7BUISO22W Cyber Security Applications

Lab Environment Setup

University Of Westminster

Dr. David Huang

1 Software, Tools and Files you need

- For this module, we will be using three different virtual machines. You can set up the lab environment either on your own device or on a university lab machine.
- If you are using the machines in CLG.43 or CLG.45, you do not need to install VMware or 7-Zip, as they are already pre-installed. You can go directly to Section 1.2
- On your own device, you first need to download and install the required tools. See Section 1.1 for instructions.
- If you encounter any problems, refer to Section 5. If the issue persists, please consult your lab instructor.

1.1 Download & Install tools

1. Virtualization software: VMware
   - Information about VMware is available on this link.
   - You can download VMware from the VMware download page
   - Ensure that you download the version appropriate for your operating system (Windows, Linux, or macOS)
2. Compression software: 7-Zip
   - You will also need to install 7-Zip to extract .7z files.
   - Information about 7-Zip is available at the following link.
   - You can download 7-Zip from the 7-Zip download page
   - Ensure that you download the version appropriate for your operating system (Windows, Linux, or macOS).

1.2 Obtain the virtual machines

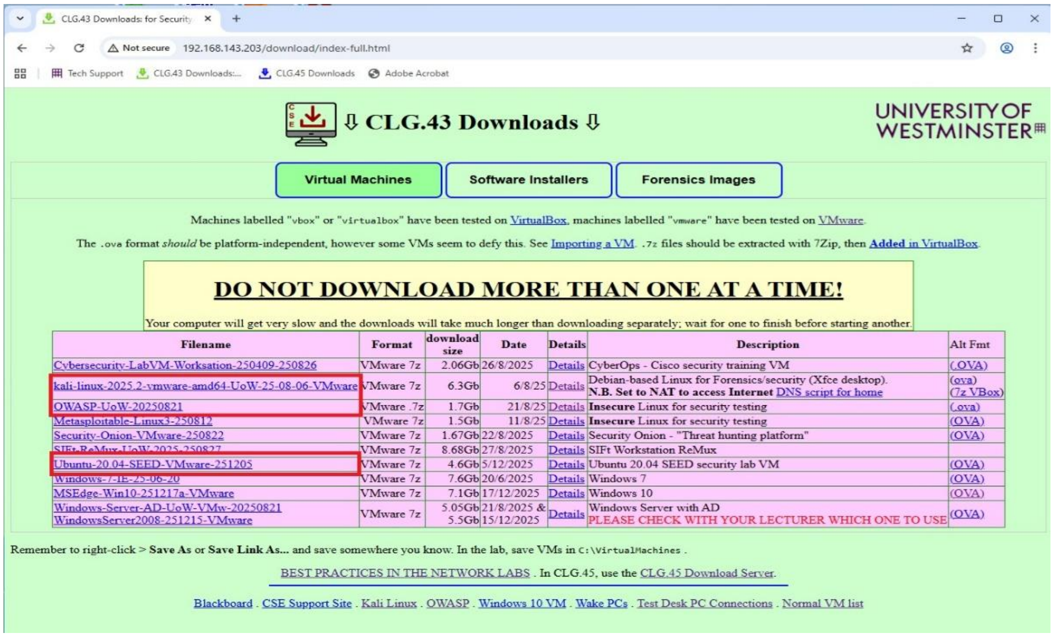
For this module, we will be using **three different virtual machines**. as shown in Fig.1

- On your **own device**, you will need to download this environment **once**.

- On a **university machine** in **CLG.43** and **CLG.45**, you must ensure that the **correct virtual machines** are available.

The three virtual machines we will use are:

1. **OWASP**
   This is the OWASP virtual machine, a deliberately vulnerable system that contains various services such as Apache, databases, and web applications.
2. **Kali Linux**
   This is the Kali Linux virtual machine, used by the attacker or penetration tester. It includes many pre-installed tools commonly used by security professionals and ethical hackers.
3. **SEED Labs (Cybersecurity Education)**
   These labs cover a wide range of topics in computer and information security, including software security, network security, web security, operating system security, and mobile application security.



⇩ CLG.43 Downloads ⇩

Machines labelled "vbox" or "virtualbox" have been tested on VirtualBox, machines labelled "vmware" have been tested on VMware.

The .ova format *should* be platform-independent, however some VMs seem to defy this. See Importing a VM. .7z files should be extracted with 7Zip, then **Added in VirtualBox**.

DO NOT DOWNLOAD MORE THAN ONE AT A TIME!

Your computer will get very slow and the downloads will take much longer than downloading separately; wait for one to finish before starting another.

Filename	Format	download size	Date	Details	Description	Alt Fmt
Cybersecurity-LabVM-Worksation-250409-250826	VMware 7z	2.06Gb	26/8/2025	Details	CyberOps - Cisco security training VM	(.OVA)
kali-linux-2025.2-vmware-amd64-UoW-25-08-06-VMware	VMware 7z	6.3Gb	6/8/25	Details	Debian-based Linux for Forensics/security (Xfce desktop). **N.B. Set to NAT to access Internet** DNS script for home	(ova) (7z VBox)
OWASP-UoW-20250821	VMware .7z	1.7Gb	21/8/25	Details	**Insecure** Linux for security testing	(.ova)
Metasploitable-Linux3-250812	VMware 7z	1.5Gb	11/8/25	Details	**Insecure** Linux for security testing	(OVA)
Security-Onion-VMware-250822	VMware 7z	1.67Gb	22/8/2025	Details	Security Onion - "Threat hunting platform"	(OVA)
SIFt-ReMux-UoW-2025-250827	VMware 7z	8.68Gb	27/8/2025	Details	SIFt Workstation ReMux	
Ubuntu-20.04-SEED-VMware-251205	VMware 7z	4.6Gb	5/12/2025	Details	Ubuntu 20.04 SEED security lab VM	(OVA)
Windows-7-IE-25-06-20	VMware 7z	7.6Gb	20/6/2025	Details	Windows 7	(OVA)
MSEdge-Win10-251217a-VMware	VMware 7z	7.1Gb	17/12/2025	Details	Windows 10	(OVA)
Windows-Server-AD-UoW-VMw-20250821 WindowsServer2008-251215-VMware	VMware 7z	5.05Gb 5.5Gb	21/8/2025 & 15/12/2025	Details	Windows Server with AD PLEASE CHECK WITH YOUR LECTURER WHICH ONE TO USE	(OVA)

Remember to right-click > **Save As** or **Save Link As...** and save somewhere you know. In the lab, save VMs in C:\VirtualMachines .

BEST PRACTICES IN THE NETWORK LABS . In CLG.45, use the CLG.45 Download Server.

Blackboard . CSE Support Site . Kali Linux . OWASP . Windows 10 VM . Wake PCs . Test Desk PC Connections . Normal VM list

Figure 1: Virtual machines included for this lab module

- Each virtual machine is provided in a compressed 7-Zip file and must be extracted before use.
  - **OWASP-UoW-20250821.7z**
  - **kali-linux-2025.2-vmware-amd64-UoW-25-08-06-VMware.7z**
  - **Ubuntu-20.04-SEED-VMware-25120**

- To download them, open the browser and please choose from below:

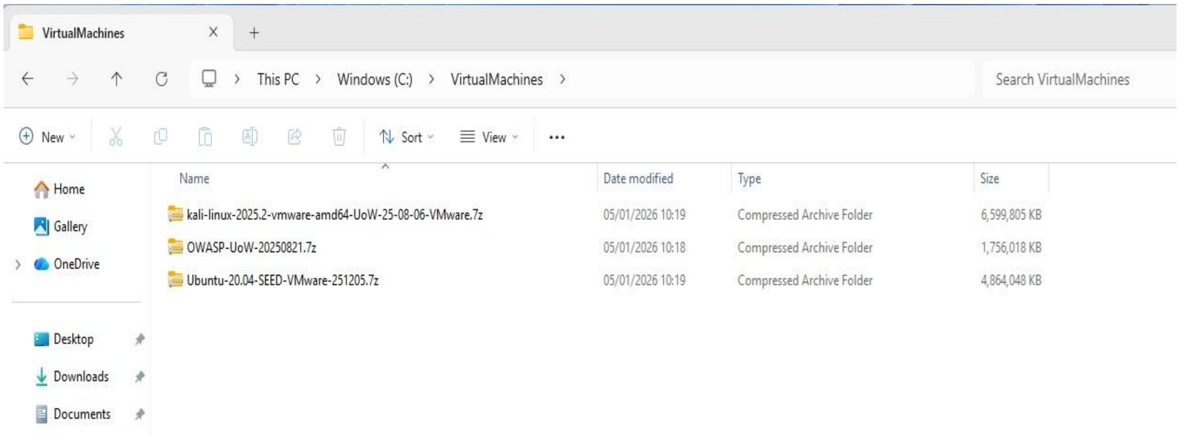
  1. **If you are using a university machine in the lab**
     - Check first that the 7zip files are NOT already in C:/VirtualMachines
     - It is more likely that someone else did this lab before you and the files exist.
     - If you find the files and some folders. It is safe to delete the folders but please do **NOT** delete the 7zip files.
     - **For CLG.43**
       - ❖ http://192.168.143.203/download/
     - **For CLG.45**
       - ❖ http://192.168.145.206/download /
  2. **If you are working from home:**
     - **Access from the CSE download page**
     - Connect to the VPN: https://remote2.westminster.ac.uk/
     - VPN setup guidance: https://support.cse.westminster.ac.uk/w/index. php/VPN
     - When prompted for the portal address, use remote2.westminster.ac.uk
     - After connecting,access: https://download.cse.westminster.ac.uk/ VirtualMachines/ and download the required VM
  3. **If you are using your own machine and**
     - **You are connected to Eduroam:**
       - ❖ http://10.20.144.78/download/VMs/

2 Setting up the machines

1) After downloading (or verifying) the virtual machine files,

2) Browse to the **VirtualMachines** folder: C:\VirtualMachines.

3) You will see **three files**, as shown in Fig. 2. These are the three virtual machine files in compressed (.7z) format to save disk space.



VirtualMachines

This PC › Windows (C:) › VirtualMachines ›

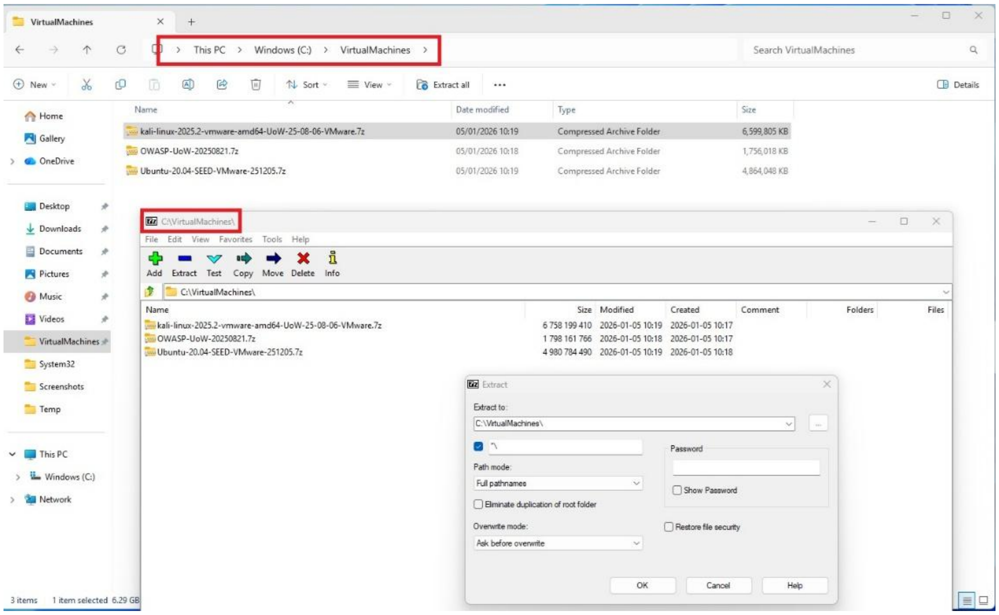
Name	Date modified	Type	Size
kali-linux-2025.2-vmware-amd64-UoW-25-08-06-VMware.7z	05/01/2026 10:19	Compressed Archive Folder	6,599,805 KB
OWASP-UoW-20250821.7z	05/01/2026 10:18	Compressed Archive Folder	1,756,018 KB
Ubuntu-20.04-SEED-VMware-251205.7z	05/01/2026 10:19	Compressed Archive Folder	4,864,048 KB

Figure 2: Virtual Machines folder

4) Right-click on each of the following files:

- kali-linux-2025.2-vmware-amd64-UoW-25-08-06-VMware.7z
- OWASP-UoW-20250821.7z
- Ubuntu-20.04-SEED-VMware-251205.7z

Then select 7-Zip → Extract Files, and extract them to C:\VirtualMachines, as shown in Fig3.



