

Welcome to Cybersecurity and Ethical hacking

VIRUS

CRACKER

INTRUDER

SPYWARE

PASSWORD

IDENTITY

CODE

UNSAFE

HACKER

THEFT

Module-2

Module 2-3: Environment Set up (Linux)



Installing Kali Linux



Basic Linux Commands



File & User Management



Kali Linux Overview



Environment Set up (Kali Linux)

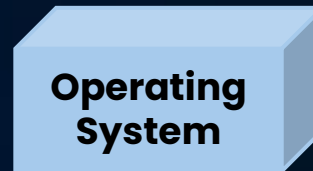


What is operating system ?

An Operating System (OS) is system software that acts as an interface between computer hardware and the user. It manages hardware resources and provides services for application programs.



User



Hardware



Key Functions of an Operating System:



Process Management

Handles creation, scheduling, and termination of processes



Memory Management

Allocates and manages RAM usage.



File System Management

Controls how data is stored and retrieved.



Device Management

Manages input/output devices like keyboard, mouse, and printer.



User Interface

Provides a way for users to interact (Command Line or Graphical UI).



Examples of Operating Systems:



Windows (e.g., Windows 10, 11)



Android (for mobile)



Linux (e.g., Ubuntu, Kali Linux)



iOS (for iPhones)



macOS

why Kali Linux is used for cybersecurity and ethical hacking



Pre-installed Hacking Tools

Kali comes with hundreds of tools for penetration testing, digital forensics, and reverse engineering.



Open Source and Free

It's completely free and open-source, making it accessible to anyone.



Official Support from Offensive Security

It is developed and maintained by Offensive Security, a trusted name in cybersecurity training.



Active Community Support

Large community and frequent updates ensure tools stay current and supported.



Customizable

Users can easily customize Kali to fit their specific needs (e.g., adding/removing tools, modifying the desktop environment).



Secure Development Environment

Designed with security professionals in mind, minimizing unnecessary features that could introduce vulnerabilities.



Install Kali Linux

1 Step 1: Download the Kali Linux VM (VMX Version)

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

KALI

GET KALI • BLOG • DOCUMENTATION • COMMUNITY • COURSES • DEVELOPERS • ABOUT •

Choose **your** Kali |

LIGHT ☒ DARK

Installer Images

- ☐ Direct access to hardware
- ☐ Customized Kali kernel
- ☐ No overhead

Single or multiple boot Kali, giving you complete control over the hardware access (perfect for in-built Wi-Fi and GPU), enabling the best performance.

☒ Recommended

Virtual Machines

- ☐ Snapshots functionality
- ☐ Isolated environment
- ☐ Customized Kali kernel
- ☐ Limited direct access to hardware
- ☐ Higher system requirements

VMware & VirtualBox pre-built images. Allowing for a Kali install without altering the host OS with additional features such as snapshots. Vagrant images for quick spin-up are also available.

☒ Recommended



Install Kali Linux

2 Step 2:


• [Installer](#) [Pre-built VMs](#) [ARM](#) [Mobile](#) [Cloud](#) [Containers](#) [Live](#) [WSL](#)

Pre-built Virtual Machines

Kali Linux [VMware](#) & [VirtualBox](#) images are available for users who prefer, or whose specific needs require a virtual machine installation.


These images have the default credentials "kali/kali".

[Virtual Machines Documentation >](#)




VMware

• 3.2G torrent docs sum




VirtualBox

• 3.2G torrent docs sum



Hyper-V

• 3.2G torrent docs sum



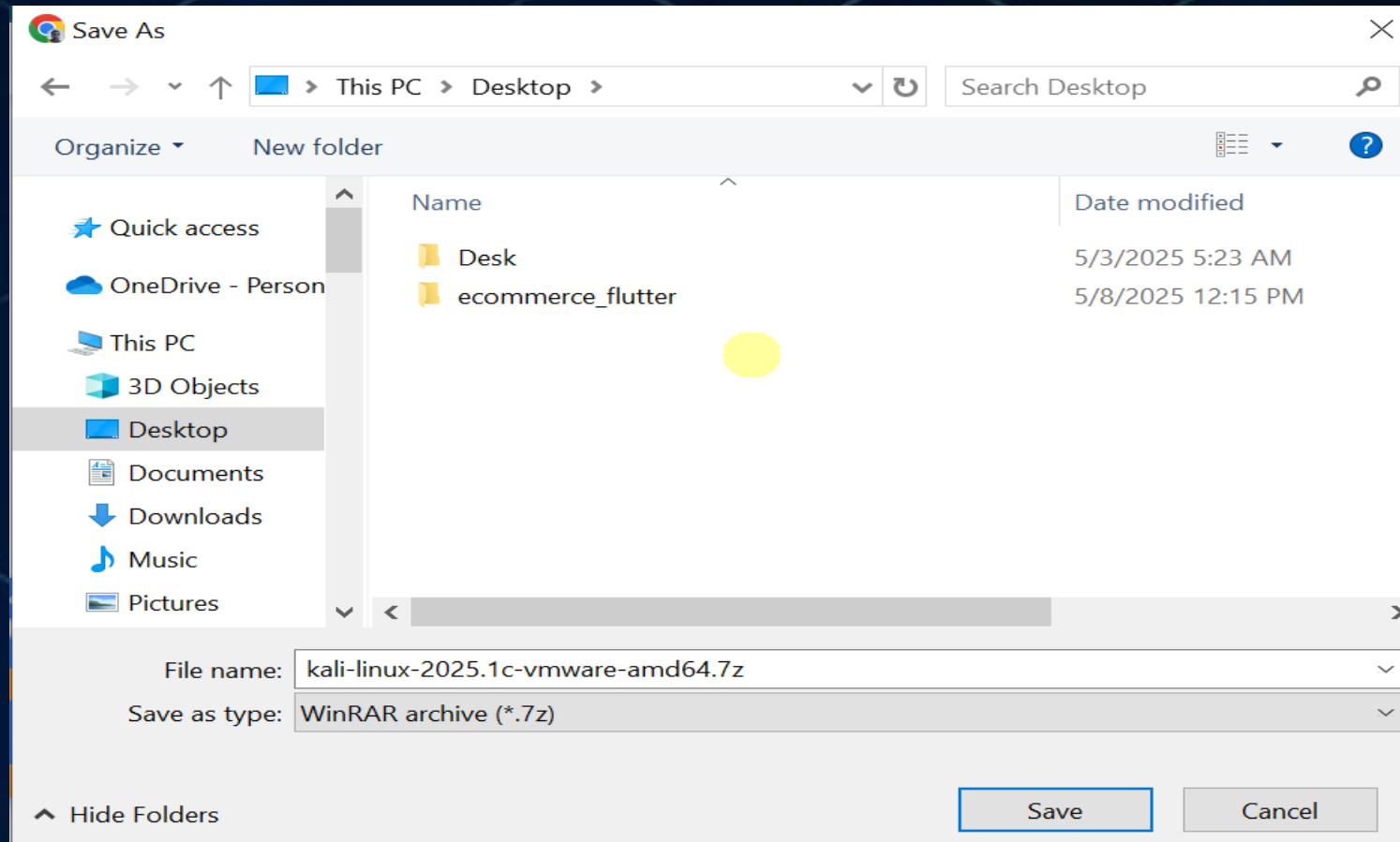
QEMU

• 3.2G torrent docs sum



Install Kali Linux

3 Step 3: Save this file in your device





Install Kali Linux

4 Step 4: Copy this file into your most available disk

5 Step 5: Extract this zip/7z file



Install VMware Workstation 17 on Windows



Step 6: Download VMware Workstation 17

Go to: <https://www.techspot.com/downloads/189-vmware-workstation-for-windows.html>



Scroll Down then click

TECHSPOT

TRENDING FEATURES REVIEWS DOWNLOADS THE BEST PRODUCT FINDER FORUMS

LOGIN

Continue to download »

different devices, platforms and clouds. IT professionals, developers and businesses rely on Workstation Pro every day to support their projects and customers. Workstation Pro makes it easy to run complex local virtual environments to simulate operating systems, platforms and clouds, all from the same desktop PC.

