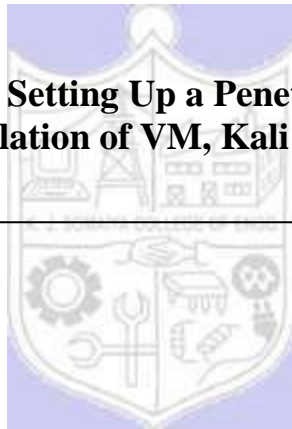


Experiment No. 2

**Title: Setting Up a Penetration Testing Environment:
Installation of VM, Kali Linux, and Metasploitable**



Batch: A2**Roll No.: 16010421073****Experiment No.:2**

Aim: Setting Up a Penetration Testing Environment: Installation of VM, Kali Linux, and Metasploitable.

Resources needed: Virtualization Software, Kali Linux ISO, Metasploitable VM, Virtualization Software (e.g., VMware Workstation, VirtualBox), Network Connectivity

Pre Lab/ Prior Concepts:

Students should have prior knowledge of Penetration Testing, Virtualization Technology, Operating System Fundamentals, Network Basics, ISO Files and Installation, Security Best Practices, Ethical Hacking Principles, File Management Skills.

Theory:

Setting up a penetration testing environment is a crucial step for individuals aspiring to enhance their skills in ethical hacking and cybersecurity. This process involves the creation of a controlled, isolated environment where security professionals can simulate real-world scenarios, identify vulnerabilities, and practice ethical hacking techniques. This one-page theory outlines the key aspects of setting up such an environment, focusing on the installation of a virtual machine (VM), Kali Linux, and Metasploitable.

Virtualization Technology: Virtualization serves as the foundation for the penetration testing environment. It allows the creation of virtual instances of operating systems on a single physical machine. Hypervisors, such as VMware Workstation or VirtualBox, enable the management of VMs, providing an isolated environment for testing without impacting the host system.

Operating System Fundamentals: Understanding the basics of operating systems is paramount. Both Kali Linux and Metasploitable are specialized operating systems designed for penetration testing purposes. Familiarity with file systems, user permissions, and system configurations ensures successful installation and effective use of these OSs.

ISO Files and Installation: The installation process often involves ISO files—disk images containing the complete contents of an optical disc. Knowing how to work with ISO files is crucial, as Kali Linux is typically installed from such an image. This step includes configuring disk partitions, setting up user accounts, and customizing system parameters.

Networking Basics: Proper networking configurations are essential for communication between the host machine, Kali Linux VM, and Metasploitable VM. A grasp of networking fundamentals, including IP addresses, subnets, and common protocols like TCP/IP, ensures seamless connectivity within the environment.

Security Best Practices: Incorporating security best practices during the setup is imperative. This includes enforcing strong authentication, applying encryption where applicable, and adhering to the principle of least privilege. Such measures enhance the overall security of the testing environment.

Ethical Hacking Principles: Setting up a penetration testing environment aligns with ethical hacking principles. Obtaining proper authorization before conducting security assessments, respecting privacy, and responsibly reporting findings are essential components. Adherence to ethical principles ensures that security testing is conducted lawfully and responsibly.

Procedure:

Kali Linux : Exploring Kali Linux involves getting familiar with its interface, understanding basic

commands, and exploring the pre-installed tools.

Step 1: Create a New Virtual Machine (VM):

1. Open virtualization software (e.g., VMware Workstation) and click on "New Virtual Machine" to start the VM creation wizard.
2. Choose "Typical" for a standard VM setup.
3. Select the Kali Linux ISO file as the installation source when prompted.
4. Complete the VM configuration, specifying the amount of RAM, hard disk size, and other settings.
5. Start the VM to begin the Kali Linux installation process.

Step 2: Install Kali Linux:

1. Follow the on-screen instructions during the Kali Linux installation process.
2. Choose language, location, and keyboard layout.
3. Configure the network settings, hostname, and domain name, and set the root password.
4. Partition the disk or use the default settings.
5. Confirm the installation summary and proceed with the installation.
6. Once the installation is complete, eject the Kali Linux ISO and reboot the VM.

Step 3: Download and Import Metasploitable VM:

1. Download the Metasploitable VM image and extract it to a folder on the host machine.
2. Open virtualization software and import the Metasploitable VM. This process may vary depending on the virtualization platform.
3. Configure the Metasploitable VM settings, ensuring it has network connectivity.

Step 4: Set Up Networking:

1. Ensure the Kali Linux and Metasploitable VM are on the same virtual network.
2. Configure the network settings of each VM, ensuring they can communicate with each other.

Step 5: Verify Connectivity:

1. Start both the Kali Linux and Metasploitable VMs.
2. Open a terminal in Kali Linux and verify the network connectivity to Metasploitable using tools like ping or nmap.

Step 6: Update and Install Tools:

1. In Kali Linux, open a terminal and run `sudo apt update` and `sudo apt upgrade` to update the system.
2. Install additional tools relevant to penetration testing using the package manager (apt).

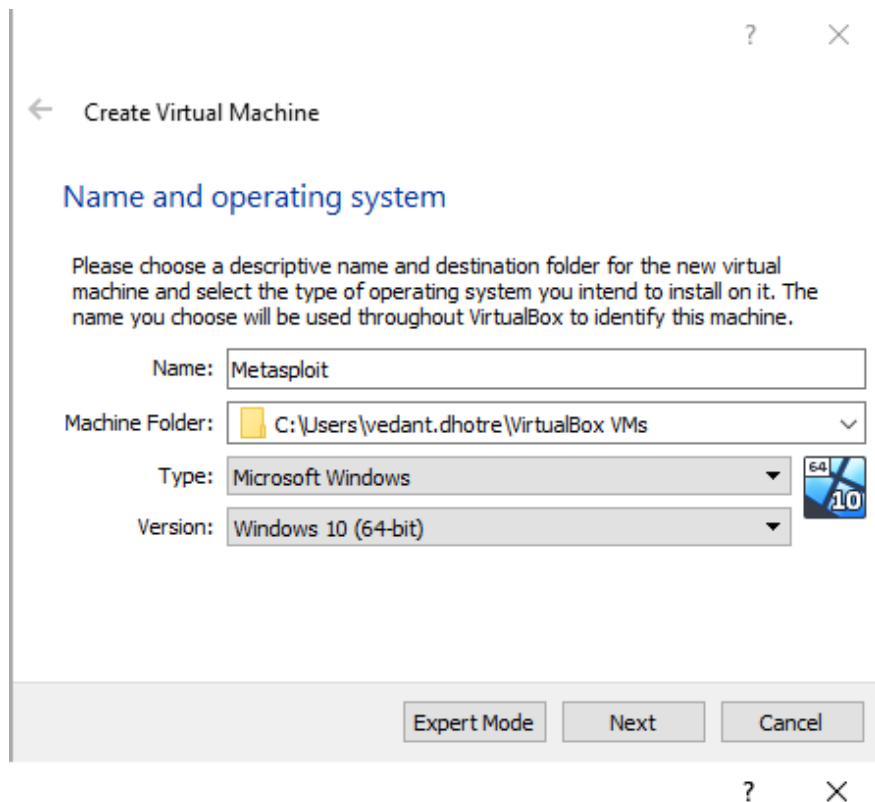
Step 7: Test the Environment:

1. Launch penetration testing tools in Kali Linux and perform basic tests on the Metasploitable VM. For example, use Nmap to scan for open ports.
2. Explore and familiarize with the tools available in Kali Linux for ethical hacking and penetration testing.

Output (Code with result Snapshot)

Metasploit

1) Creating new virtual machine Metasploit and also giving memory size to it.



