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)

This document was updated on 22 September 2024

To ensure that you have the latest instructions, please browse to https://bit.ly/sec530-ex1-0-23-2 and check the 'updated' date noted within that document (i.e., this paragraph). If that date is after 22 September 2024, then please follow those updated instructions.

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.

Please review this entire document, and **then** execute the below steps **in the listed order**.

1. **Required Steps**

   a. **Download 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.

   b. **Mount 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, including the SEC530 virtual machine (VM) files.

   c. **Decompress and Boot Virtual Machines**. Follow the guidance at https://sansurl.com/decompressing-booting-vms for decompressing and booting the course VM.

   Note

   This last page of this document includes the ***Virtual Machine Credentials*** you need to login to the VM. The credentials can also be found in the VM notes area once the VM is opened in the VMware application.

      i. Recommended: If you are using VMware Workstation Pro or VMware Fusion, then we recommend you create a snapshot of the VM immediately after opening the VM but prior to making any changes or booting the VM for the first time.

      See this document's Creating a Virtual Machine Snapshot section for details.

ii. Optional: If you wish, you may increase the RAM resources allocated to your VM. This is not necessary, as all class VMs are tested with the resources with which they are distributed. However, if your host system has more capabilities than the minimum stated requirements, you might benefit from the increased performance that additional resources can provide.

> **Do not allocate the VM more than 8 GB RAM, as your VM will not benefit significantly from the additional RAM; or more than half of your host system's physical RAM, as this will cause host performance issues.**

> **Do not change the CPU resources allocated to your VM. This will cause several Docker containers used in class to crash.**

d. Update the Electronic Workbook (EWB). This ensures your content is 100% up-to-date. These updates 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.**

e. Test OpenVPN Access. Several labs include accessing virtual lab environments via OpenVPN. This should be tested by each student on their VM.

f. **Access SANS My Labs Content**. Follow the guidance at https://sansurl.com/accessing-mylabs-content for accessing My Labs content.

   My Labs access is required to obtain an SANS-provided Azure subscription that will allow you to complete bonus Azure exercises; and for OnDemand students to gain access to the section 6 capstone event.

2. **Optional Steps**

   a. Customize the SEC530 VM with a different desktop background.

   b. Create a Virtual Machine Snapshot to create a 'known-good' state to which you can revert.

   c. Inside your SEC530 VM, start Google Chrome and review the home page for additional tips and information.

After completing the required steps and any desired optional steps, then either pause or cleanly shut down your VM.

Finally, be aware that Live Online and In-Person students may need to complete some additional steps when joining class each morning. Live Online and In-Person students may need to join a class Slack channel; Live Online students will need to join a web conference session (e.g., Zoom).

Getting Help

If you are not able to complete the required steps:

- You may contact support@sans.org with a subject line of 'Pre-Class Setup Support'. Be sure to include the name of your course, and if possible, your order number.
- If you are attending an In-Person or Live Online class and you have been unable to complete the required steps before the start of your class, then please be sure to let your instructor know as soon as you arrive in class.

- If you are taking an On Demand class, then please use the **Ask a Question** button in your On Demand course to chat with SMEs live during their office hours, send a message to SMEs to request assistance, or send a message to the SANS Customer Support team.

Do NOT Perform Operating System Updates

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

Time Zone and Region Settings Within Virtual Machines

Do not change your VM's settings for the date or time format, as this may cause labs or tools to fail. Many tools will output in the standard ISO 8601 format `YYYY-MM-DD HH:MM:SS`,[1] and labs are written specifically in this format to avoid any confusion across different regions.[2]

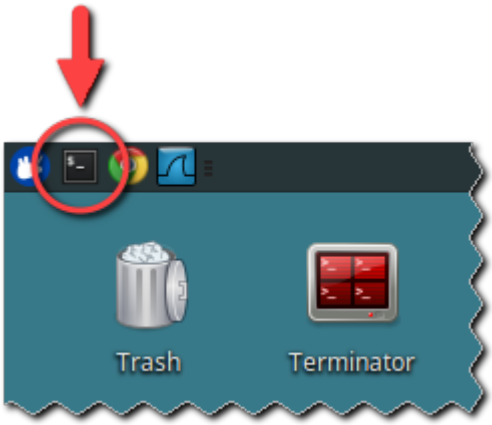
Updating the Electronic Workbook (EWB)

The electronic workbook (EWB) content is stored locally in the 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. You should update your EWB before attending class, and may be directed by your instructor, TA, or SME to pull down additional updates.