Name	Date modified	Type	Size
kali-linux-2025.2-vmware-amd64-UoW-25-08-06-VMware.7z	05/01/2026 10:19	Compressed Archive Folder	6,599,805 KB
OWASP-UoW-20250821.7z	05/01/2026 10:18	Compressed Archive Folder	1,756,018 KB
Ubuntu-20.04-SEED-VMware-251205.7z	05/01/2026 10:19	Compressed Archive Folder	4,864,048 KB

C:\VirtualMachines\
File Edit View Favorites Tools Help
Add Extract Test Copy Move Delete Info
C:\VirtualMachines\

Name	Size	Modified	Created	Comment	Folders	Files
kali-linux-2025.2-vmware-amd64-UoW-25-08-06-VMware.7z	6 758 199 410	2026-01-05 10:19	2026-01-05 10:17			
OWASP-UoW-20250821.7z	1 798 161 766	2026-01-05 10:18	2026-01-05 10:17			
Ubuntu-20.04-SEED-VMware-251205.7z	4 980 784 490	2026-01-05 10:19	2026-01-05 10:18			

Extract

Extract to: C:\VirtualMachines\

☑ *\

Path mode: Full pathnames

☐ Eliminate duplication of root folder

Overwrite mode: Ask before overwrite

Password

☐ Show Password

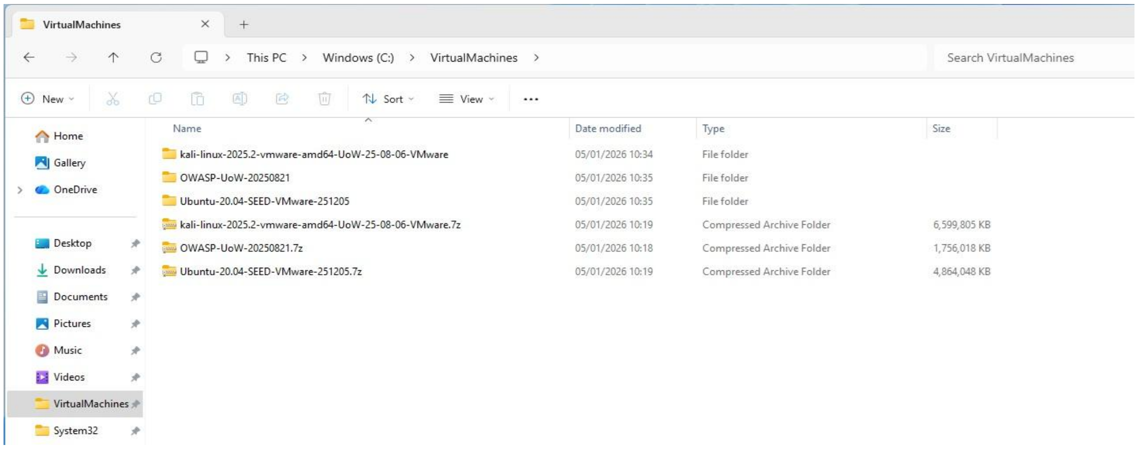
☐ Restore file security

OK Cancel Help

Figure 3: Extracting the 7-Zip files

5) Right click on **kali-linux-2025.2-vmware-amd64-UoW-25-08-06-VMware.7z** , **OWASP-UoW-20250821.7z** and **Ubuntu-20.04-SEED-VMware-251205.7z,** then select **Extract Files into C:\VirtualMachines**

6) Once the extraction is complete, you will have **three VM folders**, each named after its corresponding file, as shown in Fig. 4.



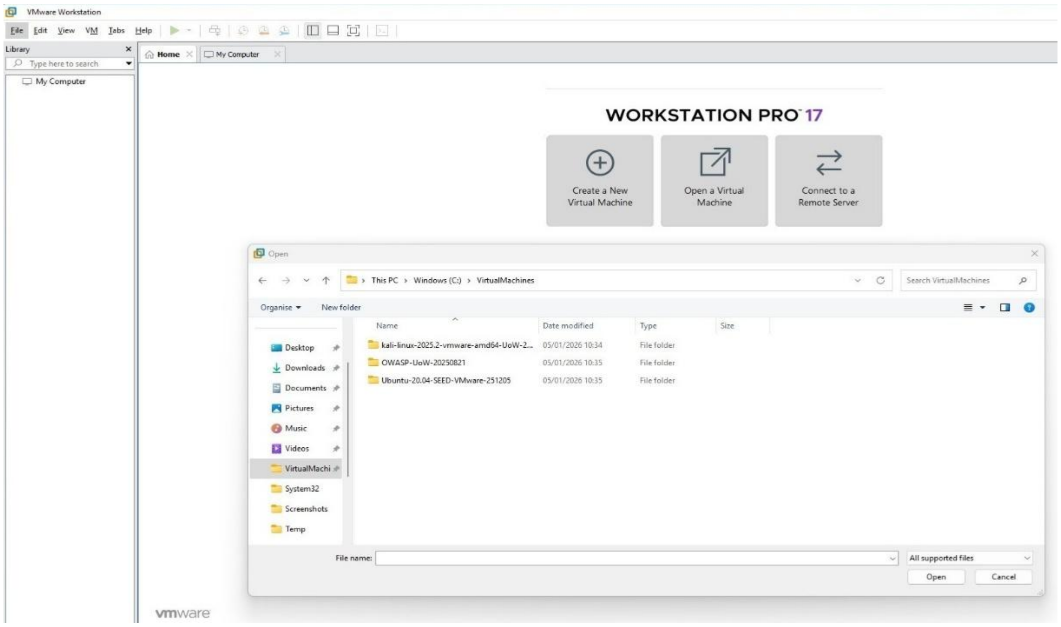
Name	Date modified	Type	Size
kali-linux-2025.2-vmware-amd64-UoW-25-08-06-VMware	05/01/2026 10:34	File folder	
OWASP-UoW-20250821	05/01/2026 10:35	File folder	
Ubuntu-20.04-SEED-VMware-251205	05/01/2026 10:35	File folder	
kali-linux-2025.2-vmware-amd64-UoW-25-08-06-VMware.7z	05/01/2026 10:19	Compressed Archive Folder	6,599,805 KB
OWASP-UoW-20250821.7z	05/01/2026 10:18	Compressed Archive Folder	1,756,018 KB
Ubuntu-20.04-SEED-VMware-251205.7z	05/01/2026 10:19	Compressed Archive Folder	4,864,048 KB

Figure 4: VMs folder after extraction

3 Setting up VMWare

- If you are using a lab machine, it is already pre-installed on your lab machine.
- If you are using your own machine, you should have installed it and set it up. See Section 1.1

You can start **VMware Workstation Pro** by either double-clicking the **VMware Workstation Pro** shortcut on the desktop, or by clicking the **Windows Start** button and typing **VMware** in Fig.5.

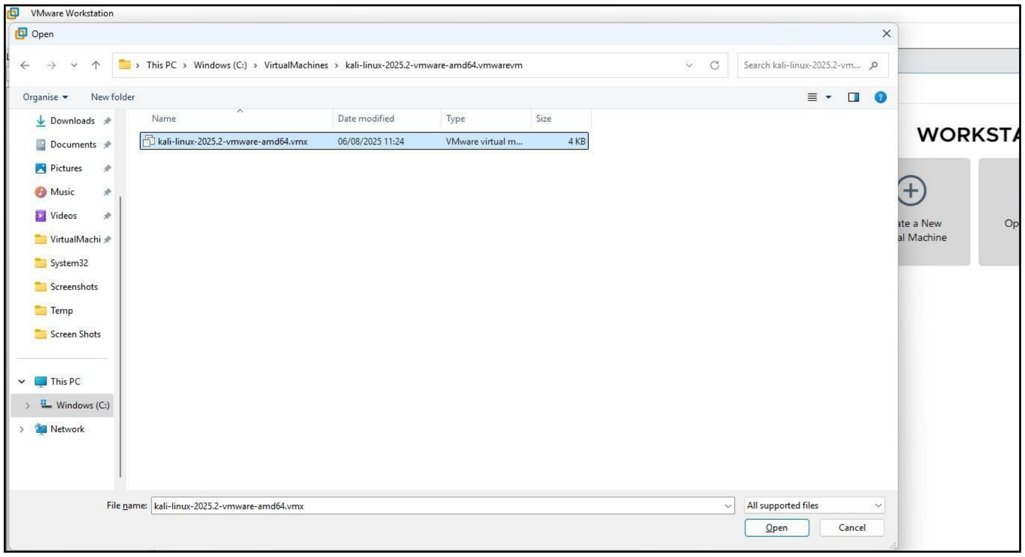


This PC › Windows (C:) › VirtualMachines

Name	Date modified	Type	Size
kali-linux-2025.2-vmware-amd64-UoW-2...	05/01/2026 10:34	File folder	
OWASP-UoW-20250821	05/01/2026 10:35	File folder	
Ubuntu-20.04-SEED-VMware-251205	05/01/2026 10:35	File folder	

Figure 5: Starting VMware and finding the Kali, OWASP, and SEED VMs

1. Browse to the virtual machines folder as shown in Fig. 5.and add Kali Linux folder and select “**kali-linux-2025.2-vmware-amd64-UoW-25-08-06-VMware**” and click open



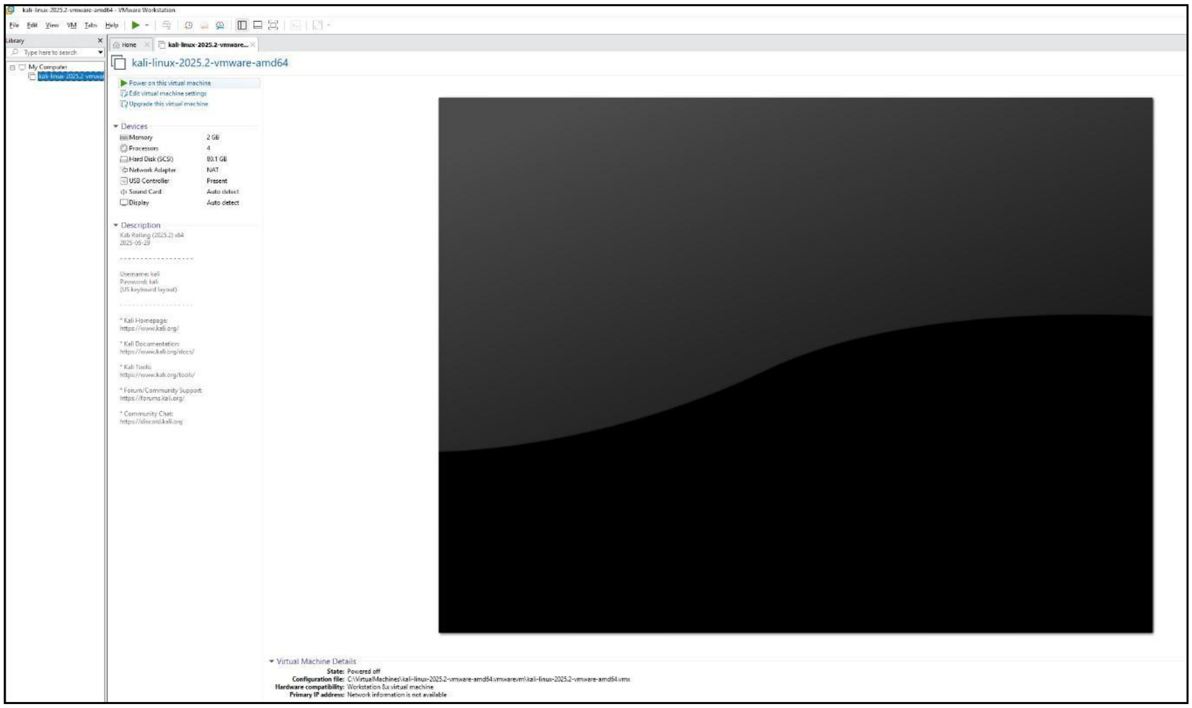
This PC › Windows (C:) › VirtualMachines › kali-linux-2025.2-vmware-amd64.vmwarevm

