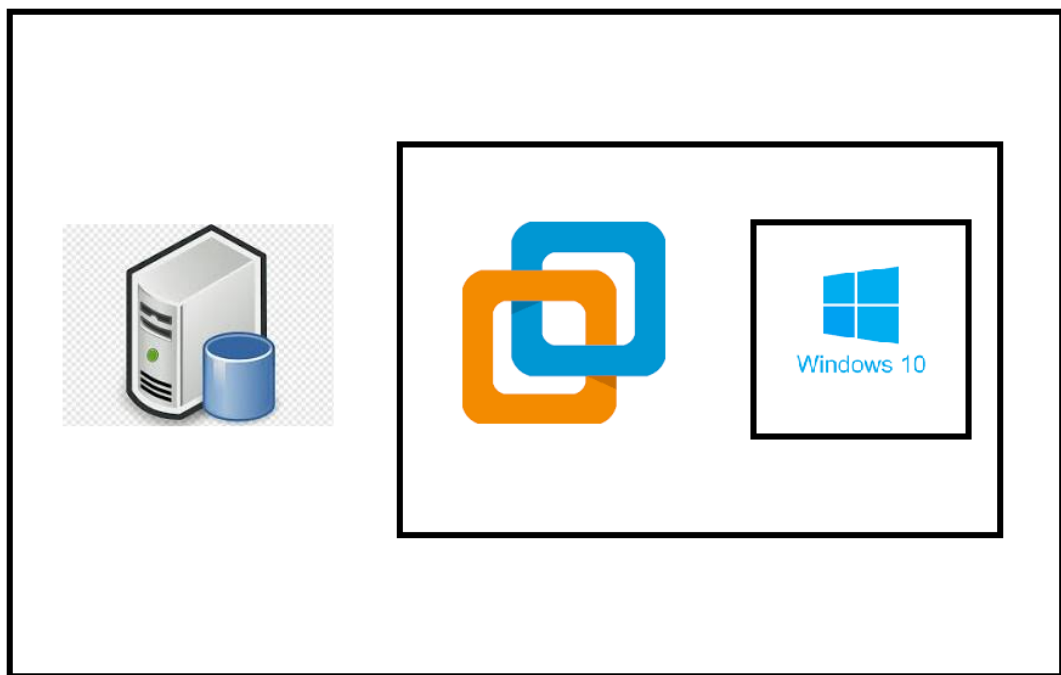


Step-by-Step Guide to Setting up a Cybersecurity Home Lab



Boni Yeamin

Cyber Security Engineer
Akij Group,
Bangladesh

CONTENT

- 1. Hardware Requirements**
- 2. Software Requirements**
- 3. Download VMware Workstation**
- 4. Choose an Operating System**
- 5. Create a Secure Host**
- 6. Create a Custom Network**
- 7. VM Configuration**
- 8. Install Operating Systems**

Introduction:

In today's interconnected world, cybersecurity plays a pivotal role in safeguarding our digital assets, personal information, and critical infrastructures. The continuous evolution of cyber threats necessitates skilled cybersecurity professionals who can defend against and mitigate these risks effectively. A cybersecurity home lab offers an ideal environment for aspiring practitioners and enthusiasts to gain hands-on experience, sharpen their skills, and explore various security concepts in a safe and controlled setting.

Introduction to a Cybersecurity Home Lab:

A cybersecurity home lab is a simulated network and computing environment created within the confines of one's home. It typically involves setting up virtual machines using virtualization software such as VMware Workstation or VirtualBox. Each virtual machine represents a different system or network component, allowing users to emulate real-world scenarios and experiment with diverse cybersecurity tools and techniques. By building a home lab, individuals can learn to identify vulnerabilities, practice ethical hacking, and devise effective strategies to defend against cyber threats without compromising real-world systems.

Advantages of a Cybersecurity Home Lab:

Hands-On Learning: The home lab provides a hands-on learning experience, which is vital in the field of cybersecurity. Practical exercises reinforce theoretical knowledge and develop problem-solving skills.

Safe Environment: With a home lab, users can experiment and test various cybersecurity tools and methodologies without the fear of causing harm to real-world systems or violating any policies.

Customizable and Scalable: A cybersecurity home lab is highly customizable, allowing users to tailor the environment to their specific learning objectives. It can be expanded with additional virtual machines and tools as one's skills progress.

Continuous Practice: Regularly using the home lab fosters continuous learning and keeps practitioners updated with the latest cybersecurity trends, tactics, and procedures.

Real-World Scenarios: The lab allows users to simulate real-world security incidents, helping them to understand the complexities and challenges of cybersecurity in practical settings.

01. Hardware Requirements: Ensure that your computer meets the hardware requirements to run VMware Workstation smoothly. You'll need a decent CPU, sufficient RAM (at least 8GB or more), and ample storage space for creating virtual machines (VMs).

02. Software Requirements

Operating Systems: You will need various operating systems to set up different virtual machines in your lab. Common choices include:

Kali Linux: A specialized Linux distribution for penetration testing and ethical hacking.

Windows: For testing and practicing cybersecurity concepts on Microsoft systems.

Ubuntu: A versatile Linux distribution for general-purpose use and learning.

Virtualization Software: Choose a virtualization platform that allows you to run multiple VMs simultaneously. Popular options include:

VMware Workstation: A powerful virtualization software for Windows and Linux hosts.

VirtualBox: A free and open-source virtualization software with cross-platform support.

VMware Fusion (for macOS): If you're using macOS, VMware Fusion is a suitable alternative to VMware Workstation.

2.1 virtualization software:

❖ download vmware workstation 16

<https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html>

My Study plan E-learning Gmail YouTube Maps SOC

16

Commercial organization Workstation Player.