← Create Virtual Machine

Name and operating system

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

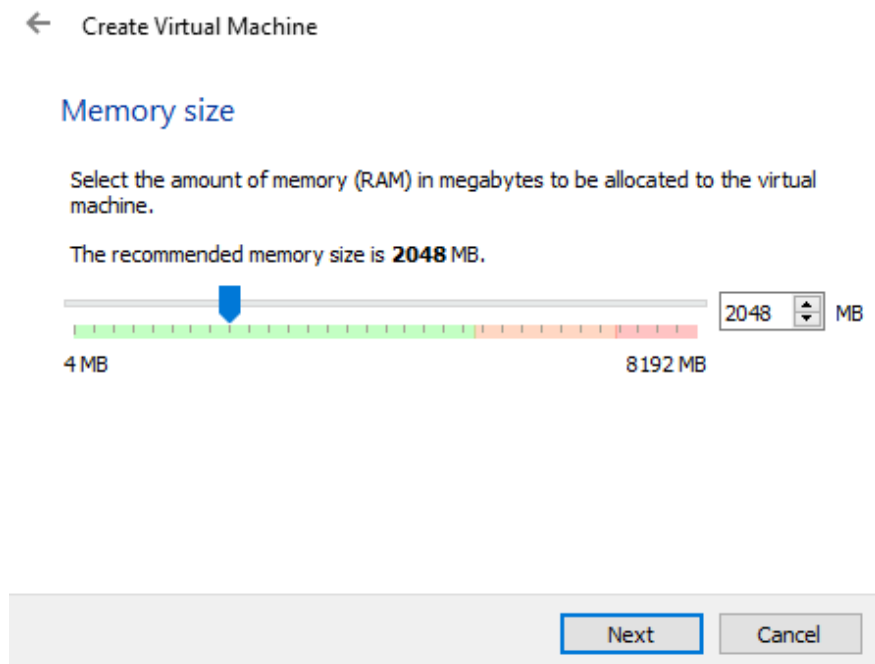
Name:

Machine Folder:

Type:

Version:

Expert Mode Next Cancel



← Create Virtual Machine

Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

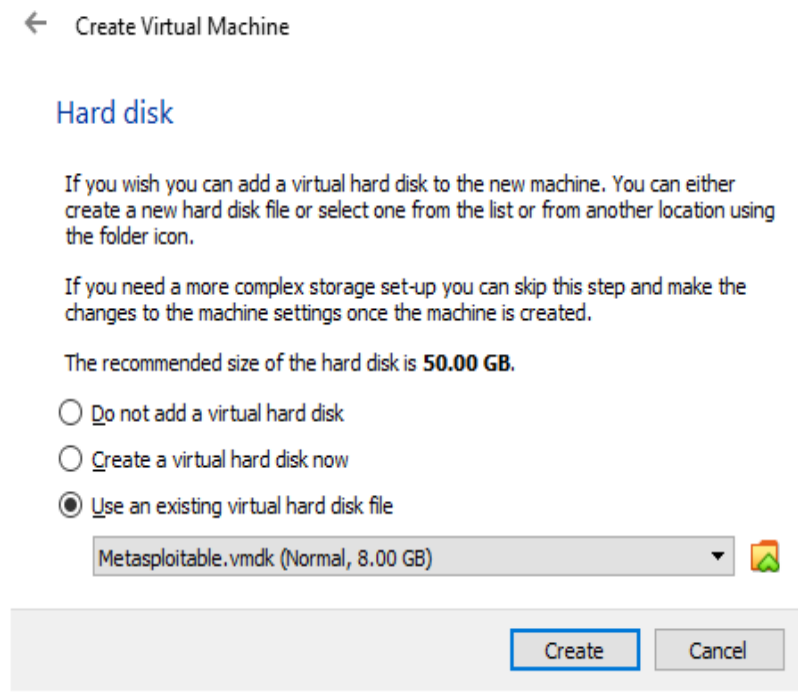
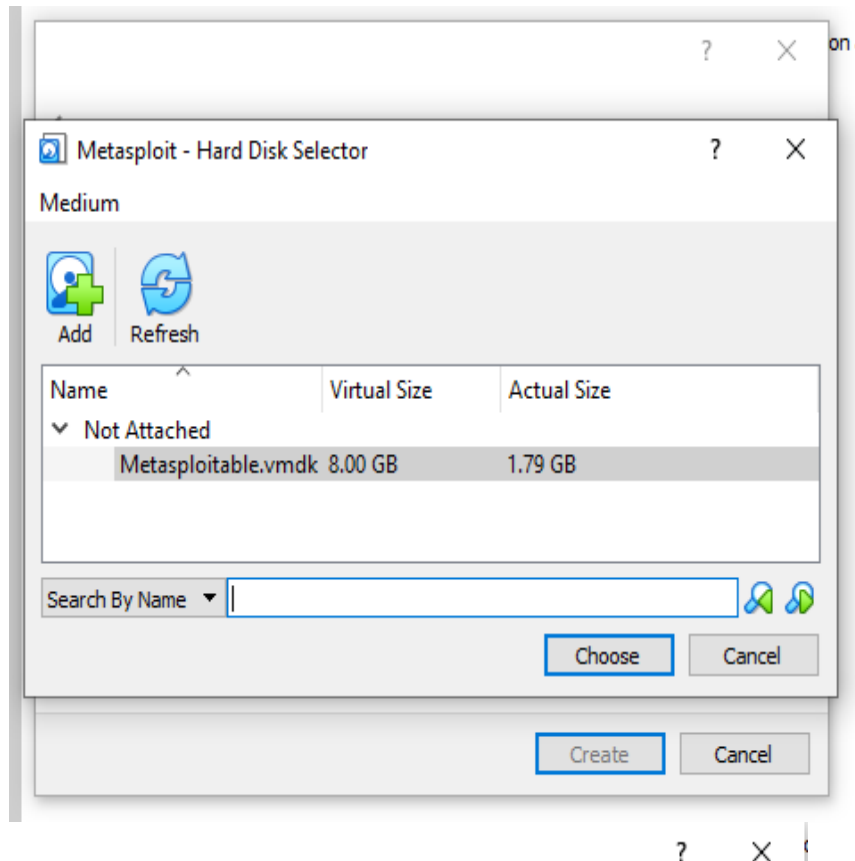
The recommended memory size is **2048 MB**.

4 MB 8192 MB

2048 MB

Next Cancel

2) Adding the Metasploit.vmdk file to hard disk selector.



3) After creating virtual machine you can see the VM information about Metasploitable.

Oracle VM VirtualBox Manager

File Machine Help

Tools

New Settings Discard Start

Metasploit
Powered Off

General

Name: Metasploit
Operating System: Windows 10 (64-bit)

System

Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: SATA
SATA Port 0: Metasploitable.vmdk (Normal, 8.00 GB)
SATA Port 1: [Optical Drive] Empty

Audio

Host Driver: Windows DirectSound
Controller: Intel HD Audio

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: OHCI
Device Filters: 0 (0 active)

Shared folders

None

Description

None

Preview

Metasploit

General

Name: Metasploit
Operating System: Windows 10 (64-bit)

System

Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: SATA
SATA Port 0: Metasploitable.vmdk (Normal, 8.00 GB)
SATA Port 1: [Optical Drive] Empty

Audio

Host Driver: Windows DirectSound
Controller: Intel HD Audio

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: OHCI
Device Filters: 0 (0 active)

Shared folders

None

Description

None

Preview

Metasploit

4) Starting Metasploit virtual box .

```

Metasploit [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: _

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Sun May 20 15:50:42 EDT 2012 from 172.16.123.1 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ _

```

DVWA


? ×


← Create Virtual Machine

Name and operating system

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name:

Machine Folder:  ▼

Type: ▼ 

Version: ▼

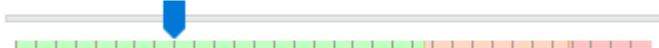
? ×

← Create Virtual Machine

Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **2048** MB.



MB

? ×

← Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **50.00 GB**.

☐ Do not add a virtual hard disk

☒ Create a virtual hard disk now

☐ Use an existing virtual hard disk file

Metasploitable.vmdk (Normal, 8.00 GB) 📁

Create

Cancel

? ×

← Create Virtual Hard Disk

Hard disk file type

Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

☒ VDI (VirtualBox Disk Image)

☐ VHD (Virtual Hard Disk)

☐ VMDK (Virtual Machine Disk)

Expert Mode

Next

Cancel



← Create Virtual Hard Disk

Storage on physical hard disk

Please choose whether the new virtual hard disk file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).

A **dynamically allocated** hard disk file will only use space on your physical hard disk as it fills up (up to a maximum **fixed size**), although it will not shrink again automatically when space on it is freed.

A **fixed size** hard disk file may take longer to create on some systems but is often faster to use.

