Setting up the CTF VM

Step 0 - Prerequisites:

In order to play the CTF, you will need to have a Virtual Machine Manager installed. The setup script will work in Kali, which should be able to run in any Virtual Machine Manager. Some of the most popular Virtual Machine Managers include:

- Virtual Box [FREE] - https://www.virtualbox.org/wiki/Downloads

  > ⚠ **Warning**
  > DOES NOT WORK ON MACOS

- VMware Workstation Pro (Windows/Linux) or VMware Fusion (Mac OS) [FREE] - https://blogs.vmware.com/cloud-foundation/2024/05/13/vmware-workstation-pro-now-available-free-for-personal-use/
- MacOS Parallels [PAID only] - https://www.parallels.com/
- Virtual Manager, Gnome Boxes, etc. [LINUX only] - Install via your repo

> 🖉 **Note**
>
> If you already have a Kali VM set up, then you can skip down to **Step 2 - Install Kali** in these instructions.
> If you have a dedicated Kali installed on laptop (bare metal), then you can skip to **Step 3 - Run the setup script** in these instructions.

VMWare Workstation Pro

To ensure first-time CTF players have a working Virtual Machine Manager, we have provided the following instructions for VMware Workstation Pro, which is free. You will need to register on the Broadcom website (they own VMware).

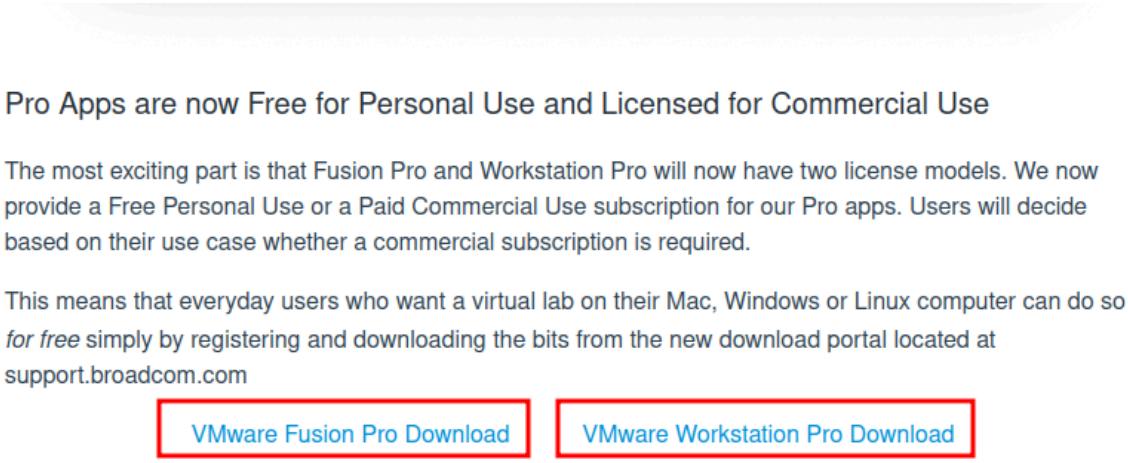
If you do not like providing your information to Broadcom, we suggest looking at VirtualBox as your Virtual Machine Manager, just remember it only works in Linux and Windows and DOES NOT WORK on Mac OS.

> 🖉 **Note**

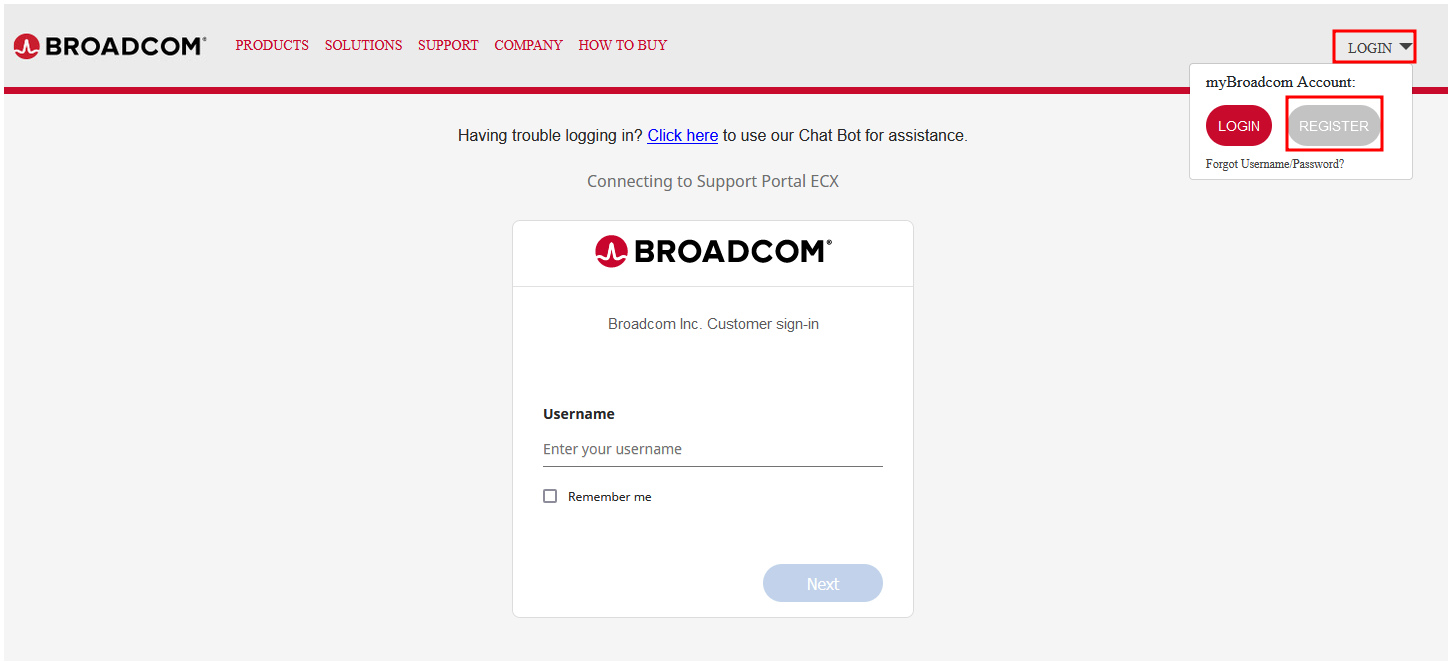
If you already have a Kali VM set up, then you can skip down to **Step 2 - Install Kali** in these instructions.
If you have a dedicated Kali installed on laptop (bare metal), then you can skip to **Step 3 - Run the setup script** in these instructions.

