CompTIA Security+ SY0-701
Lab Setup Guide

Follow these instructions to prepare your lab environment. Perform each task in sequence until done.

Pre-requisites

- Windows 10 64-bit Home or Pro 22H2 (build 19045) or higher
- 64-bit processor with Second Level Address Translation (SLAT)
- Hardware virtualization enabled in BIOS
- 16 GB RAM (minimum)
- 60 GB free disk space (minimum)
- Your local Windows account must be a member of the administrators group
    - In most cases, it will be
    - If you can install software on the computer, then it is
- A working webcam

Software

Download the following items to your Host PC. You will install them later in this Setup Guide.

- VMware Workstation Player 17
  https://www.vmware.com/products/workstation-player.html
- 7-zip
  https://www.7-zip.org/download.html
- PuTTY
  https://putty.org
- .NET Framework 4.8
  https://go.microsoft.com/fwlink/?linkid=2088631
- JetBrains dotPeek
  https://www.jetbrains.com/decompiler/
- Valhalla Honeypot (English)
  https://sourceforge.net/projects/valhalahoneypot/files/valhalahoneypot/valhala180/valhala180-english.zip/download
- Windows XP Pro SP2 eval ISO
  https://archive.org/details/xp_pro_w_sp2_slipstreamed
- Kali Linux VM
  https://cdimage.kali.org/kali-2023.4/kali-linux-2023.4-vmware-amd64.7z
- Metasploitable2 VM
  https://sourceforge.net/projects/metasploitable/
- BlueStacks v5.20 or later
  Note: Do not download BlueStacks 10! That version is for multi-player platforms.

https://www.bluestacks.com/

- Docker Desktop for Windows
  https://docs.docker.com/desktop/install/windows-install/

Optional Hardware

These devices are used in two of the activities. You can obtain them or not as desired.

- O.MG Cable Basic USB-A to Apple Lightning cable
  https://shop.hak5.org/products/omg-cable?variant=39808315195505
- Flipper Zero
  https://flipperzero.one/

Prepare Your Host PC

1. Back Up Your PC

When working with hacking tools, there is always a chance that you could accidentally damage your operating system, apps, or data. Be sure to back up all important data to a removable drive or the cloud before you start.

2. Disable any anti-virus programs

Disable any anti-virus program you have running on your Host PC, including real-time protection. If you use Windows Security, follow these steps:

1. Go to **Settings** → **Update & Security** → **Windows Aecurity** → **Virus & threat protection** → **Manage settings**.
2. Turn off all of the protection features.
3. At the bottom, under **Exclusions**, click **Add an exclusion**→ **Folder** → **Local Disk** (C:) → **Select folder**.
4. Close Settings.

Note: You will have to disable Real-time protection every time you restart your computer.

3. Uninstall Hyper-V

Microsoft Hyper-V is incompatible with VMware. If you have it installed, you will need to uninstall it for VMware Workstation Player to run.

1. Search for and open **Control Panel**.
2. Click **Uninstall a program**.
3. Click **Turn Windows Features on or Off**.
4. Ensure that Hyper-V is unchecked (un-ticked) and click **OK**.
5. If prompted to reboot, do not do so yet.
6. Click **Start** → **Command Prompt**.
7. Right-click **Command Prompt → Run as administrator**. When prompted, click **Yes**.
8. Type the following command and press Enter:

```
bcdedit /set hypervisorlaunchtype off
```

