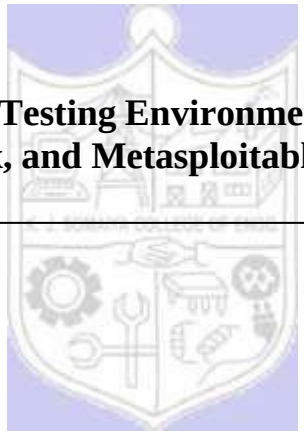
Experiment No. 2

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



Batch: A3 **Roll No.: 16010421119** **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 Linix : 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:

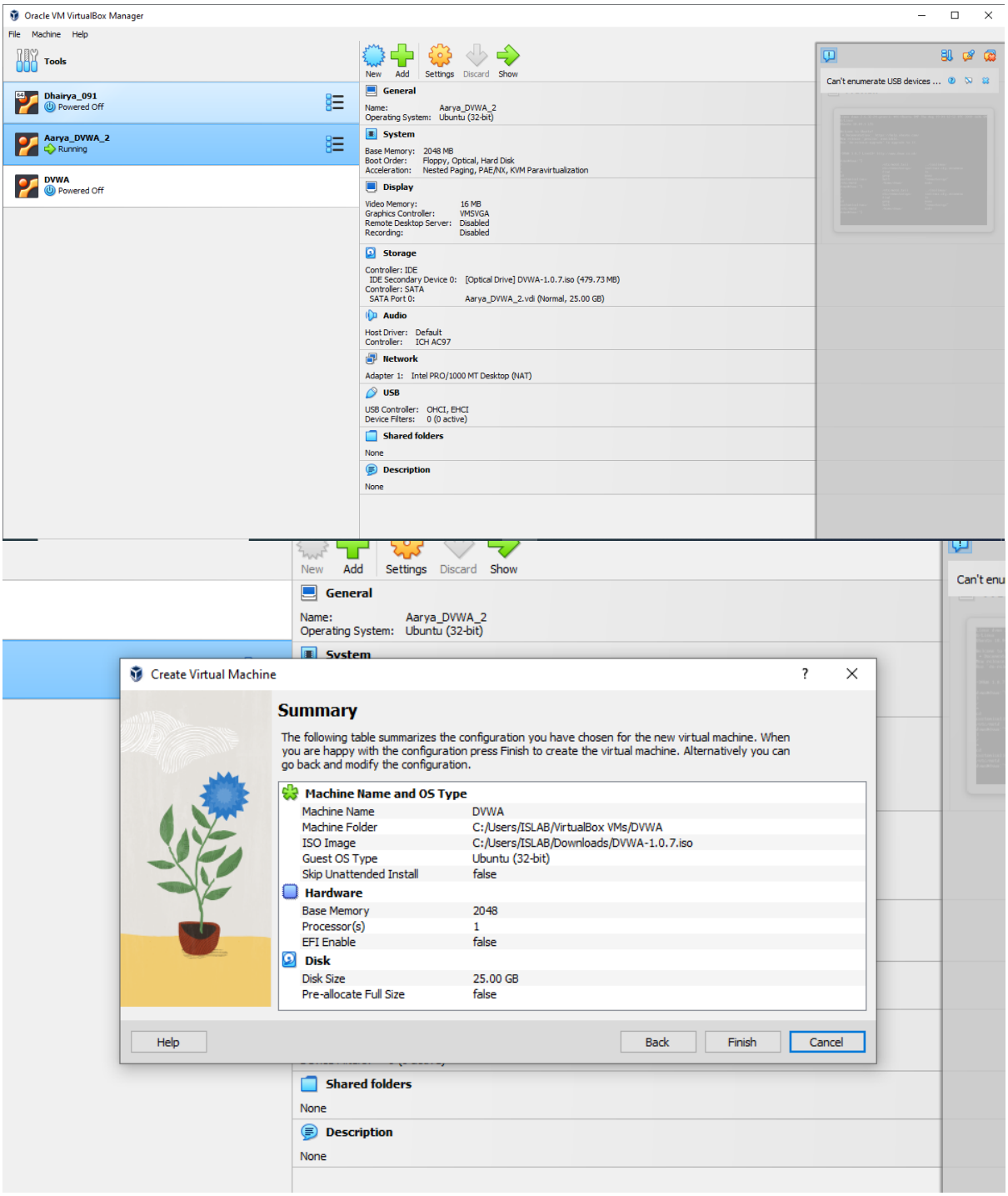
1. In Kali Linux, open a terminal and run *sudo apt update sudo apt upgrade* to update the system.
2. Install additional tools relevant to penetration testing using the package manager (apt).