To register with on the Broadcom site:

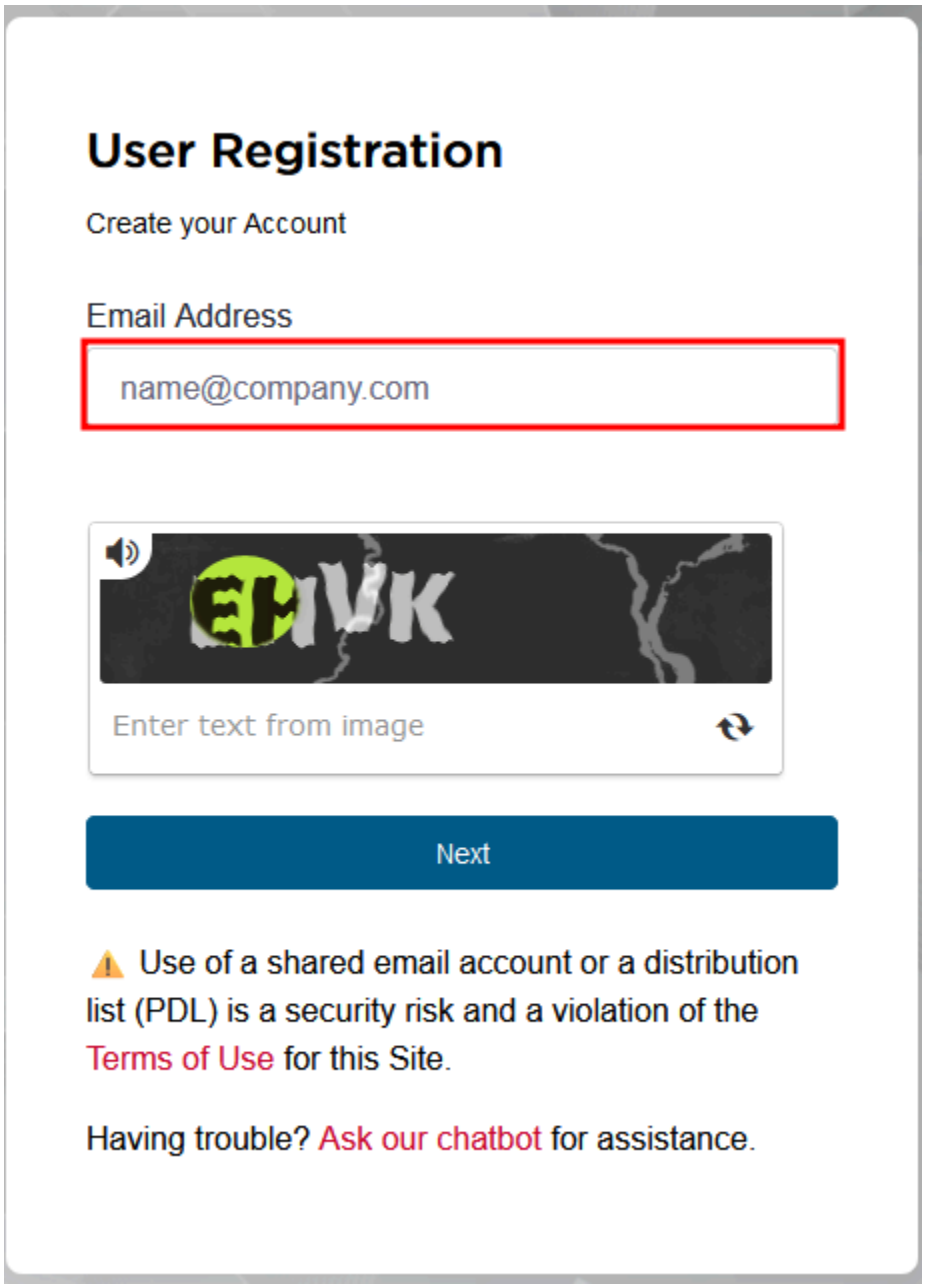
- Go to the following VMware site: https://blogs.vmware.com/cloud-foundation/2024/05/13/vmware-workstation-pro-now-available-free-for-personal-use/
- Look for the download link for VMware Fusion (about 1/3 down the page) and click it:



- This will open up the Broadcom site for the download. If you don't already have an account, click the Login link in the upper right of the page, then select the register button:

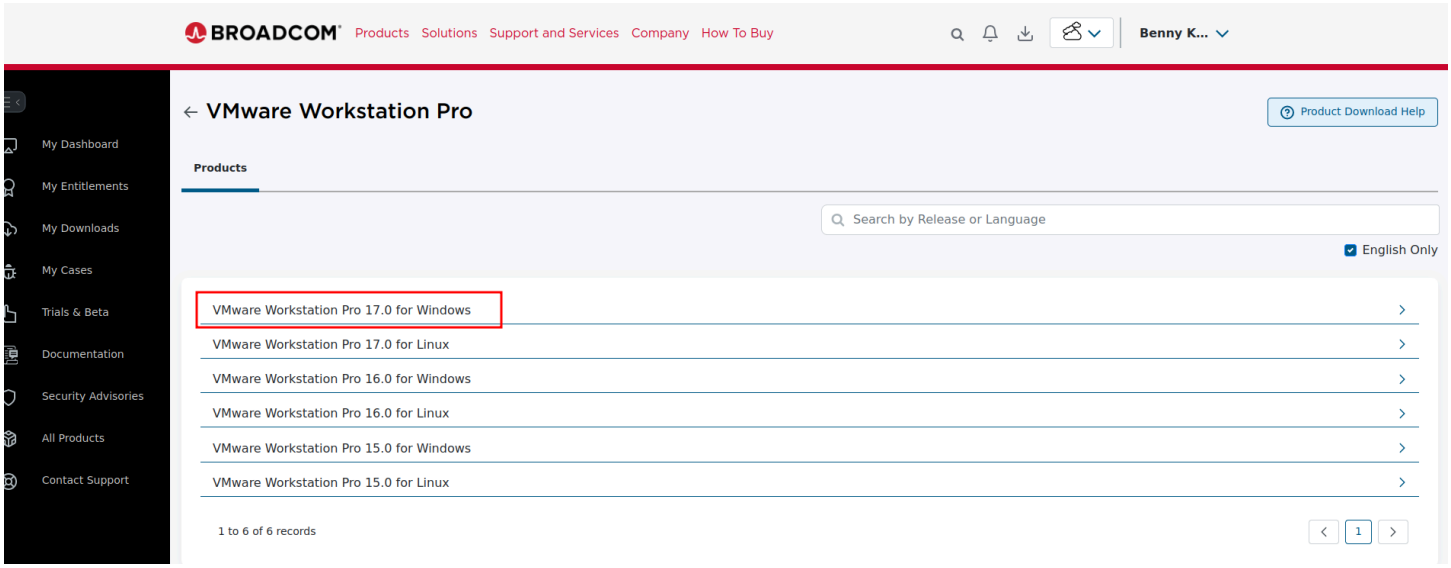


- On the User Registration page, enter your Genesys email:

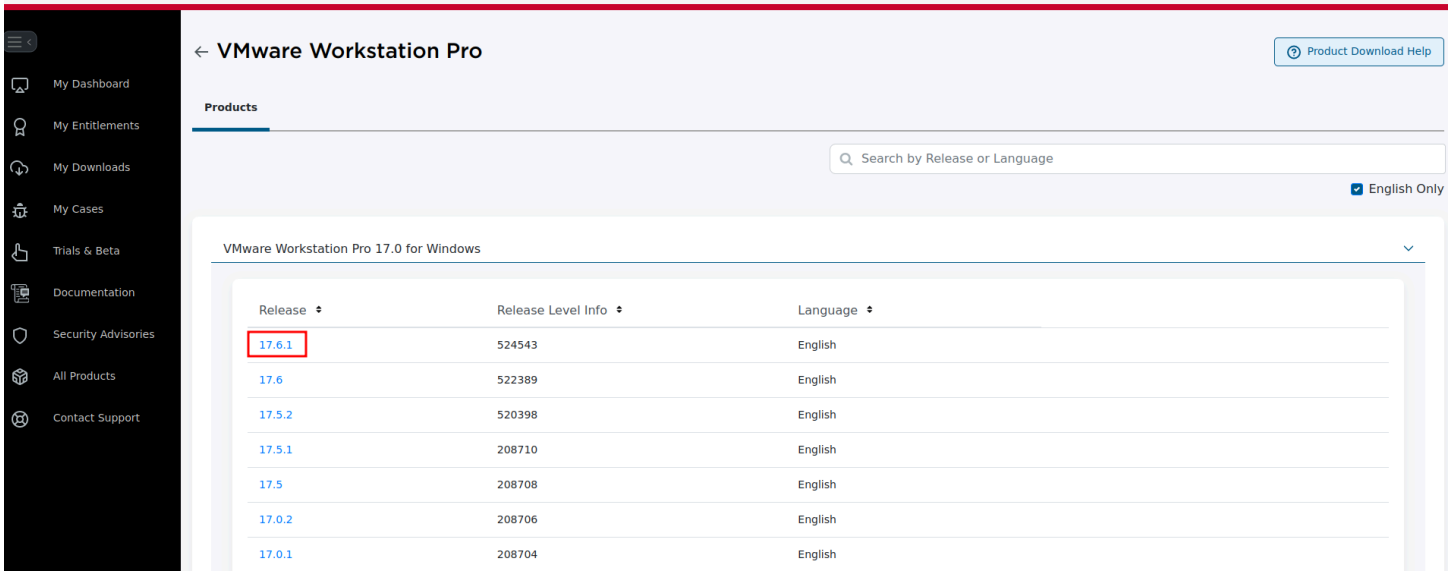


- You will then have to finish the user account. Once your account is created, then you can go and download the software.
- After logging into the Broadcom site, go to the Fusion Download page: https://support.broadcom.com/group/ecx/productdownloads?subfamily=VMware%20Workstation%20Pro&freeDownloads=true

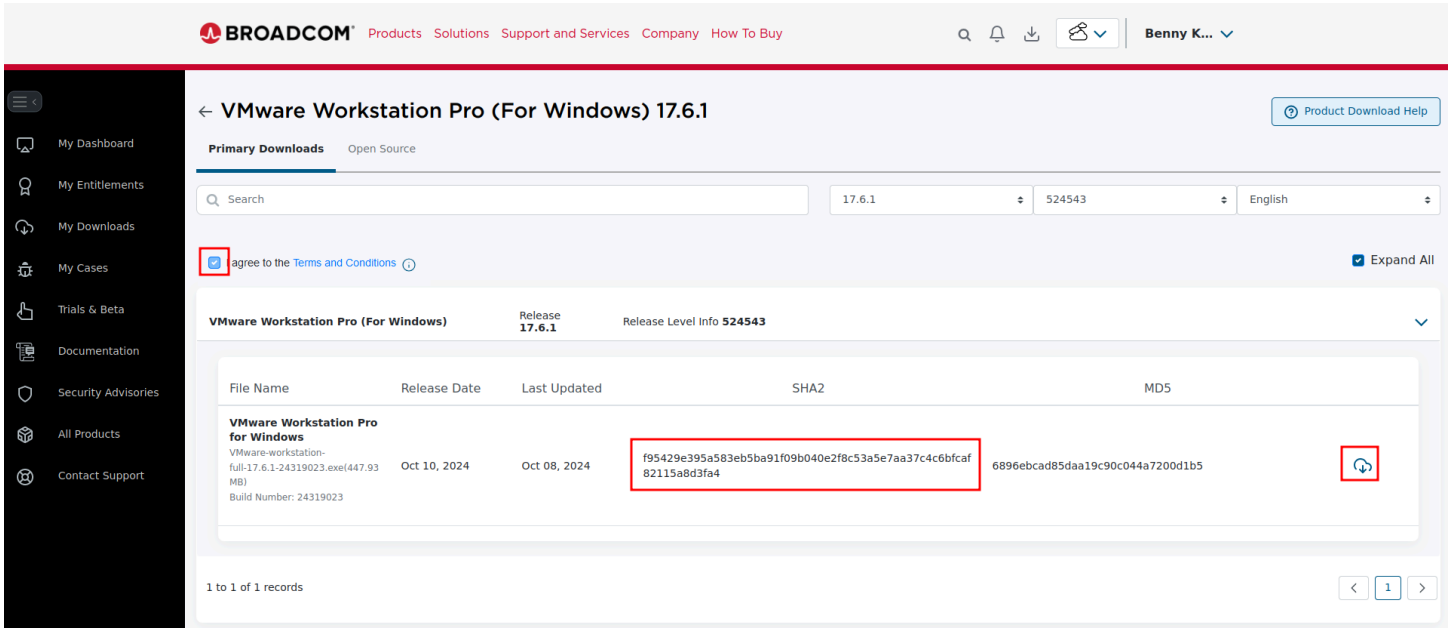
- Select VMware Workstation 17 for Windows:



- Then, click on the latest release (which is 17.6.1 at the time of this documentation):



- Click on the I agree to the Terms and Conditions and then click on the Download button. Also, copy the SHA256 check sum for reference later.



Step 1 - Install VMware Workstation:

> **Note**
>
> If you already have a Kali VM set up, then you can skip down to **Step 2 - Install Kali** in these instructions.
> If you have a dedicated Kali installed on laptop (bare metal), then you can skip to **Step 3 - Run the setup script** in these instructions.