Name	Date modified	Type	Size
kali-linux-2025.2-vmware-amd64.vmx	06/08/2025 11:24	VMware virtual m...	4 KB

File name: kali-linux-2025.2-vmware-amd64.vmx

Figure 6: Adding the Kali machine to VMware

2. The **Kali Linux virtual machine** will now be added to VMware as shown in Fig. 6 and Fig.7



kali-linux-2025.2-vmware-amd64 - VMware Workstation

File
Edit
View
VM
Tabs
Help
Library
Type here to search
My Computer
kali-linux-2025.2-vmwar
Home
kali-linux-2025.2-vmware...

kali-linux-2025.2-vmware-amd64

Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine

Devices

Memory 2 GB
Processors 4
Hard Disk (SCSI) 80.1 GB
Network Adapter NAT
USB Controller Present
Sound Card Auto detect
Display Auto detect

Description

Kali Rolling (2025.2) x64
2025-06-29

Username: kali
Password: kali
(US keyboard layout)

* Kali Homepage:
https://www.kali.org/

* Kali Documentation:
https://www.kali.org/docs/

* Kali Tools:
https://www.kali.org/tools/

* Forum/Community Support:
https://forums.kali.org/

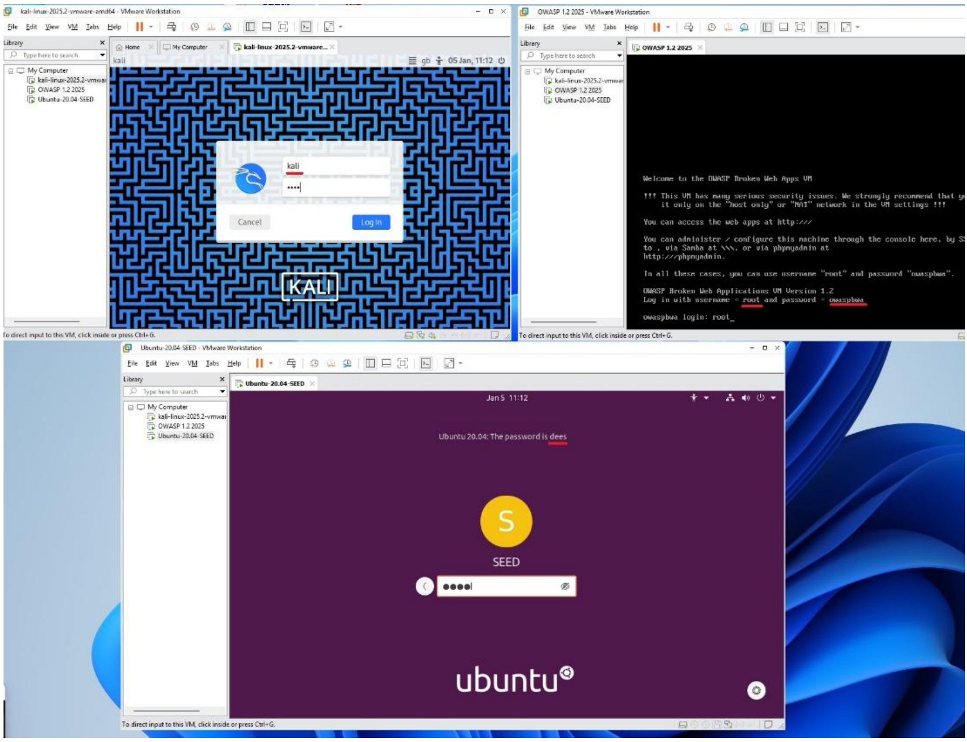
* Community Chat:
https://discord.kali.org

Virtual Machine Details

State: Powered off
Configuration file: C:\VirtualMachines\kali-linux-2025.2-vmware-amd64.vmwarevm\kali-linux-2025.2-vmware-amd64.vmx
Hardware compatibility: Workstation 8.x virtual machine
Primary IP address: Network information is not available

Figure 7: Kali VM added

3. In VMware, click **File → Open**. Repeat the same steps to add the remaining virtual machines.
4. You should now see three virtual machines set up in VMware, as shown in Fig. 8



kali-linux-2025.2-vmware-amd64 - VMware Workstation

To direct input to this VM, click inside or press Ctrl+G.

OWASP 1.2 2025 - VMware Workstation

```
Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that yo
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http:///

You can administer / configure this machine through the console here, by SS
to , via Samba at \\\, or via phpmyadmin at
http:///phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

OWASP Broken Web Applications VM Version 1.2
Log in with username = root and password = owaspbwa

owaspbwa login: root_
```

To direct input to this VM, click inside or press Ctrl+G.

Ubuntu-20.04-SEED - VMware Workstation

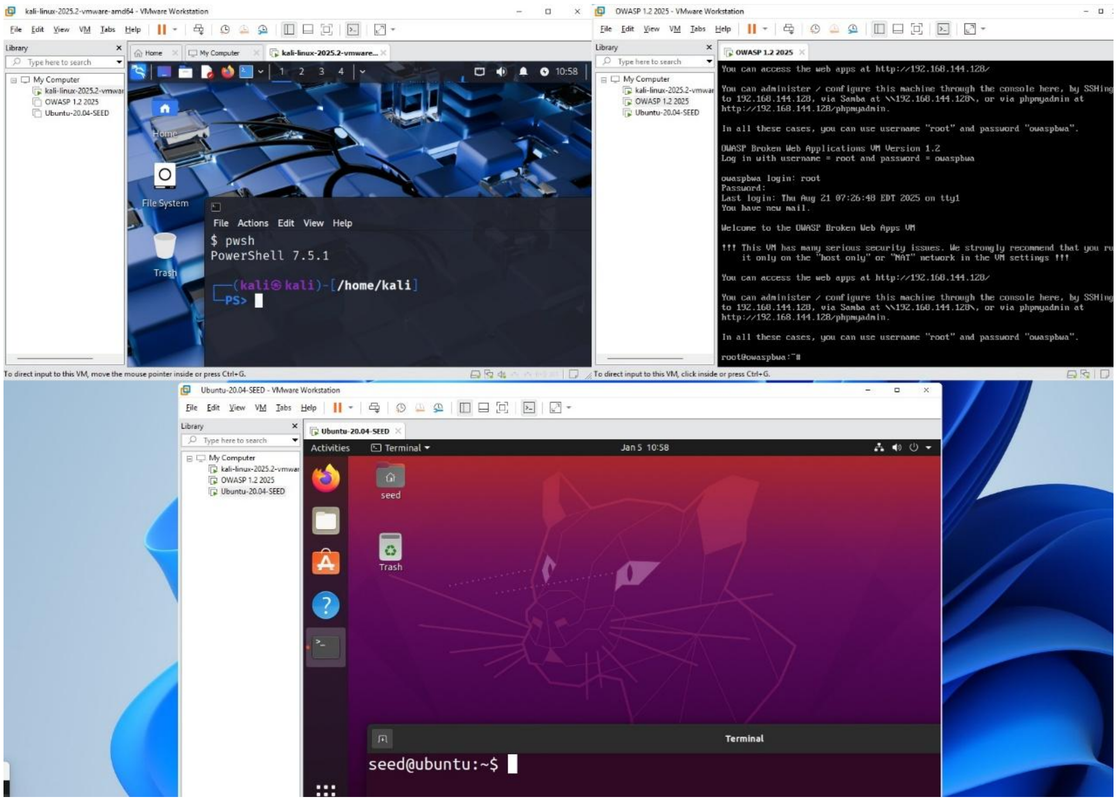
Ubuntu 20.04: The password is dees

To direct input to this VM, click inside or press Ctrl+G.

Figure 8: Kali Linux, OWASP, and SEED virtual machines listed in VMware

5. You are now able to log in to the three virtual machines, as shown in Fig. 9.

- **Kali Linux** (kali-linux-2025.2-vmware-amd64-UoW-25-08-06-VMware)
  - username**: kali**
  - password: **kali**
- **OWASP** (OWASP-UoW-20250821)
  - username**: root**
  - password: **owaspbwa**
- **Ubuntu SEED** (Ubuntu-20.04-SEED-VMware-251205)
  - username: **SEED**
  - password: **dees**


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2025.2-vmwar
OWASP 1.2 2025
Ubuntu-20.04-SEED
Home
My Computer
kali-linux-2025.2-vmware...
1 2 3 4
10:58
Home
File System
Trash
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
OWASP 1.2 2025 - VMware Workstation
OWASP 1.2 2025
To direct input to this VM, click inside or press Ctrl+G.
Ubuntu-20.04-SEED - VMware Workstation
Ubuntu-20.04-SEED
Activities
Terminal
Jan 5 10:58
seed
Trash
Terminal

```
$ pwsh
PowerShell 7.5.1

┌──(kali㉿kali)-[/home/kali]
└─PS> 
```

```
You can access the web apps at http://192.168.144.128/

You can administer / configure this machine through the console here, by SSHing
to 192.168.144.128, via Samba at \\192.168.144.128\, or via phpmyadmin at
http://192.168.144.128/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

OWASP Broken Web Applications VM Version 1.2
Log in with username = root and password = owaspbwa

owaspbwa login: root
Password:
Last login: Thu Aug 21 07:26:48 EDT 2025 on tty1
You have new mail.

Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you ru
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://192.168.144.128/

You can administer / configure this machine through the console here, by SSHing
to 192.168.144.128, via Samba at \\192.168.144.128\, or via phpmyadmin at
http://192.168.144.128/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

root@owaspbwa:~#
```

```
seed@ubuntu:~$ 
```

Figure 9: Logging into the Kali Linux, OWASP, and SEED virtual machines in VMware

4 Network Setup

- While working in the lab environment, you must ensure that it is isolated from the Internet.
- One way to achieve this is by creating a private network.
- All devices will join this network and remain isolated from the Internet.
- In some cases, Kali Linux needs to be connected to the Internet to download scripts and tools or to perform Open Source Intelligence (OSINT) activities.
- However, it is essential that vulnerable virtual machines (VMs) remain on the private network at all times.

In this section, we will cover the following:

- First, we will create a private virtual network environment, as described in Section/ 4.1.
- Once the private virtual network environment is in place, we will switch VMs between Internet-connected mode and private network mode.
- To connect a VM either to the Internet or to the virtual private network environment (called **"Host-Only Network"** in VMware), refer to Section 4.2

The lab environment and network topology with static IP addressing are illustrated in Fig. 10.