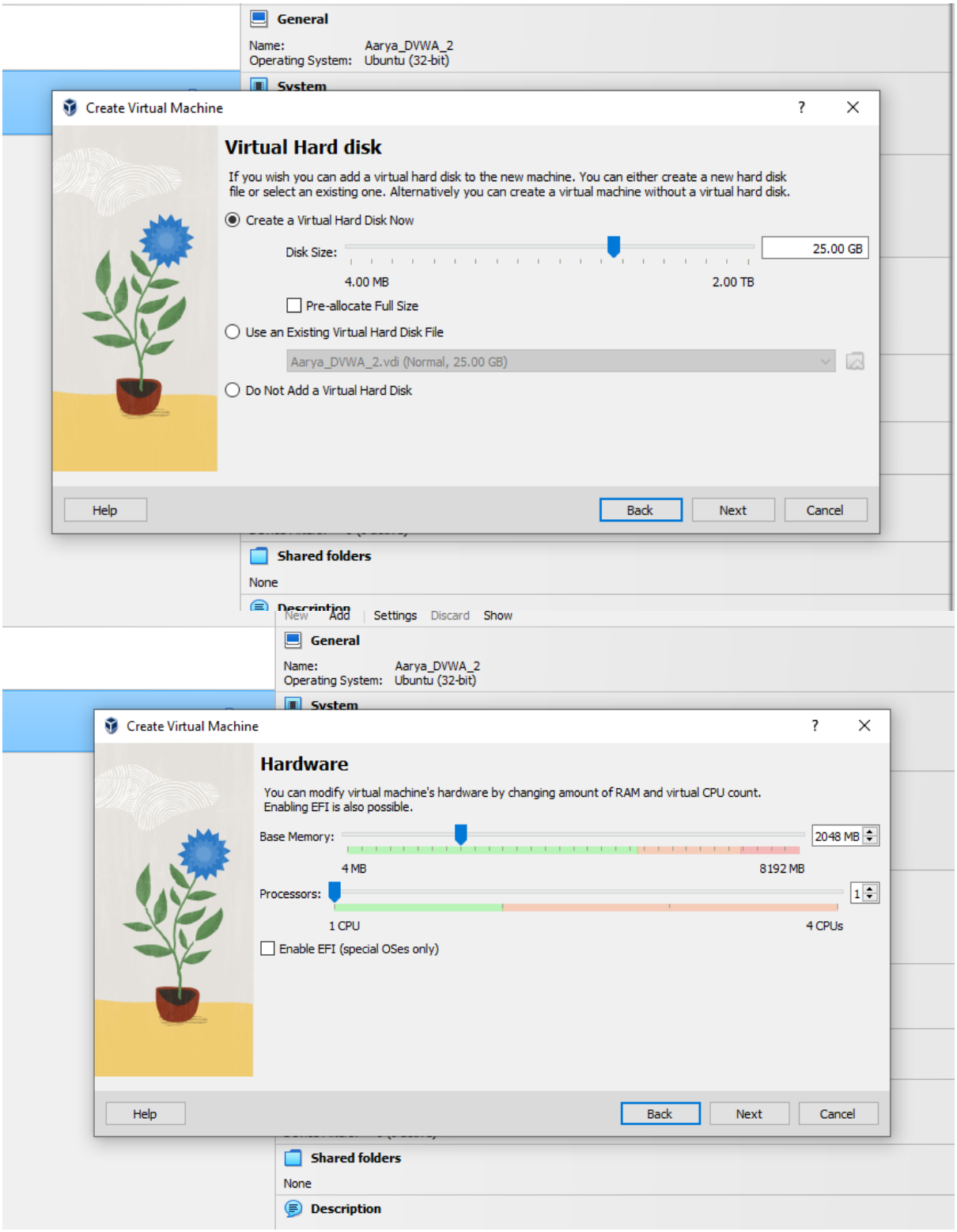
Step 7: Test the Environment:

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.