What are the different editions of VMware Workstation?

The VMware Workstation product line consists of two products: Workstation Pro and Workstation Player. Collectively they are referred to as 'VMware Workstation,' and when there are differences, they are called out.

What are the differences between Workstation Pro and Workstation Player?

Download options:

- Workstation Windows
- VMware Player Windows
- Workstation Linux
- VMware Player Linux
- Workstation Windows 17.6.2**
- Workstation Windows 17.6.1**
- Workstation Windows 17.5.2
- Workstation Linux 17.6.1

DOWNLOADS

- Google Chrome Browser 136.0.7103.93
Popular app in Browsers
- Chris-PC RAM Booster 7.25.0508
3 similar apps in Optimization
- Mozilla Firefox 138.0.1
13 similar apps in Browsers
- Visual Studio Code 1.100.0
12 similar apps in For Developers
- Chris-PC CPU Booster 3.25.0508
4 similar apps in Optimization

<https://www.techspot.com/downloads/downloadnow/189/?evp=f14a48a23bc560f5f8e81b8d83387b41&file=241>



Install VMware Workstation 17 on Windows




Step 7: Download VMware in your device (exe) file

TECHSPOT

LOGIN

TRENDING FEATURES REVIEWS DOWNLOADS THE BEST PRODUCT FINDER FORUMS

Now downloading...

 **VMware Workstation Pro 17.6.3**

Software for developers and system administrators for software development, testing and deployment. Learn [what's new](#) on this latest version. [Click here](#) if the download does not begin automatically.

MOST POPULAR

24 comments

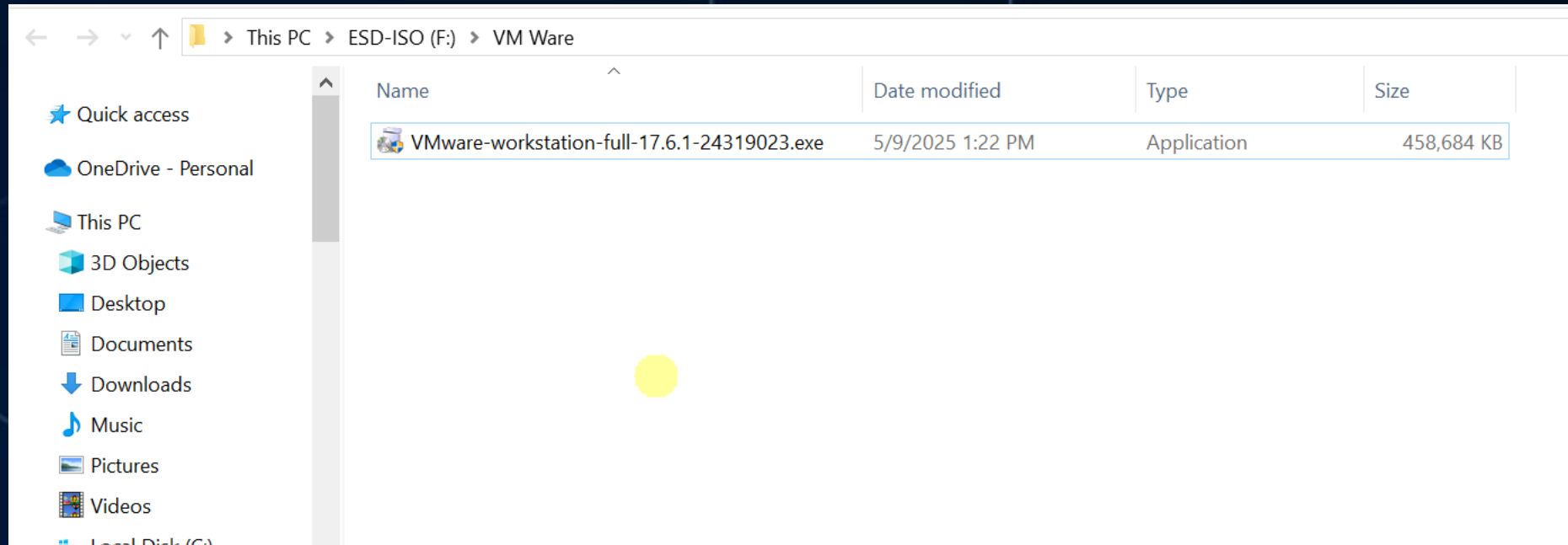
Nvidia's RTX 5060 Ti 8GB is Even Slower than the Intel Arc B580



Install VMware Workstation 17 on Windows



Step 8: Run VMware exe file

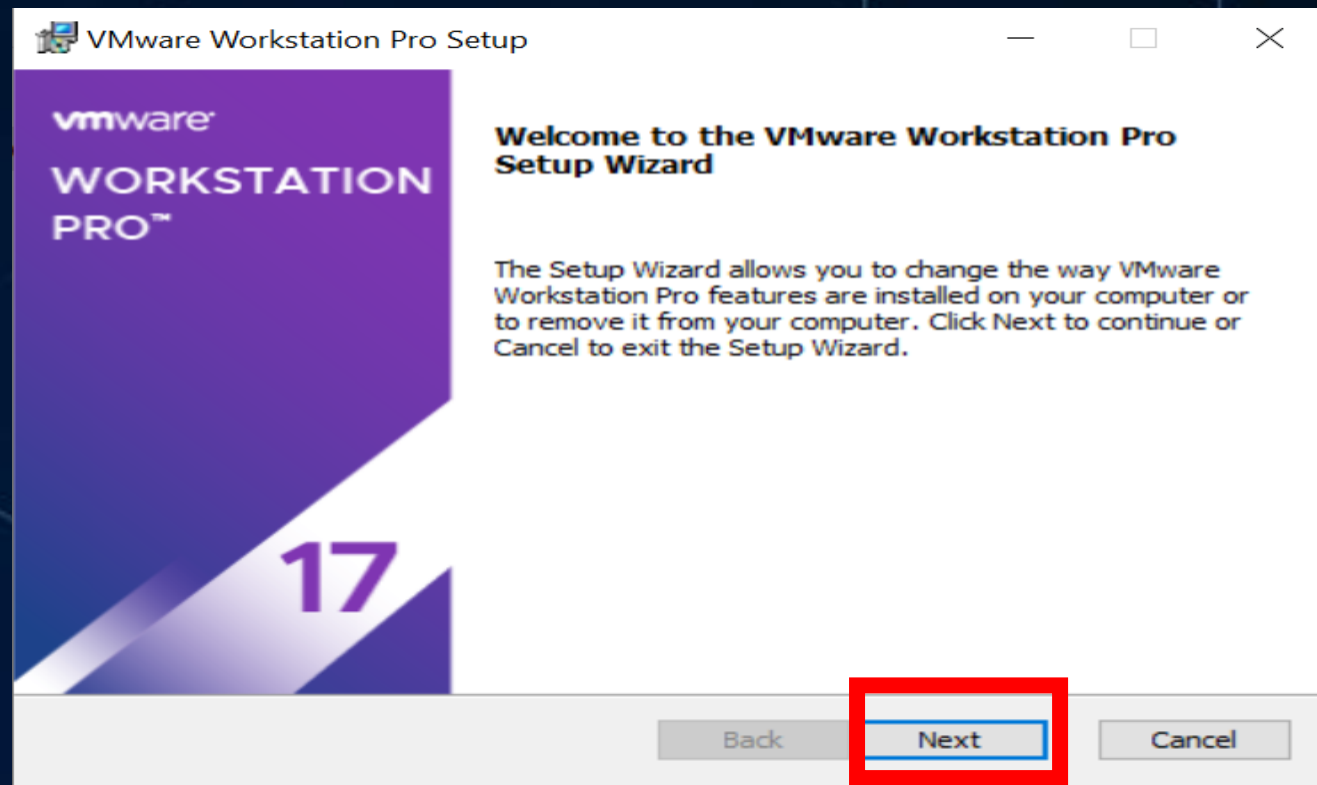




Install VMware Workstation 17 on Windows



Step 9: Click "Next"