- ☒ Dynamically allocated
- ☐ Fixed size

Next

Cancel

Oracle VM VirtualBox Manager

File Machine Help

Tools

Metasploit
Powered Off

DVWA
Powered Off

New Settings Discard Start

General

Name: DVWA
Operating System: Windows 10 (64-bit)

System

Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: SATA
SATA Port 0: DVWA.vdi (Normal, 50.00 GB)
SATA Port 1: [Optical Drive] Empty

Audio

Host Driver: Windows DirectSound
Controller: Intel HD Audio

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: OHCI
Device Filters: 0 (0 active)

Shared folders

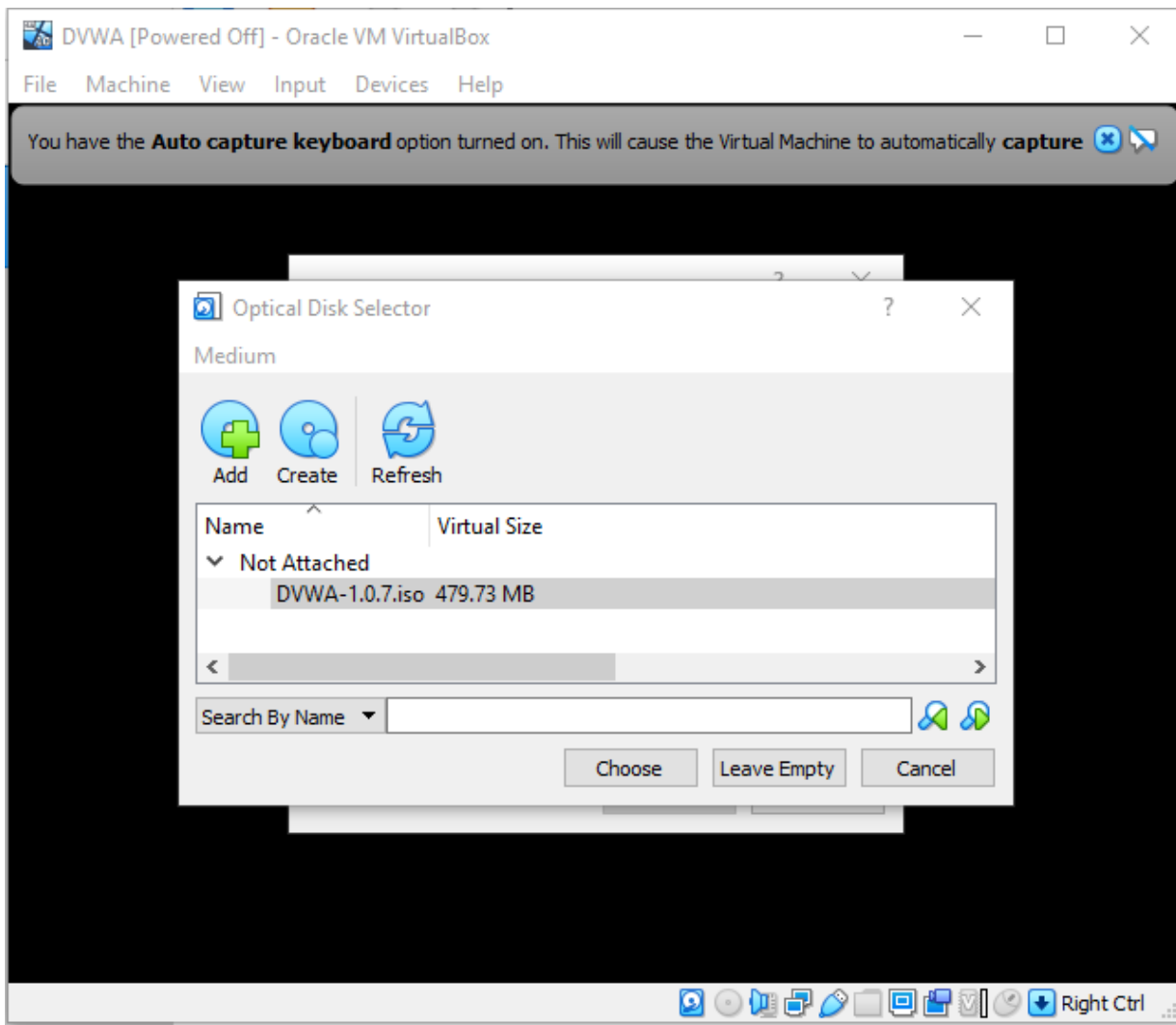