First log in to the SEC530 VM.

- Username: student
- Password: Security530

After login, open a terminal window by **clicking** on the terminal icon near the top-left corner of the desktop panel.



Update your EWB by running the following command in the terminal window:

SEC530 VM Terminal Input

```
workbook-update
```

The script will check for updates across multiple sections of content. For each section checked, you should see either an 'Updated!' message or an 'Already up to date' message.

SEC530 VM Terminal Output

```
[~]$ workbook-update
Updating EWB    in /var/www/html/workbook ... Updated!
Updating Videos in /var/www/html/video    ... Already up to date
Updating Labs   in /labs                  ... Updated!

[~]$
```

Run the command a second time. The script should report 'Already up to date' for every section checked.

SEC530 VM Terminal Output

```
[~]$ workbook-update
Updating EWB    in /var/www/html/workbook ... Already up to date
Updating Videos in /var/www/html/video    ... Already up to date
Updating Labs   in /labs                  ... Already up to date

[~]$
```

Auto-Updates

The EWB also attempts to auto-update once every six hours, at a random time within each 12 am and 6 am window, 6 am and 12 pm window, 12 pm and 6 pm window, and 6 pm and 12 am window. Each auto-update only occurs if the VM is running when the auto-update is scheduled to run.

Testing OpenVPN Access

Several SEC530 labs include accessing virtual lab environments via OpenVPN. This should be tested by each student on their VM.

Note

The OpenVPN connection only tunnels traffic to and from your SEC530 VM. It does not affect **any** traffic sent to or from your host computer.

Warning

If you are using a corporate or personal VPN on your host computer, then you should disconnect it before executing this step. **An active host VPN connection may disallow a second VPN connection to the OpenVPN environment.**

Within your open terminal window, execute the following command:

SEC530 VM Terminal Input

```
sudo openvpn --config /etc/openvpn/sec530.ovpn
```

You will receive a prompt to enter a '[sudo] password for student'. Enter:

SEC530 VM Terminal Input

```
Security530
```

The output for this command should end with 'Initialization Sequence Completed'.

Do not close this terminal window or stop this process.

Open a **second** terminal window. Within the second terminal window, execute the ping command below.

SEC530 VM Terminal Input

```
ping -c 4 10.5.30.10
```

The output for this command should include '4 packets transmitted, 4 packets received, 0% packet loss' and look similar to the following example:

SEC530 VM Terminal Output

```
[~]$ ping -c 4 10.5.30.10
PING 10.5.30.10 (10.5.30.10) 56(84) bytes of data.
64 bytes from 10.5.30.10: icmp_seq=1 ttl=254 time=25.8 ms
64 bytes from 10.5.30.10: icmp_seq=2 ttl=254 time=23.8 ms
64 bytes from 10.5.30.10: icmp_seq=3 ttl=254 time=21.1 ms
64 bytes from 10.5.30.10: icmp_seq=4 ttl=254 time=19.4 ms

--- 10.5.30.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 19.428/22.565/25.871/2.475 ms

[~]$
```

After completing this test, you can close both terminal windows. Please note that you may see several messages related to the tear-down of the VPN connection, including some final messages:

SEC530 VM Terminal Output

```
WARNING: Failed running command (--up/--down): external program exited with error status: 2

Exiting due to fatal error
```

This is normal expected behavior.

Customizing the SEC530 VM

You can select a new desktop background for your SEC530 VM.

1. **Right-click** on the desktop to activate the context menu.
2. **Click** on the **Desktop settings...** context menu option.
3. **Click** on the **Background** tab.
4. **Click** on the **Folder** popup-menu control and select **backgrounds**.
5. Select a background image.
6. Close the dialog.

Creating a Virtual Machine Snapshot

If you are using VMware Workstation Pro or VMware Fusion, then consider creating a virtual machine (VM) snapshot. This is an **optional** step that allows you to easily revert your VM to a known good state. A VM snapshot includes the VM's virtual disk and RAM at the time of the snapshot creation, including any applied EWB updates; and the VM configuration at the time of the snapshot creation, including allocated RAM.