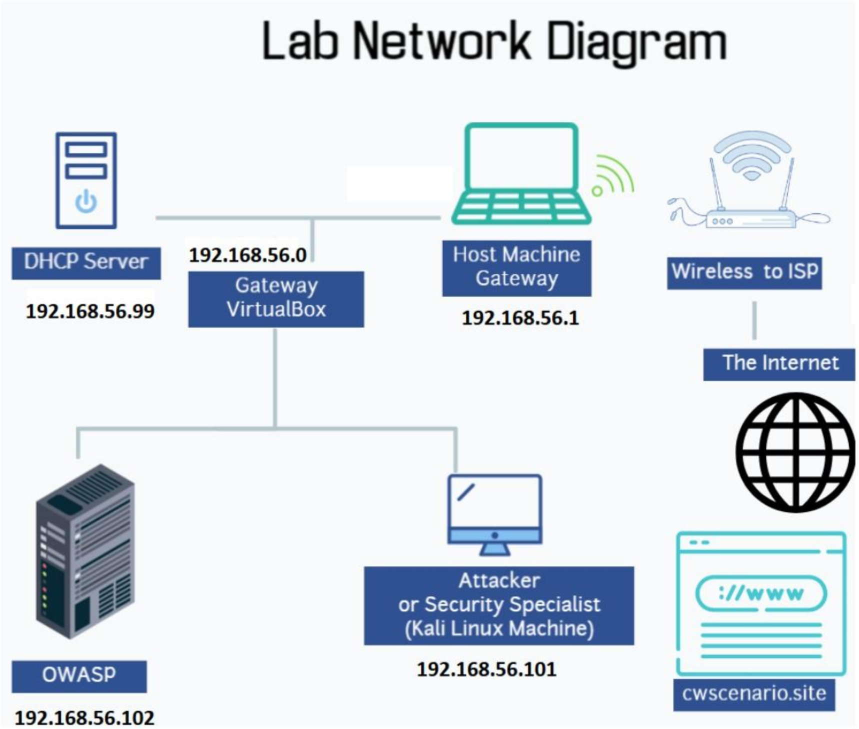


Fig. 10. Lab environment and network topology with static IP addressing.

4.1 Private Virtual Lab Network Environment (VMware)

- Let us first create a **Host-Only Network** environment in VMware Workstation and configure it using the following steps, as shown in Fig. 10.

Step 1: Open the Virtual Network Editor

- In VMware Workstation, navigate to **Edit → Virtual Network Editor**.
- You may need to run VMware as an **Administrator**.
- Refer to Fig. 11 and Fig. 12.

Step 2: Select or Create a Host-Only Network

- Check for an existing **VMnet1 (Host-Only)** network.
- If VMnet1 already exists, there is no need to create it again; simply ensure that the IPv4 subnet address is configured as described in Step 3.
- If VMnet1 does not exist, click **Add Network**, select **Host-Only**, and assign it to **VMnet1**.

Step 3: Configure the Subnet IP

- Set the Subnet IPv4 Address to: **192.168.56.0**
- Set the Subnet Mask to: **255.255.255.0**

Step 4: Enable the DHCP Server

- In the same Virtual Network Editor, enable **Use local DHCP service to distribute IP addresses to VMs**.

Step 5: Configure the DHCP Range

- Modify the DHCP settings as follows and click Apply:
    - Server Address (VMware DHCP): **192.168.56.99**
    - Lower Address Bound: **192.168.56.100**
    - Upper Address Bound: **192.168.56.254**

- This configuration ensures that each virtual machine is automatically assigned an IP address within the range **192.168.56.100–192.168.56.254**

- Once the Host-Only Network is configured in VMware, virtual machines can be switched between **Host-Only mode** (private lab environment) and **NAT mode** (Internet connectivity) by modifying the VM’s network adapter settings.

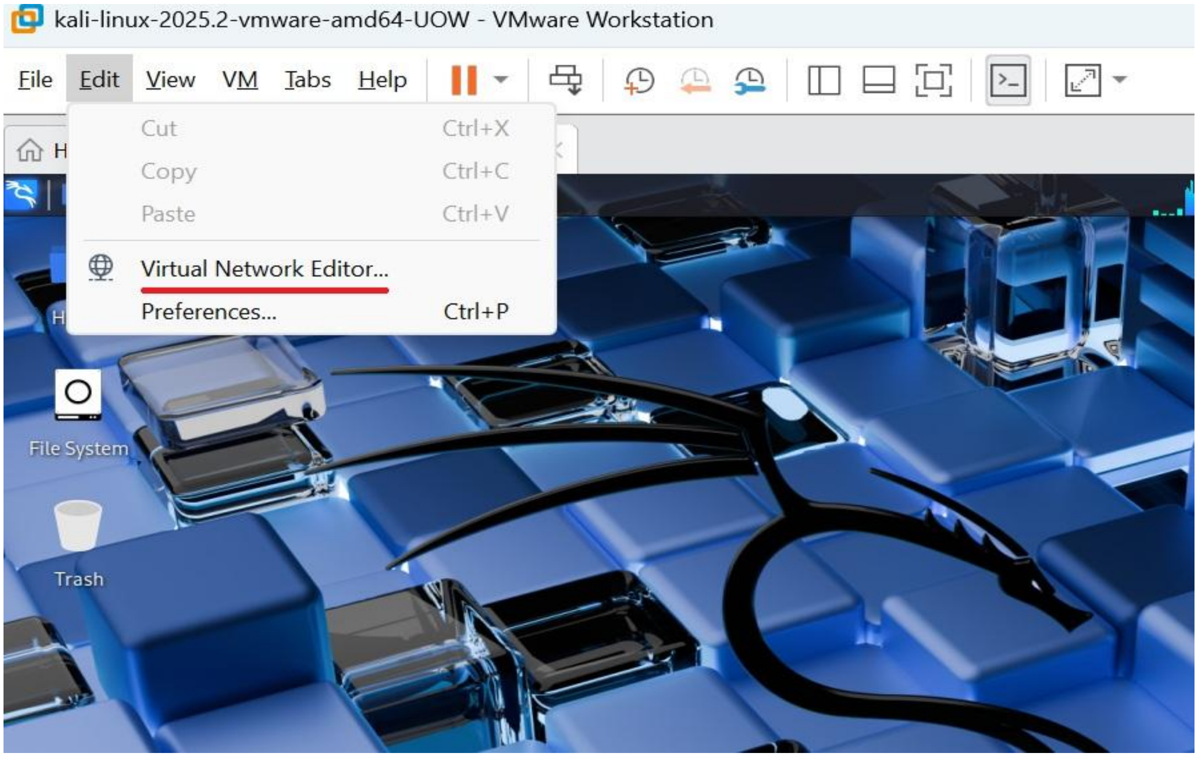
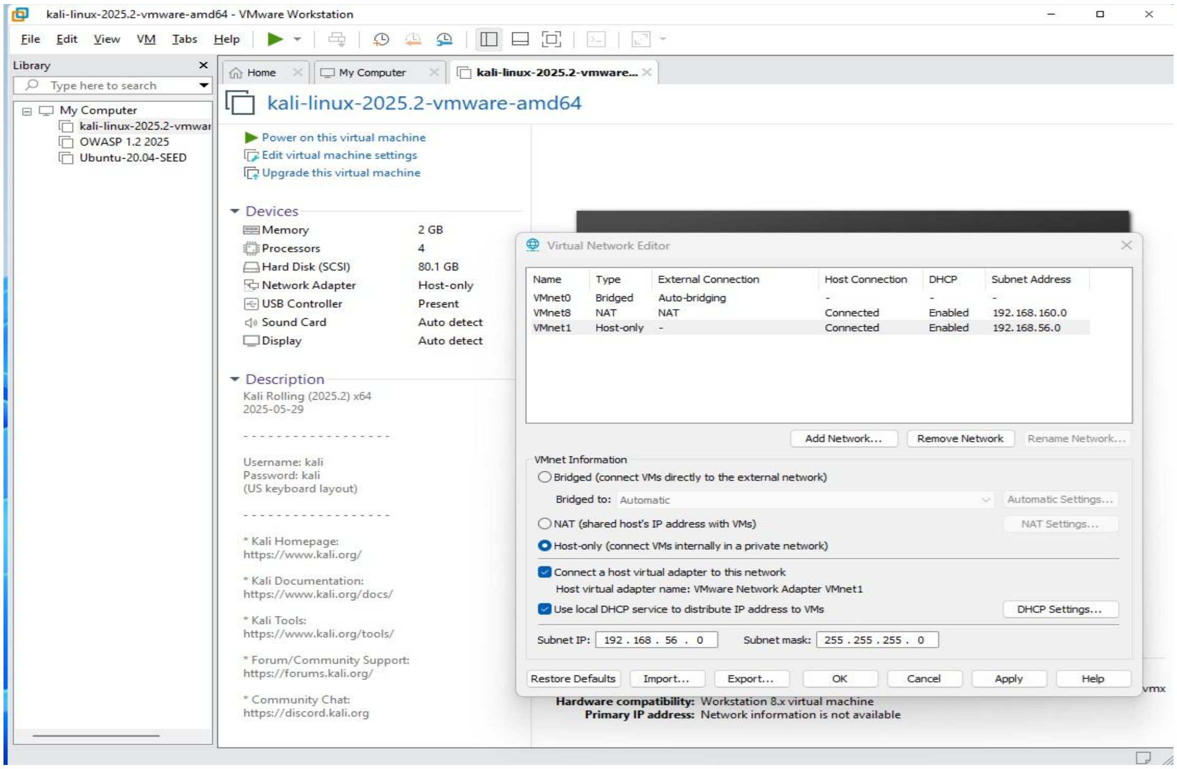


Figure 11. Open the Virtual Network Editor



kali-linux-2025.2-vmware-amd64

Devices

Memory	2 GB
Processors	4
Hard Disk (SCSI)	80.1 GB
Network Adapter	Host-only
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Description

Kali Rolling (2025.2) x64
2025-05-29

- - - - - - - - - - - - - - - - - -

Username: kali
Password: kali
(US keyboard layout)

- - - - - - - - - - - - - - - - - -

* Kali Homepage:
https://www.kali.org/

* Kali Documentation:
https://www.kali.org/docs/

* Kali Tools:
https://www.kali.org/tools/

* Forum/Community Support:
https://forums.kali.org/

* Community Chat:
https://discord.kali.org

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet8	NAT	NAT	Connected	Enabled	192.168.160.0
VMnet1	Host-only	-	Connected	Enabled	192.168.56.0

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to: Automatic

○ NAT (shared host's IP address with VMs)

● Host-only (connect VMs internally in a private network)