None

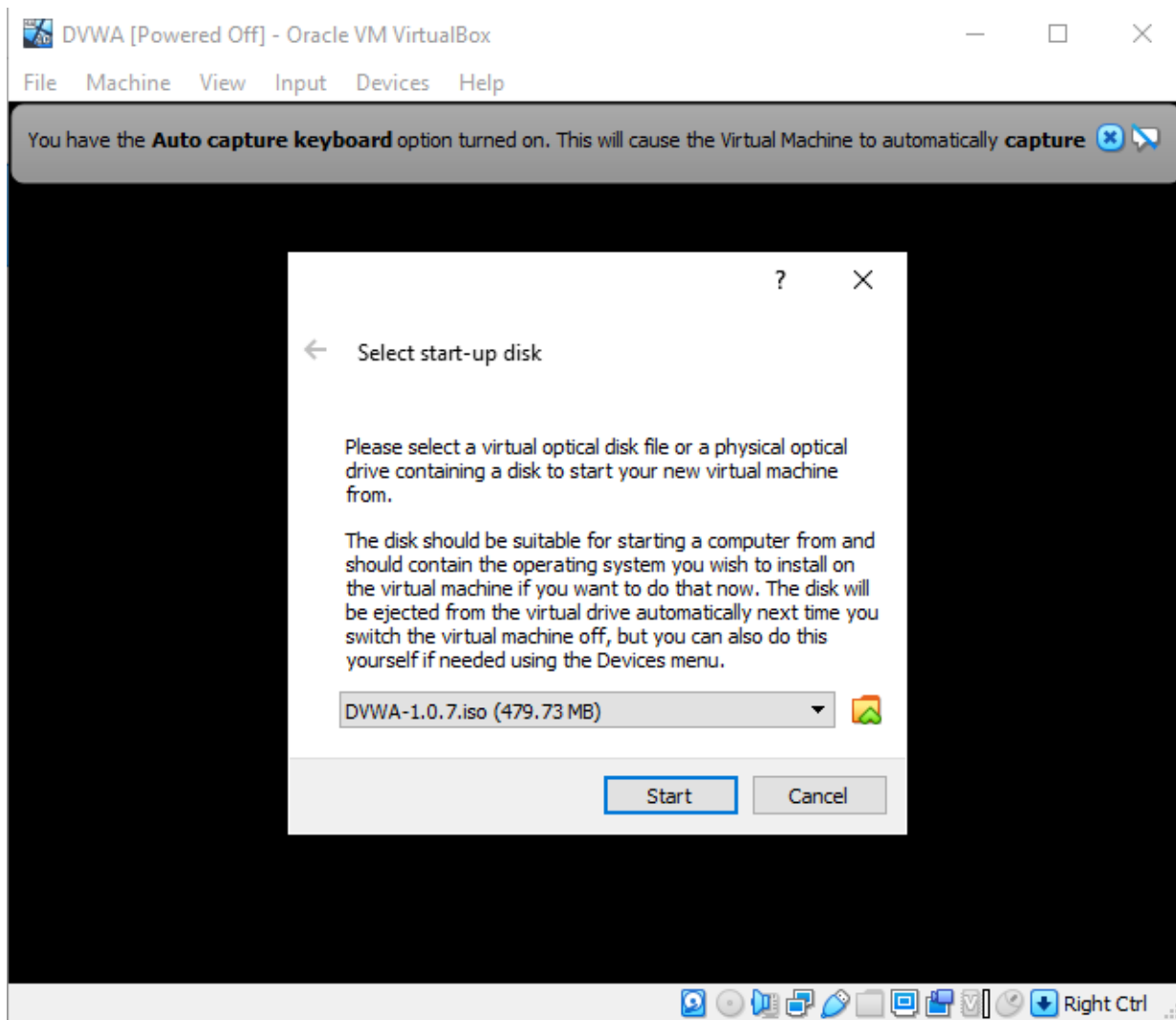
Description

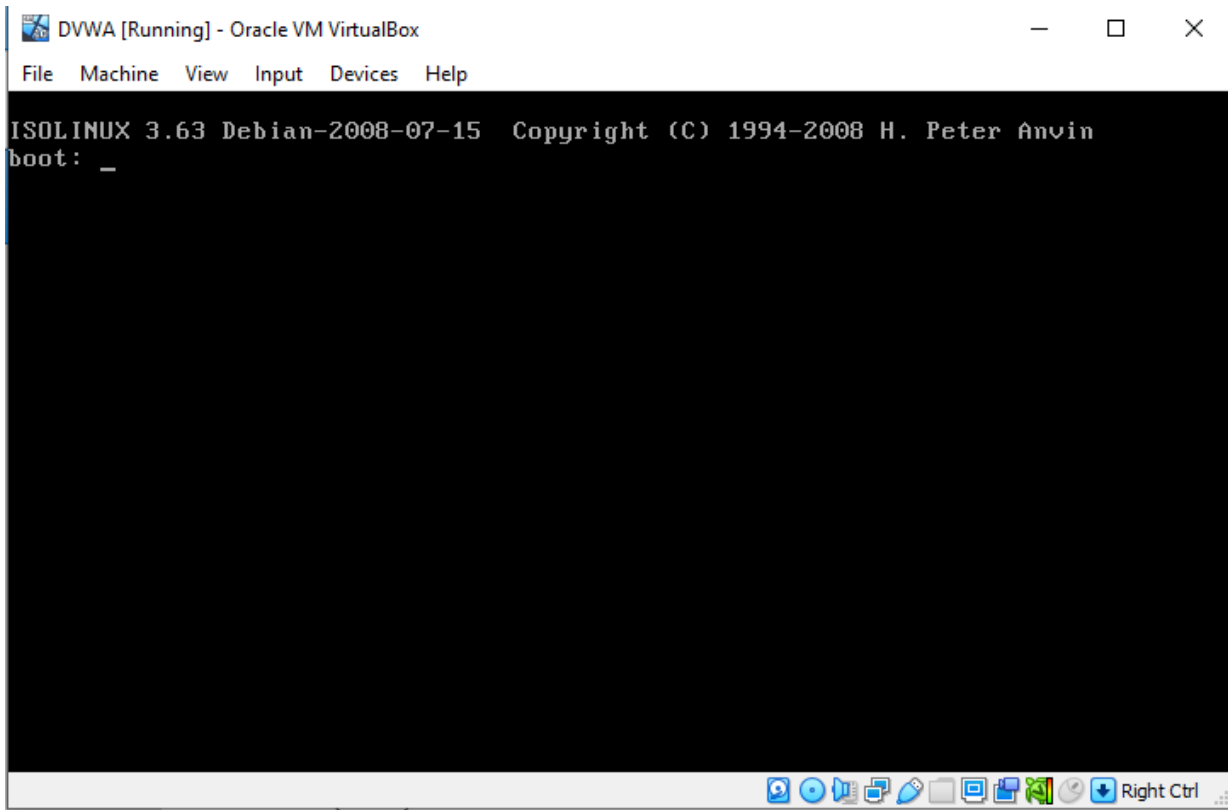
None

Preview

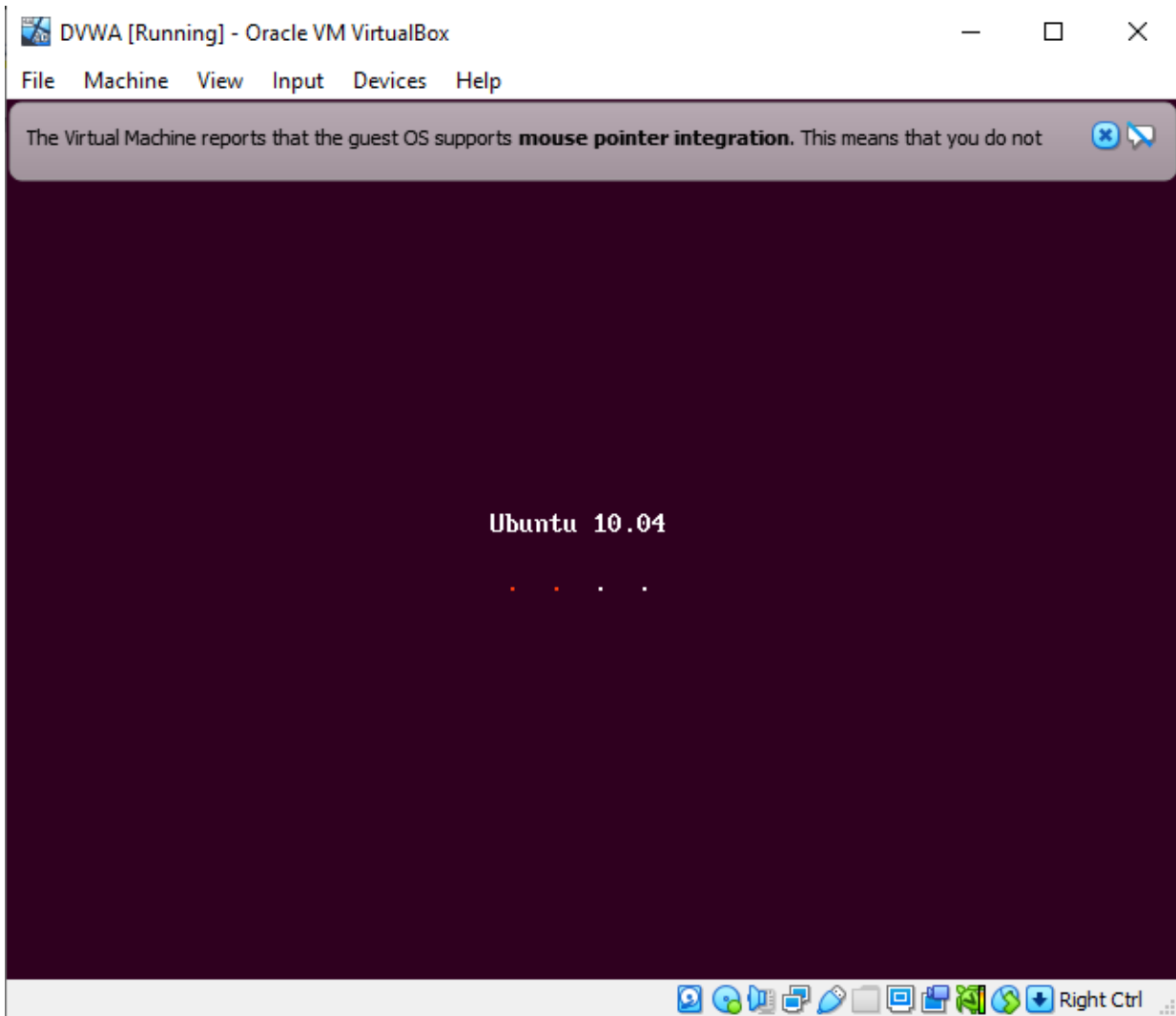
DVWA

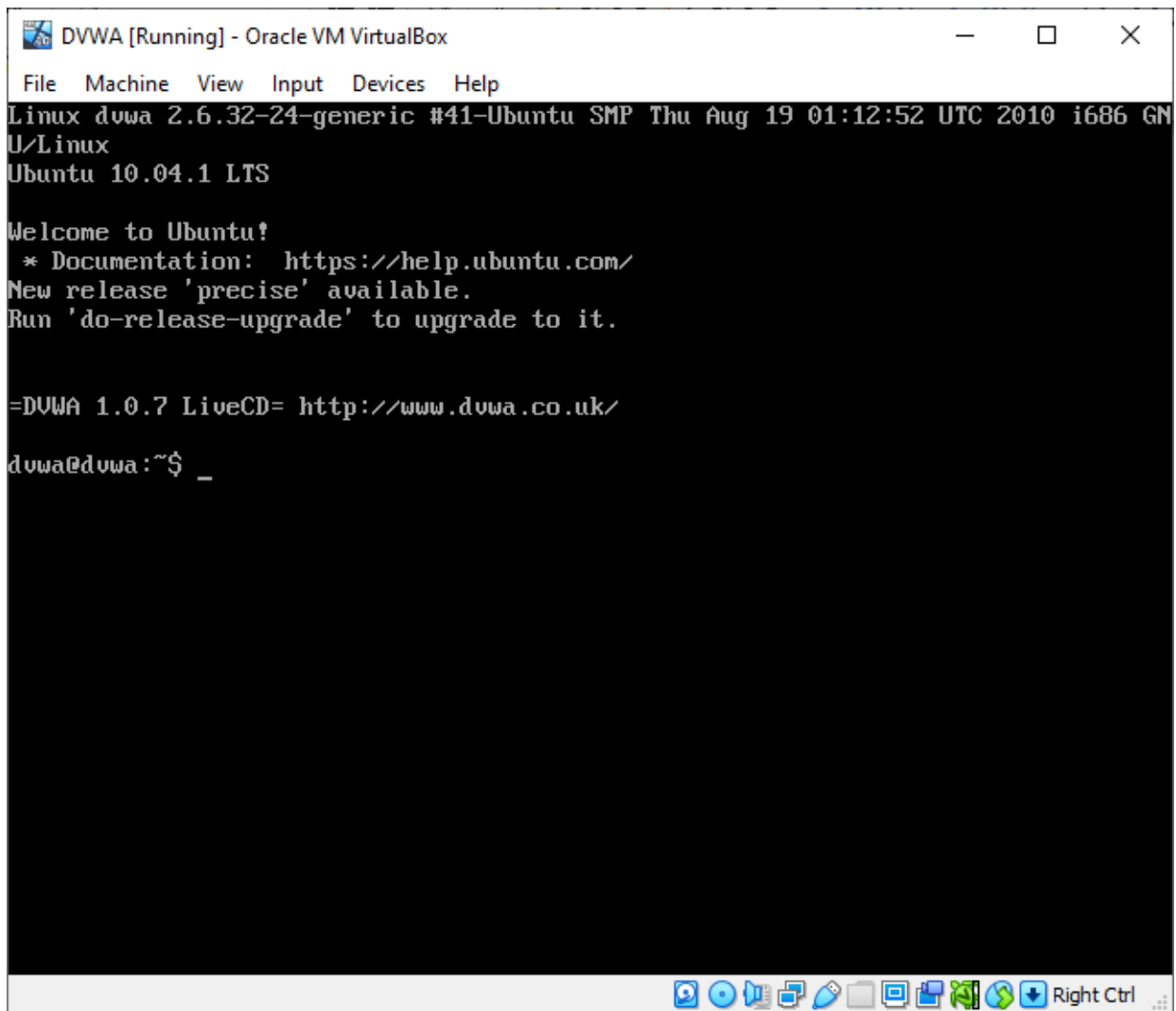












```
DVWA [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Linux duwa 2.6.32-24-generic #41-Ubuntu SMP Thu Aug 19 01:12:52 UTC 2010 i686 GNU/Linux
Ubuntu 10.04.1 LTS

Welcome to Ubuntu!
 * Documentation:  https://help.ubuntu.com/
New release 'precise' available.
Run 'do-release-upgrade' to upgrade to it.

=DVWA 1.0.7 LiveCD= http://www.dvwa.co.uk/

duwa@duwa:~$ _
```