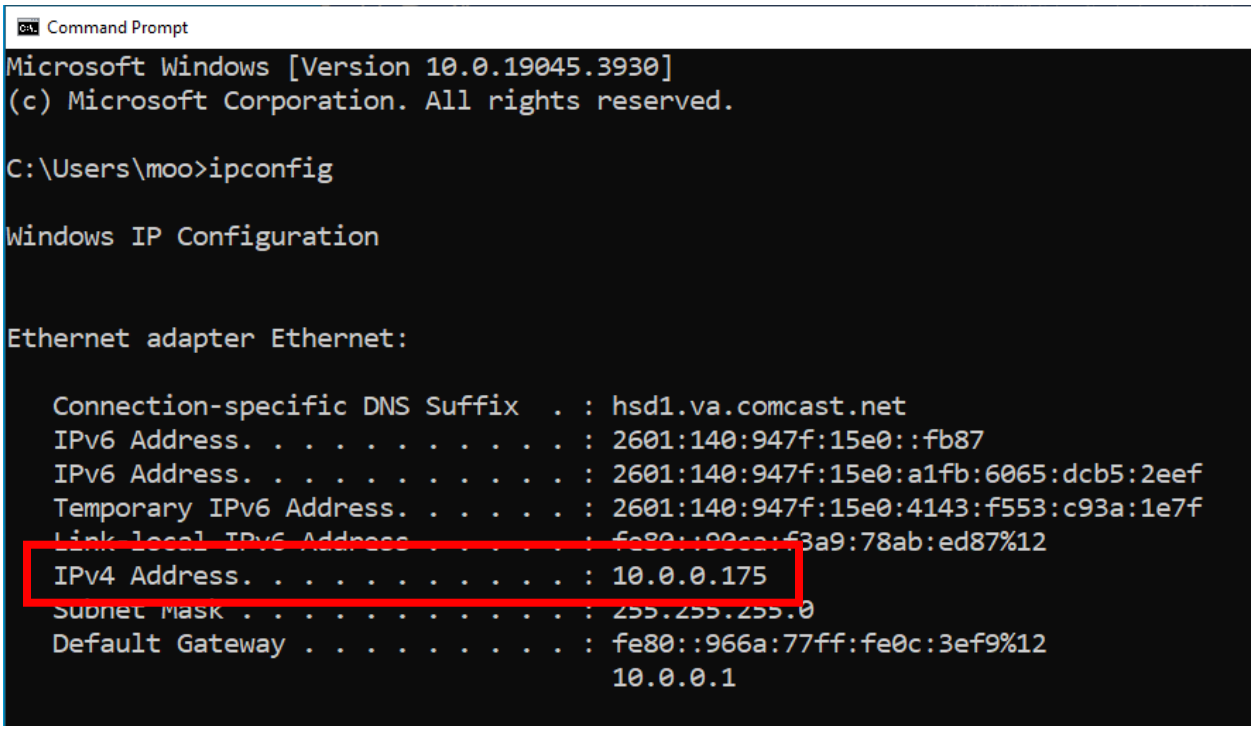
9. Close the Command Prompt window.
10. Reboot your Host PC and then log back in.

4. Obtain the Host PC IP Address

1. Search for ***Command Prompt*** and open it.
2. At the command prompt, type:

```
ipconfig
```

3. Press Enter.
4. In the results, scroll up to the first adapter and make note of the IPv4 Address.
   Note: Your address and adapter name may be quite different from the example shown.



5. Download the Activity Files

1. In the LMS, on the same page where you found this Lab Setup Guide, locate and download **Activity-Files.zip**.
2. Unzip the zip file.
3. Verify that there are five folders inside, one for each course module, and that each has various activity files inside them.

6. Install Software on Your Host PC

1. Locate the software that you downloaded for this lab.
2. Perform a default installation of each the following items:
   - 7-zip

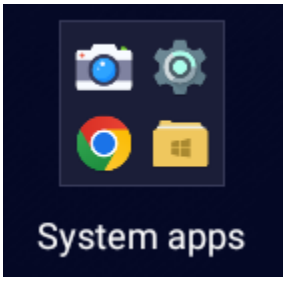
- VMware Workstation 17 Player (or later)
- PuTTY
- .NET Framework 4.8
- JetBrains dotPeek

7. Install and Test BlueStacks 5

Note:

- BlueStacks is actually Android 7.1.2 (Nougat) running in its own virtual machine.
- Previous versions of Bluestacks 5.x required Hyper-V, which is disabled for this lab.
- Bluestacks 5.20 does not require Hyper-V.

1. If necessary, plug your webcam into your Host PC.
2. Locate the BlueStacks 5.20 installer and double-click it.
3. Click **Yes**, then **Install Now**.
4. When the installation is complete, ensure that the BlueStacks App Player opens.
5. In the lower right corner of the BlueStacks Player, click the Settings button  .
6. In Settings, click **Devices**.
7. Set the **Camera** to your webcam.
8. Set the Microphone to a working mic (the webcam should be fine) and click **Save Changes**.
9. Close **Settings**.
10. On the App Player desktop, in **System Apps** click the **Camera** icon.