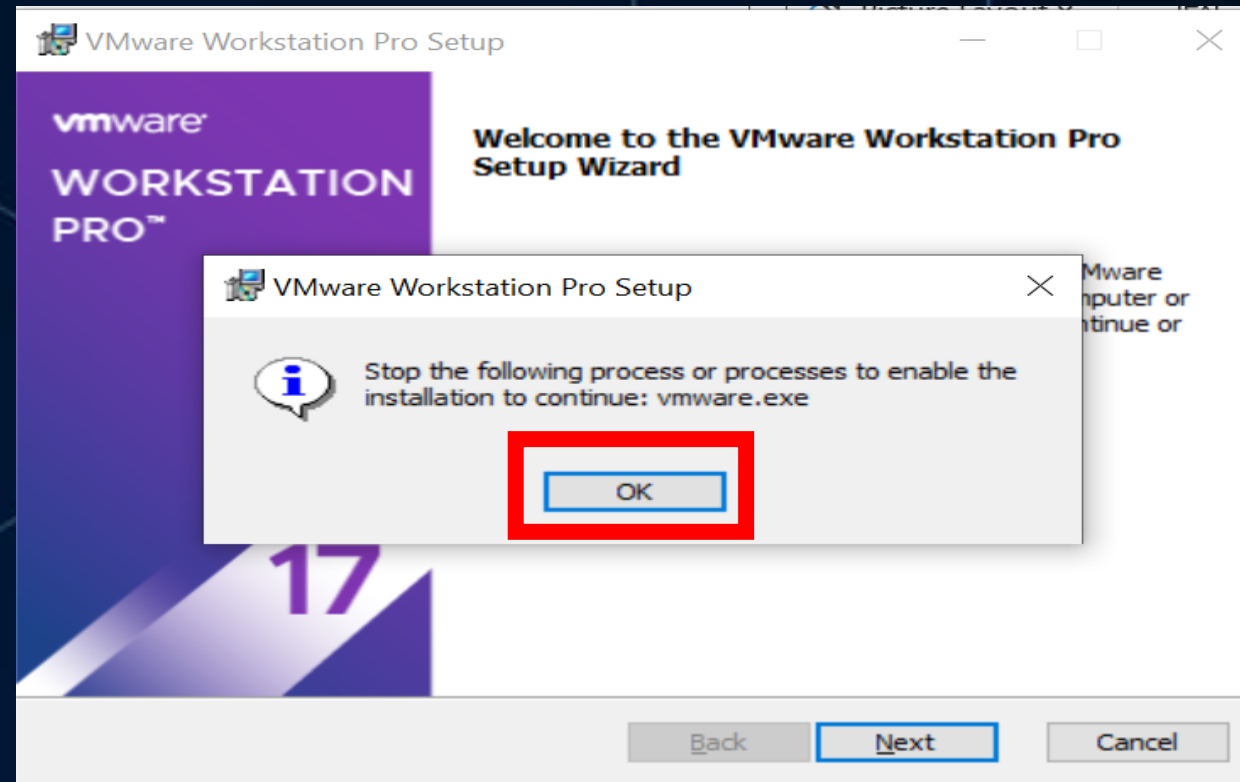




Install VMware Workstation 17 on Windows



Step 10: Click "Ok"