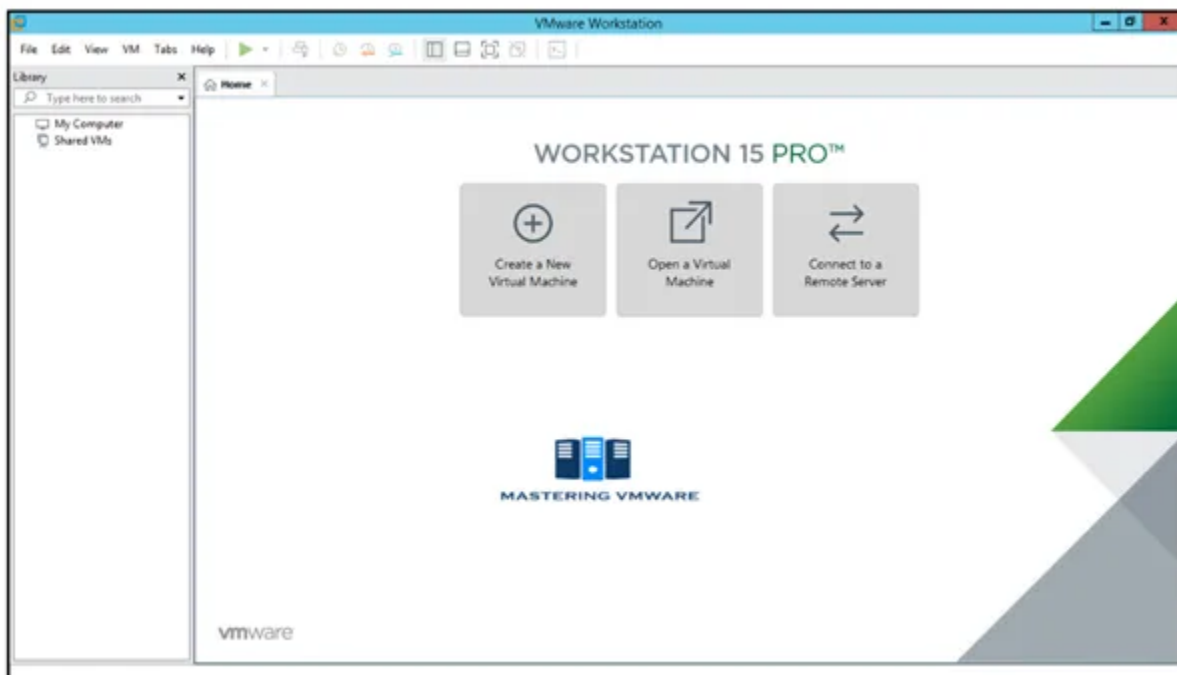
Need a more advanced Pro.

Try Workstation 16.0 Player for Windows

DOWNLOAD NOW >

Try Workstation

DOWNLOAD NOW >



03. Choose an Operating System:

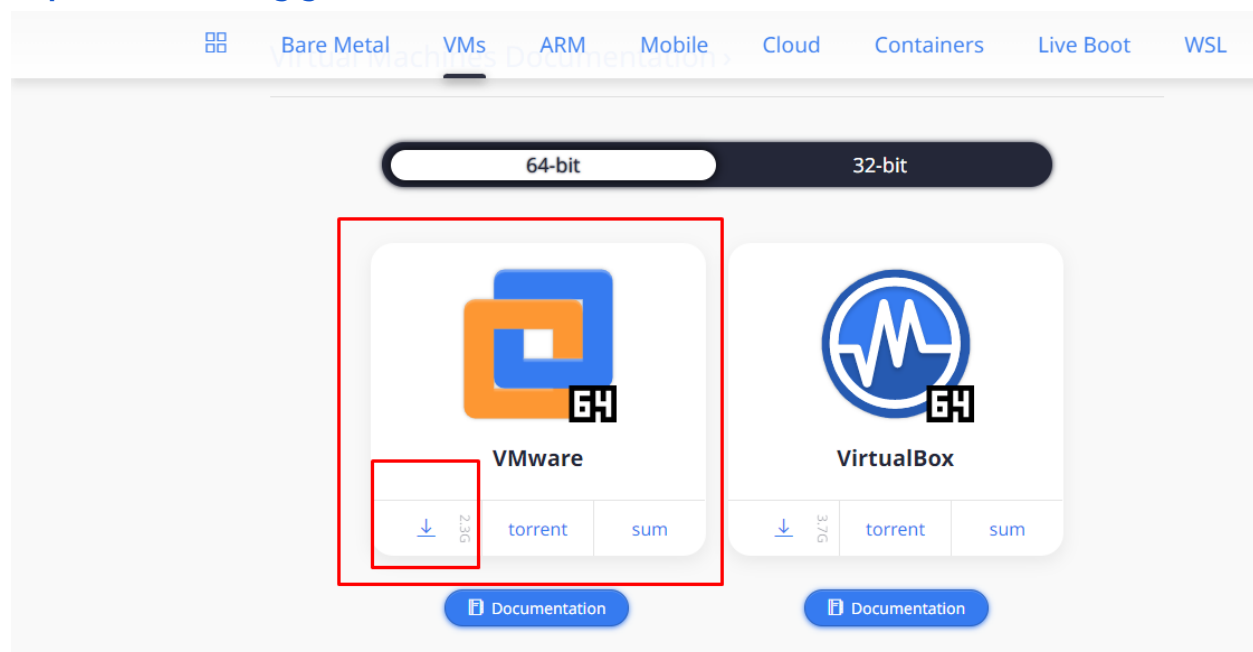
Distributed deployment:

2.

| S.I | Distributed OS | File format |
|-----|----------------|-------------|
| 01 | Kali Linux | Ova |
| 02 | Ubuntu | iso |
| 03 | centos 7 | iso |

2.1 Kali Linux Ova downloads

<https://www.kali.org/get-kali/#kali-virtual-machines>



2.2 :Ubuntu 20.04.4 LTS Downloads

<https://ubuntu.com/download/desktop>

CANONICAL We are hiring Products

ubuntu® Enterprise Developer Community Download Search Sign in

Downloads Overview Cloud IoT Raspberry Pi Server Desktop Xilinx Alternative downloads Ubuntu flavours

Download Ubuntu Desktop

Ubuntu 20.04.4 LTS


Download the latest LTS version of Ubuntu, for desktop PCs and laptops. LTS stands for long-term support — which means five years, until April 2025, of free security and maintenance updates, guaranteed.