11. Click **Allow**, then click **Next**.
12. Verify that the camera works.
13. In either the upper left or lower right corner of the App Player, click the Home button  .
14. Close BlueStacks 5.
15. To reduce confusion, on your Host PC desktop, locate and delete the shortcuts for:
    - BlueStacks Multi-Instance Manager
    - BlueStacks X

8. Download and Install Packet Tracer

In order to run Packet Tracer, you will first need a free Cisco Network Academy student login.

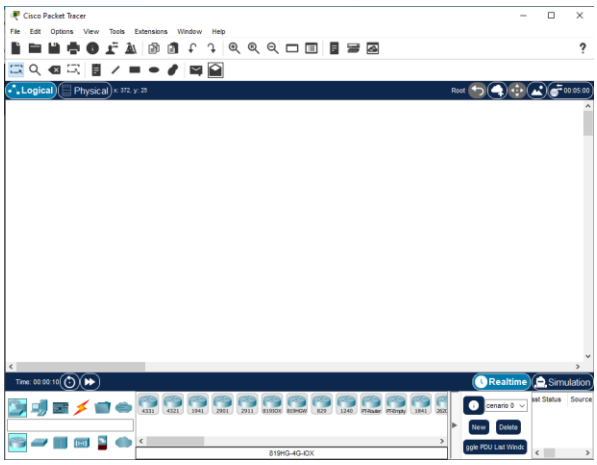
1. Sign up for a free Cisco Network Academy account.

a. Open a browser to https://id.cisco.com
b. Click **Sign up.**
c. Enter the required information and click **Register**.
d. Return to the login page and log in with your new credentials.

2. Download and install Packet Tracer.
   e. Download from https://archive.org/details/packet-tracer-821-64bit-setup-signed

   Alternatively, obtain the latest version of Packet Tracer from skillsforall.com:
   f. Open a browser to https://skillsforall.com/resources/lab-downloads?courseLang=en-US
   g. Click **Login.**
   h. Provide your Cisco Network Academy credentials.
   i. Scroll down, locate and download the latest version of Packet Tracer.

3. Start Packet Tracer.
   a. Double-click the Packet Tracer installer and perform a default installation.
   b. When prompted, provide your Cisco Network Academy credentials.
   c. Verify that Packer Tracer opens to a blank palette.



4. Close Packet Tracer.

5. Create a Test Gmail account

You will use a live Gmail account for two activities.

1. Open a browser to ***gmail.com***.
2. At the **Sign in** page click **Create account**.
3. Select **For my personal use**.
4. Enter details and verify account as required.
5. When finished, send/receive a test email to ensure that the account is working ok.
6. Close Gmail.

6. Install Docker Desktop for Windows

You will need Docker Desktop for Windows for the Containers activity. Docker Desktop requires the Windows Subsystem for Linux (WSL).

Install the Windows Subsystem for Linux (WSL)

1. Open PowerShell as administrator.
    a. Search for ***powershell***
    b. Right-click **Windows PowerShell → Run as administrator**
2. Check to see if you already have WSL installed. Enter this command:

```
wsl -l -v
```

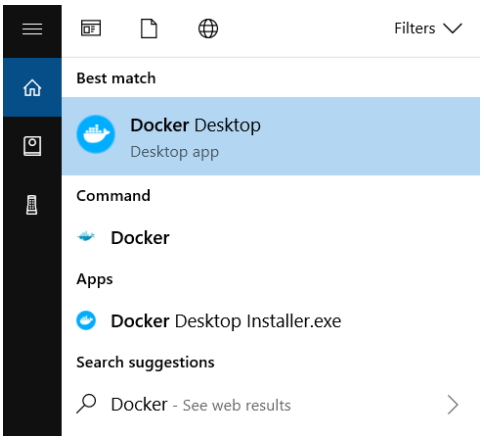
3. If you do not already have WLS installed, then enter this command:

```
wsl –install
```

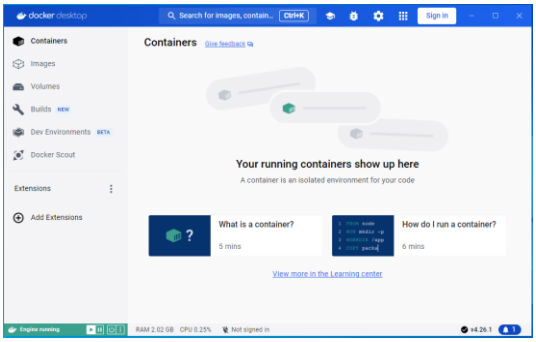
4. Allow WSL to finish installing.