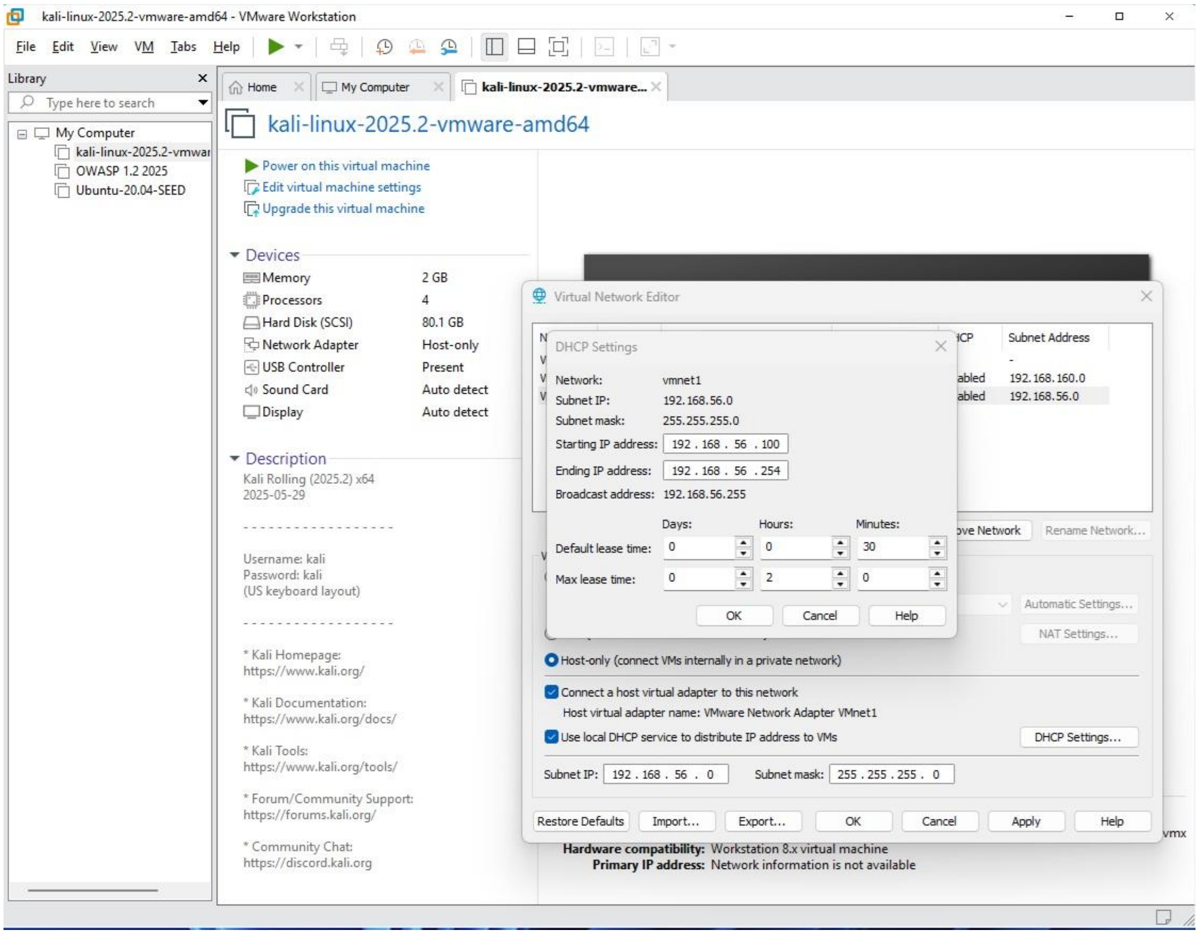
☑ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet1

☑ Use local DHCP service to distribute IP address to VMs

Subnet IP: 192 . 168 . 56 . 0 Subnet mask: 255 . 255 . 255 . 0

Hardware compatibility: Workstation 8.x virtual machine
Primary IP address: Network information is not available



kali-linux-2025.2-vmware-amd64

Devices	
Memory	2 GB
Processors	4
Hard Disk (SCSI)	80.1 GB
Network Adapter	Host-only
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Kali Rolling (2025.2) x64
2025-05-29

Username: kali
Password: kali
(US keyboard layout)

----

* Kali Homepage:
https://www.kali.org/

* Kali Documentation:
https://www.kali.org/docs/

* Kali Tools:
https://www.kali.org/tools/

* Forum/Community Support:
https://forums.kali.org/

* Community Chat:
https://discord.kali.org

...CP	Subnet Address
	-
...abled	192.168.160.0
...abled	192.168.56.0

Network: vmnet1
Subnet IP: 192.168.56.0
Subnet mask: 255.255.255.0
Starting IP address: 192 . 168 . 56 . 100
Ending IP address: 192 . 168 . 56 . 254
Broadcast address: 192.168.56.255

	Days:	Hours:	Minutes:
Default lease time:	0	0	30
Max lease time:	0	2	0

● Host-only (connect VMs internally in a private network)

☑ Connect a host virtual adapter to this network
Host virtual adapter name: VMware Network Adapter VMnet1

☑ Use local DHCP service to distribute IP address to VMs

Subnet IP: 192 . 168 . 56 . 0 Subnet mask: 255 . 255 . 255 . 0

Hardware compatibility: Workstation 8.x virtual machine
Primary IP address: Network information is not available

Figure 12. Host-Only Network Configuration

4.2 Change VM Network Connection

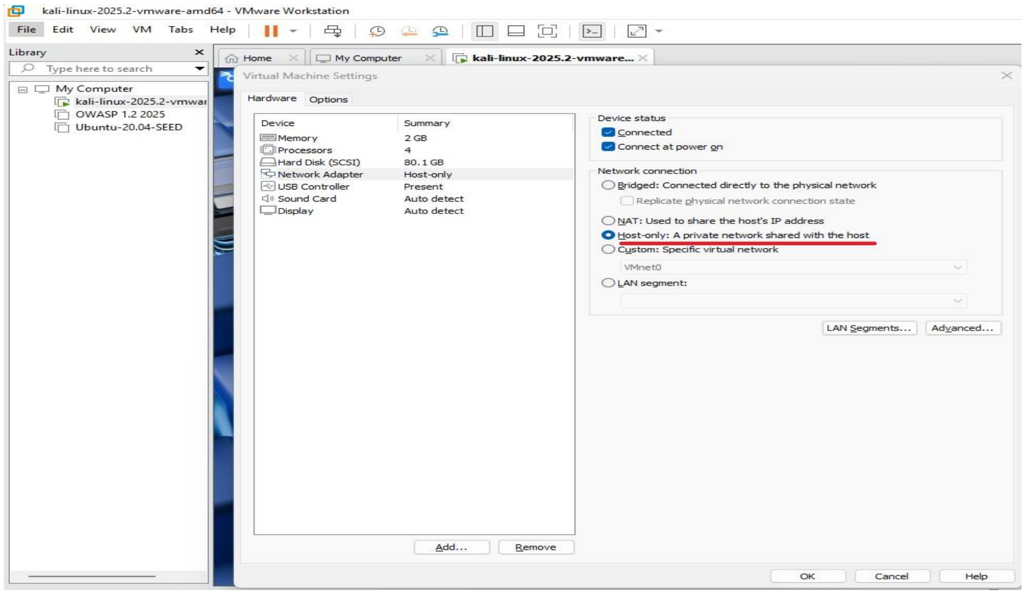
- The network to which a virtual machine (VM) is currently connected can be viewed by selecting the VM in VMware Workstation. For example, **Kali Linux** is connected to the Internet by default via a **NAT** connection.

- To change the network connection (e.g., switch from NAT to Host-Only):
  1. Select the VM to be modified.
  2. Navigate to **VM → Settings**.
  3. In the **Virtual Machine Settings** dialog box, select **Network Adapter** (see Fig. 12).
  4. Select one of the following options:
     - **Bridged**: The VM is fully exposed to the local network and behaves like a real machine on that network. (**Warning:** Bridged networking is not recommended in lab environments because it exposes virtual machines directly to the physical network, increasing security risks and reducing isolation).
     - **NAT (Network Address Translation)**: Connects the VM to the Internet through the host machine. The VM shares the host’s IP address for external communication

and can access the host’s network resources.

  - **Host-Only**: Connects the VM to the host-only network, isolating it from the Internet while allowing communication with the host machine and other VMs on the same host-only network.

- Repeat these steps for each VM to ensure:
  - All VMs are on the same network when inter-VM communication is required (e.g., **Host-Only for lab exercises**).
  - **VMs are set to NAT if Internet access** is needed.



Device	Summary
Memory	2 GB
Processors	4
Hard Disk (SCSI)	80.1 GB
Network Adapter	Host-only
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

○ NAT: Used to share the host's IP address

● Host-only: A private network shared with the host

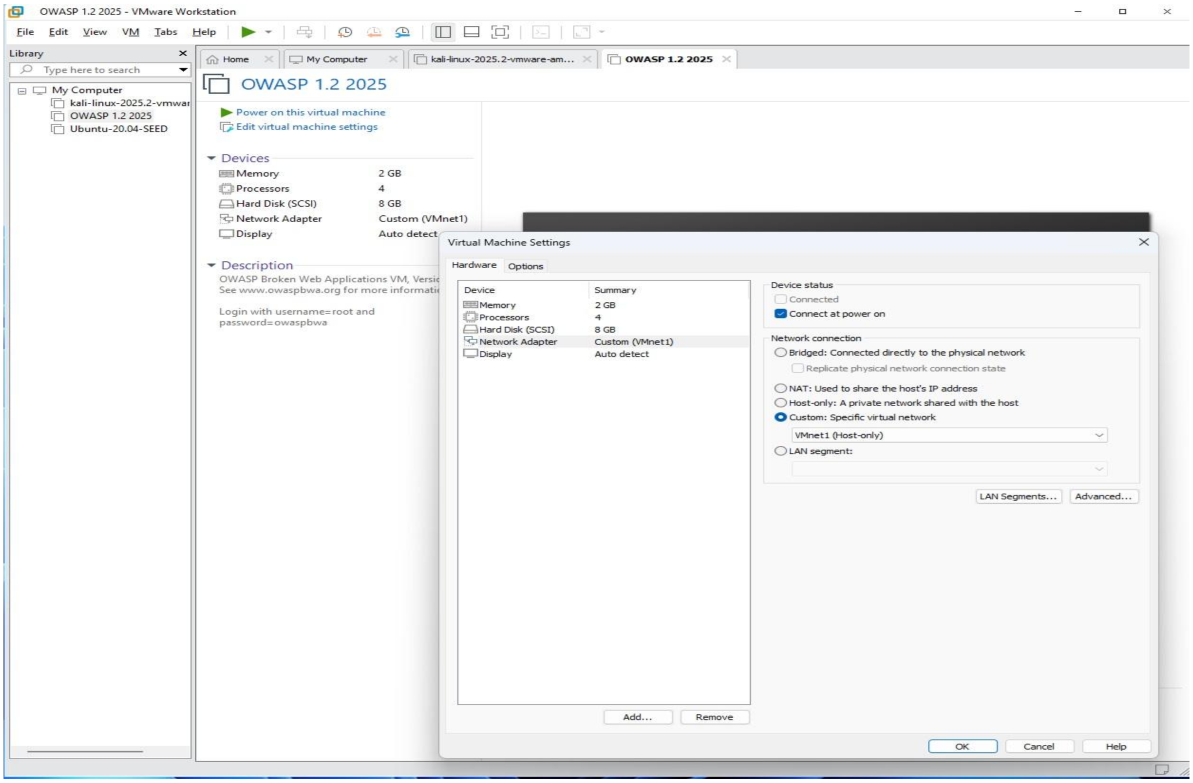
○ Custom: Specific virtual network

VMnet0

○ LAN segment:

Figure 13. Host-Only Network Kail VM

- Select the **NAT** option to connect the virtual machine to a NAT network. NAT, or **Network Address Translation**, allows the VM to access the host machine’s network resources. The VM will share the host’s IP address when connecting to the Internet.
- Repeat these steps for each VM to ensure that all VMs are on the same network or that a VM has Internet access when required.



OWASP 1.2 2025

Device	Summary
Memory	2 GB
Processors	4
Hard Disk (SCSI)	8 GB
Network Adapter	Custom (VMnet1)
Display	Auto detect

OWASP Broken Web Applications VM, Versio
See www.owaspbwa.org for more informati

Login with username=root and
password=owaspbwa

Device status

□ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

● Custom: Specific virtual network

VMnet1 (Host-only)

○ LAN segment:

Figure 14: Choose a network and select the required connectivity

4.3 Start the VMs Test connectivity

VMs usernames and passwords

1. Kali Linux (kali-linux-2025.2-vmware-amd64-UoW-25-08-06-VMware)
   - username: kali
   - password: kali
2. Owaspbwa linux (OWASP-UoW-20250821)
   - username: root
   - password: owaspbwa

- Start both virtual machines (VMs) to test connectivity.
- To start a VM, either **double-click** on it or select it and click the **Start** button.
- Enter the **username** and **password** for each VM.
  - **Note:** On any Linux terminal, including the OWASP VM, the password will not be displayed as you type. This is intended to conceal the password length from anyone nearby.