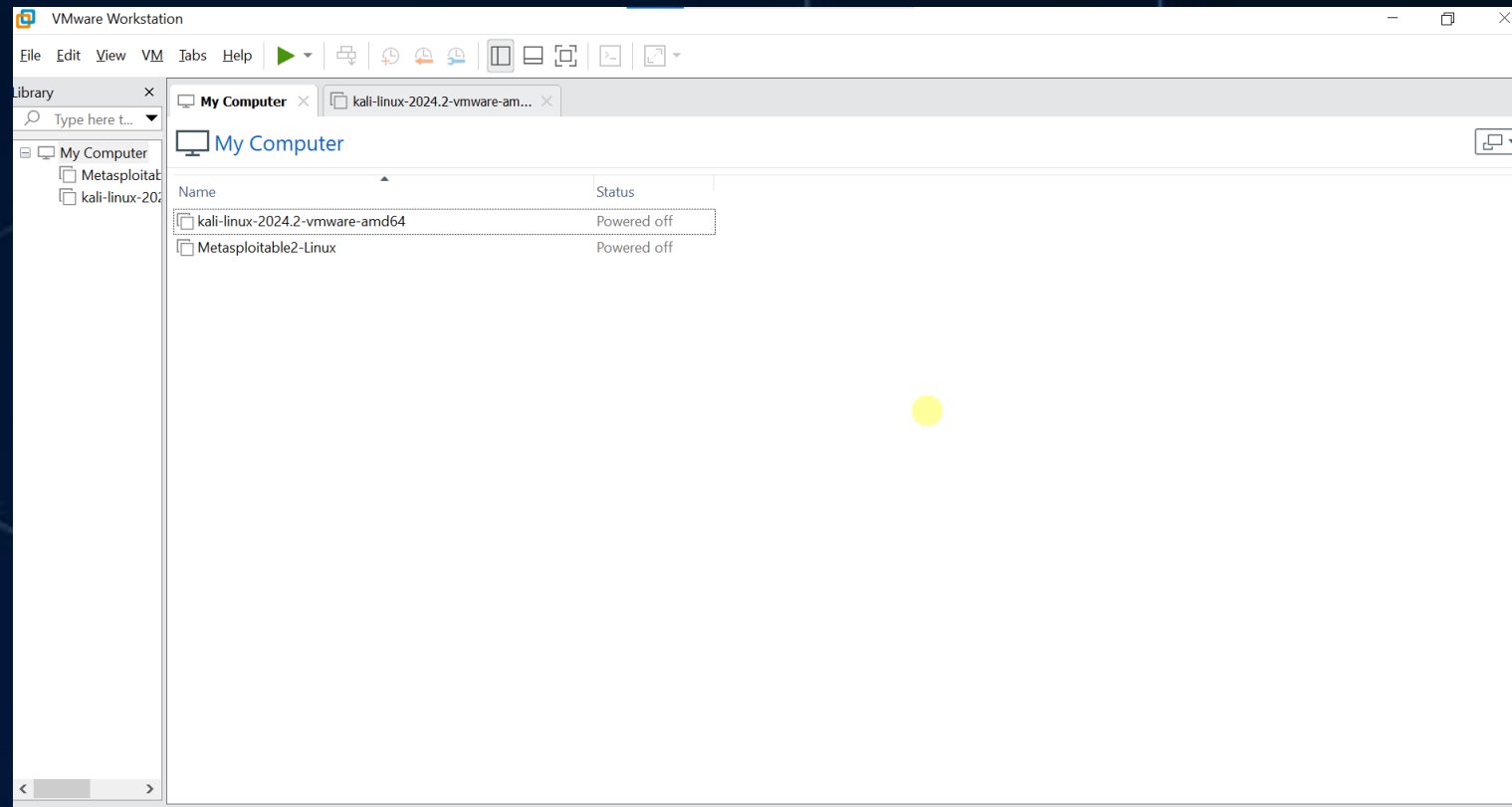




Install VMware Workstation 17 on Windows



Step 11: This interface will be showed

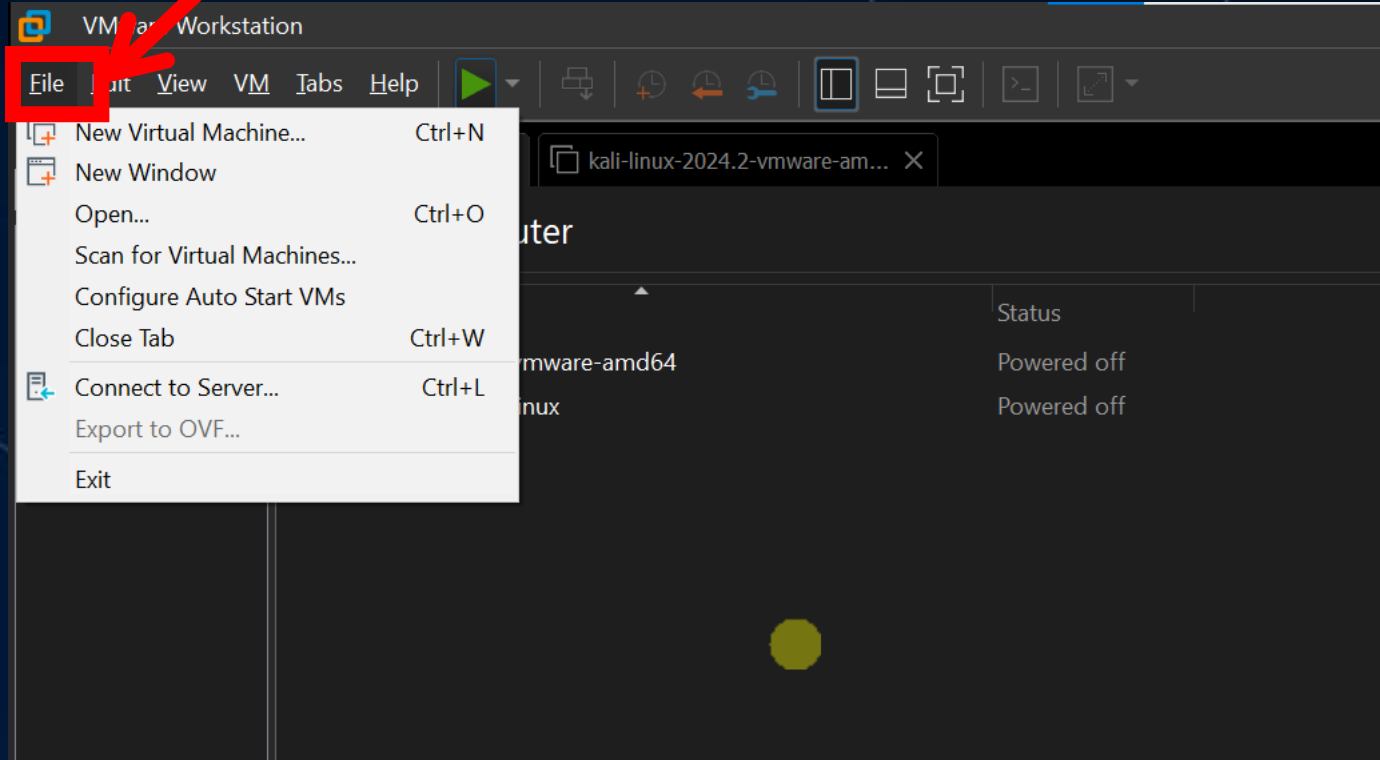




Install VMware Workstation 17 on Windows



Step 12: Go to "File"

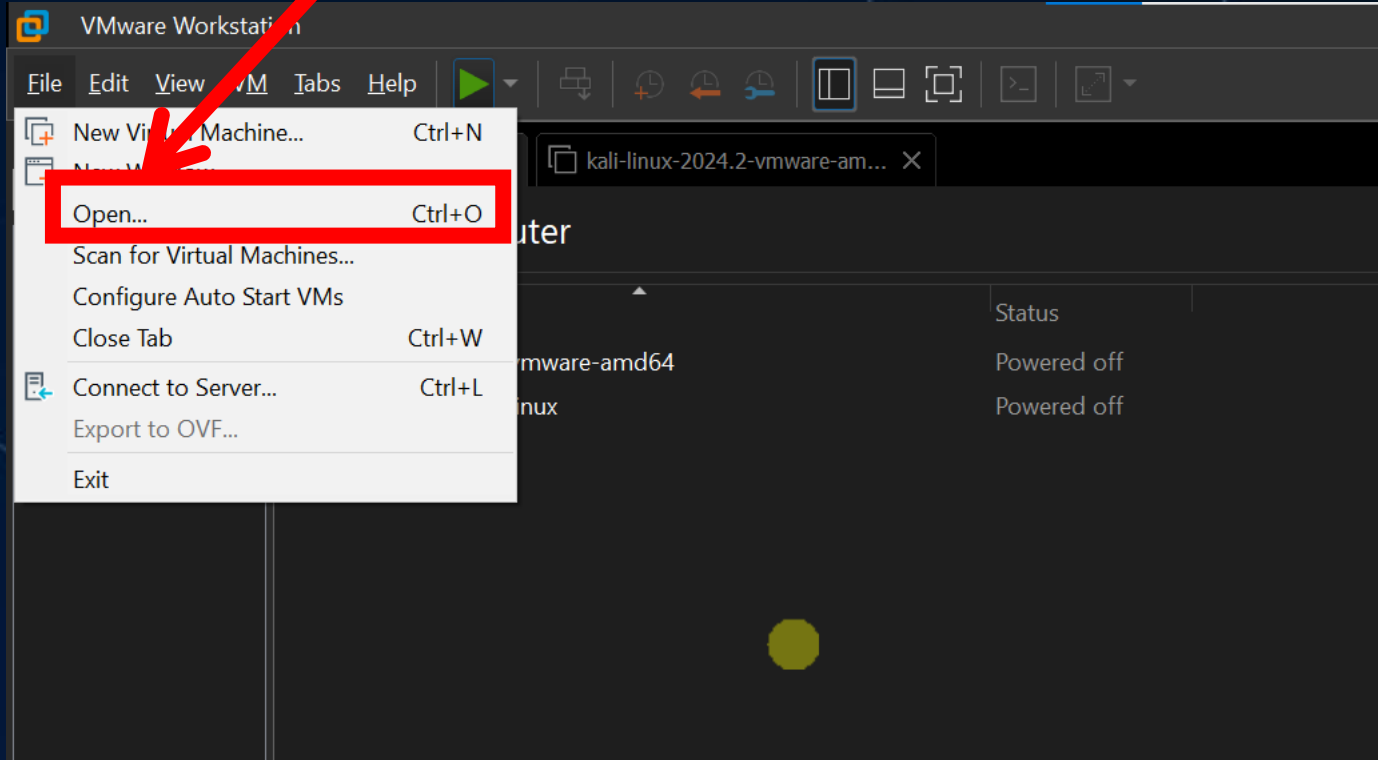




Install VMware Workstation 17 on Windows



Step 13: Click "Open"