[Download](#)

For other versions of Ubuntu Desktop including

2.3 :centos 7 download

<http://isoredirect.centos.org/altarch/7/isos/aarch64/>

 CentOS Download About Commu

CentOS Linux CentOS Stream

7-2009

| Architectures | Packages | Others |
|----------------------|----------|------------------------------|
| x86_64 | RPMs | Cloud Containers Vagrant |
| ARM64 (aarch64) | RPMs | Cloud Containers Vagrant |
| IBM Power BE (ppc64) | RPMs | Cloud Containers Vagrant |
| IBM Power (ppc64le) | RPMs | Cloud Containers Vagrant |

Home /

On this page

- > Cloud
- > Geogra
- > Source
- > Older
- > Export

In order to conserve the limited bandwidth available, ISO images are not downloadable from mirror.centos.org

The following mirrors should have the ISO images available:

<http://mirrors.bfsu.edu.cn/centos-altarch/7.9.2009/isos/aarch64/>
<http://mirrors.tuna.tsinghua.edu.cn/centos-altarch/7.9.2009/isos/aarch64/>
<http://mirror.xtom.com.hk/centos-altarch/7.9.2009/isos/aarch64/>
<http://mirror.worria.com/centos-altarch/7.9.2009/isos/aarch64/>
<http://mirror.aktkn.sg/centos-altarch/7.9.2009/isos/aarch64/>
<http://mirror.hoster.kz/centos-altarch/7.9.2009/isos/aarch64/>
<http://vpsmurah.jagoanhosting.com/centos-altarch/7.9.2009/isos/aarch64/>
<http://mirror.cepatcloud.id/centos-altarch/7.9.2009/isos/aarch64/>
<http://mirror.webmaster.my.id/centos-altarch/7.9.2009/isos/aarch64/>
<http://mirror.cloudweeb.com/centos-altarch/7.9.2009/isos/aarch64/>
<http://mirror.papua.go.id/centos-altarch/7.9.2009/isos/aarch64/>
<http://mirror.gi.co.id/centos-altarch/7.9.2009/isos/aarch64/>
<http://mirror.beon.co.id/centos-altarch/7.9.2009/isos/aarch64/>
<http://mirror.repository.id/centos-altarch/7.9.2009/isos/aarch64/>
<http://mirror.truenetwork.ru/centos-altarch/7.9.2009/isos/aarch64/>
<http://mirror.gouvernet.com.ru/centos-altarch/7.9.2009/isos/aarch64/>

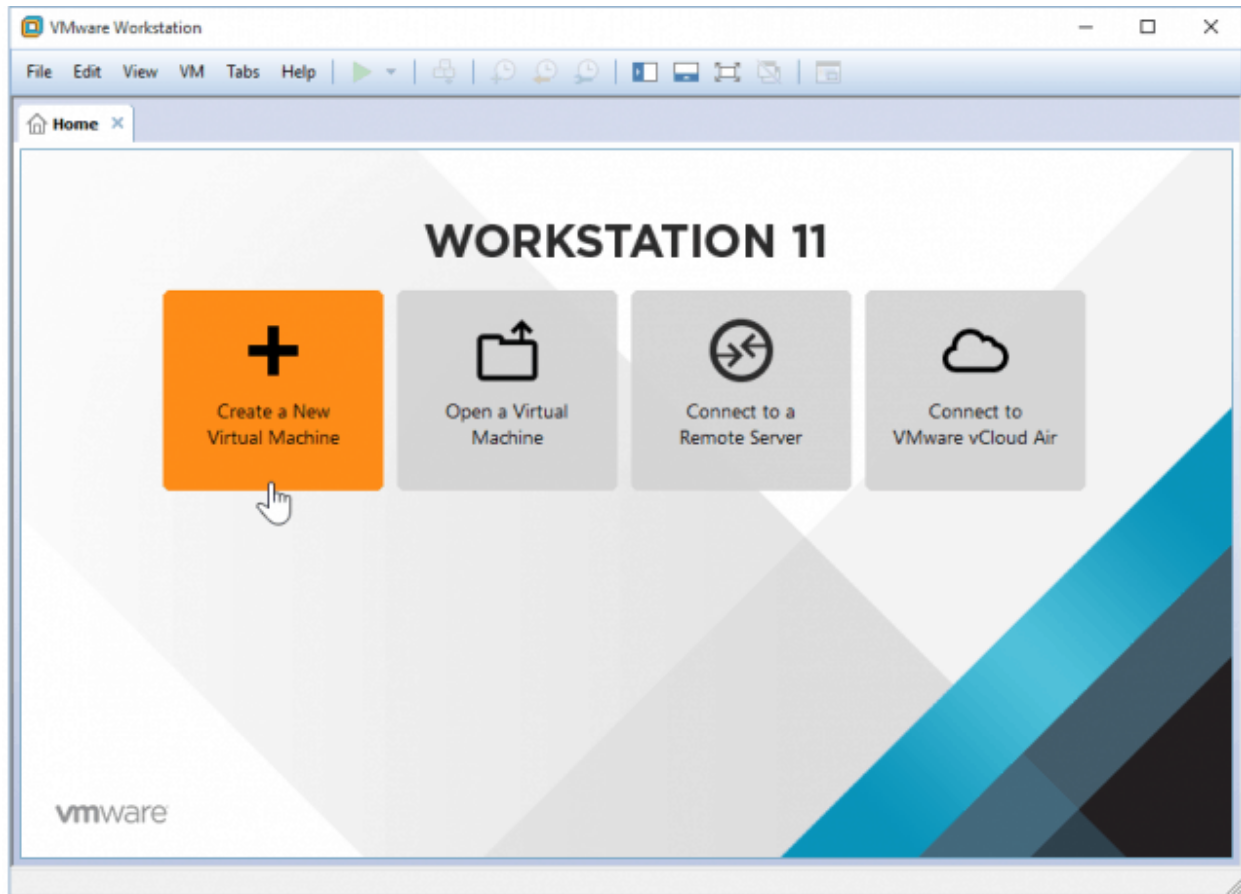
Create a Secure Host: Ensure that your host operating system is secure. Keep it up to date with the latest security patches, use a strong password, and consider setting up disk encryption if possible.

Create a Custom Network: Within VMware Workstation, create a custom network to isolate your lab environment from the internet and your home network. This prevents any accidental security breaches from impacting your home devices.