Install Docker Desktop

1. Locate your download of Docker Desktop.
2. Double-click **Docker Desktop Installer.exe** to run the installer.
   Note: By default, Docker Desktop is installed at C:\Program Files\Docker\Docker.
3. On the **Configuration** page, when prompted, ensure the **Use WSL 2 instead of Hyper-V** option is selected.
4. Follow the instructions on the installation wizard to authorize the installer and proceed with the install.
5. When the installation is successful, select **Close** to complete the installation process.
6. Start the Docker Desktop app.



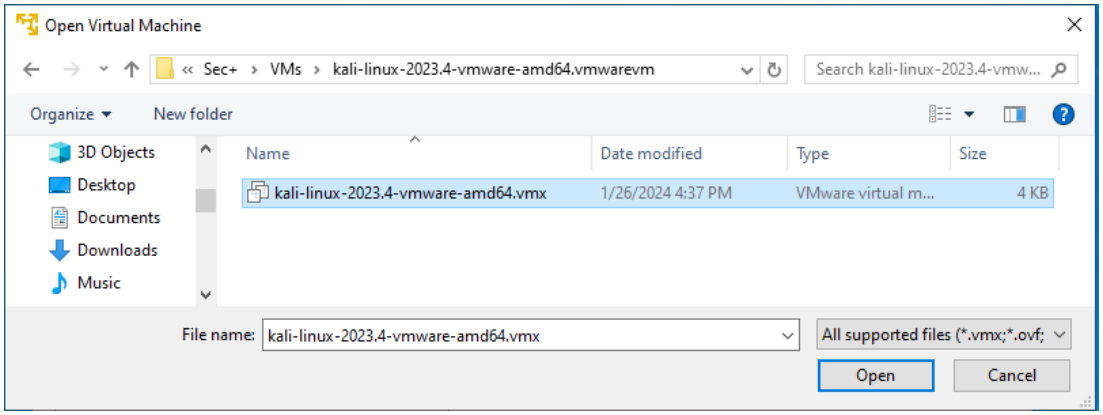
7. Verify that Docker Desktop opens.



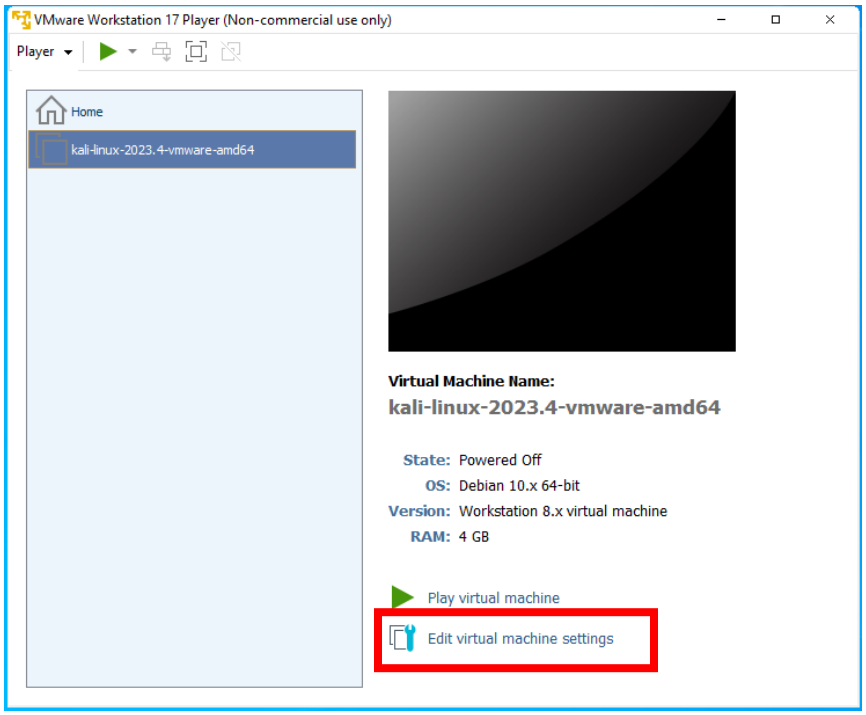
8. Close Docker Desktop.