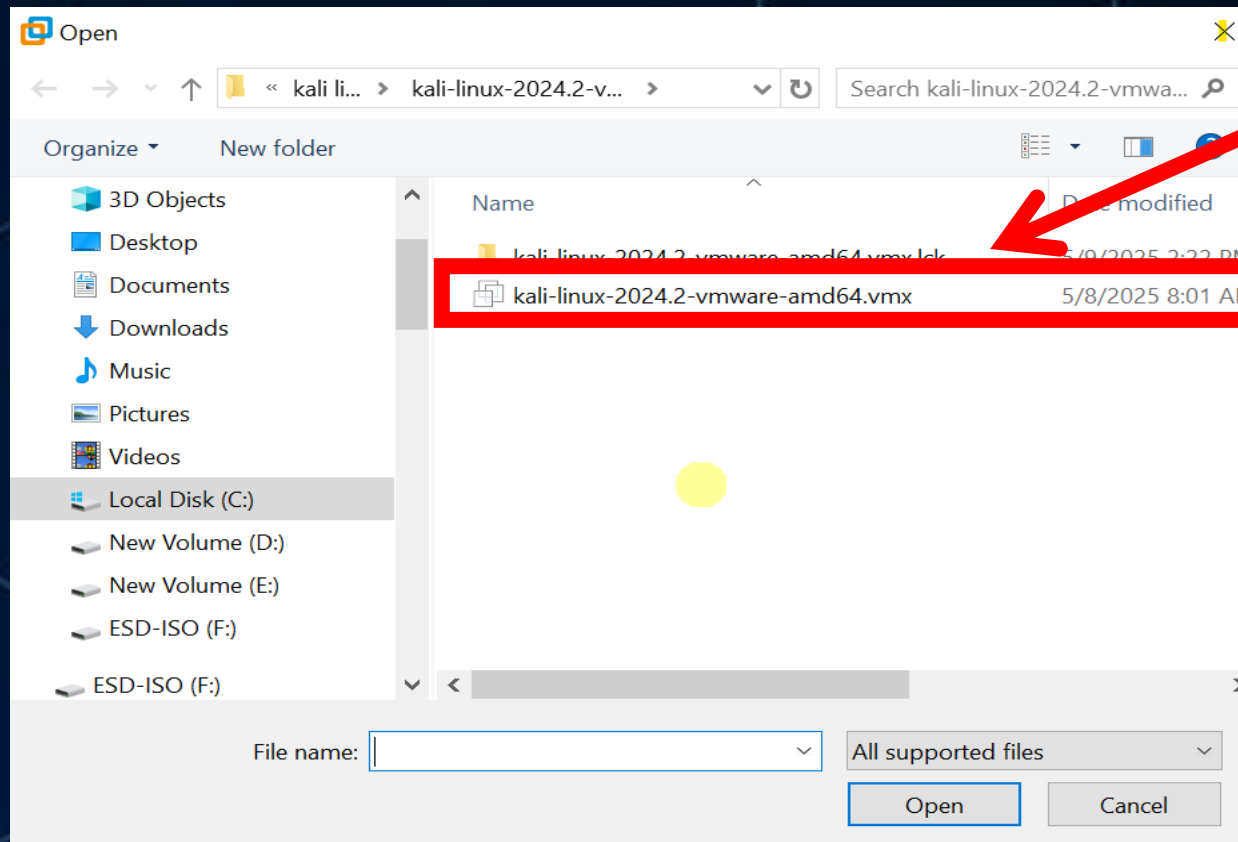




Install VMware Workstation 17 on Windows



Step 14: Go to your folder where Kali Linux is downloaded, and select “.vmx” file

