# VAPT LAB

It is the process intended to reveal flaws in the security mechanisms, protect data and maintain functionality as intended.

**What is VAPT?**

A form of stress testing, which exposes weakness or flaws in a computer system

- The art of finding an Open Door
- A valued Assurance Assessment tool
- VAPT can be used to find flaws in Specifications, Architecture, Implementation, Software, Hardware, and many more.
- Vulnerability assessment is the process of identifying, quantifying, and prioritizing the vulnerabilities in a system.
- Penetration test is an attack on a computer system that looks for security weaknesses, potentially gaining access to the computer's features and data.

## VAPT: -

- V-Vulnerability
- A-Assessment
- P-Penetration
- T-Testing
- **Vulnerability Assessment**
- A process to evaluate and review key systems, networks and applications. To identify vulnerabilities and configuration issues that may put the organization at risk of being breached or exploited Effective in identifying vulnerabilities, but it cannot

differentiate between exploitable vs non-exploitable vulnerabilities.

- **Penetration Testing**
- Goal-driven test focused on identifying all possible routes of entry an attacker could use to gain unauthorized entry into the target. Identifies the potential damage and further internal compromise an attacker could carry out once they are past the perimeter. Proof of concept strategy to investigate, exploit and validate the extent of the identified vulnerability.

**Difference between Vulnerability and Penetration Testing**

**Vulnerability Assessment:**

» Typically, is general in scope and includes a large assessment.

» Predictable.

» Unreliable at times and high rate of false positives.

» Vulnerability assessment invites debate among System Admins.

» Produces a report with mitigation guidelines and action items.

**Penetration Testing:**

» Focused in scope and may include targeted attempts to exploit

specific vectors (Both IT and Physical)

» Unpredictable by the recipient. (Don’t know the “how?” and “when?”)

» Highly accurate and reliable. (I’ve got root!)

» Penetration Testing = Proof of Concept against vulnerabilities.

» Produces a binary result: Either the team owned you, or they didn't

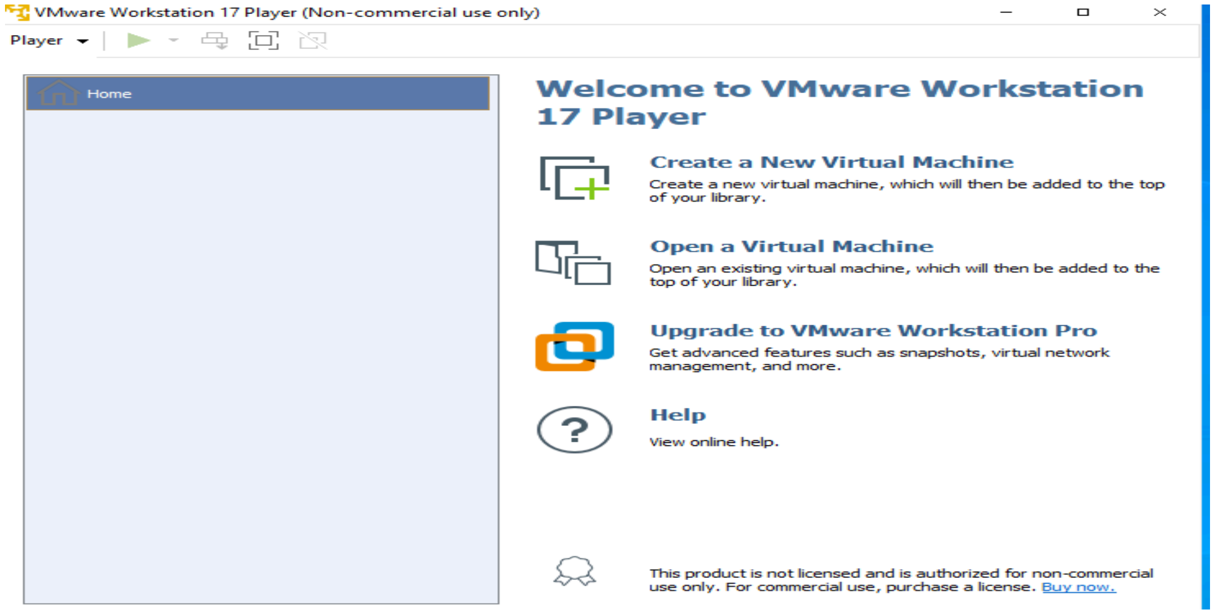
# **Lab Setup:-**

1. VMware workstation player 17 download and install.

https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html

2. Download and Install kali Linux on VMware
   https://www.kali.org/get-kali/#kali-virtual-machines

   In prebuilt virtual machines, download kali Linux for VMware and Extract files.