Kali Linux

1) Naming the new virtual machine Kali-Linux ,path to folder ,type and version.

?

×

← Create Virtual Machine

Name and operating system

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name:

Kali Linux

Machine Folder:

C:\Users\vedant.dhotre\VirtualBox VMs

Type:

Linux

Version:

Linux 2.6 / 3.x / 4.x (64-bit)

64

2.6

Expert Mode

Next

Cancel

?

×

← Create Virtual Machine

Name and operating system

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name:

Kali Linux

Machine Folder:

C:\Users\vedant.dhotre\VirtualBox VMs

Type:

Microsoft Windows

Version:

Windows 10 (64-bit)

64

10

Expert Mode

Next

Cancel

2) Giving memory size to Kali linux along with creating new virtual hard disk.

The image shows two screenshots of the 'Create Virtual Machine' wizard. The top screenshot is the 'Memory size' step, and the bottom screenshot is the 'Hard disk' step.

Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **2048 MB**.

A slider bar shows the memory range from 4 MB to 8192 MB. The current value is 2048 MB, indicated by a blue arrow and a text box.

Next **Cancel**

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **50.00 GB**.

☐ Do not add a virtual hard disk

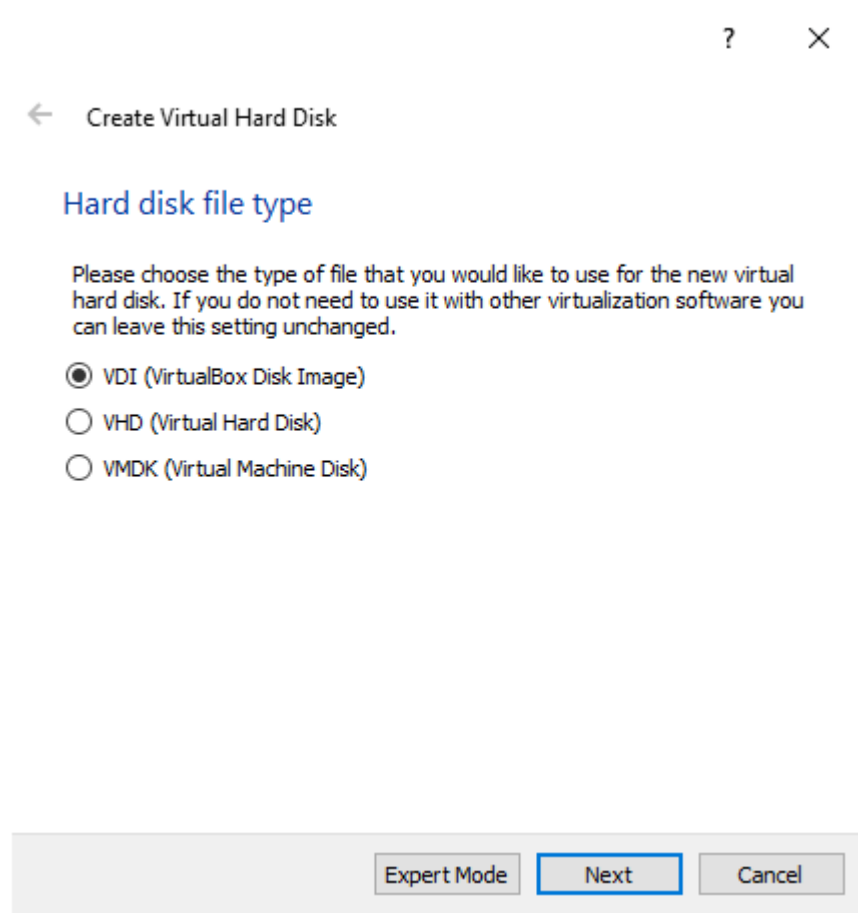
☒ Create a virtual hard disk now

☐ Use an existing virtual hard disk file

Metasploitable.vmdk (Normal, 8.00 GB)

Create **Cancel**

3) Selecting Hard disk file type.



← Create Virtual Hard Disk

Hard disk file type

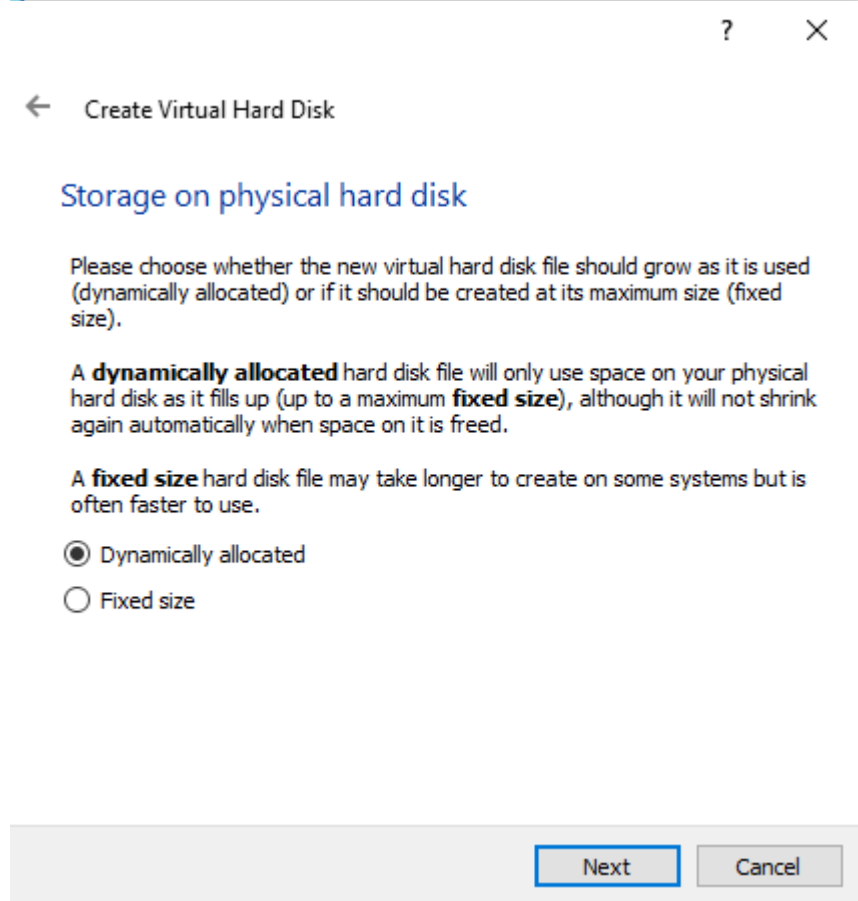
Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

☒ VDI (VirtualBox Disk Image)

☐ VHD (Virtual Hard Disk)

☐ VMDK (Virtual Machine Disk)

Expert Mode Next Cancel



← Create Virtual Hard Disk

Storage on physical hard disk

Please choose whether the new virtual hard disk file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).