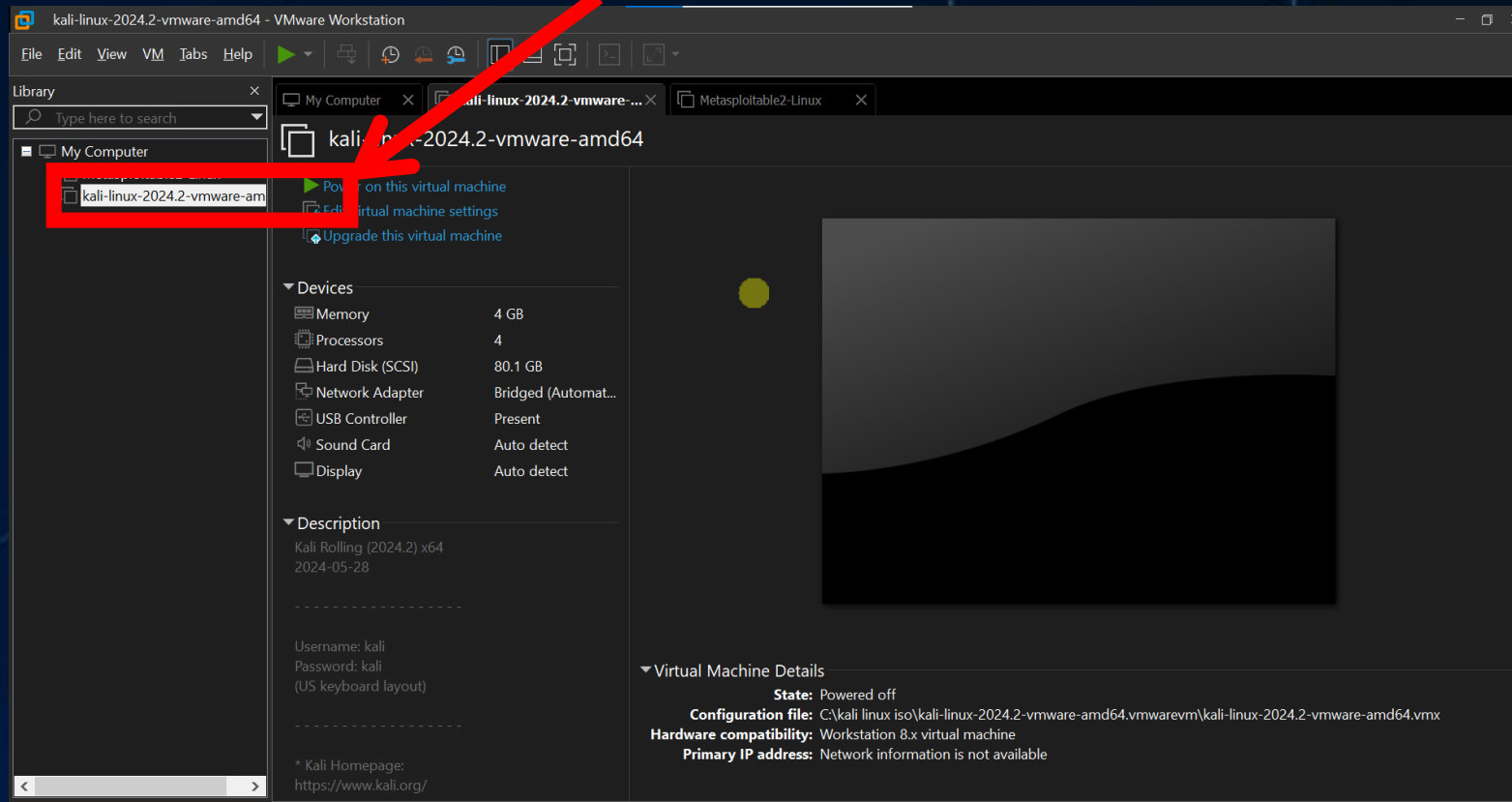




Install VMware Workstation 17 on Windows



Step 15: Click here

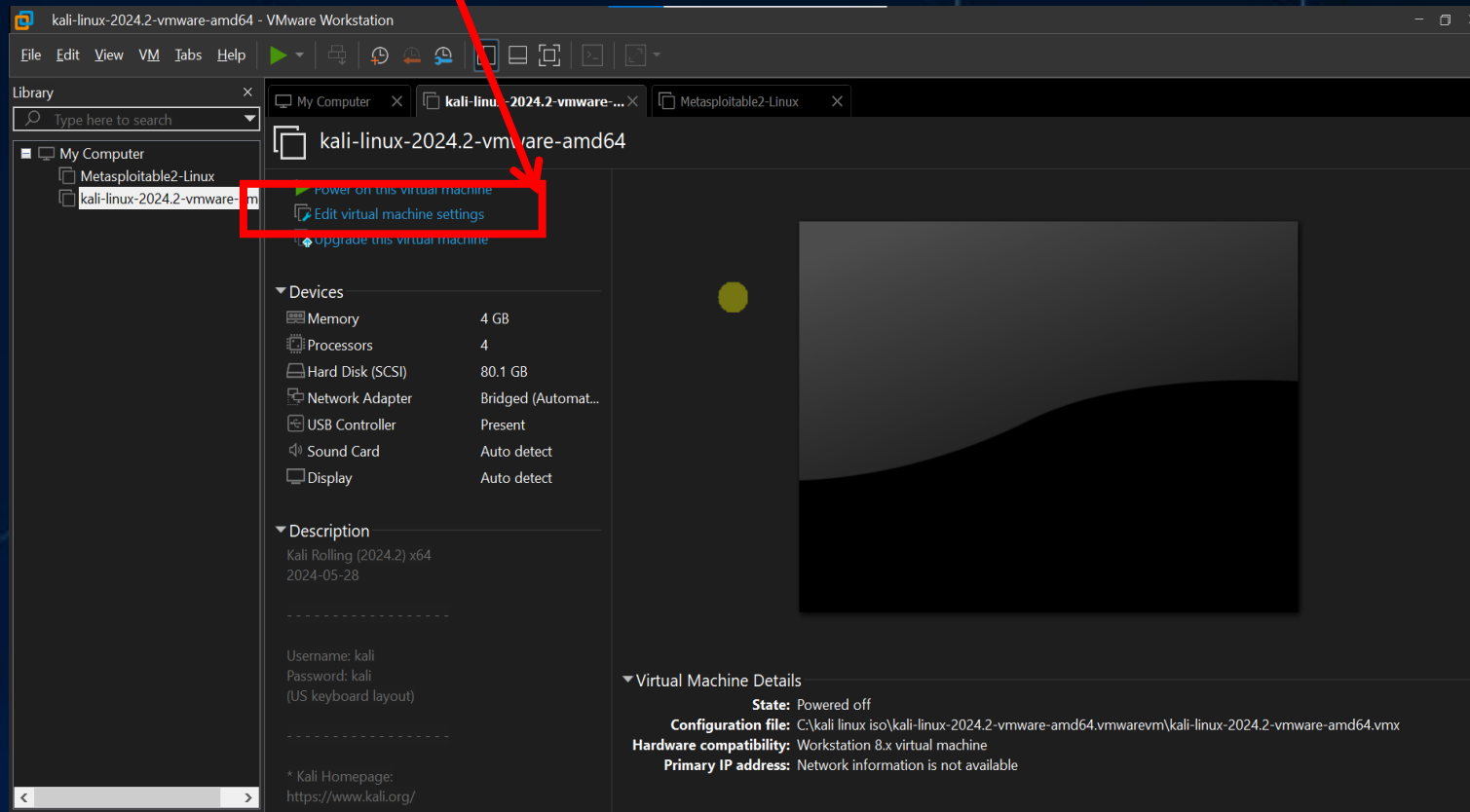




Install VMware Workstation 17 on Windows



Step 16: Click here

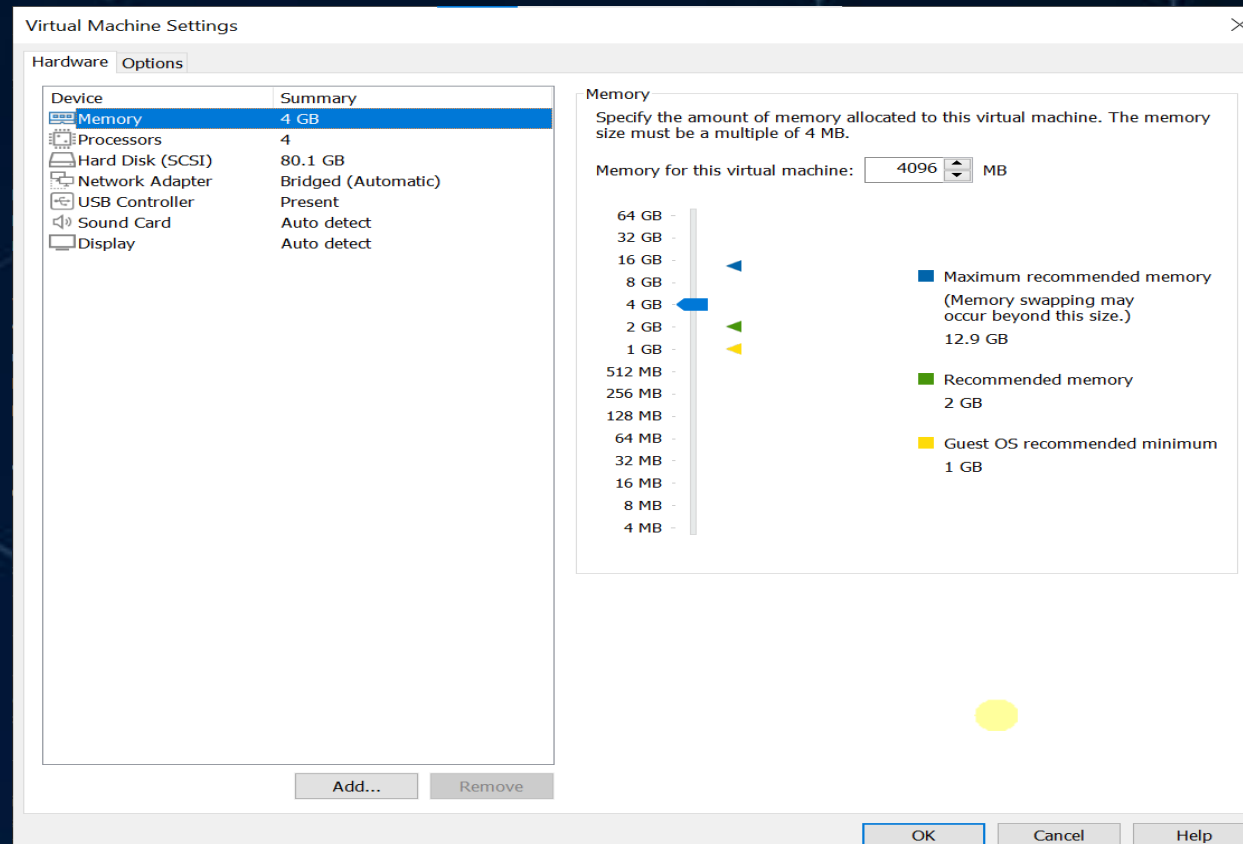




Install VMware Workstation 17 on Windows



Step 17: Set your memory

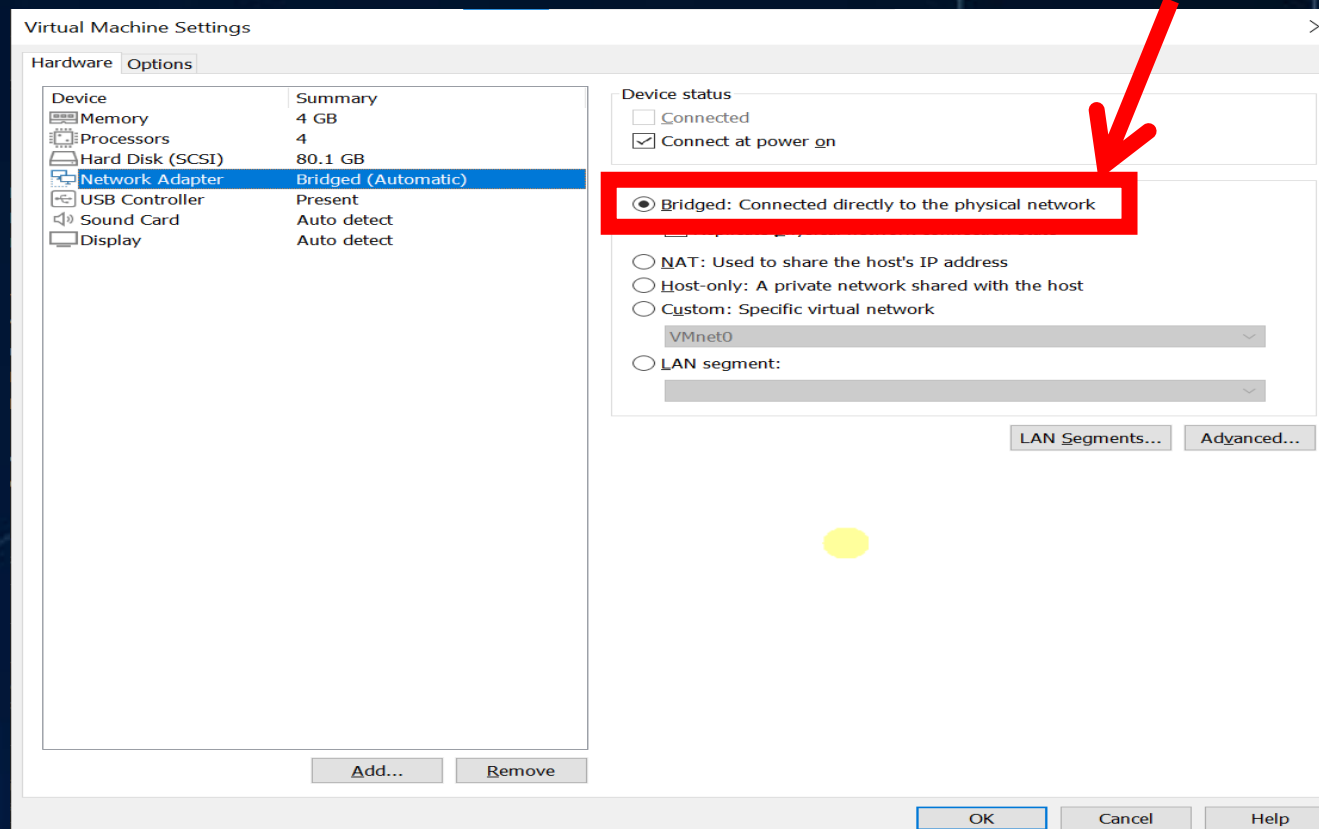




Install VMware Workstation 17 on Windows



Step 18: Check this "Bridge Connection"

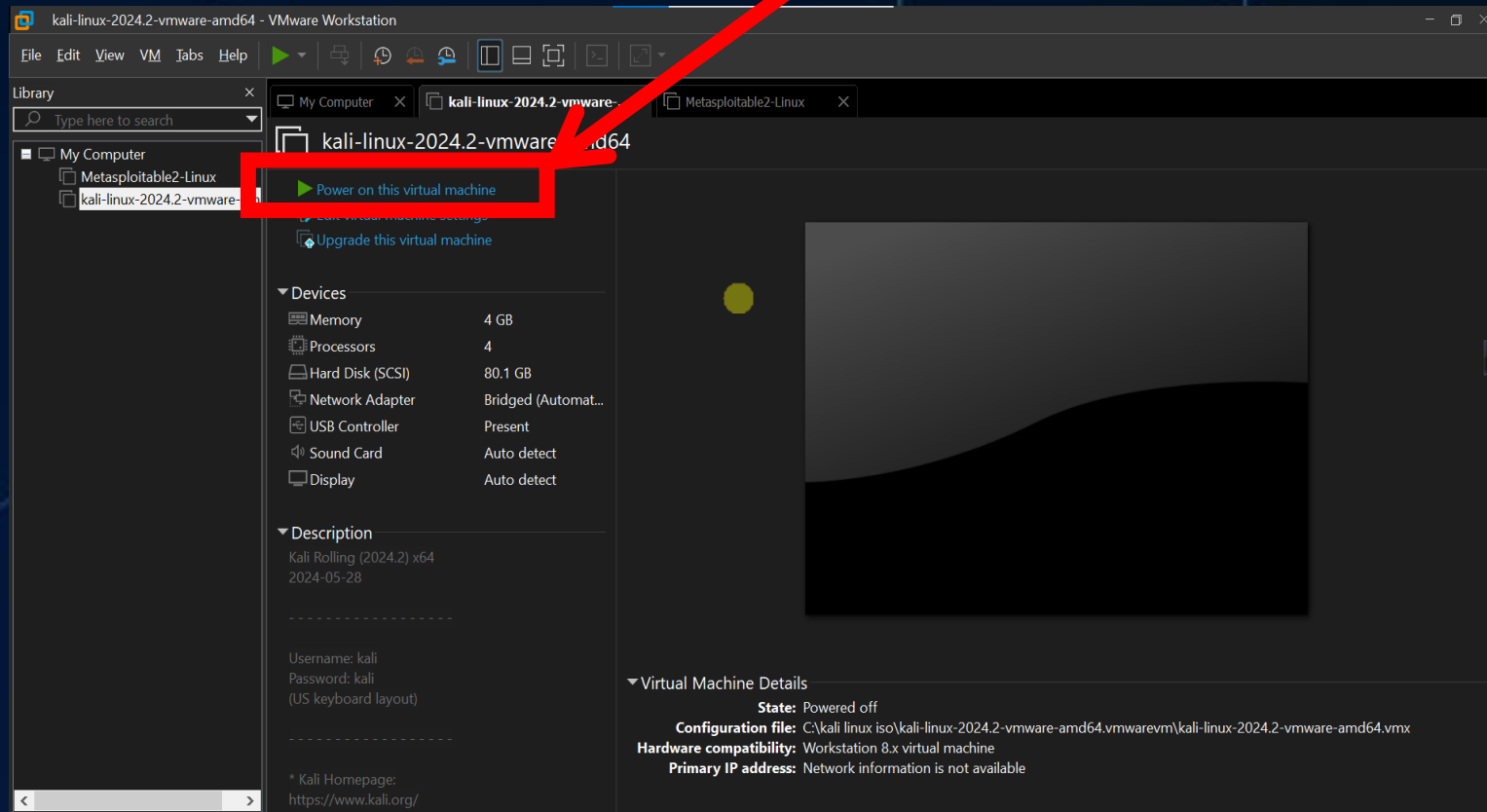




Install VMware Workstation 17 on Windows



Step 19: Run your Kali Machile





Install VMware Workstation 17 on Windows



Step 20: username : kali and password: kali





Essential Linux Commands



Important commands After installation

- `sudo apt update`
- `sudo apt upgrade`



Essential Linux Commands



Navigation & File Management

- **pwd** : Show current directory
 - ◆ ex: `pwd`
- **ls** : List directory contents
 - ◆ ex: `ls -la`
- **cd** : Change directory
 - ◆ ex: `cd /var/www/html`
- **cp** : Copy files or directories
 - ◆ ex: `cp file.txt /tmp/`
- **mv** : Move or rename files
 - ◆ ex: `mv old.txt new.txt`
- **rm** : Remove files or directories
 - ◆ ex: `rm -rf test/`
- **cat** : Show file contents
 - ◆ ex: `cat /etc/passwd`
- **nano / vim** : Edit text files
 - ◆ ex: `nano config.txt`