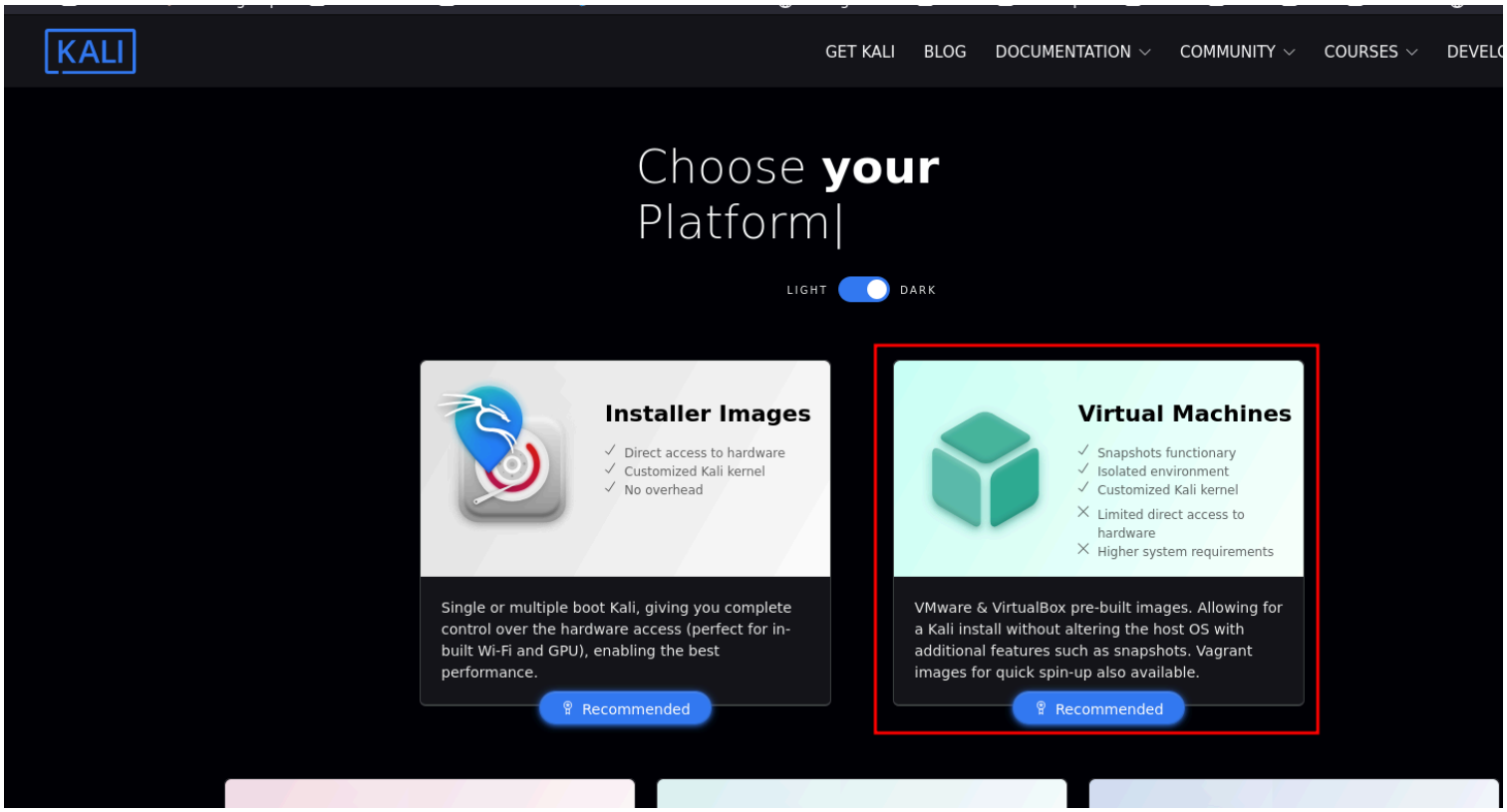
- [ ] Download the required EXE file (from above)
- [ ] Do CheckSums for the EXE
    - If you are unsure how to do this, see the appendix below
- [ ] Install VMware normally (Next, next, etc.)
- [ ] You are now ready for **Step 2 - Install Kali**.