A **dynamically allocated** hard disk file will only use space on your physical hard disk as it fills up (up to a maximum **fixed size**), although it will not shrink again automatically when space on it is freed.

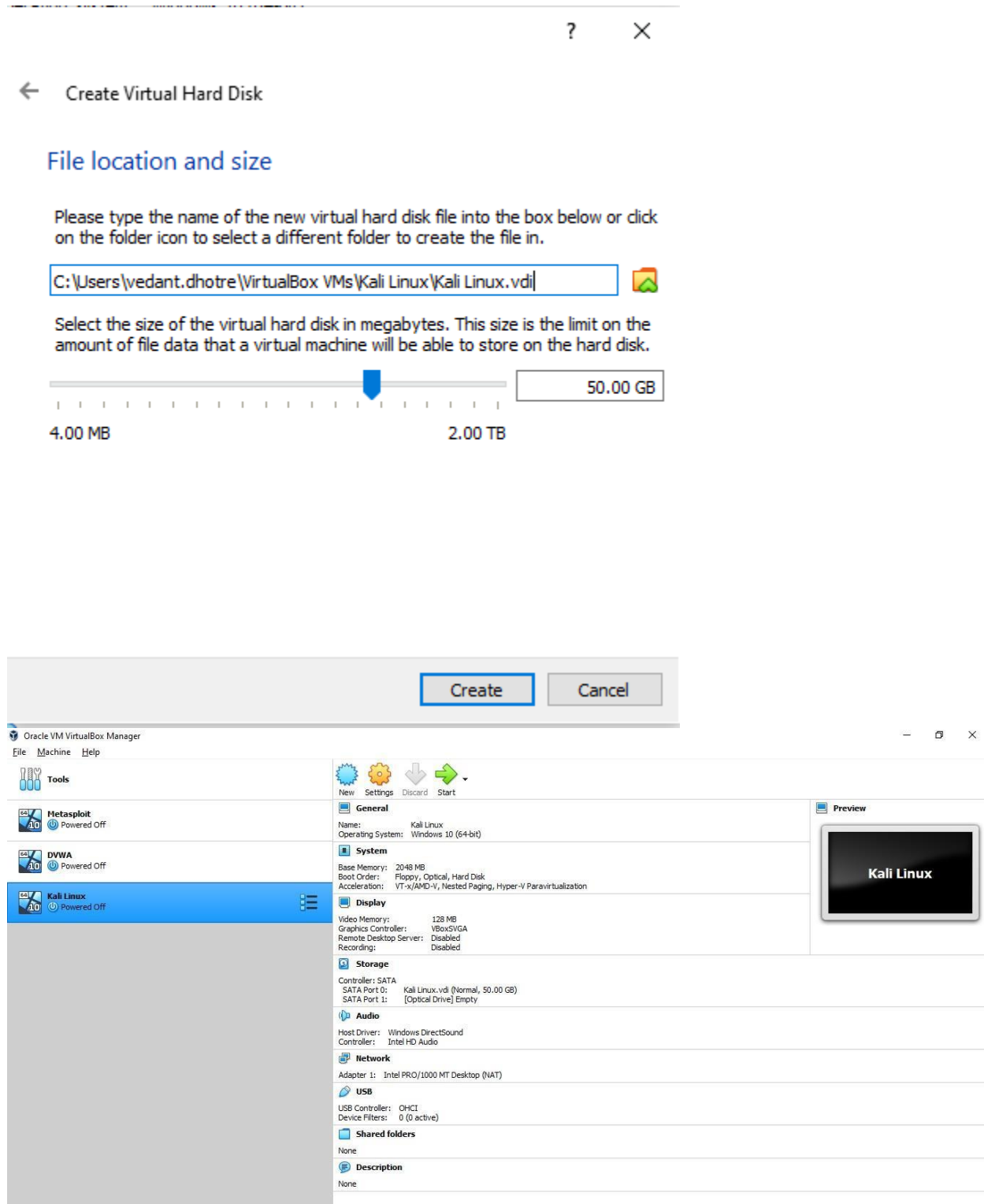
A **fixed size** hard disk file may take longer to create on some systems but is often faster to use.

☒ Dynamically allocated

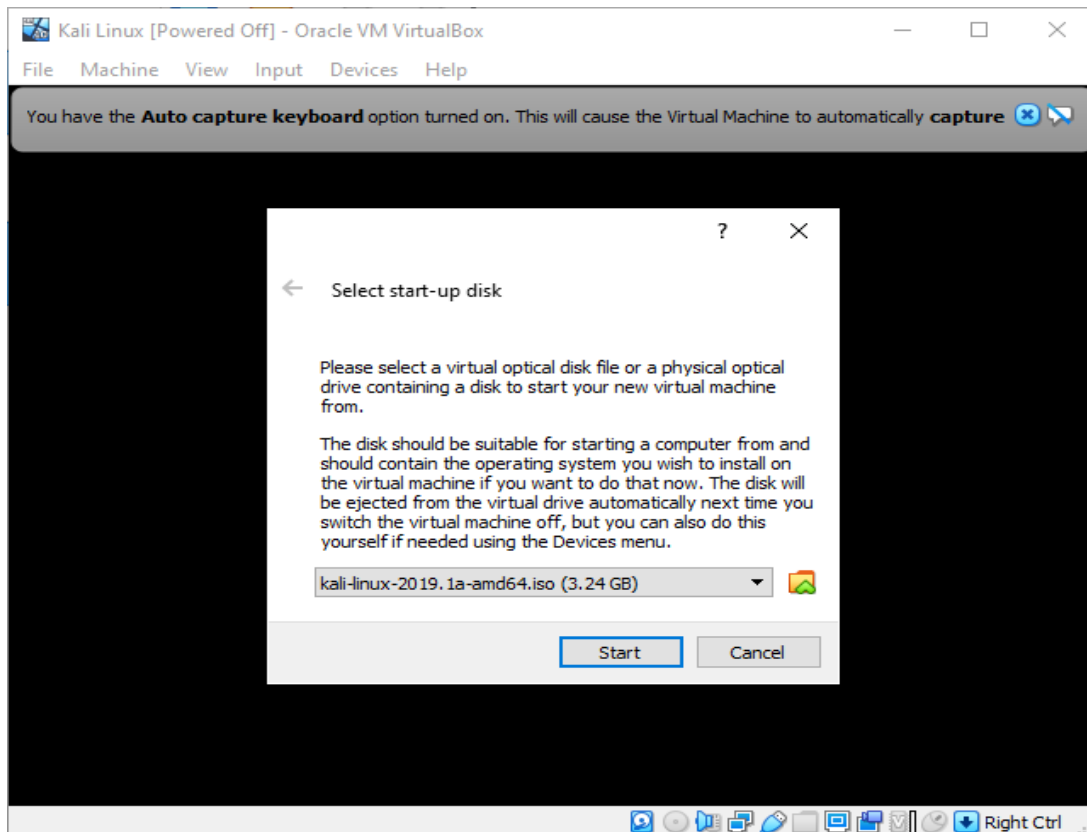
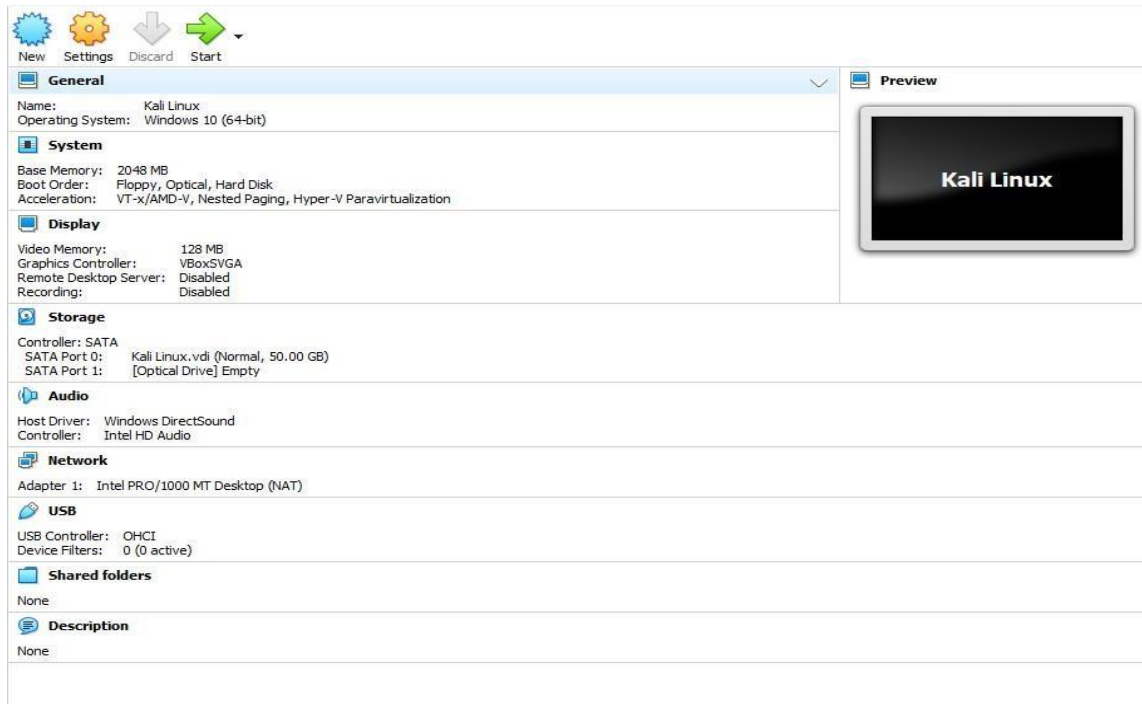
☐ Fixed size