Prepare Kali Linux VM

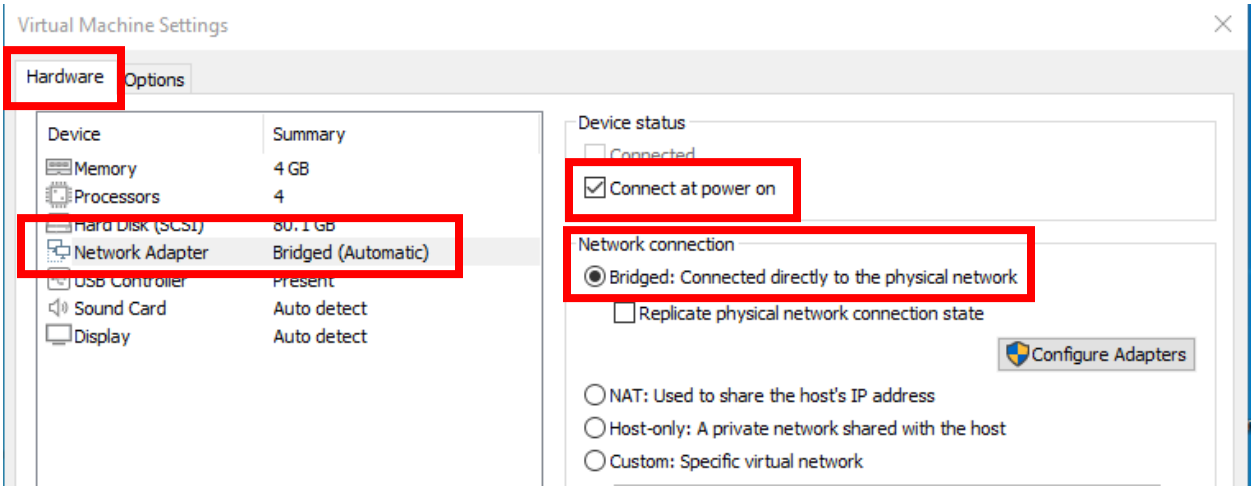
1. Add the Kali VM to the VMware Workstation 17 Player library.
    a. Locate the downloaded kali-linux 7z file (for example, kali-linux-2023.4-vmware-amd64.7z)
    b. Right-click the Kali zip file → **7-Zip** → **Extract Here**.
    c. Allow the VM to finish extracting.
    d. Launch **VMware Workstation 17 Player.**
    e. On the **VMware Workstation 17 Player Home** page, click **Open a Virtual Machine.**
    f. Browse into the unzipped Kali Linux VM folder.
    g. Select the kali-linux vmx file and click **Open.**



2. Set the Kali VM Network Adapter to Bridged mode.
    a. Select the Kali VM and click **Edit virtual machine settings**.



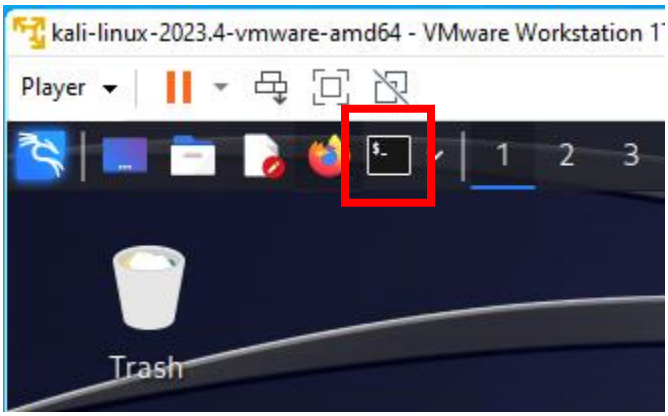
b. On the **Hardware** tab, select **Network Adapter**.
c. Under **Network connection**, change the adapter to **Bridged**. Ensure that under **Device status** it is set to **Connect at power on**.



d. Click **OK**.