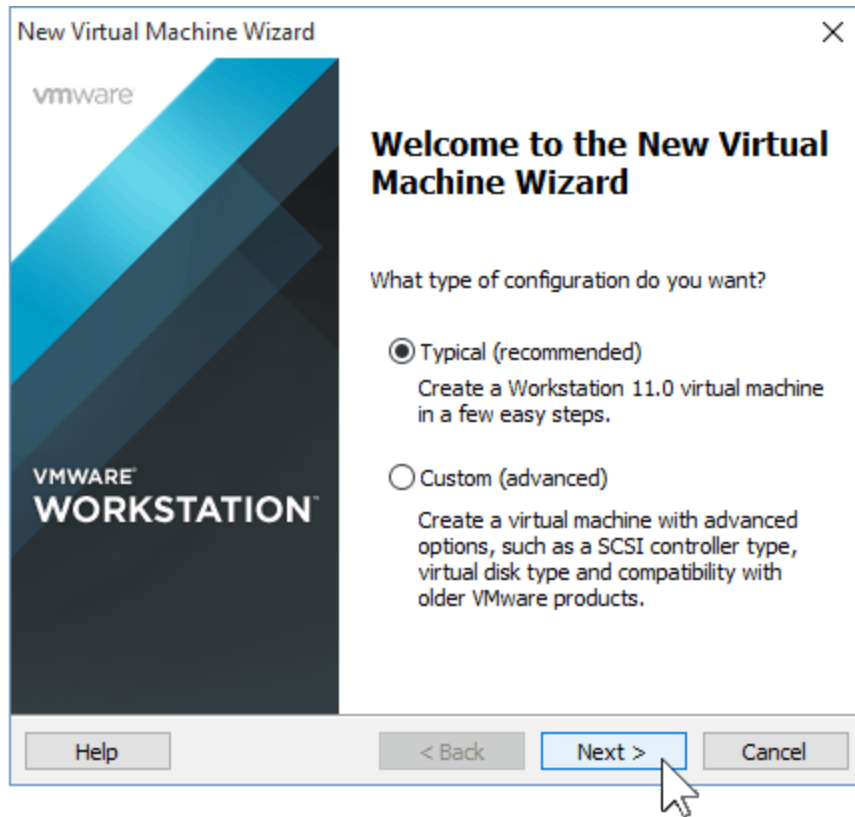
VM Configuration: For each VM you create, configure the settings appropriately. Allocate sufficient resources (CPU cores, RAM, and disk space) based on the requirements of the virtual machine's intended purpose.

Step 1: Set up a VMware Virtual Machine

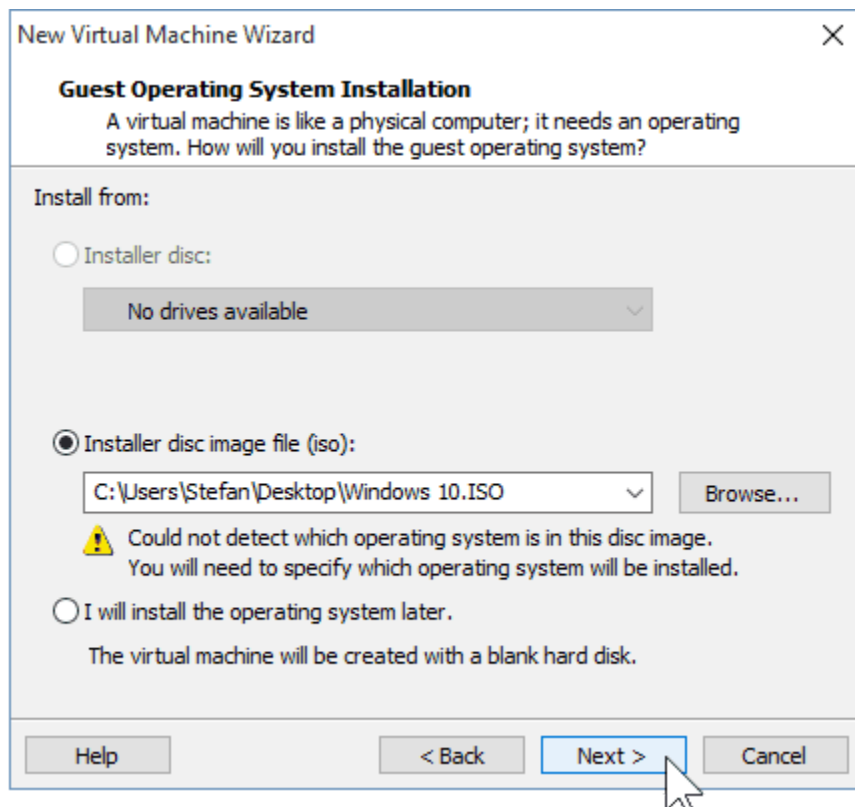
Start by opening VMware and selecting “**Create a New Virtual Machine**”



We'll go with a **Typical configuration**. If you're feeling fancy and really want to tweak the parameters, you can pick a Custom one, but we won't be going through a full Custom setup in this tutorial.