Next Cancel

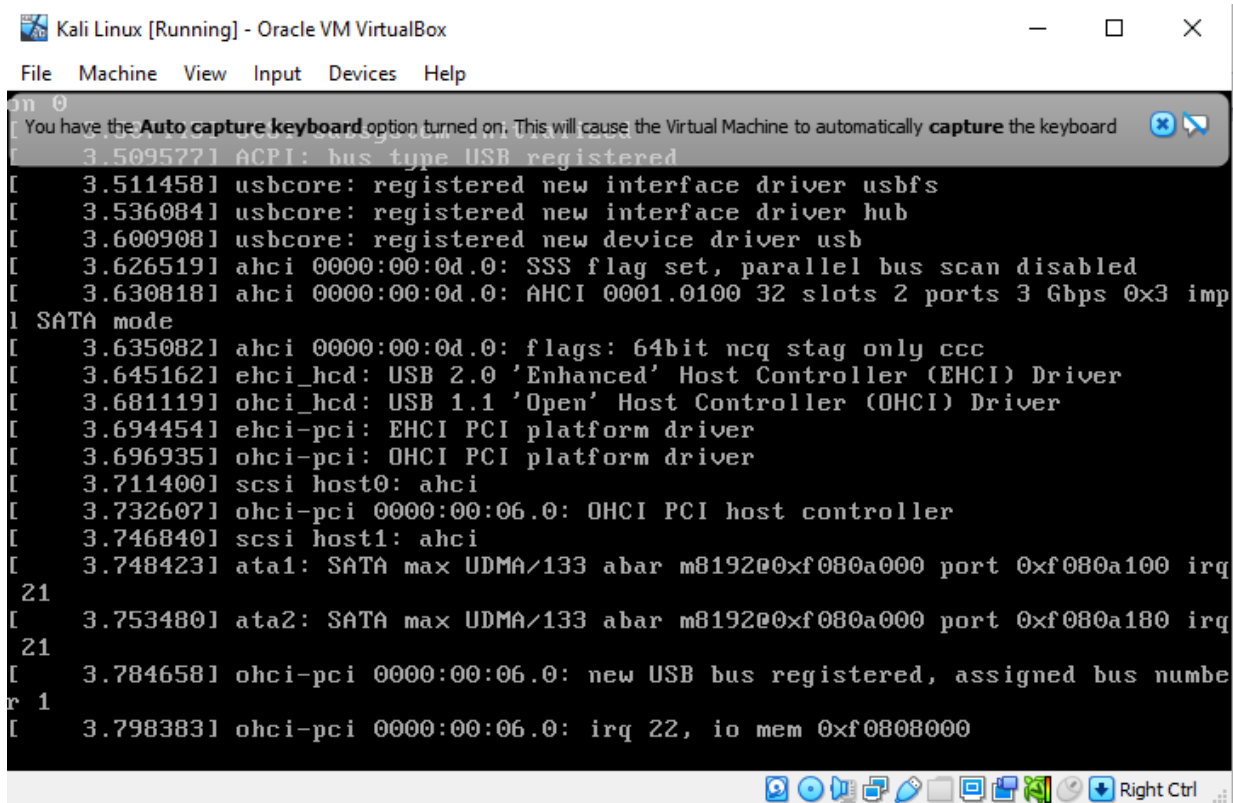
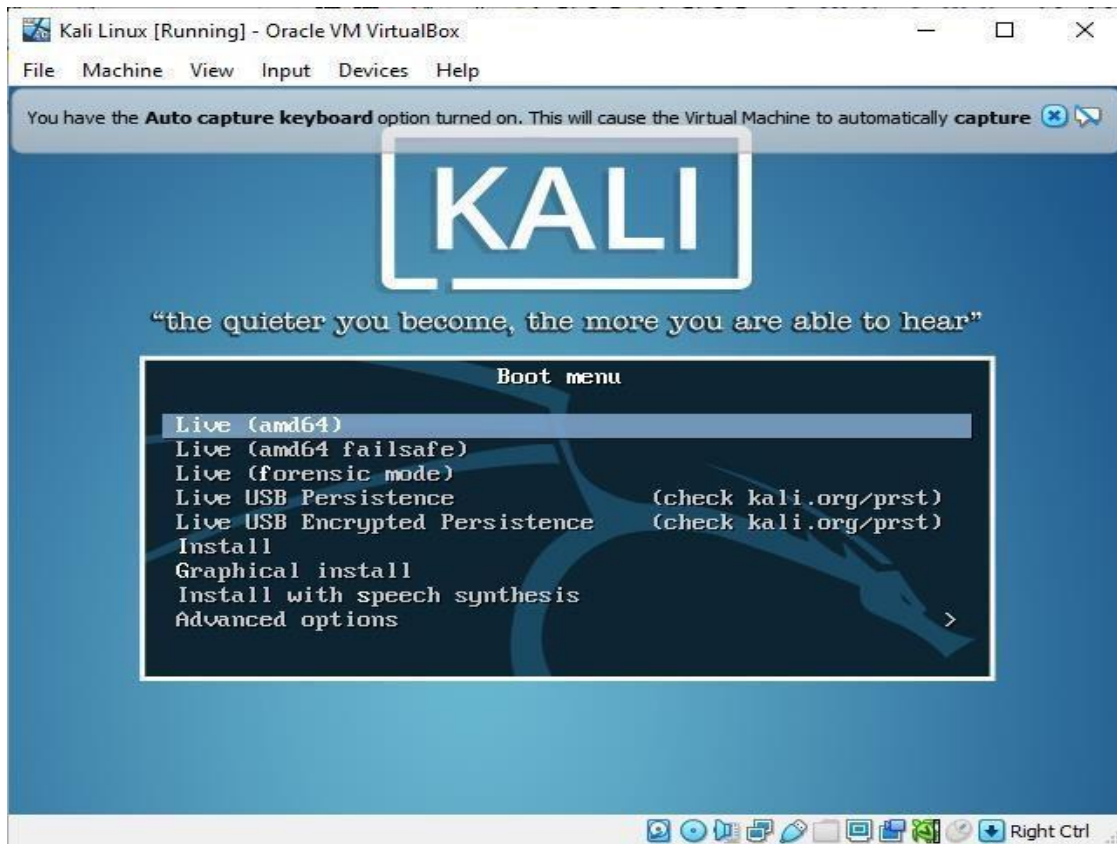
- 4) After giving memory to Virtual hard disk click 'create'.