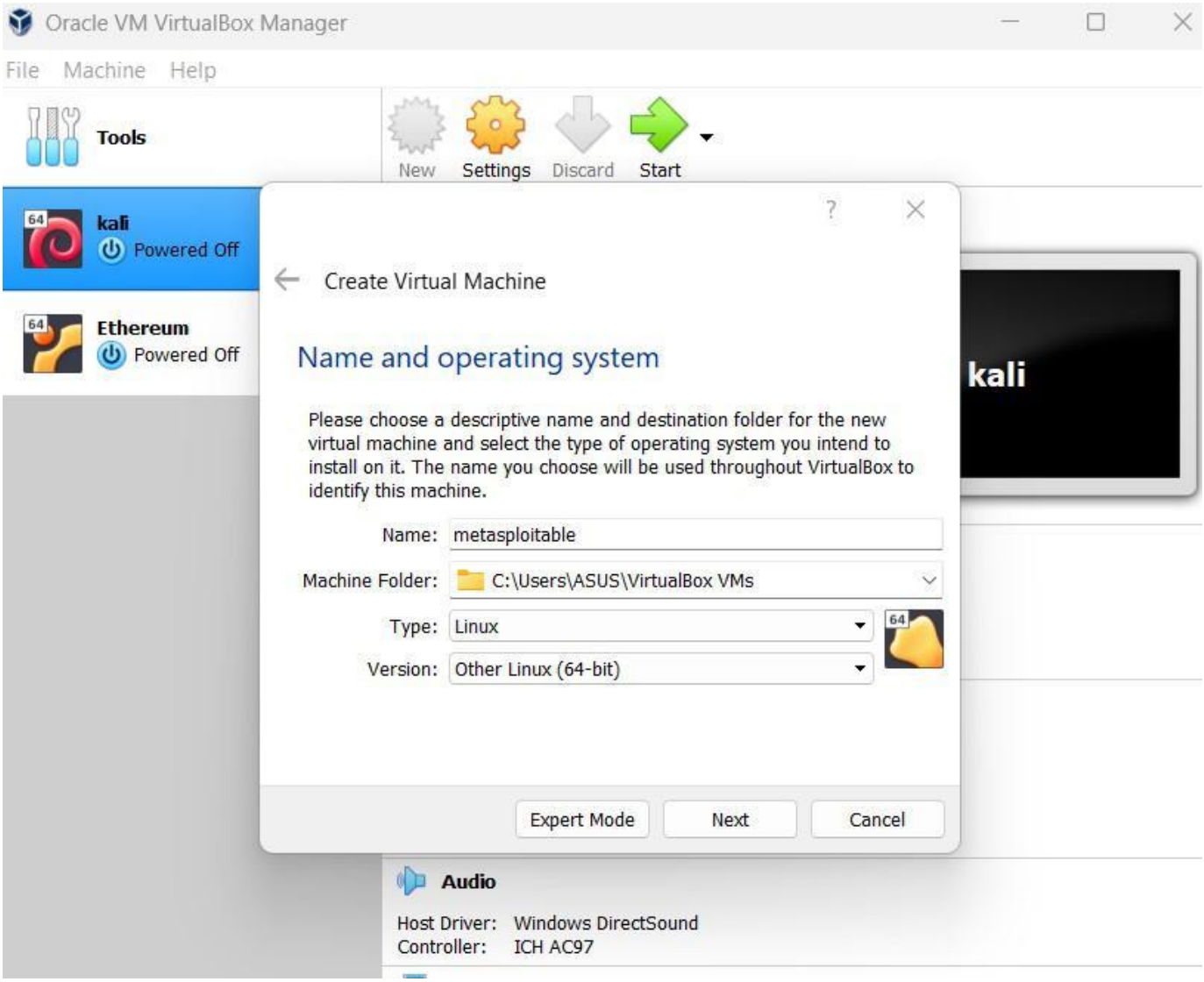
Output (Code with result Snapshot)