- **touch** : Create empty file
 - ◆ ex: `touch hello.txt`
- **mkdir** : Create a directory
 - ◆ ex: `mkdir myfolder`



Essential Linux Commands



User & Permission Management

- **whoami** : Show current user
 - ◆ ex: `whoami`
- **id** : Show user and group IDs
 - ◆ ex: `id`
- **sudo** : Run command as root
 - ◆ ex: `sudo apt update`
- **chmod** : Change file permissions
 - ◆ ex: `chmod 755 script.sh`
- **passwd** : Change password
 - ◆ ex: `passwd user`



Essential Linux Commands



Networking Commands

- **ping** : Check network connectivity
 - ◆ ex: `ping google.com`
- **ifconfig / ip a** : Show IP addresses
 - ◆ ex: `ifconfig`
- **netstat / ss** : Show open ports
 - ◆ ex: `ss -tuln`
- **nmap** : Scan network
 - ◆ ex: `nmap -sV 192.168.1.1`
- **curl / wget** : Download or fetch from web
 - ◆ ex: `curl http://example.com`
- **traceroute** : Trace network path
 - ◆ ex: `traceroute google.com`
- **dig / nslookup** : DNS lookup
 - ◆ ex: `dig example.com`



Essential Linux Commands



File Search & Manipulation

- **find** : Search files
 - ◆ ex: `find / -name "*.php"`
- **grep** : Search inside files
 - ◆ ex: `grep "admin" config.php`
- **locate** : Quickly find files
 - ◆ ex: `locate php.ini`
- **file** : Detect file type
 - ◆ ex: `file shell`
- **history** : View command history
 - ◆ ex: `history | grep nmap`