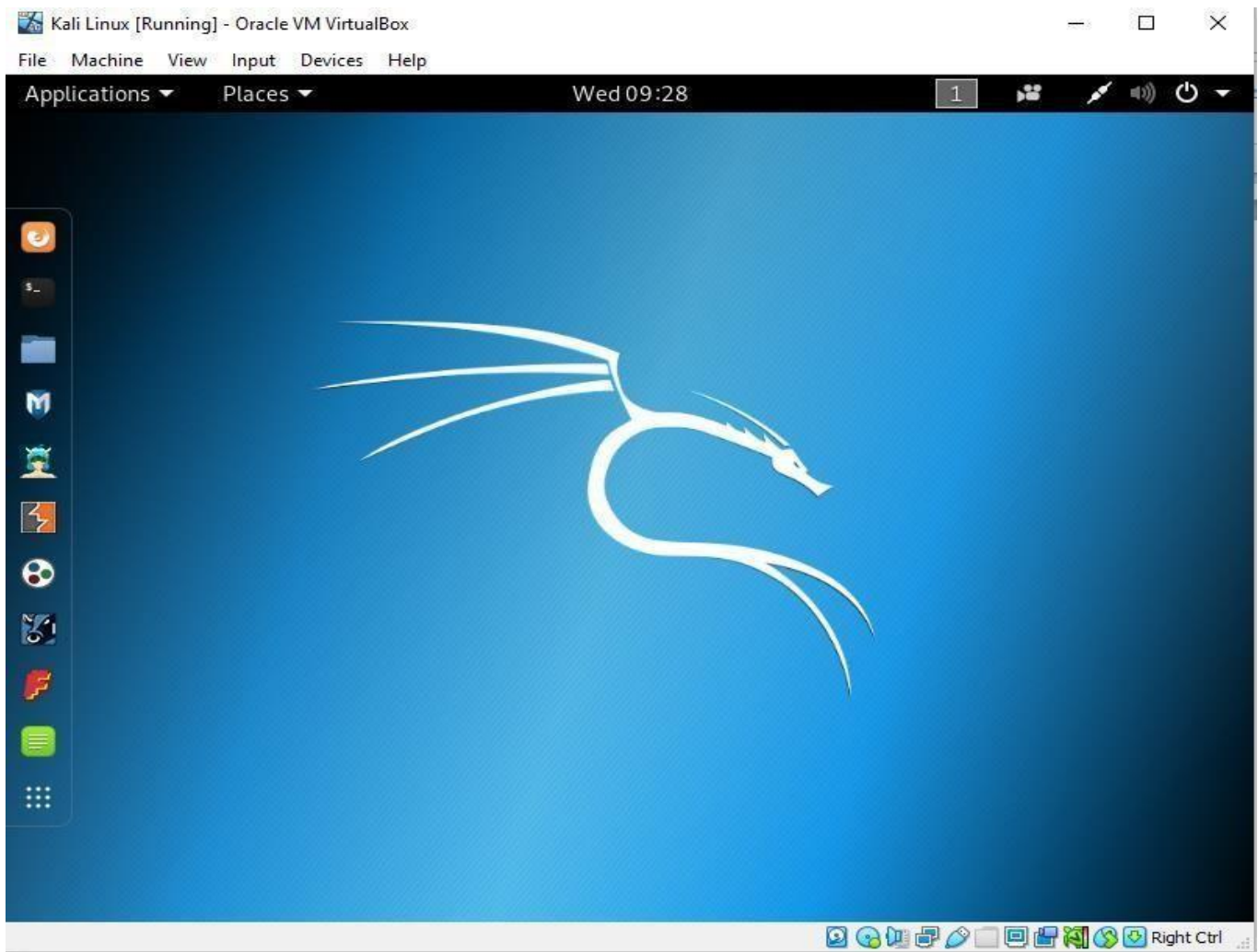
5) Start Kali Linux



6) Kali linux displays boot menu.



7) Kali linux Desktop.



Post Lab Questions: -

- 1. Describe the networking setup to ensure communication between the host machine, Kali Linux VM, and Metasploitable VM. What challenges could be encountered during the network configuration, and how can they be overcome? How can a well-established network contribute to the effectiveness of penetration testing?**

Ans: To ensure communication between the host machine, Kali Linux VM, and Metasploitable VM in penetration testing environment, a suitable networking setup needs to be established. This setup typically involves configuring network adapters and settings for each virtual machine and ensuring they can communicate with each other and with the host machine.

- 1. Configuring Virtual Machine Network Adapters:**

- Set the network adapter of each virtual machine to the appropriate mode, such as bridged, NAT, or host-only, depending on the requirements and the desired network topology.
- For communication between VMs and the host, a common choice is to use a bridged or host-only network mode.
- Bridged mode allows VMs to appear as separate devices on the physical network, while host-only mode enables communication only between VMs and the host machine.

- 2. Assigning IP Addresses:**

- Ensure each VM has a unique IP address within the same subnet to facilitate communication.
- Configure static IP addresses or utilize DHCP services, depending on the network setup and requirements.

- 3. Firewall and Security Considerations:**

- Disable firewalls or configure them to allow necessary traffic for communication and penetration testing activities.
- Ensure network security policies do not interfere with the intended communication between VMs.

- 4. Routing and Network Configuration:**

- Verify routing tables and network configurations to ensure packets are routed correctly between VMs and the host.
- Troubleshoot any connectivity issues by checking network settings and configurations.

- 5. Network Services and Protocols:**

- Ensure necessary network services and protocols (e.g., ICMP, TCP/IP) are enabled and functioning properly for communication and testing purposes.
- Challenges that could be encountered during network configuration include:

- 6. IP address conflicts:** Ensure each VM has a unique IP address to prevent conflicts.
- 7. Network segmentation:** If using multiple subnets or VLANs, ensure proper routing and network configuration.

8. **NAT traversal issues:** NAT configurations can sometimes hinder direct communication between VMs or between VMs and the host.
9. **Firewall restrictions:** Firewall rules may block certain types of traffic required for penetration testing. A well-established network contributes to the effectiveness of penetration testing in several ways:
 - Facilitates realistic testing scenarios by simulating real-world network environments.
 - Allows for comprehensive vulnerability assessment and exploitation testing across different network segments.
 - Enables the detection of security weaknesses and misconfigurations in network devices, services, and applications.
 - Provides a safe and isolated environment for conducting security testing without affecting production systems.
 - Supports collaboration and teamwork among penetration testers by providing a shared testing infrastructure.

2. **Evaluate the implemented security measures during the setup, including authentication, encryption, and the principle of least privilege. How to ensure that the penetration testing environment is secure and isolated? Discuss the ethical considerations and why ethical hacking principles are crucial.**

Answ:

1. Authentication:

- Ensure strong authentication mechanisms are in place for accessing the penetration testing environment, including strong passwords or multi-factor authentication (MFA).
- Utilize unique credentials for each user or administrator, and enforce password policies to prevent unauthorized access.

2. Encryption:

- Encrypt sensitive data such as credentials, configuration files, and communication channels to protect against eavesdropping and unauthorized access.
- Use secure protocols like SSH (Secure Shell) or TLS (Transport Layer Security) for remote access and communication.

3. Principle of Least Privilege:

- Follow the principle of least privilege by granting users and processes only the minimum permissions necessary to perform their tasks.
- Limit administrative privileges to trusted individuals and restrict access to sensitive resources and functions.

4. Network Isolation:

- Segment the penetration testing environment from production networks and systems to prevent accidental impact on operational systems.
- Utilize virtualization or containerization technologies to create isolated testing environments that can be easily controlled and reset.

To ensure that the penetration testing environment is secure and isolated:

- Regularly update and patch all software and operating systems within the environment to address known vulnerabilities and security weaknesses.
- Employ network segmentation and access controls to restrict communication between the testing

environment and external networks.

- Monitor and log all activities within the environment to detect and respond to any suspicious or unauthorized behavior.
- Conduct regular security assessments and audits to identify and remediate security issues proactively. Implement network and host-based intrusion detection and prevention systems to detect and block malicious activities.

Ethical considerations are paramount in penetration testing and ethical hacking practices. Ethical hacking principles ensure that security testing is conducted in a responsible and lawful manner, with the goal of improving security posture and protecting against malicious attacks. Some key reasons why ethical hacking principles are crucial include:

- I. **Legal Compliance:** Adhering to ethical hacking principles helps ensure compliance with relevant laws, regulations, and industry standards governing cybersecurity and data protection.
- II. **Minimize Harm:** Ethical hacking practices aim to minimize the risk of harm to systems, networks, and data during security testing activities. Testers must exercise caution to avoid causing disruption or damage to critical infrastructure.
- III. **Protect Privacy:** Ethical hackers must respect user privacy and confidentiality by handling sensitive information appropriately and obtaining necessary permissions before conducting security assessments.
- IV. **Maintain Trust:** Following ethical hacking principles helps build trust and credibility with clients, stakeholders, and the broader cybersecurity community. It demonstrates a commitment to ethical conduct and responsible security practices.
- V. **Promote Collaboration:** Ethical hacking fosters collaboration and information sharing among security professionals, researchers, and organizations to address common security challenges and threats effectively.

Outcomes: CO 1: Realize that premise of vulnerability analysis and penetration testing (VAPT)

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

In this experiment we downloaded and set up DVWA, Metasploit and Kali Linux and understood the working of it.

Signature of faculty in charge with date

References:

1. <https://www.tutorialsfreak.com/nmap-tutorial/metasploit-installation>
2. <https://medium.com/@nickhandy/kali-linux-metasploit-getting-started-with-pen-testing-89d28944097b>
3. <https://subscription.packtpub.com/book/security/9781788623179/1/ch01lv11sec16/setting-up-a-penetration-testing-lab>