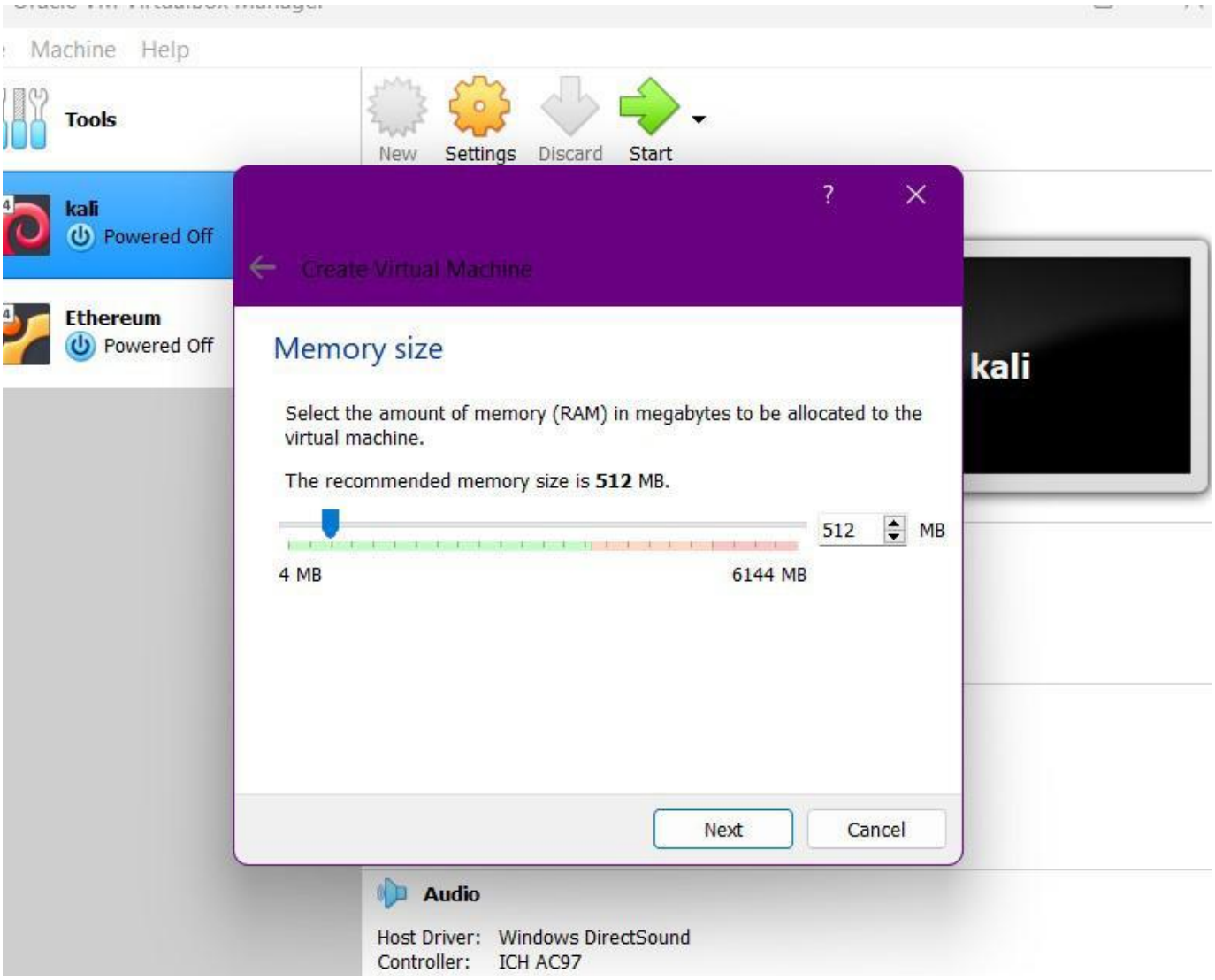
1. DVWA Installation

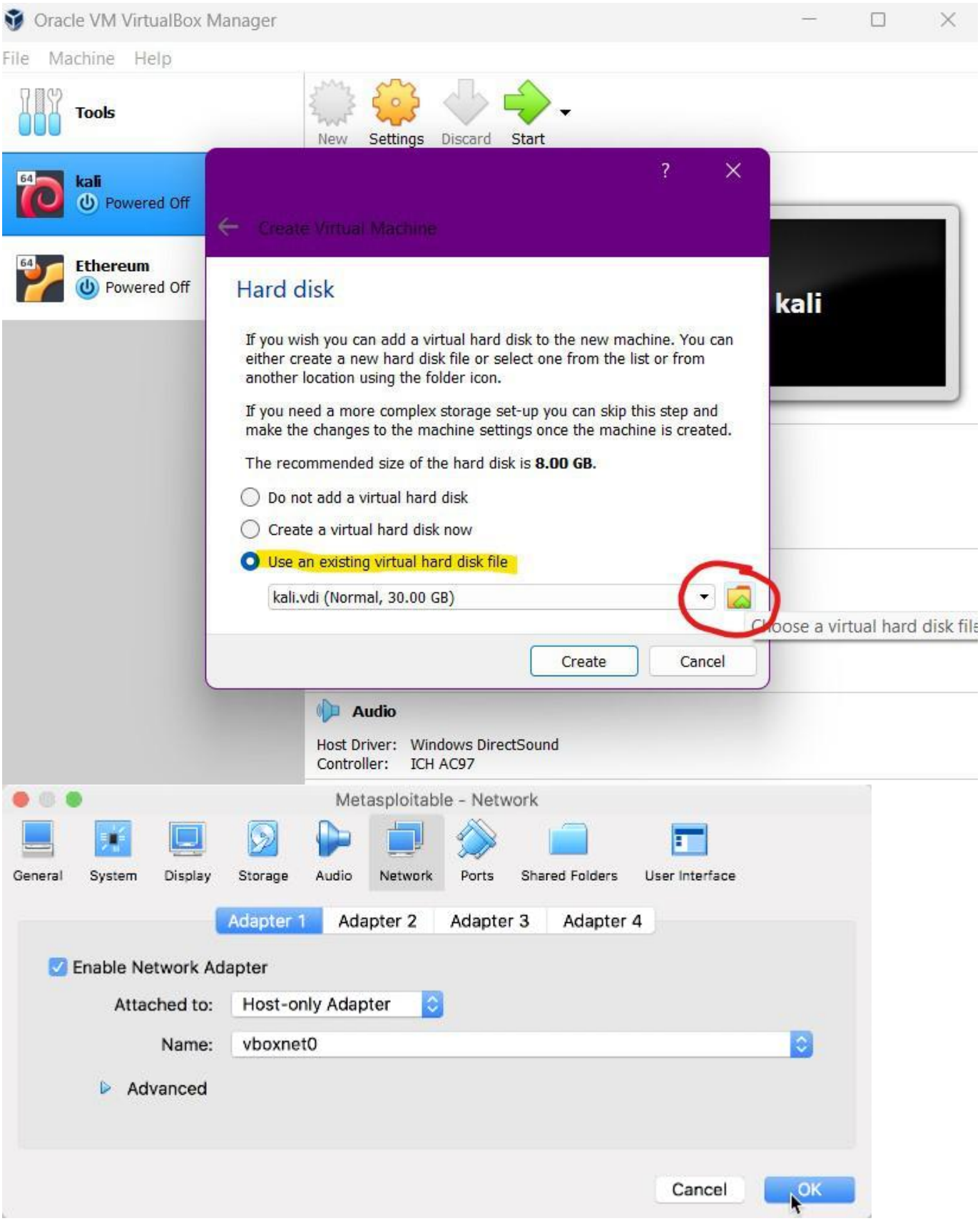


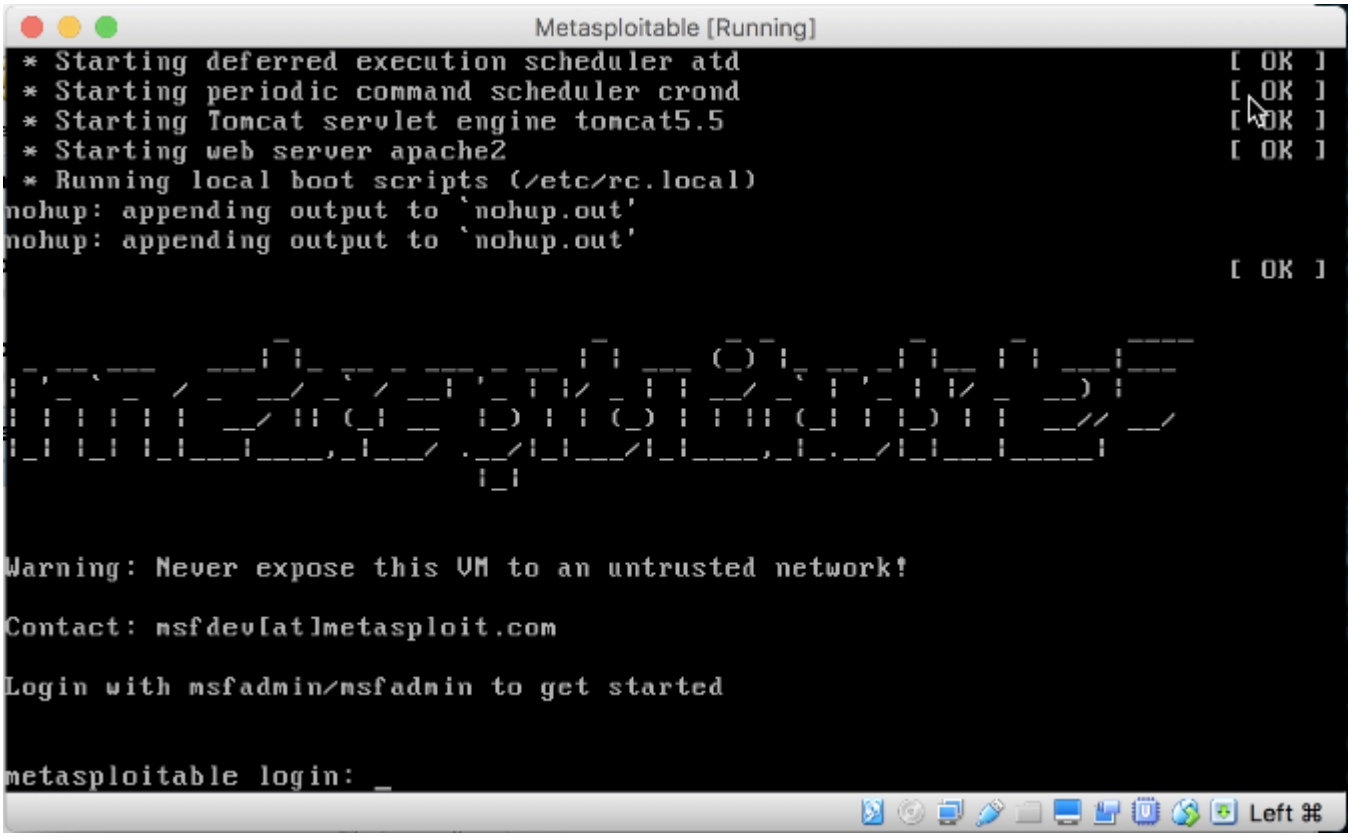

General
Name: Aarya_DVWA_2
Operating System: Ubuntu (32-bit)
System
Create Virtual Machine
Virtual Hard disk
If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.
Create a Virtual Hard Disk Now
Disk Size:
25.00 GB
4.00 MB
2.00 TB
Pre-allocate Full Size
Use an Existing Virtual Hard Disk File
Aarya_DVWA_2.vdi (Normal, 25.00 GB)
Do Not Add a Virtual Hard Disk
Help
Back
Next
Cancel
Shared folders
None
New
Add
Settings
Discard
Show
General
Name: Aarya_DVWA_2
Operating System: Ubuntu (32-bit)
System
Create Virtual Machine
Hardware
You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count.
Enabling EFI is also possible.