3. Start the Kali VM and log in.
   a. In the VMware Workstation Player home page, with the Kali Linux VM selected, click **Play virtual machine**. If prompted, click **I copied it**.
   b. Allow Kali to boot up.
   c. Log into Kali Linux as ***kali*** with the password of ***kali***

4. Obtain Kali's IP address.
    a. At the top of the Kali desktop, click the terminal button.

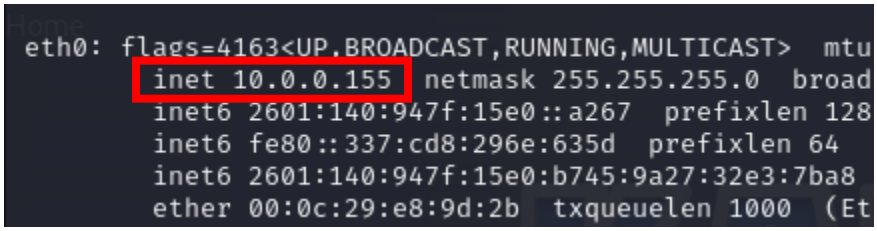


    b. In the terminal, type the following and press Enter (note: Linux is case sensitive!):

```
ifconfig
```

    c. Under **eth0:** make note of the IP address listed after **inet**.
    d. Verify that the IP address is in the same subnet as the Host PC.
        - The first three numbers (octets) should be the same on both your Host PC and Kali Linux.
        - For example: Host PC = **10.0.0.**175, Kali Linux = **10.0.0.**155

    Note: The IP addresses of your VMs may change periodically as you boot the VMs up and down.



5. Set the root password to ***kali*** and log out.
    a. In the terminal, enter:

```
sudo passwd root
```

    b. When prompted, enter ***kali*** (you will do this three times).
    c. Close the terminal window.

6. Leave Kali Linux VM running, and switch to your Host PC.

Prepare Metasploitable2 VM

Note: Metasploitable2 has no GUI. If your mouse becomes trapped in the Metasploitable2 VM, press Ctrl+Alt to release it.

1. Using the procedure you used for Kali Linux:
   - Add the Metasploitable2 VM to the VMware Workstation 17 Player library
   - Set its Network Adapter to **Bridged**
   - Start the VM
   - Log in as ***msfadmin*** / ***msfadmin***
   - Obtain and make note of Metasploitable2's IP address
   - Verify that the IP address is in the same subnet as Kali Linux and the Host PC

   Note: If you are prompted to install VMware Tools, click **Never Remind Me**

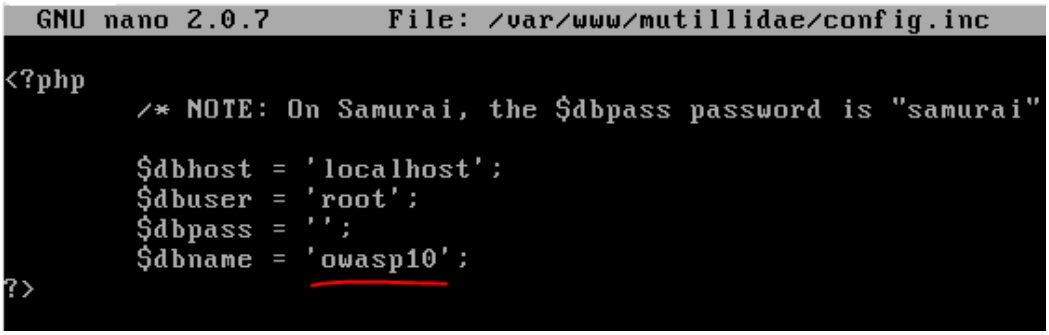
2. Correct the mutillidae configuration error.

   Metasploitable2 shipped with a configuration error. You will manually correct this.

   a. At the metasploitable prompt, enter the following command:

   ```
   sudo nano /var/www/mutillidae/config.inc
   ```

   b. When prompted for the password, enter ***msfadmin***
   c. Using the arrow keys on your keyboard to navigate, and the backspace key to erase, replace 'metasploit' with 'owasp10'.



   d. Press Ctrl+o
   e. Press Enter
   f. Press Ctrl+x
   g. Verify that the correction was successful by entering this command:

   ```
   cat /var/www/mutillidae/config.inc
   ```

3. Leave Metasploitable2 VM running, and switch to your Host PC (remember, if necessary press Ctrl+Alt to release your mouse).