- To check the IP address on a Linux VM, open a terminal and enter:

  ifconfg or ip address/ip a

- On a Windows VM, open the Command Prompt by clicking **Start** and typing **cmd**, then enter:

  ipconfig

- For example, on the Kali Linux VM, the IP address can be verified using the steps illustrated in Fig. 14.

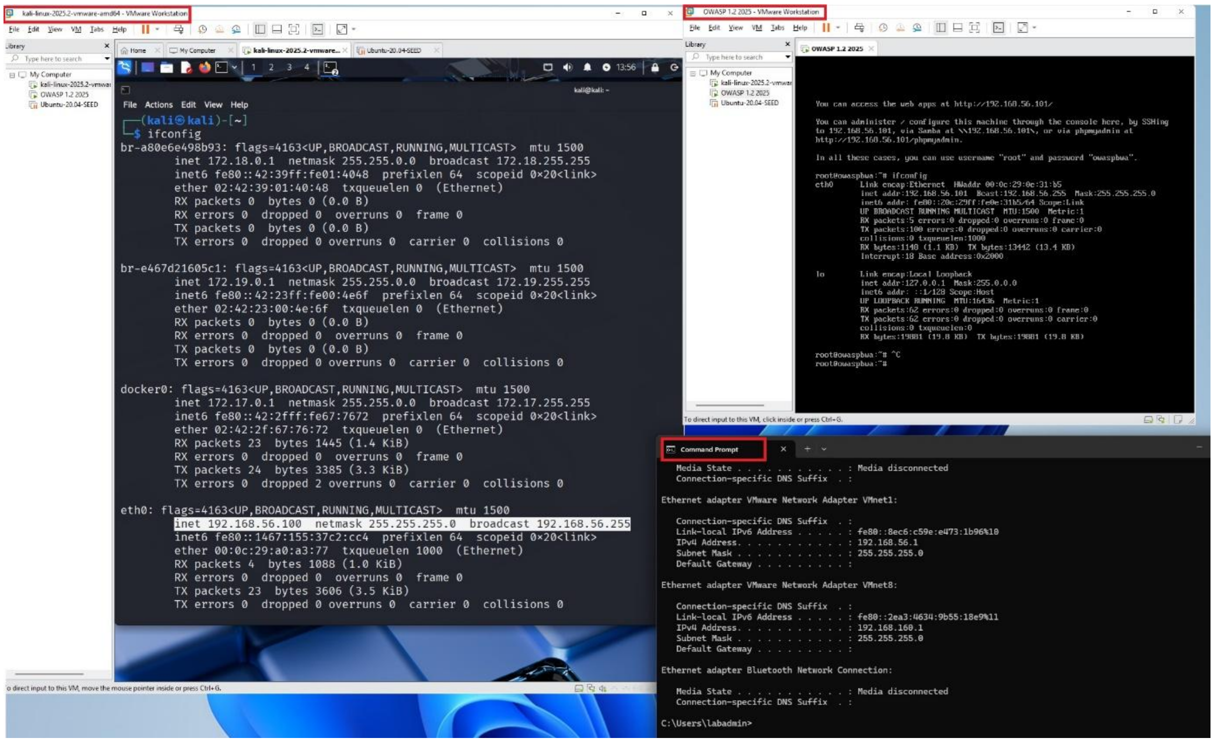
Step 1: Click on the **Terminal Emulator** shortcut to open the terminal.

Step 2: To check your IP address, type:

ifconfig or ip a

Explanation of the output:

- **eth0** is the virtual network interface that connects the virtual machine to the host (physical) machine. In this example, it is 192.168.56.100, indicating that the VM is connected to the virtual private network created earlier in Section 4.1.
- **lo** is the **localhost interface** (also called the loopback interface). The localhost IP 127.0.0.1 is used for testing services on the same machine. Any connection to this IP loops back to the machine itself. While it is not needed for this exercise, it will appear when you run ifconfig.


kali-linux-2025.2-vmware-amd64 - VMware Workstation
OWASP 1.2 2025 - VMware Workstation
Command Prompt

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
br-a80e6e498b93: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.18.0.1  netmask 255.255.0.0  broadcast 172.18.255.255
        inet6 fe80::42:39ff:fe01:4048  prefixlen 64  scopeid 0x20<link>
        ether 02:42:39:01:40:48  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

br-e467d21605c1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.19.0.1  netmask 255.255.0.0  broadcast 172.19.255.255
        inet6 fe80::42:23ff:fe00:4e6f  prefixlen 64  scopeid 0x20<link>
        ether 02:42:23:00:4e:6f  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        inet6 fe80::42:2fff:fe67:7672  prefixlen 64  scopeid 0x20<link>
        ether 02:42:2f:67:76:72  txqueuelen 0  (Ethernet)
        RX packets 23  bytes 1445 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 3385 (3.3 KiB)
        TX errors 0  dropped 2 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.100  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::1467:155:37c2:cc4  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:a0:a3:77  txqueuelen 1000  (Ethernet)
        RX packets 4  bytes 1088 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 3606 (3.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
You can access the web apps at http://192.168.56.101/

You can administer / configure this machine through the console here, by SSHing
to 192.168.56.101, via Samba at \\192.168.56.101\, or via phpmyadmin at
http://192.168.56.101/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

root@owaspbwa:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:0e:31:b5
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe0e:31b5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5 errors:0 dropped:0 overruns:0 frame:0
          TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1140 (1.1 KB)  TX bytes:13442 (13.4 KB)
          Interrupt:18 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:62 errors:0 dropped:0 overruns:0 frame:0
          TX packets:62 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19881 (19.8 KB)  TX bytes:19881 (19.8 KB)

root@owaspbwa:~# ^C
root@owaspbwa:~#
```

```
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8ec6:c59e:e473:1b96%10
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2ea3:4634:9b55:18e9%11
   IPv4 Address. . . . . . . . . . . : 192.168.160.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\labadmin>
```

Figure 15: Verify the IP addresses of Kali, OWASP, and Windows.

- All steps should be performed on the **OWASP VM** as well as on any other virtual machines (VMs) that you need to connect.

Changing IP Without Restarting

- It is **not necessary to restart the virtual machine** to change its network settings.
- To change the IP, follow these steps:

Step 1: Select the VM you want to modify.

Step 2: Navigate to **VM → Settings** (see Fig. 12).

Step 3: In the **Virtual Machine Settings** dialog box, select **Network Adapter**.

Step 4: Choose the desired network type (**NAT** or **Host-Only**).

Step 5: Open the terminal and execute the following commands:

```
sudo ifconfig eth0 down
```

- This will disable the **eth0** interface (see Fig. 15).

```
sudo ifconfig eth0 up
```

- This will re-enable the **eth0** interface, and the VM will obtain a new IP address (see Fig. 15).
- To verify the new IP address, type:

```
ifconfig
```

- The IP should now reflect the selected network type (e.g., the NAT IP, as shown in Fig. 15).

4.4 Test Connectivity

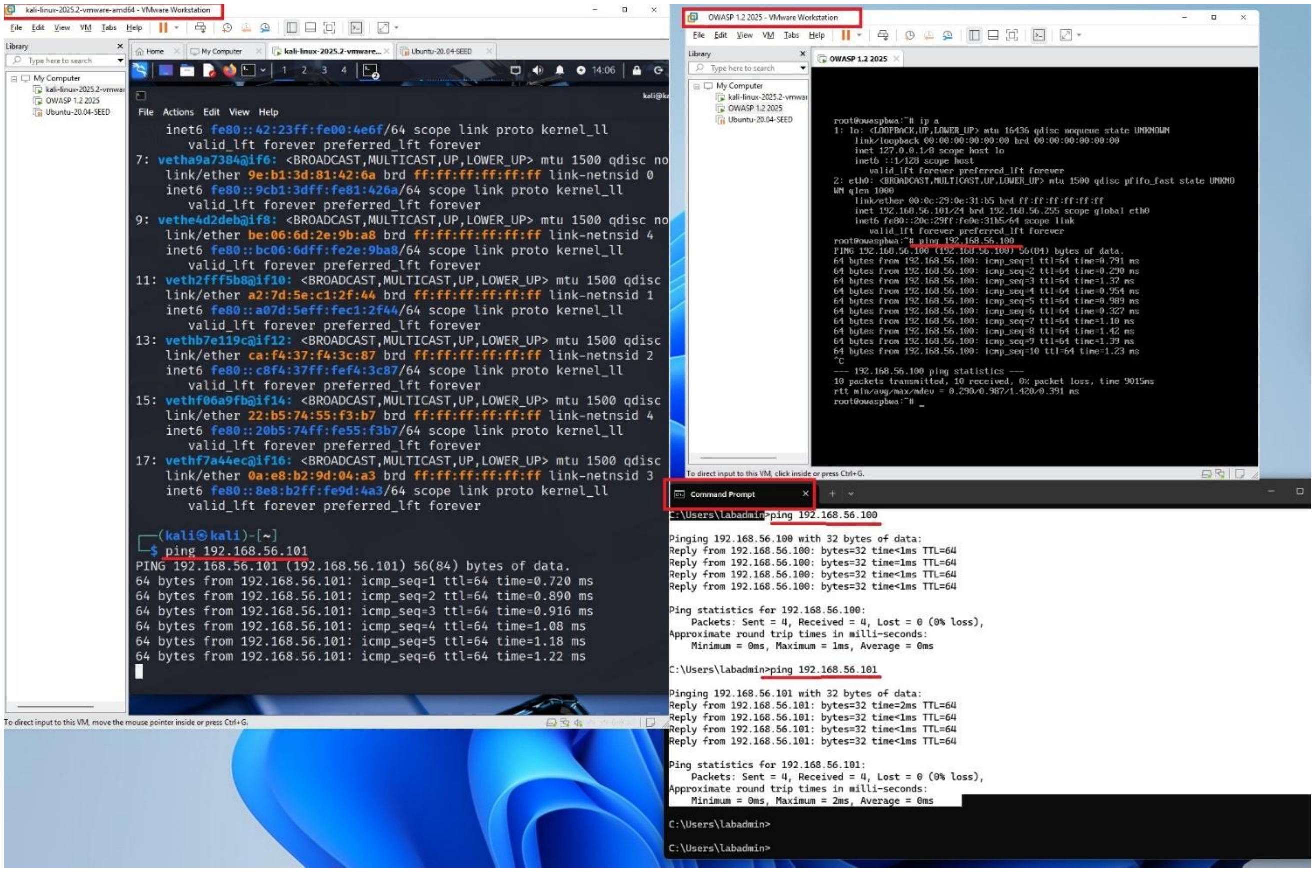
- To test the connection between devices, they **must be on the same network**.
- Connectivity can be tested using the **ping** command on both Linux and Windows terminals.

Note: Verify the IP addresses of your VMs before performing this step, as they may differ from the examples shown below.

To check connectivity between devices:

- From Kali Linux, ping the vulnerable machine (see Fig. 16):

```
ping 192.168.56.101
```


kali-linux-2025.2-vmware-amd64 - VMware Workstation
OWASP 1.2 2025 - VMware Workstation
Command Prompt