Base Memory:
2048 MB
4 MB
8192 MB
Processors:
1
1 CPU
4 CPUs
Enable EFI (special OSes only)
Help
Back
Next
Cancel
Shared folders
None
Description

2. Metasploitable Installation on Kali Linux




Machine
Help
Tools
New
Settings
Discard
Start
kali
Powered Off
Ethereum
Powered Off
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 512 MB.
512
MB
4 MB
6144 MB
Next
Cancel
kali
Audio
Host Driver: Windows DirectSound
Controller: ICH AC97


Oracle VM VirtualBox Manager
File Machine Help
Tools
New Settings Discard Start
kali
Powered Off
Ethereum
Powered Off
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 8.00 GB.
Do not add a virtual hard disk
Create a virtual hard disk now
Use an existing virtual hard disk file
kali.vdi (Normal, 30.00 GB)
Create
Cancel
kali
Audio
Host Driver: Windows DirectSound
Controller: ICH AC97
Metasploitable - Network
General System Display Storage Audio Network Ports Shared Folders User Interface
Adapter 1 Adapter 2 Adapter 3 Adapter 4
Enable Network Adapter
Attached to: Host-only Adapter
Name: vboxnet0
Advanced
Cancel
OK



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?

   Networking Setup:

   To ensure communication between the host machine, Kali Linux VM, and Metasploitable VM, a common approach is to set up a virtual network using a hypervisor such as VMware or VirtualBox. Here's a typical networking setup:

   Host Machine: This is the physical computer running the hypervisor software. It serves as the base for running virtual machines (VMs).