Essential Linux Commands



Privilege Escalation & Enumeration

- **sudo -l** : List sudo permissions
 - ◆ ex: `sudo -l`
- **ps aux** : Running processes
 - ◆ ex: `ps aux | grep apache`
- **uname -a** : Kernel/system info
 - ◆ ex: `uname -a`
- **env** : Show environment variables
 - ◆ ex: `env`



Essential Linux Commands

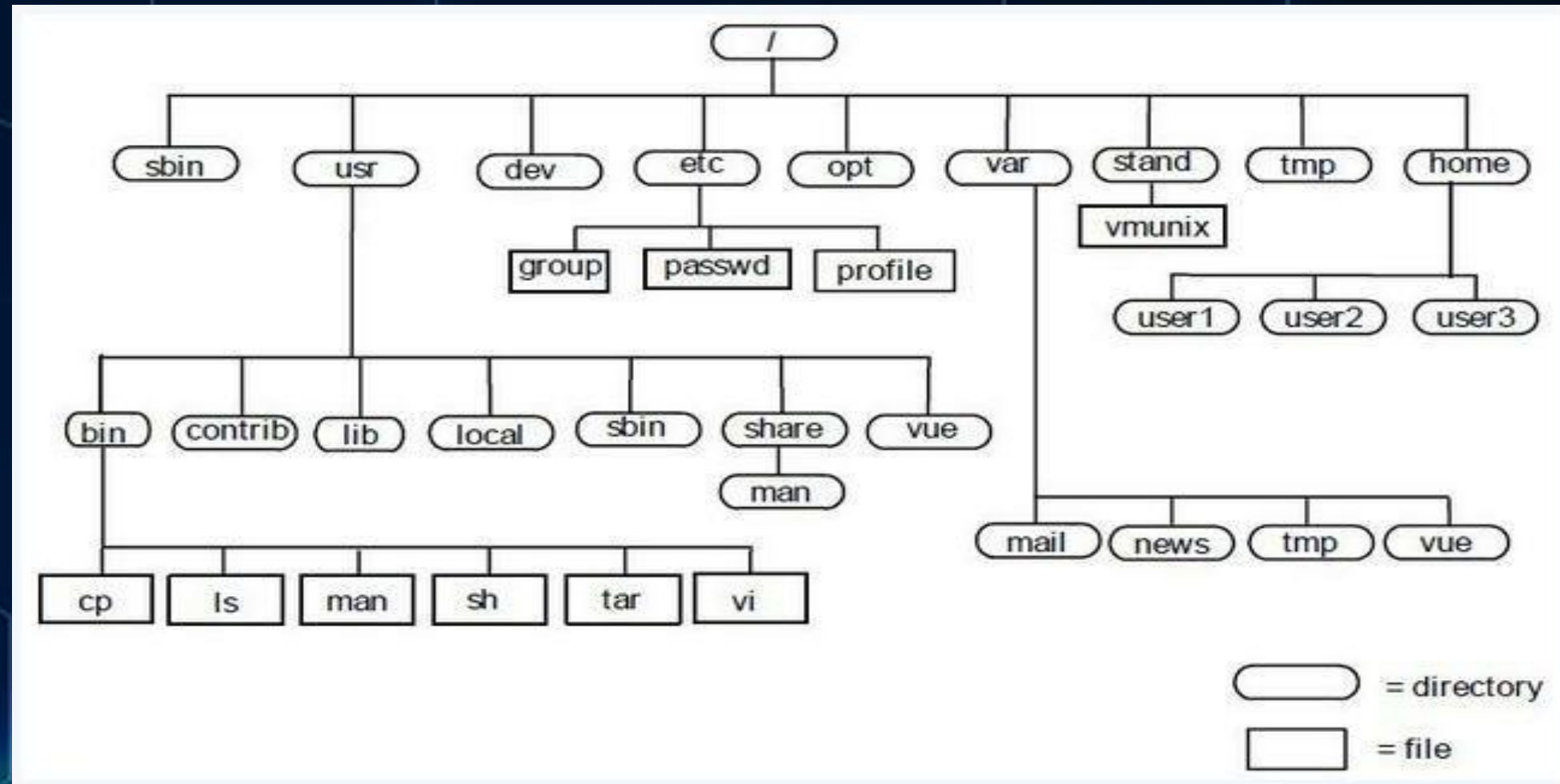


Tool Usage & Exploitation

- **msfconsole** : Start Metasploit Framework
 - ◆ ex: `msfconsole`
- **hydra** : Brute force tool
 - ◆ ex: `hydra -l admin -P passwords.txt 192.168.1.5 ssh`
- **john** : Password cracker
 - ◆ ex: `john --wordlist=rockyou.txt hashes.txt`
- **nikto** : Web server scanner
 - ◆ ex: `nikto -h http://target`
- **sqlmap** : SQL injection automation
 - ◆ ex: `sqlmap -u "http://site.com?id=1" --dbs`
- **burpsuite** : Web proxy (GUI tool)
 - ◆ ex: `burpsuite`
- **dirb / gobuster** : Directory bruteforcing
 - ◆ ex: `gobuster dir -u http://site -w wordlist.txt`
- **wireshark** : Packet sniffer (GUI)
 - ◆ ex: `wireshark`



Linux File System



Linux File permissions

Linux File Permissions

 blog.bytebytego.com

Binary	Octal	String Representation	Permissions
000	0 (0+0+0)	---	No Permission
001	1 (0+0+1)	--x	Execute
010	2 (0+2+0)	-w-	Write
011	3 (0+2+1)	-wx	Write + Execute
100	4 (4+0+0)	r--	Read
101	5 (4+0+1)	r-x	Read + Execute
110	6 (4+2+0)	rw-	Read + Write
111	7 (4+2+1)	rwX	Read + Write + Execute

Owner			Group			Other		
r	W	x	r	W	-	r	-	x
r	Read	4	r	Read	4	r	Read	4
w	Write or Edit	2	w	Write or Edit	2	-	No Permission	0
x	Execute	1	-	No Permission	0	x	Execute	1
7			6			5		



Final Overview



Top 50 Linux Commands you must know



1.is	1.clear	1.diff	1.kill and killall	1.apt, pacman, yum, rpm
2.pwd	2.echo	2.cmp	2.df	2.sudo
3.cd	3.less	3.comm	3.mount	3.cal
4.mkdir	4.man	4.sort	4.chmod	4.alias
5.mv	5.unman	5.export	5.chown	5.dd
6.cp	6.whoami	6.zip	6.ifconfig	6.whereis
7.rm	7.tar	7.unzip	7.traceroute	7.whatis
8.touch	8.grep	8.ssh	8.wget	8.top
9.in	9.head	9.service	9.ufw	9. useradd
10.cat	10.tail	10.ps	10.iptables	10.passwd



Answer these questions below

- ❖ What does the **pwd** command do? Provide an example of its output.
- ❖ How do you **list all** files, **including hidden** ones, in a directory with details?
- ❖ What is the purpose of the **chmod +x script.sh** command? When would you use it?
- ❖ Explain the difference between **chmod 755** and **chmod 777** with examples.



Solutions of above questions below

❖ Ans-1:

The “pwd” command stands for “print working directory.” It shows the current directory path you are in.

Ex: `/home/kali`

❖ Ans-2:

Use the `ls -la` command to list all files, including hidden files (those starting with a dot), with permissions and other details.

Ex: `ls -la /var/www/html`

❖ Ans-3

This command makes the script file `script.sh` executable. You use it when you want to run the script directly from the terminal.

Ex: `chmod +x reverse_shell.sh`
`./reverse_shell.sh`

❖ Ans-4:

`chmod 755` file gives owner full permission (read/write/execute) and others only read and execute.
`chmod 777` file gives everyone full permissions (read/write/execute), which can be a security risk.

Ex: `chmod 755 script.sh`

Ex: `chmod 777 script.sh`





The End



Thank You

Presented by:

Shajalal

Cybersecurity & Ethical Hacking Enthusiast
BSc in Engineering, University of Chittagong

Contact :01850989488
shajalal.cse.cu@gmail.com
<https://www.linkedin.com/in/shajal-cse-cu/>