```
    inet6 fe80::42:23ff:fe00:4e6f/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
7: vetha9a7384@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc no
    link/ether 9e:b1:3d:81:42:6a brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::9cb1:3dff:fe81:426a/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
9: vethe4d2deb@if8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc no
    link/ether be:06:6d:2e:9b:a8 brd ff:ff:ff:ff:ff:ff link-netnsid 4
    inet6 fe80::bc06:6dff:fe2e:9ba8/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
11: veth2fff5b8@if10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
    link/ether a2:7d:5e:c1:2f:44 brd ff:ff:ff:ff:ff:ff link-netnsid 1
    inet6 fe80::a07d:5eff:fec1:2f44/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
13: vethb7e119c@if12: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
    link/ether ca:f4:37:f4:3c:87 brd ff:ff:ff:ff:ff:ff link-netnsid 2
    inet6 fe80::c8f4:37ff:fef4:3c87/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
15: vethf06a9fb@if14: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
    link/ether 22:b5:74:55:f3:b7 brd ff:ff:ff:ff:ff:ff link-netnsid 4
    inet6 fe80::20b5:74ff:fe55:f3b7/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
17: vethf7a44ec@if16: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
    link/ether 0a:e8:b2:9d:04:a3 brd ff:ff:ff:ff:ff:ff link-netnsid 3
    inet6 fe80::8e8:b2ff:fe9d:4a3/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=0.720 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.890 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.916 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=1.08 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=1.18 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=64 time=1.22 ms
```

```
root@owaspbwa:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNO
WN qlen 1000
    link/ether 00:0c:29:0e:31:b5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global eth0
    inet6 fe80::20c:29ff:fe0e:31b5/64 scope link
       valid_lft forever preferred_lft forever
root@owaspbwa:~# ping 192.168.56.100
PING 192.168.56.100 (192.168.56.100) 56(84) bytes of data.
64 bytes from 192.168.56.100: icmp_seq=1 ttl=64 time=0.791 ms
64 bytes from 192.168.56.100: icmp_seq=2 ttl=64 time=0.290 ms
64 bytes from 192.168.56.100: icmp_seq=3 ttl=64 time=1.37 ms
64 bytes from 192.168.56.100: icmp_seq=4 ttl=64 time=0.954 ms
64 bytes from 192.168.56.100: icmp_seq=5 ttl=64 time=0.989 ms
64 bytes from 192.168.56.100: icmp_seq=6 ttl=64 time=0.327 ms
64 bytes from 192.168.56.100: icmp_seq=7 ttl=64 time=1.10 ms
64 bytes from 192.168.56.100: icmp_seq=8 ttl=64 time=1.42 ms
64 bytes from 192.168.56.100: icmp_seq=9 ttl=64 time=1.39 ms
64 bytes from 192.168.56.100: icmp_seq=10 ttl=64 time=1.23 ms
^C
--- 192.168.56.100 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9015ms
rtt min/avg/max/mdev = 0.290/0.987/1.420/0.391 ms
root@owaspbwa:~# _
```

```
C:\Users\labadmin>ping 192.168.56.100

Pinging 192.168.56.100 with 32 bytes of data:
Reply from 192.168.56.100: bytes=32 time<1ms TTL=64
Reply from 192.168.56.100: bytes=32 time=1ms TTL=64
Reply from 192.168.56.100: bytes=32 time<1ms TTL=64
Reply from 192.168.56.100: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.56.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\labadmin>ping 192.168.56.101

Pinging 192.168.56.101 with 32 bytes of data:
Reply from 192.168.56.101: bytes=32 time=2ms TTL=64
Reply from 192.168.56.101: bytes=32 time<1ms TTL=64
Reply from 192.168.56.101: bytes=32 time<1ms TTL=64
Reply from 192.168.56.101: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.56.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Users\labadmin>

C:\Users\labadmin>
```

Figure 16: Use ping from Kali and Windows to verify connectivity with the vulnerable machine.

- To ping the **Kali machine** from the vulnerable machine:

  ping 192.168.56.100

- When using a Host-Only network, a private network is created between the VMs, completely isolated from the external network.
- The **host machine** also has a VMware network interface that connects it to these private networks.
- To ping the Kali and OWASP VMs, use the host (physical) machine.

  ping 192.168.56.100

  ping 192.168.56.101

Figure 16 also shows the lab environment setup based on the tests performed above.

If you are working on the University Kali VM, you can skip all Docker installation steps. The required security environments (**DVWA**, **OWASP Juice Shop**, etc.) are already installed (Fig. 17) and running within Docker containers on your machine."

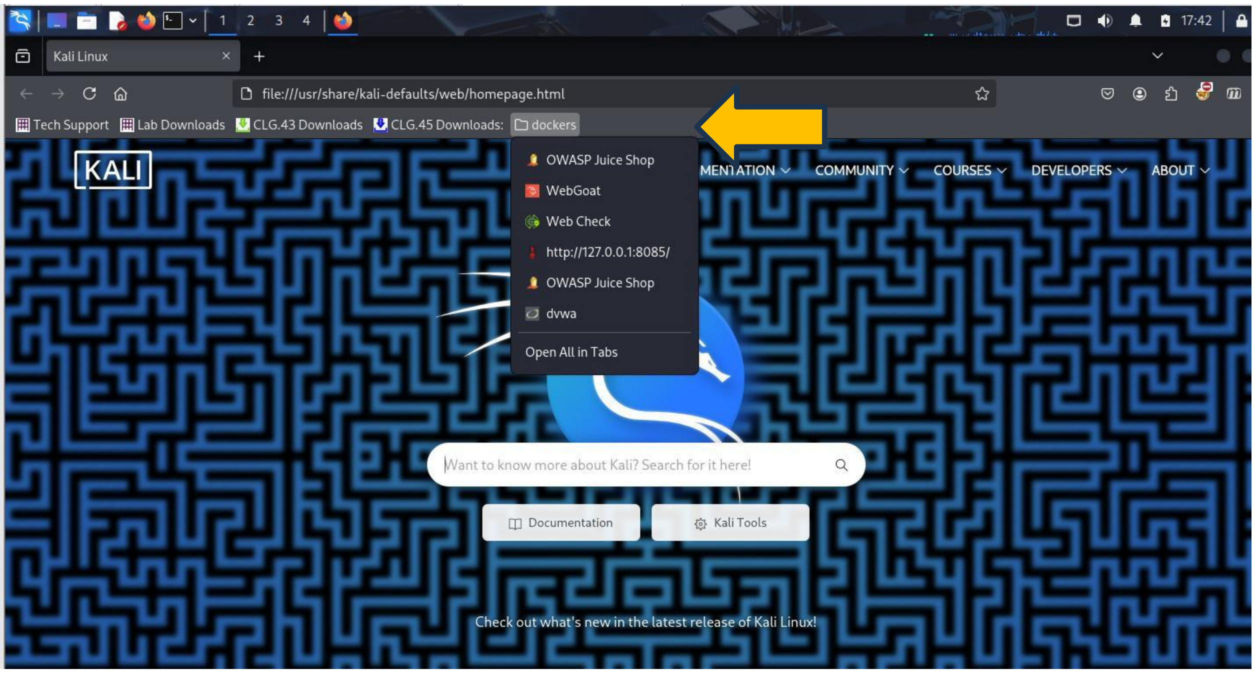


Figure 17: Docker containers – Kali Web

Instructions

Setup for the Vulnerable Juice shop server

- The penetration test for your assessment should be conducted on the Juice Shop website (locally installed)
- Instructions on how to install the Juice Shop website site on Kali VM is provided below.
- No further information including passwords will be provided.

This assignment requires only a **Kali Linux virtual machine (VM)** and **Burp Suite**.

- Ensure that the Kali Linux VM is running and that its network interface is set to **NAT**.
- Before starting the installation, update the Kali Linux package repository:

```
sudo apt-get update
```

- Install **Docker**, which is required to run the vulnerable machine:

```
sudo apt-get install docker-compose docker.io
```

- Navigate to your home directory:

```
cd ~
```

- Download the vulnerable **OWASP Juice Shop** server image:

```
sudo docker pull bkimminich/juice-shop
```

- (Optional) Add a local domain name to the **hosts** file. This allows access to the server using a custom domain name such as http://juiceshop.local:

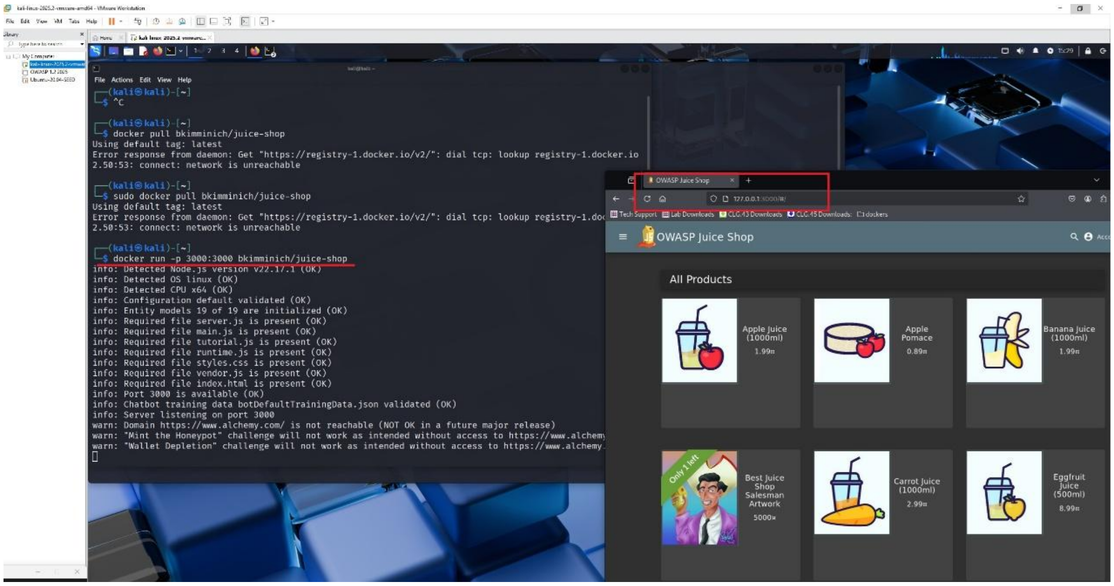
```
sudo sed -i '$a127.0.0.1 juiceshop.local' /etc/hosts
```

- Run the Juice Shop server:

```
sudo docker run --rm -p 3000:3000 bkimminich/juice-shop
```

- Once the Juice Shop server running, open your browser and go to the server's URL as shown below in Fig.18

http://juiceshop.local:3000 or 127.0.0.1:3000



```
┌──(kali㉿kali)-[~]
└─$ ^C

┌──(kali㉿kali)-[~]
└─$ docker pull bkimminich/juice-shop
Using default tag: latest
Error response from daemon: Get "https://registry-1.docker.io/v2/": dial tcp: lookup registry-1.docker.io
2.50:53: connect: network is unreachable

┌──(kali㉿kali)-[~]
└─$ sudo docker pull bkimminich/juice-shop
Using default tag: latest
Error response from daemon: Get "https://registry-1.docker.io/v2/": dial tcp: lookup registry-1.doc
2.50:53: connect: network is unreachable

┌──(kali㉿kali)-[~]
└─$ docker run -p 3000:3000 bkimminich/juice-shop
info: Detected Node.js version v22.17.1 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Entity models 19 of 19 are initialized (OK)
info: Required file server.js is present (OK)
info: Required file main.js is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file runtime.js is present (OK)
info: Required file styles.css is present (OK)
info: Required file vendor.js is present (OK)
info: Required file index.html is present (OK)
info: Port 3000 is available (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Server listening on port 3000
warn: Domain https://www.alchemy.com/ is not reachable (NOT OK in a future major release)
warn: "Mint the Honeypot" challenge will not work as intended without access to https://www.alchemy
warn: "Wallet Depletion" challenge will not work as intended without access to https://www.alchemy.
```

File Actions Edit View Help
OWASP Juice Shop
127.0.0.1:3000/#/
Tech Support
Lab Downloads
CLG.43 Downloads
CLG.45 Downloads
dockers
OWASP Juice Shop
All Products
Apple Juice (1000ml) 1.99¤
Apple Pomace 0.89¤
Banana Juice (1000ml) 1.99¤
Only 1 left
Best Juice Shop Salesman Artwork 5000¤
Carrot Juice (1000ml) 2.99¤
Eggfruit Juice (500ml) 8.99¤

Figure 18: Kali Web and OWASP Juice Shop

Extra machine to test your skills DVWS

- The penetration test should be conducted on the Juice Shop website (locally installed)
- Instructions on how to install the Juice Shop website site on Kali VM is provided below.
- No further information including passwords will be provided.

This assignment requires only a **Kali Linux virtual machine (VM)** and **Burp Suite**.

- Ensure that the Kali Linux VM is running and that its network interface is configured to **NAT**.
- Navigate to your home directory:

```
cd ~
```

- Download the vulnerable API server **DVWS**:

```
git clone https://github.com/snoopysecurity/dvws-node.git
```

- (Optional) Add a local domain name to the **hosts** file. This allows you to access the server using a custom domain such as http://dvws.local:

```
sudo sed -i '$a127.0.0.1 dvws.local' /etc/hosts
```

- Navigate to the DVWS directory:

```
cd dvws-node
```

- Start the DVWS server:

```
sudo docker-compose up
```

- Once the DVWS server is running, open a web browser and navigate to(see in Fig.19):

```
http://dvws.local
```

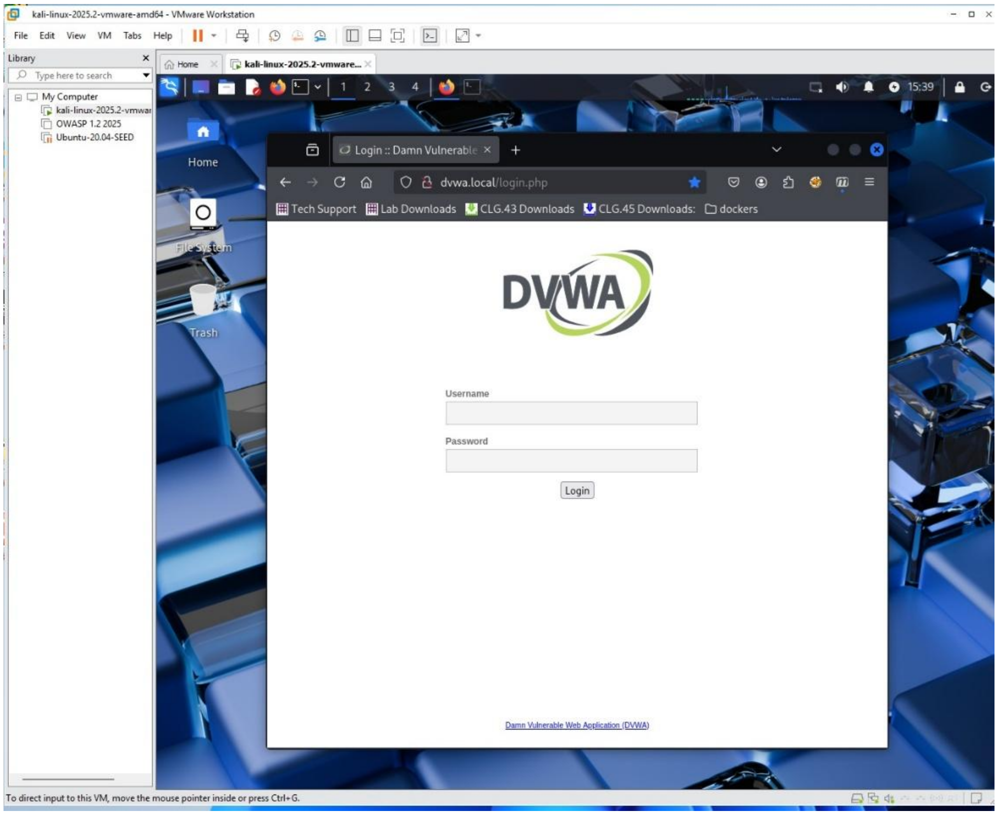


Figure 19: OWASP DVWA (Damn Vulnerable Web Application)

5 Potential Problems on Your Personal Machine

The following issues may occur when running virtual machines on your personal computer:

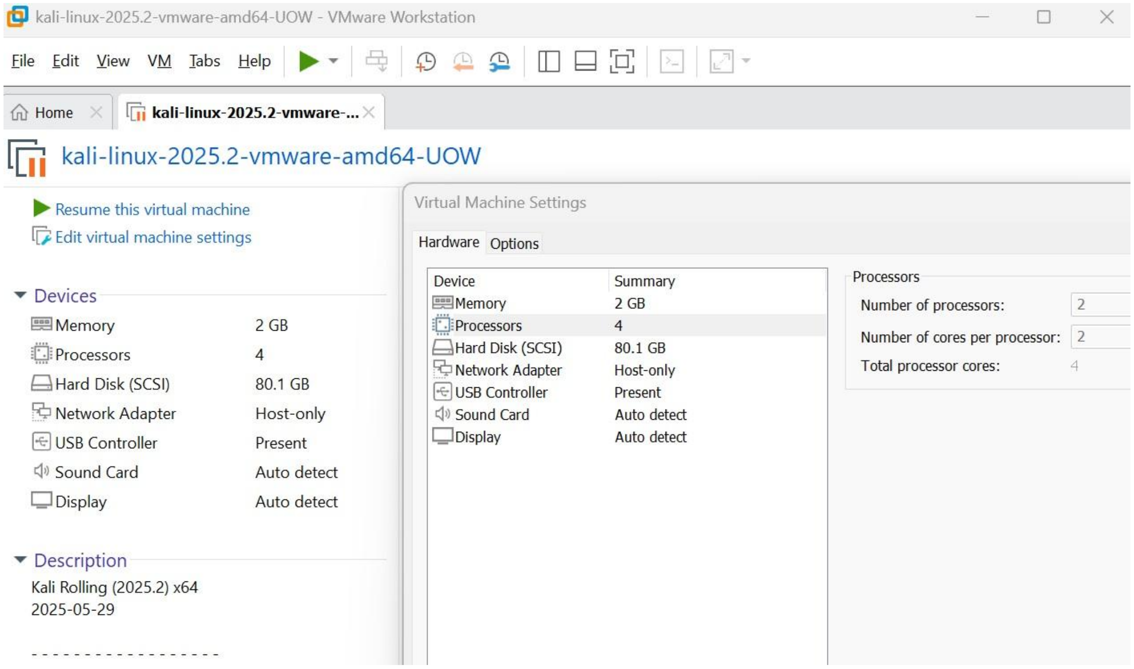
1. **Resource Allocation Issues**
   - **High CPU Usage**: Virtual machines are resource-intensive, particularly when running multiple VMs at once. Each VM consumes CPU power, which could lead to your personal computer becoming sluggish or unresponsive if the hardware (CPU, RAM) isn't powerful enough.
   - **Memory Overload**: VMs require significant amounts of RAM. If you allocate too much

memory to the VM, your host system might not have enough left to run smoothly, resulting in system slowdowns.

- **Storage Space**: VMs can take up a lot of disk space, especially if you’re running large operating systems or complex environments. This can quickly fill up your hard drive, especially if you're running multiple VMs.

2. **Virtualization Support**
   - **BIOS/UEFI Settings**: Many computers require virtualization to be enabled in the BIOS/UEFI settings to run VMs (e.g., Intel VT-x or AMD-V). If this is not enabled, VMs may not run at all or may experience poor performance.
3. **System Stability and Crashes**
   - **System Instability**: If your computer doesn’t have enough resources (CPU, RAM, disk space) to handle multiple VMs, it could lead to system crashes or blue screens, especially if you're running resource-heavy applications inside the VMs.
   - **VM Crashes**: Virtual machines themselves are not immune to crashes, and if one VM crashes, it may cause performance degradation for the host system or other running VMs.

     A quick solution is to increase the number of VM processes and the size of memory to improve reliability, as shown in Fig. 20.


kali-linux-2025.2-vmware-amd64-UOW - VMware Workstation
File
Edit
View
VM
Tabs
Help
Home
kali-linux-2025.2-vmware-...
kali-linux-2025.2-vmware-amd64-UOW
Resume this virtual machine
Edit virtual machine settings
Virtual Machine Settings
Hardware
Options

Devices

Memory	2 GB
Processors	4
Hard Disk (SCSI)	80.1 GB
Network Adapter	Host-only
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Description

Kali Rolling (2025.2) x64
2025-05-29

Device	Summary
Memory	2 GB
Processors	4
Hard Disk (SCSI)	80.1 GB
Network Adapter	Host-only
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Processors

Number of processors: 2

Number of cores per processor: 2

Total processor cores: 4

Fig. 20: Increase the number of VM processes and memory size to improve reliability

4. **VMs fail to start or show an error**

   The error message usually indicates the cause. Common reasons include:
   - **Insufficient disk space**: Free up space on your machine to allow the VM to start.
   - **Virtualization not enabled**: Ensure that virtualization is enabled in your BIOS. For guidance, refer to Microsoft’s instructions or ask your lab tutor for assistance.
5. **Host-Only adapter not visible**
   - This indicates that the Host-Only network was not created. In VMware, make sure a

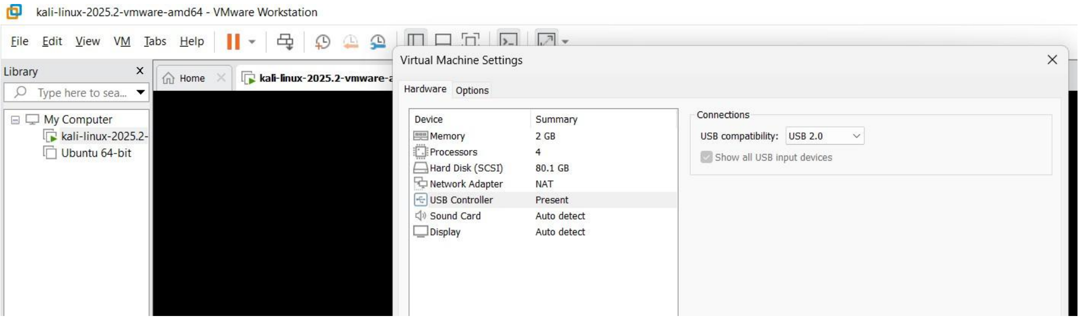
Host-Only network interface is created before starting the VM.

6. **Compatibility and Driver Issues:**
   - **Hardware Compatibility**: Some virtual machine platforms (e.g., VMware, VirtualBox) might not be fully compatible with all hardware, particularly older or more specialized components. This can lead to missing drivers, poor performance, or lack of support for certain devices.
   - **Peripheral Support**: Accessing external devices like printers, USB drives, or GPUs from within the VM can sometimes be tricky. VM software often requires specific drivers to pass hardware support through to the virtualized OS.

   For example: Incorrect USB Controller Configuration: USB controller error when starting the VM

   - On some machines, a USB controller error may occur. To fix it:
     - Go to **VM → Settings → USB Controller**
     - Change the controller to **USB 1.1 (USB 1.1 Controller)** (see Fig. 21).
7. **Network does not switch from NAT to Host-Only**
   - If the VM network does not switch correctly, open a terminal inside the VM and run:

```
sudo dhclie
```



Device	Summary
Memory	2 GB
Processors	4
Hard Disk (SCSI)	80.1 GB
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

USB compatibility: USB 2.0

☑ Show all USB input devices

Figure 21: USB error

Safety and Ethics Note

- This lab uses intentionally vulnerable systems solely for educational purposes.
- All activities must be conducted within the local lab virtual machine (VM) environment. Testing against external or production systems is strictly prohibited.