   Kali Linux VM: This VM is used as the penetration testing platform. It is configured with network adapters to connect to the host machine's virtual network.

   Metasploitable VM: This VM simulates vulnerable systems and is used as a target for penetration testing. Like the Kali Linux VM, it is configured with network adapters to connect to the virtual network.

   Challenges and Solutions:

Networking Configuration: Configuring network adapters in the VM settings can sometimes be tricky, leading to connectivity issues. Ensure that all VMs are connected to the same virtual network and have appropriate IP configurations (e.g., IP addresses, subnet masks, default gateways).

Firewall Rules: Firewalls running on the host machine or VMs may block incoming or outgoing traffic, hindering communication. Adjust firewall rules to allow necessary traffic between the VMs.

Network Address Translation (NAT): If using NAT mode for networking, ensure that port forwarding rules are correctly configured to allow communication between the host machine and VMs.

Virtual Network Misconfiguration: Incorrectly configured virtual networks can lead to isolation issues, preventing VMs from communicating with each other. Double-check network settings in the hypervisor and ensure VMs are connected to the correct virtual network adapter.

Effectiveness of Penetration Testing:

A well-established network contributes to the effectiveness of penetration testing in several ways:

Realistic Testing Environment: A properly configured network environment mirrors real-world scenarios, allowing testers to assess vulnerabilities and exploits in a controlled yet realistic setting.

Accurate Assessment of Risks: With interconnected systems accurately represented, penetration testers can identify potential attack vectors, assess risks, and prioritize remediation efforts effectively.

Comprehensive Security Testing: A robust network setup enables testers to conduct thorough security assessments, including vulnerability scanning, penetration testing, and network traffic analysis.

Validation of Defenses: By simulating attacks and exploiting vulnerabilities, penetration testing validates the effectiveness of security measures and helps organizations identify areas for improvement in their defense strategies.

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.

Evaluation of Implemented Security Measures:

Authentication: Ensure that strong authentication mechanisms are in place for accessing the penetration testing environment. This may include using unique usernames and complex passwords for each VM, implementing multi-factor authentication where possible, and disabling default or weak credentials.

Encryption: Implement encryption protocols such as HTTPS, SSH, and VPNs to protect sensitive data transmitted over the network. Encrypting communication channels between the host machine, Kali Linux VM, and Metasploitable VM enhances confidentiality and integrity.

Principle of Least Privilege: Assign minimal privileges necessary for each user or system within the penetration testing environment. Restrict access to sensitive resources and limit administrative privileges to prevent unauthorized actions that could compromise security.

Ensuring Security and Isolation in the Penetration Testing Environment:

Network Segmentation: Segment the penetration testing environment from production networks to prevent accidental or malicious interference with operational systems. Use separate VLANs or physical network adapters for the testing environment and configure firewall rules to restrict traffic flow.

Network Isolation: Use host-only or internal networking modes in the hypervisor to create isolated networks for the penetration testing environment. This prevents external access to the VMs from outside networks, reducing the risk of unauthorized access.

Isolated Test Environment: Maintain a dedicated environment specifically for penetration testing activities, separate from production systems. This ensures that any exploits or vulnerabilities discovered during testing do not impact operational systems.

Ethical Considerations and Importance of Ethical Hacking Principles:

Respect for Privacy: Ethical hackers must respect individuals' privacy and confidentiality by ensuring that sensitive information obtained during testing is handled securely and not disclosed without proper authorization.

Legal Compliance: Adherence to laws and regulations governing cybersecurity and privacy is essential. Ethical hackers must obtain proper authorization before conducting penetration tests and ensure that their activities comply with applicable legal requirements.

Mitigation of Harm: Ethical hacking principles emphasize the importance of minimizing harm to systems and data during testing. Testers should exercise caution to avoid causing disruptions to critical services or data loss.

Professional Responsibility: Ethical hackers have a professional responsibility to act ethically and transparently, maintaining the trust of stakeholders and fostering a culture of cybersecurity awareness and responsibility.

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 conclusion, establishing a penetration testing environment with VMs, Kali Linux, and Metasploitable ensures a secure and isolated setup for assessing security vulnerabilities. By upholding ethical hacking principles and configuring necessary security measures, this environment facilitates effective testing and helps improve overall cybersecurity defenses.

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/ch01lvl1sec16/setting-up-a-penetration-testing-lab