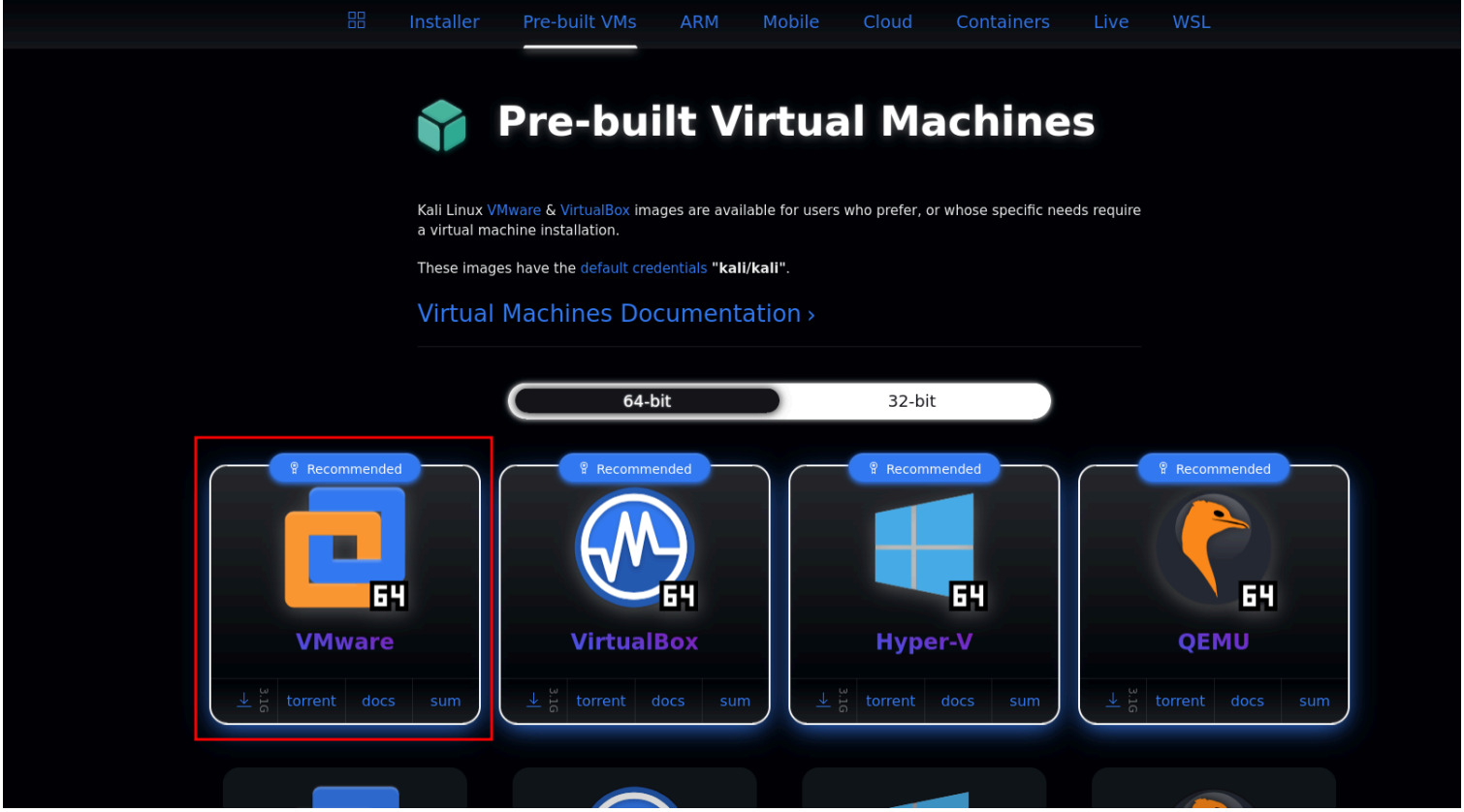
Step 2 - Install Kali:

Kali inside VMware (Guest VM)

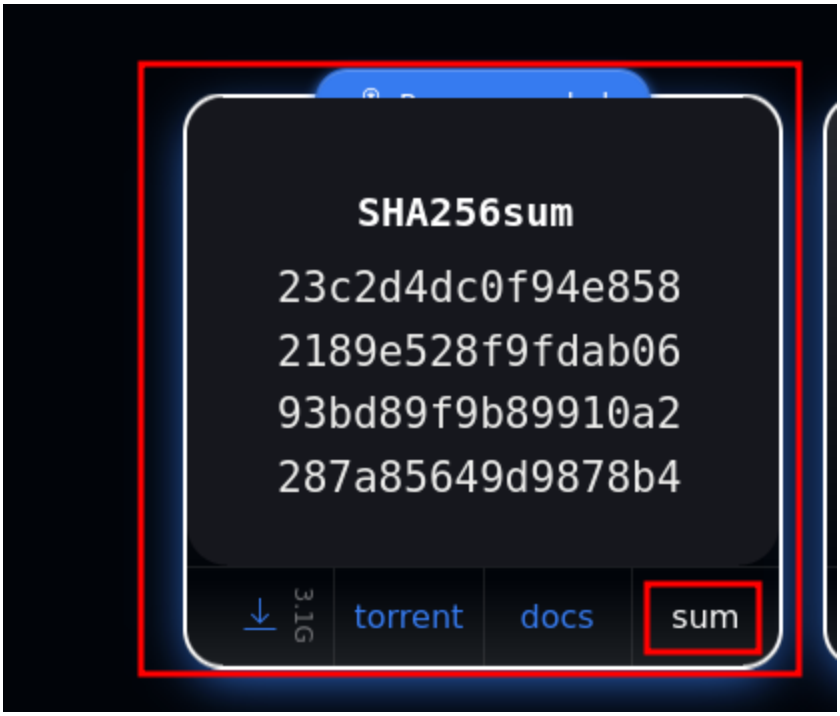
> **Note**
>
> You may need to enable virtualization in your BIOS/UEFI for (e.g. Intel VT-x/AMD-V)

If you are installing on Windows, Linux or an Intel Mac, you will want the 64-bit ISO:



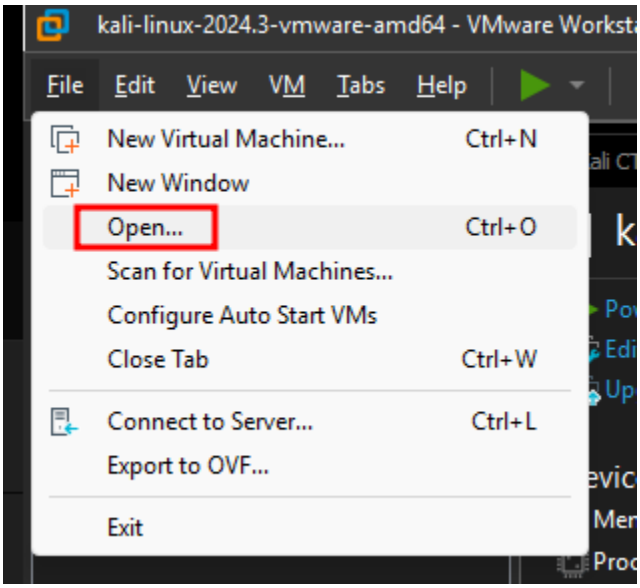


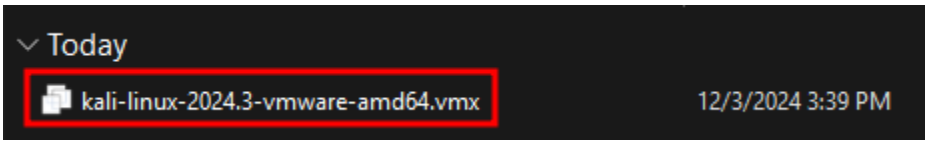
As you are downloading the pre-made VM, be sure to copy the CheckSum from the page:



After doing a checksum on the downloaded file, unzip it where you downloaded it.

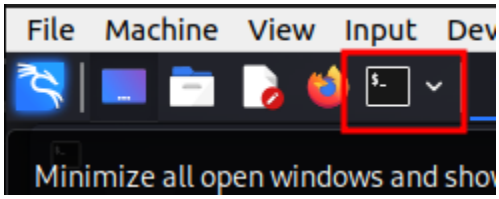
Lauch VMware Workstation and select the unzipped VMX file





Step 3 - Run the setup script:

- Start the new Kali VM and log in using the following creds:
  Username: kali
  Password: kali
- Open the Terminal
  - The button can be found in the upper left of the desktop:



- The following commands will need to be run from within the terminal:

> **⚠ Warning**
> If you copy from the PDF, you may need to fix the lines in a text file first before using it in the terminal (it may chop it up in the copy). Copy it, then paste into you're favorite text editor and then re-copy it.

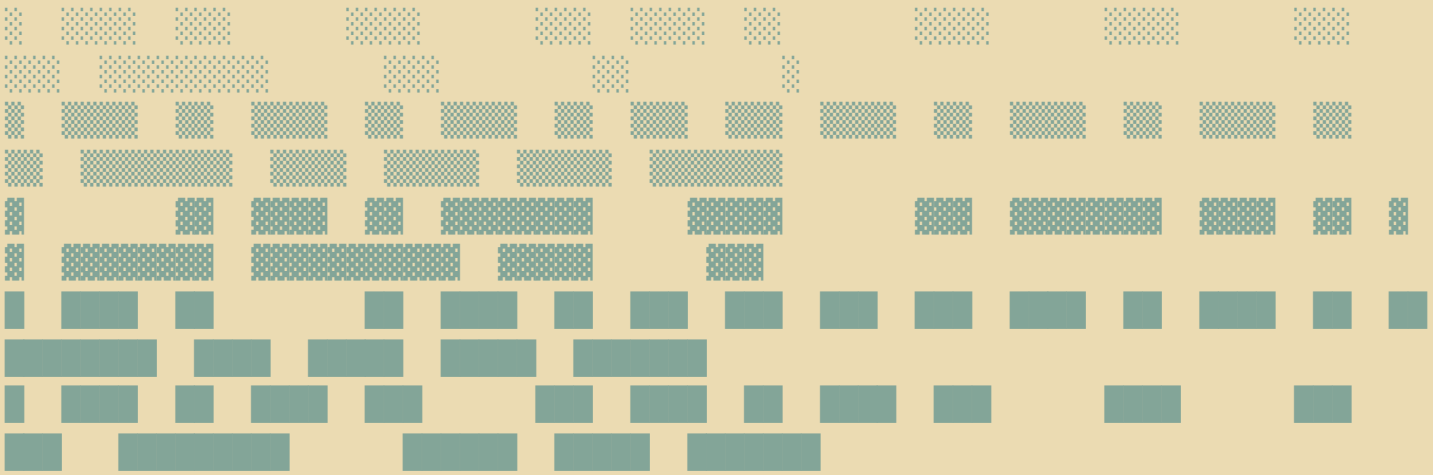
```
mkdir Projects && cd Projects && git clone https://github.com/bkarnes/hack3rcon_ctf.git && cd hack3rcon_ctf && chmod u+x setup_vm.sh && ./setup_vm.sh
```

Explanation of the above commands:

- We make a Projects directory in kali's home directory:
  `mkdir Projects`
- We then change into the Projects directory
  `cd Projects`
- We clone my Repo:
  `https://github.com/bkarnes/hack3rcon_ctf.git`
- We then change into the LinuxAdminClass directory that is created:
  `cd hack3rcon_ctf`
- We make the setup_vm.sh script executable:
  `chmod u+x setup_vm.sh`
- We then run the script:
  `./setup_vm.sh`