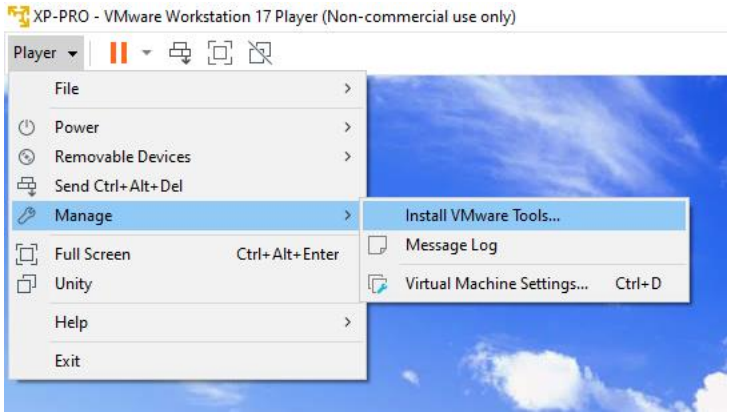
Prepare XP-PRO VM

1. Create the XP-PRO VM.
    a. In **VMware Workstation 17 Player**, on the **Home** page, **click Create a New Virtual Machine**
    b. On the Welcome page, select **I will install the operating system later** and click **Next**.
    c. On the Select a Guest Operating System page, choose Microsoft Windows / Windows XP Professional and click **Next**.
    d. Change the **Virtual machine name**: to ***XP-PRO*** and click **Next**.
    e. Click **Next**, and then click **Finish**.
    f. Click **Edit virtual machine settings**
    g. On the Hardware tab, set:
        - **CD/DVD** to use **xp_pro_w_sp2_slipstreamed.iso**
        - **Network Adapter** to **Bridged**
    h. Click **OK**, and start the virtual machine.

2. Install XP Professional.
    a. At the **Welcome to Setup** page, click into the screen and press Enter.
    b. At the **Windows XP Licensing Agreement page**, Press F8.
    c. At the partition page, press Enter.
    d. Press Enter again.
    e. Allow XP to install. If necessary, press Ctrl+Alt to release your mouse.
    f. In the GUI stage, at the **Regional and Language Options** page, click Next.
    g. At the **Personalize Your Software** page, for the **Name** and **Organization**, enter anything you like and click Next.
    h. At the **Your Product Key** page enter ***H36CC-HFBHM-FVY9Q-VFPVC-4H9VG*** and click **Next**.
    i. At the **Computer Name and Administrator Password** page, enter the following information:
        - Computer name: ***XP-PRO***
        - Administrator password: ***password***
        - Confirm password: ***password***
    j. Click **Next**.
    k. At the **Date and Time Settings** page, click **Next**.
    l. Click **Next** two more times.
    m. In the **Display Settings** popup box, click **OK**.
    n. In the **Monitor Settings** popup box, click **OK**.
    o. On the **Welcome to Microsoft Windows** page, click **Next**.
    p. On the **Help protect your PC** page, click **Not right now**, then click **Next**.
    q. On the Internet connection page, click **Next**.
    r. On the **Ready to register with Microsoft** page, select **No, not at this time**, and then click **Next**.
    s. On the **Who will use this computer?** page, in **Your name:** enter ***admin*** then click **Next**.

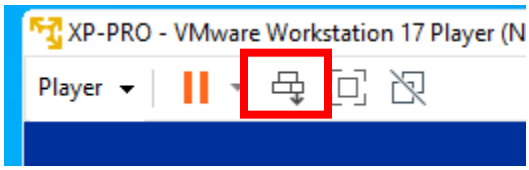
t. Click **Finish**.

3. Install VMware tools.
   a. In the upper left, above the XP desktop, click **Player → Manage → Install VMware Tools.**