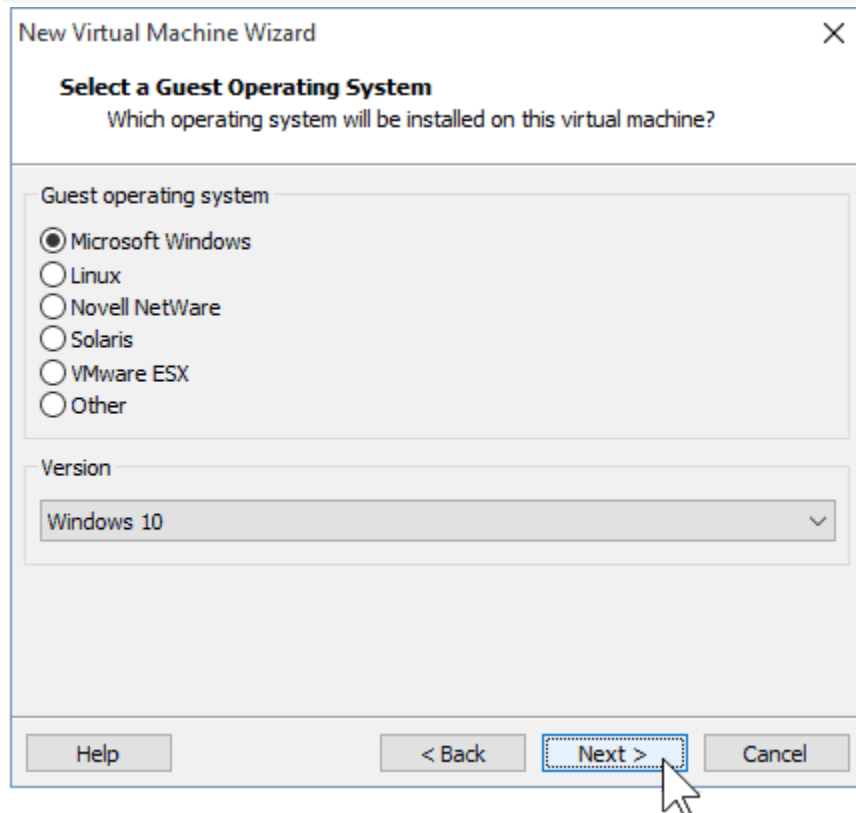


You will now need to show VMWare the **path to your Windows 10 ISO**.



If VMware doesn't automatically detect the OS from the ISO, you'll need to select it manually. You'll have the option to pick between **32 and 64-bit** versions of Windows OS.

Tip: If you don't have a lot of RAM and CPU to spare, I'd advise you to go with the 32-bit variant.



Choose a name for your Virtual Machine as well as **a location where it will be stored**. I stuck with the defaults here.

New Virtual Machine Wizard

Name the Virtual Machine
What name would you like to use for this virtual machine?

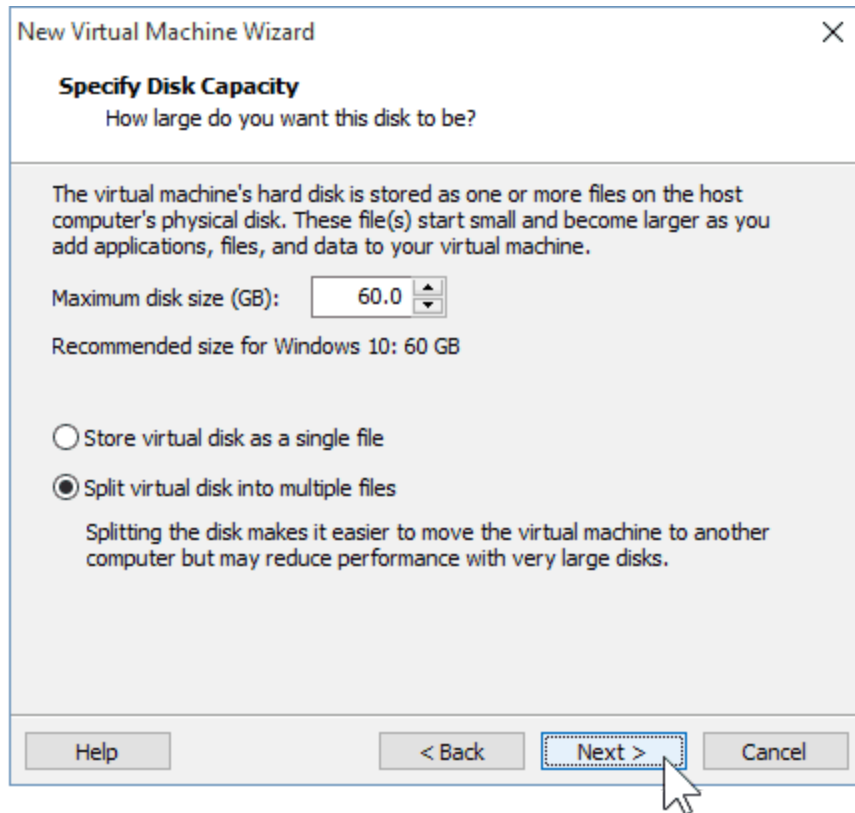
Virtual machine name:
Windows 10

Location:
C:\Users\Stefan\Documents\Virtual Machines\Windows 10 Browse...

The default location can be changed at Edit > Preferences.

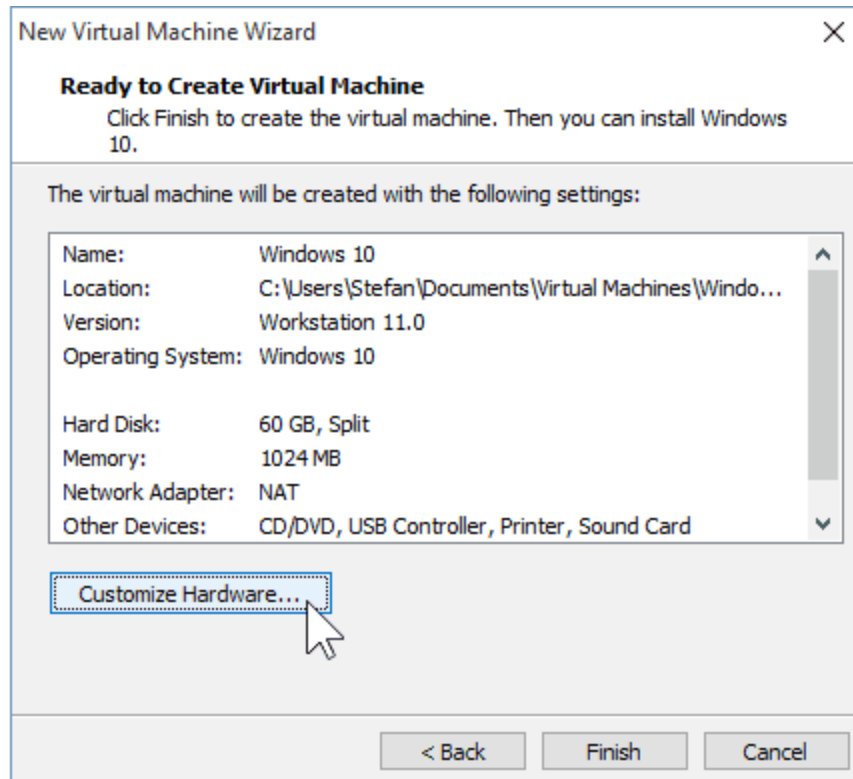
< Back Next > Cancel

Next up is **creating your virtual disk**. The advised **maximum limit is 60 GB, which is okay**. I advise you to stay with the “**Split virtual disk into multiple files**” option; otherwise, VMware will immediately allocate the space on your hard drive.