Software Requirements

Creating snapshots is available in VMware Workstation Pro and VMware Fusion, but not VMware Workstation Player or VMware Fusion Player.

We recommend creating a snapshot of your VM:

- immediately after opening the VM but prior to making any changes or booting the VM for the first time; and
- immediately after completing all other required and optional preparation steps.

EWB Updates and Snapshots

Remember that a VM snapshot will include only the EWB updates applied prior to the snapshot creation, and that any EWB updates applied after snapshot creation will **not** be retained if you revert to that snapshot.

If you create a 'configured and updated' snapshot and then later retrieve significant EWB updates, then you may want to create a new snapshot and then delete the previous 'configured and updated' snapshot.

EWB Updates and VM Configuration

Remember that a VM snapshot includes the VM configuration at the time of the snapshot creation, including allocated RAM; and that any VM configuration changes made after snapshot creation will **not** be retained if you revert to that snapshot.

If you create a 'configured and updated' snapshot and then later make changes to the VM configuration, then you may want to create a new snapshot and then delete the previous 'configured and updated' snapshot.

Each SEC530 Snapshot Can Consume Up to 44 GB of Disk Space

The disk space consumed by **each snapshot** depends on the amount of changes made to the VM after the snapshot is created.

The minimum disk space consumed is approximately either 16 MB or, if the VM is running when the snapshot is created, the size of the VM's virtual RAM. In the case of the SEC530 VM, a snapshot of the running VM will consume a minimum of 4 GB of disk space.

The maximum disk space consumed is approximately the combined size of the VM's virtual disk(s) and, if the VM is running when the snapshot is created, the size of the VM's virtual RAM. In the case of the SEC30 VM, a snapshot of the running VM will consume a maximum of 44 GB of disk space.

The disk space required by snapshots is **in addition to** the minimum disk space requirements for the class.

Completing the Setup Process

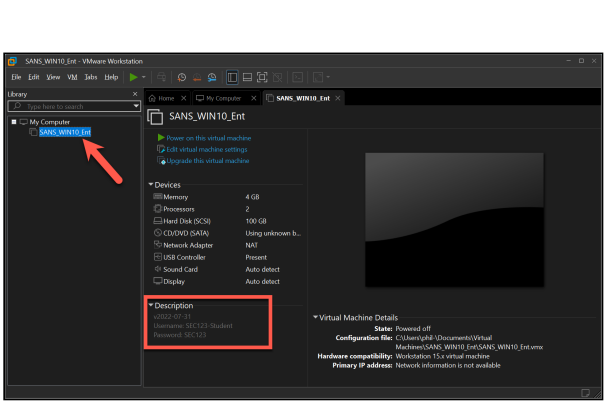
Once you have reviewed this document, completed the required steps and any desired optional steps, and either paused or cleanly shut down your VM, then you will be ready for class!

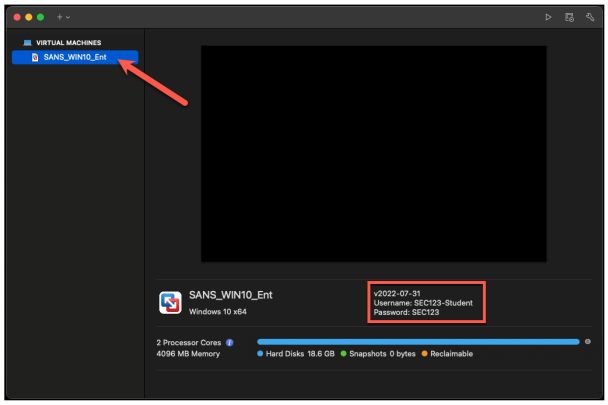
1. International Organization for Standardization. (2020, March 11). *ISO 8601 - date and Time Format*. ISO. Retrieved January 18, 2024 from https://www.iso.org/iso-8601-date-and-time-format.html.
2. Scott, Tom. (2013, December 30). *The Problem with Time & Time Zones - Computerphile*. YouTube. Retrieved January 18, 2024 from https://www.youtube.com/watch?v=-5wpm-gesOY.

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.





- SEC530 VIRTUAL MACHINE
  - Username: `student`
  - Password: `Security530`

  This user has `sudo` privileges for all commands on the virtual machine.