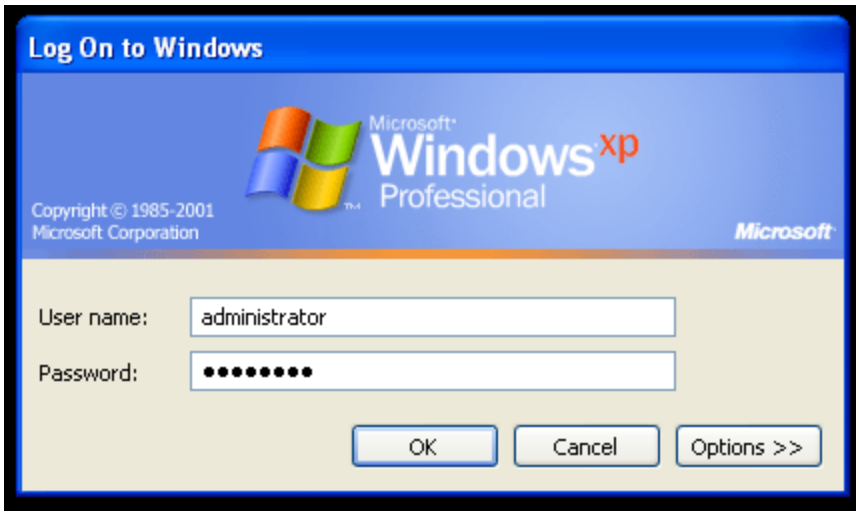


   b. In the **VMware Tools Setup** wizard, **click Next.**
   c. Click **Next**, click **Install**.
   d. Click **Finish**.
   e. Click **Yes** and allow XP-PRO to restart.

4. Log into XP-PRO.
   a. If necessary, expand the XP VM window by clicking and dragging the lower right corner of the VM.
   b. Above the Windows XP login screen, click the Ctrl+Alt+Del button twice.



   c. Verify that the alternate logon screen appears.
   d. Log in as ***administrator*** with the password of ***password*** and then click **OK.**



5. Disable the XP-PRO firewall.
    a. In the XP-PRO desktop, click **Start → Control Panel**.
    b. In the upper left, click **Switch to Classic View.**
    c. Scroll down to find **Windows Firewall** and open it.
    d. On the **General** tab, click **Off (not recommended)**.
    e. Click **OK**.
    f. Close the Control Panel.

6. Set the admin password to password.
    a. Click **Start → All Programs → Run.**
    b. In the **Run** line, type ***cmd*** and click **OK.**
    c. Enter the following command:

```
net user admin password
```

    d. Verify that you receive the message "Command completed successfully".

7. Obtain XP-PRO's IP address.
    a. In the command prompt, enter:

```
ipconfig
```

    b. Make note of the IP address. Ensure that it belongs to the same subnet as the Host PC and other VMs.

8. Install Valhalla on XP-PRO.
    a. Switch to your Host PC.
    b. Locate **valhala180-english.zip.**
    c. Drag and drop **valhala180-english.zip** to the XP-PRO desktop.
    d. Click into the VM, then right-click **valhala180-english.zip → Extract All**.

e. In the **Extraction Wizard**, click **Next** twice, then click **Finish.**
f. Double-click **honeypot** to ensure that it launches.
g. Close **Valhala Honeypot**.

9. Leave XP-PRO VM running and switch to your Host PC.

Final Preparation

1. Verify that the Host PC can ping all VMs.
   a. On your Host PC, open a Command Prompt.
   b. Ping Kali Linux VM. Enter the following command. Substitute <Kali IP Address> with Kali's actual IP:

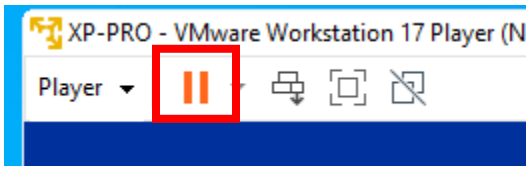
      ```
      ping <Kali IP Address>
      ```

      For example: `ping 10.0.0.155`

   c. Verify that you receive four replies from Kali.
   d. Using the same technique, verify that you can ping Metasploitable2 and XP-PRO.

2. Verify that the Kali Linux VM can ping Metasploitable2 and XP-PRO.
   a. Switch to Kali.
   b. Open a terminal.
   c. Use the ping command to ping Metasploitable2.
   d. After receiving a few replies, press Ctrl+c to stop the ping.
   e. Repeat the process to ping XP-PRO.

3. Suspend the VMs.
   Perform this on all three VMs.
   a. In upper left of the VMware Player, click the **Suspend guest** button.



   b. When prompted, click **Yes**.
   c. Verify that all three VMs suspend, and that their windows disappear.

   Note: To resume a suspended VM, open VMware Workstation 17 Player. Select the VM and click **Play Virtual Machine**.

Congratulations! Your Security+ SY0-701 lab setup is complete!