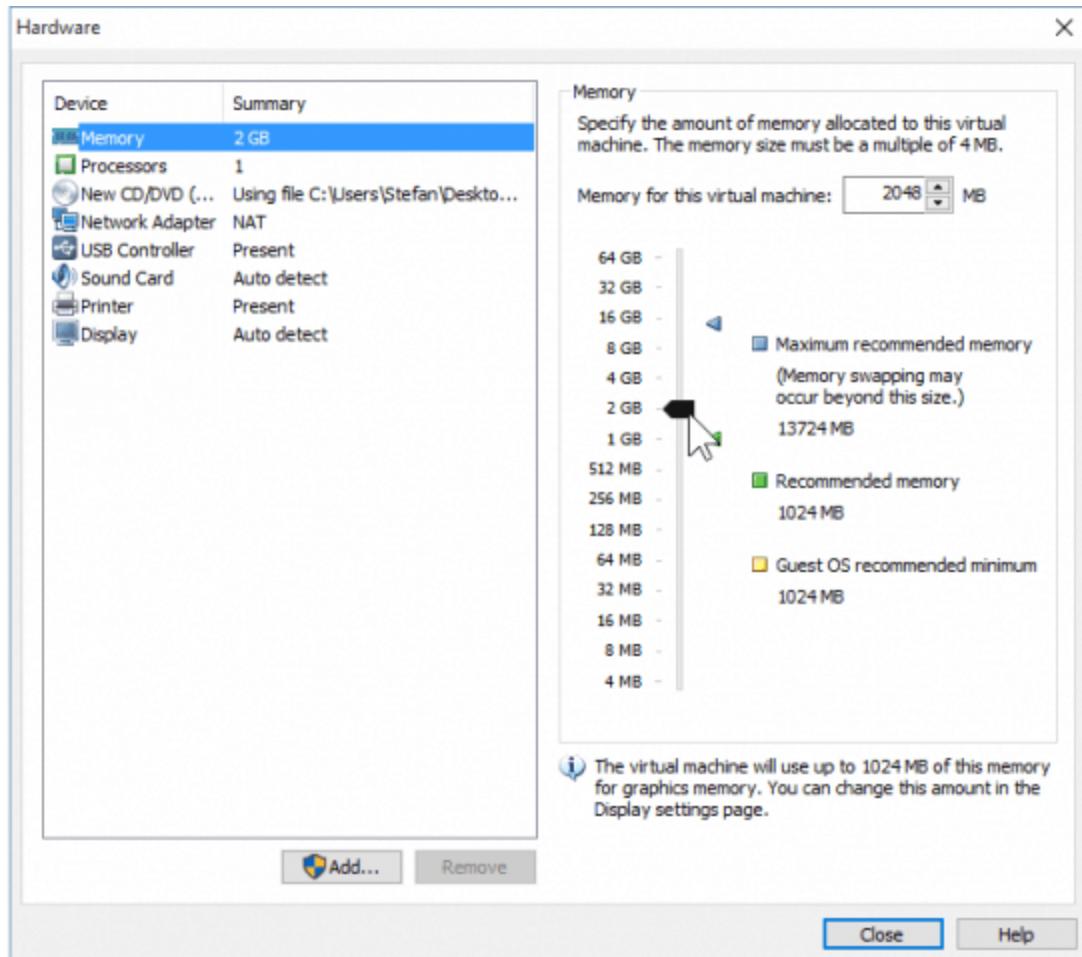


Step 2: Customizing the Virtual Machine Hardware (optional)

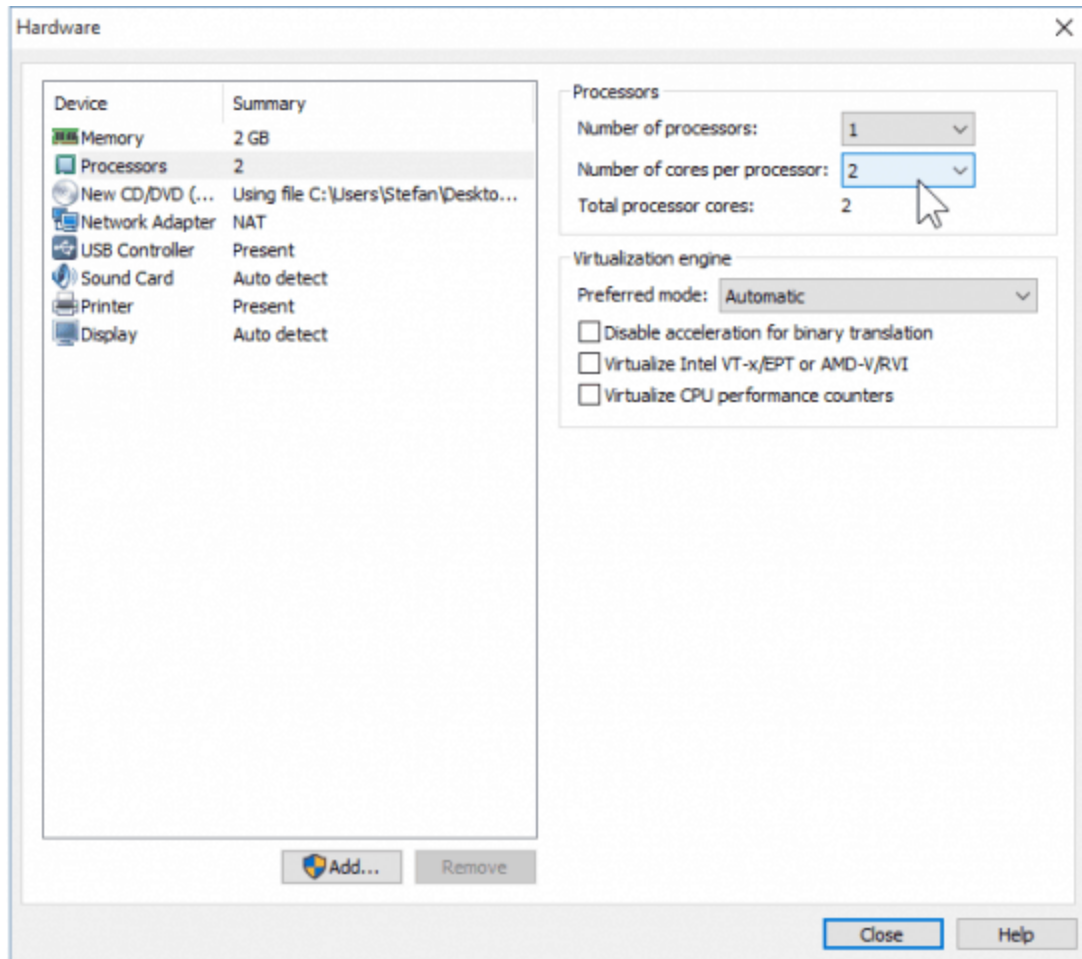
If you want to get fancy, **you can customize the hardware that your VM will use**. I'll go ahead and do this to show you some of the options you can change, but if you're okay with the VMware defaults, you can go ahead and select "Finish."