Running the Script:

> ⚠ **Warning**
>
> The script has only been tested on Kali, but may not work on ParrotOS.
> Also, use the user creds you set above instead of the kali creds from the VM
> To restart the script after the first step, run the following:
> `./Projects/hack3rcon_ctf/setup_vm.sh`



```
Today is: Sat May 24 02:08:09 PM EDT 2025
What can I do for you today?

1) Setup CLI logging and default directories.  Will require a reboot.
2) Update VM.  Will reboot after update.
3) Install Docker.  Will reboot after install.
4) Install netbird client.  Will reboot after install.
```

```
5) Install Project Discovery Tools.(Optional)  Will reboot after install.

(Q)uit
```

- Now, perform the following actions in the following order (reboot as needed):

> **Note**
> The VM will reboot after each step

1. Setup CLI logging.
   You will need to put in kali's password twice
2. Update VM.
   This step is optional if you've already updated your VM this before running the script or can be done after other steps are completed.

   This could take a long time depending on your Internet speed and HD. Plus, you may need to watch it a bit as you will need to put in kali's password a couple of times and maybe answer a question or two.
3. Install Docker.
4. Install the netbird client step.
   - You will use a netbird setup key below
5. Install the Project Discovery tools if you would like (not required for the CTF)

> **Warning**
> You will need to enter the user's creds to reboot after this step is finished.

Step 4 - Test the setup:

- Reboot it one last time and run the following command to change the kali user's password: `passwd`
  - You will need the current password (`kali`)
  - Put the new password
- Once that is complete, run the following tests:
  - [ ] Ensure that the kali user has the BASH shell loaded:

```
┌──(kali㉿kali)-[~]
└─$ echo $SHELL
/bin/bash
```

- If you don't see **/bin/bash** like above, then run the following command: `chsh -s /bin/bash`
- Reboot the VM and rerun the echo command from above to ensure is says **/bin/bash**.
- Change the hostname of the VM from the default Kali:

```
┌──(kali㉿kali)-[~]
└─$ sudo hostnamectl hostname <NEW HOSTNAME>
[sudo] password for kali:
```

- You will also need to update the /etc/hosts file with your new hostname:

```
┌──(kali㉿kali)-[~]
└─$ sudo vim /etc/hosts
[sudo] password for kali:

127.0.0.1   localhost
127.0.1.1   kali  <-- Put in your new hostname
::1     localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
```

- Reboot to help the hostname to set:

```
sudo reboot
```

- When it comes back up and you log in and open the terminal, you should see the new hostname:

```
┌──(kali㉿ninja-robot)-[~]
└─$ hostname
<NEW HOSTNAME>
```

- [ ] Check to make sure Netbird installed properly:

```
┌──(kali㉿kali)-[~]
└─$ netbird version
0.29.1

Your version may be newer.
```

- [ ] Make sure netbird is not connected to anything and then connect it to the CTF network:

```
┌──(kali㉿kali)-[~]
└─$ netbird down
```

```
Disconnected

┌──(kali㉿kali)-[~]
└─$ sudo netbird up --setup-key 61321F92-BF18-4D44-A6EB-9E72C84D9ABD
[sudo] password for kali:
Connected
```

Step 5 - Playing the CTF:

- To play the CTF this year, you will work from your VM and connect to the servers in the CTF Network using Netbird. The scoreboard will be available the day of the event so teams can sign up on Friday, Oct. 24th, starting at 9 am.

Appendix

Doing Check Sums on downloaded files:

After downloading the following files, you will need to do a check sum on the file to ensure it is exactly as the one on the server. To do that, select one of the following to run the checksums:

Check Sums (Windows):

- File Checksum & Integrity Check on Windows 10 - File Security [Hash SHA-1/256/384/512/MD5] - https://www.youtube.com/watch?v=UrHhsF1q3rU
- Verifying a SHA Checksum on Windows 10 - https://www.youtube.com/watch?v=6Xpmku3kwjo
- Use the following command for checking the sums on windows: `certutil -hashfile "filename.zip" sha256`

Check Sums (MacOS):

Verifying a SHA Checksum on a Mac is the same as the Linux Commands below due to their similar nature.

Check Sums (Linux):

```
echo "sha256 hash line" | shasum -a 256 --check

Example:
echo "6a9faee5c0a2573598704a09864d6072a0685269707c186dfc8ebde4551ee5c3
VMware-Fusion-13.6.1-24319021_universal.dmg" | shasum -a 256 --check
```

```
Result:
VMware-Fusion-13.6.1-24319021_universal.dmg: OK
```

Alternatives ways to do it on the CommandLine:

```
shasum -a 256 SecureWV-PlayerVM.7z

sha256sum VMware-Fusion-13.6.1-24319021_universal.dmg
6a9faee5c0a2573598704a09864d6072a0685269707c186dfc8ebde4551ee5c3  VMware-
Fusion-13.6.1-24319021_universal.dmg

Then you will need to compare with the number from the website.
```