machine Snapshots

> **Note**
>
> VMware Player and VMware Fusion Player do not have snapshot capabilities. If you are using VMware Player or VMware Fusion Player, you will not be able to complete the steps in this section. Where possible, we recommend using VMware Workstation Pro or VMware Fusion to take advantage of snapshot capabilities.

Consider creating a snapshot in case you need to revert one or more VMs to a known good state. At a minimum, we recommend taking a snapshot of each VM immediately after extracting it from the archive file. We also recommended periodically taking snapshots during the class to ensure that you can recover from any problems that might occur.

Updating the Electronic Workbook

The electronic workbook content is stored locally in the Windows VM so it is always available. However, course authors may update the source content with minor fixes, such as correcting typos or clarifying explanations, or add new content such as updated bonus labs. The electronic workbook in your Windows VM self-updates several times per day, so you should rarely need to refresh the content manually. However, if your instructor, TA, or SME advises, you can pull down any available updates into the VM by running the following command in the Ubuntu bash window via the Windows Subsystem for Linux (WSL).

Here are specific instructions for the Windows VMs:

- In a Windows VM, open Ubuntu bash window via the Windows Subsystem for Linux (WSL) from the taskbar as shown here:

- In the Ubuntu bash window, run the command `workbook-update` as shown here:

Command lines

```
workbook-update
```

Expected results (when updates are available)

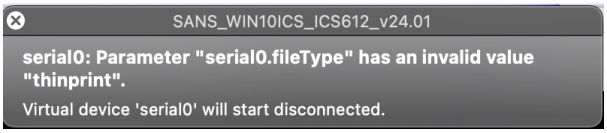
```
ics612@DESKTOP-BR131UQ:~$
$ workbook-update
Beginning update process...
- Updating workbook files

Complete!
```

Expected results (when no updates are available)

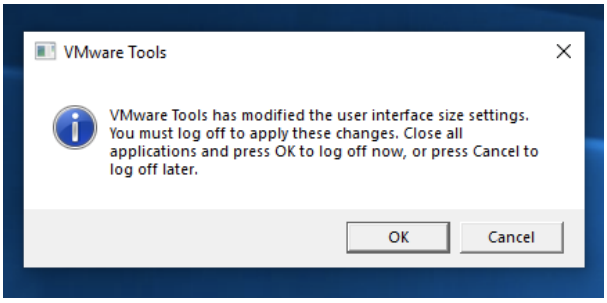
```
ics612@DESKTOP-BR131UQ:~$
$ workbook-update
Beginning update process...
- No workbook updates available

Complete!
```

General Virtual Machine Pop-Ups on Boot

The following pop-up may appear during the start of a virtual machine. This can be ignored and should disappear shortly.



The following pop-up may appear during after you log in to the Windows virtual machine. Click `Cancel` to proceed.



Completing the Setup Process

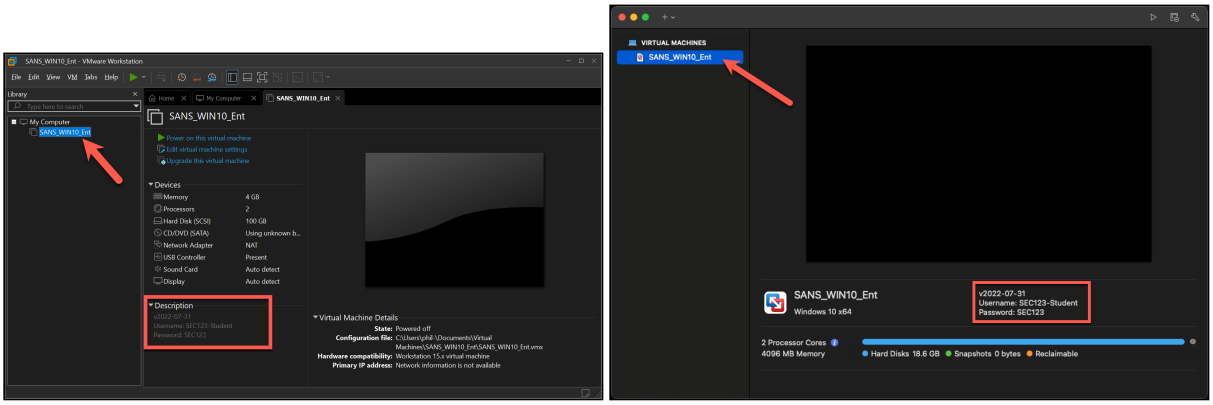
Once you have downloaded all the course materials, decompressed and booted the virtual machines, and reviewed the specific notes above about the course VMs, you will be ready for class!

1. Date and time format - ISO 8601 https://sansurl.com/iso8601
2. The Problem with Time & Time Zones - Computerphile - YouTube https://sansurl.com/tz-probs

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. Windows VM
    - Username: `ICS612`
    - Password: `ICS612`
2. RELICS VM
    - Username: `relics`
    - Password: `relics`
3. Kali VM
    - Username: `root`
    - Password: `toor`