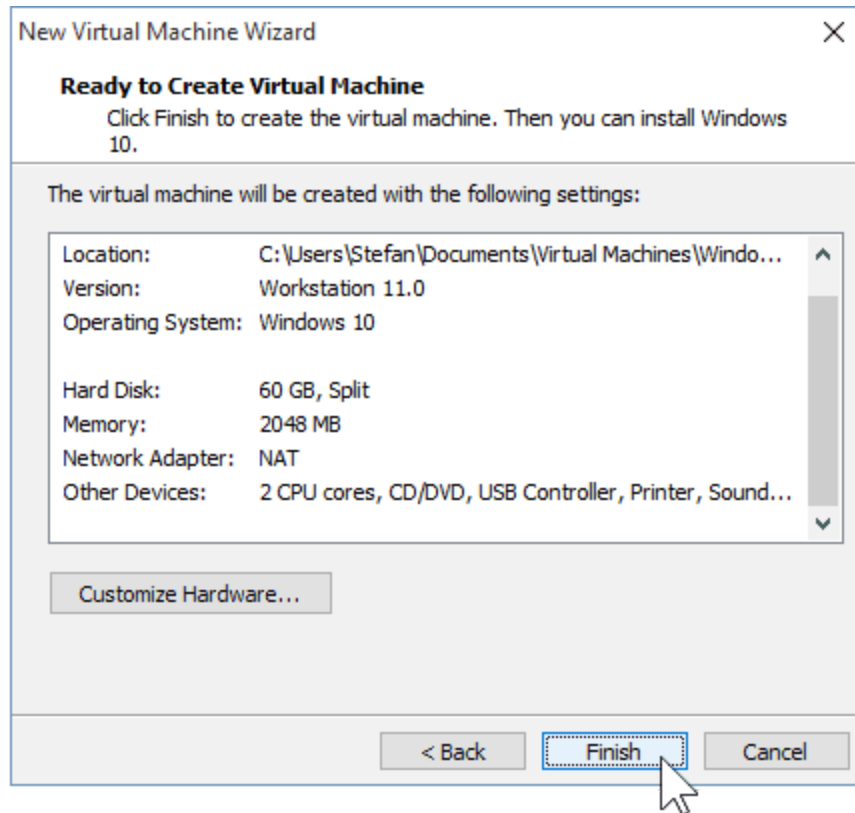
Selecting the Memory option, I can **increase or decrease the available RAM** for this VM. I'll go for 2GB instead of the default 1GB.



I'll also give my VM **some extra CPU power** by allowing it to use two cores instead of one.

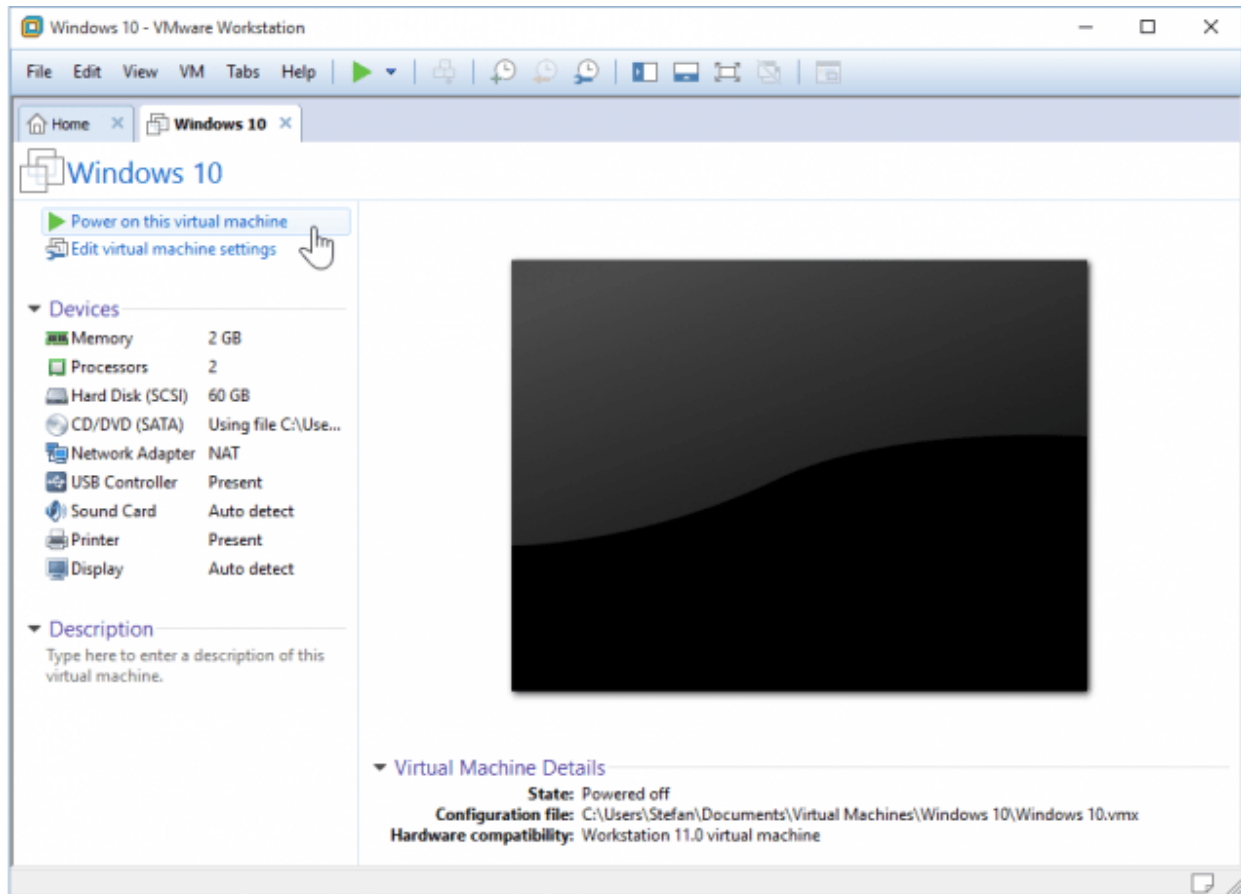


When you're done tweaking the hardware, you can close the windows and **click "Finish" on the New VM Wizard.**

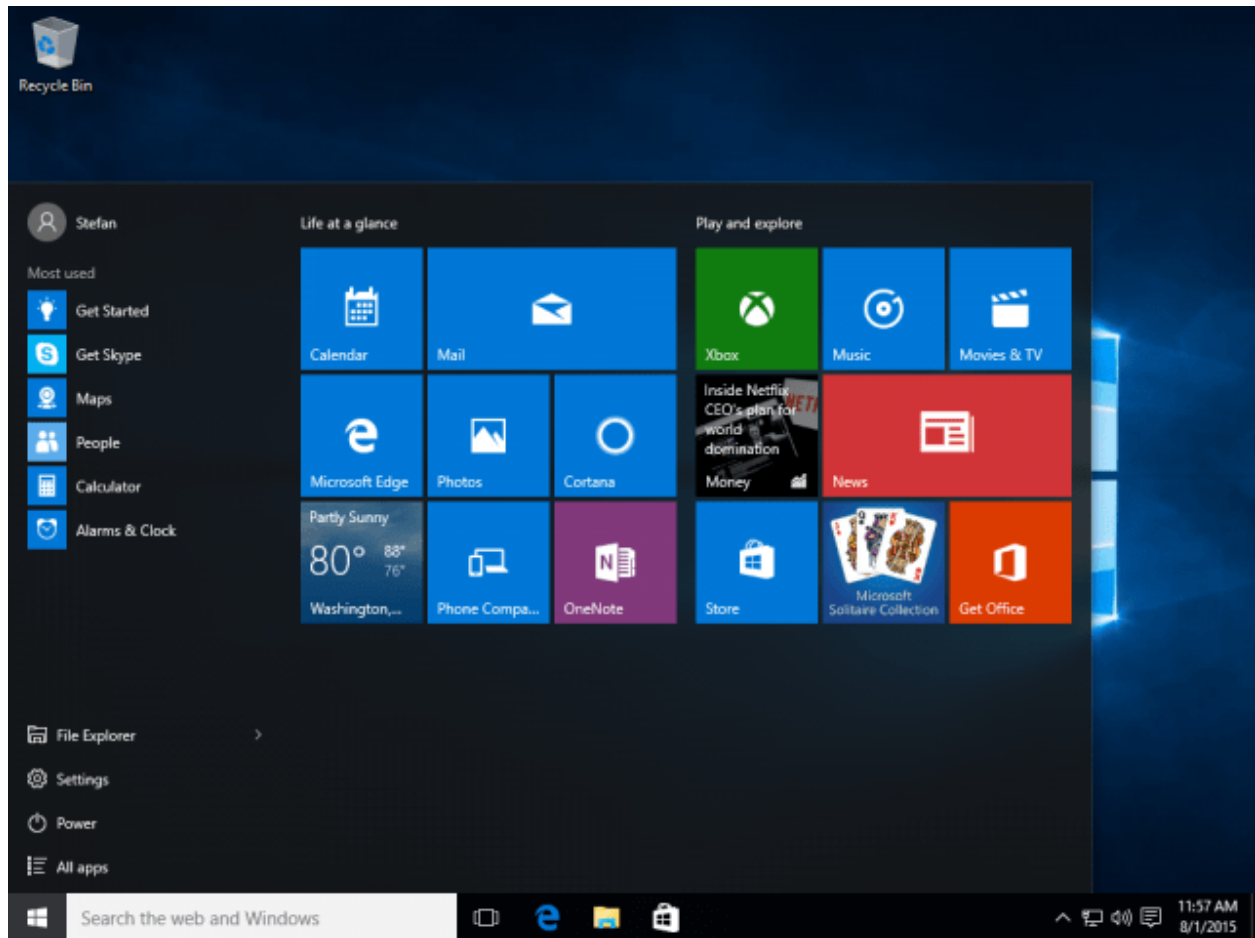


Step 3: Installing Windows 10

Once you're ready to begin installing, **click on "Power on this virtual machine."** From here on, the install should begin.



Installing Windows as a virtual machine is no different from making a clean install of Windows. If you're not sure how to perform one, check out our article:



Conclusion:

In conclusion, a cybersecurity home lab is an invaluable resource for anyone aspiring to excel in the field of cybersecurity. It serves as a safe and controlled environment where individuals can enhance their knowledge, hone their skills, and gain practical experience in defending against cyber threats. By leveraging virtualization software and a range of cybersecurity tools, enthusiasts can simulate real-world scenarios, conduct ethical hacking, and devise effective security strategies. The continuous learning and hands-on

practice offered by a home lab empowers cybersecurity professionals to stay ahead in this ever-evolving landscape of digital security, ultimately contributing to a safer and more secure digital world.

Reference:

01. <https://cyberwoxacademy.com/building-a-cybersecurity-homelab-for-detection-monitoring/>
02. <https://medium.com/analytics-vidhya/step-by-step-install-vmware-workstation-on-windows-1027abc3fadc>
03. <https://kb.vmware.com/s/article/2057907>

Boni Yeamin

Phone: 01914638653

Email: boniyeamin.cse@gmail.com

<https://www.linkedin.com/in/boniyeamin/>