Welcome to VMware Workstation 17 Player

Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.

Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.

Upgrade to VMware Workstation Pro
Get advanced features such as snapshots, virtual network management, and more.

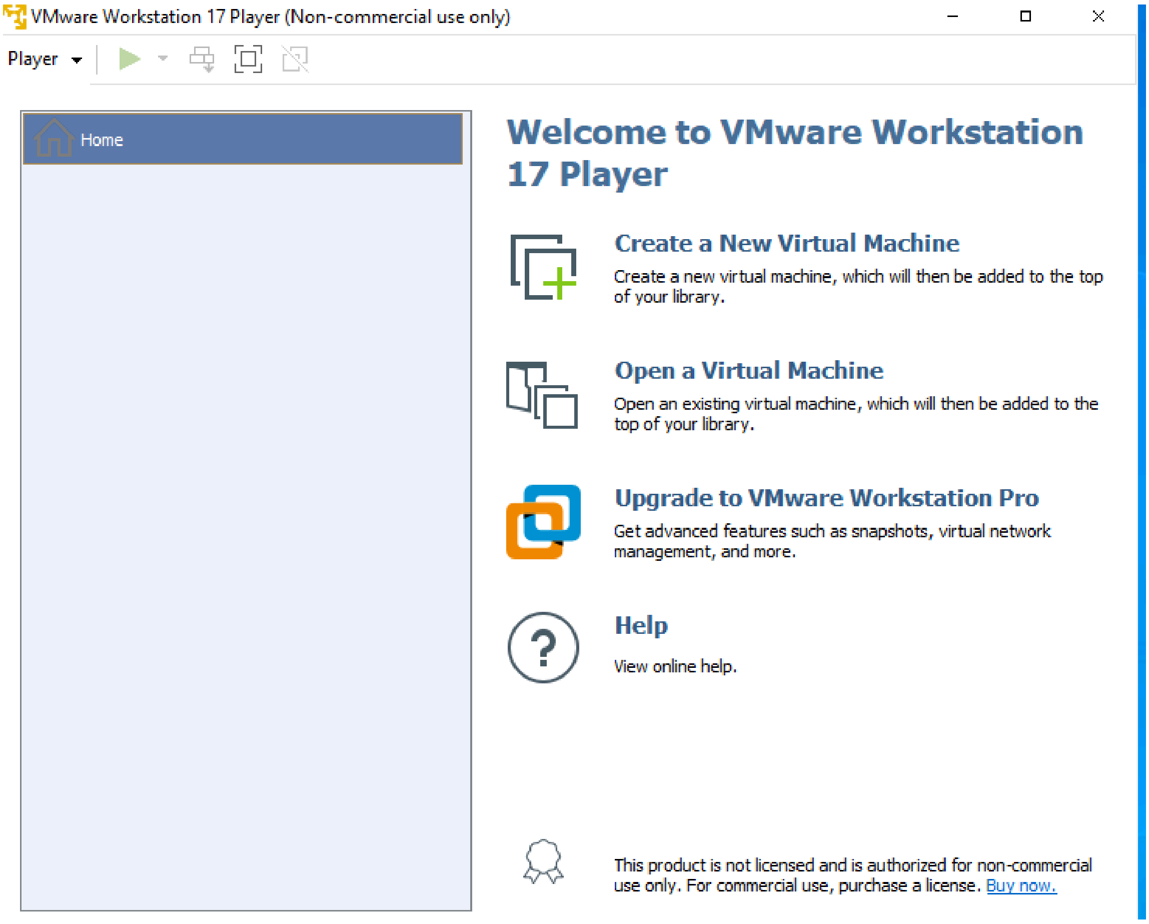
Help
View online help.

This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.

Click on Open Virtual Machine, browse for kali-linux-2024.1-vmware-amd64.vmx file and click on play virtual machine and set the username and password (Ex: kali)

3. Download and Install Metaspoiltable2 target machine on VM ware.
   https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

Download Metaspoiltable2 target and extract files.



VMware Workstation 17 Player (Non-commercial use only)

Welcome to VMware Workstation 17 Player

Create a New Virtual Machine

Create a new virtual machine, which will then be added to the top of your library.

Open a Virtual Machine

Open an existing virtual machine, which will then be added to the top of your library.

Upgrade to VMware Workstation Pro

Get advanced features such as snapshots, virtual network management, and more.

Help

View online help.

This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.

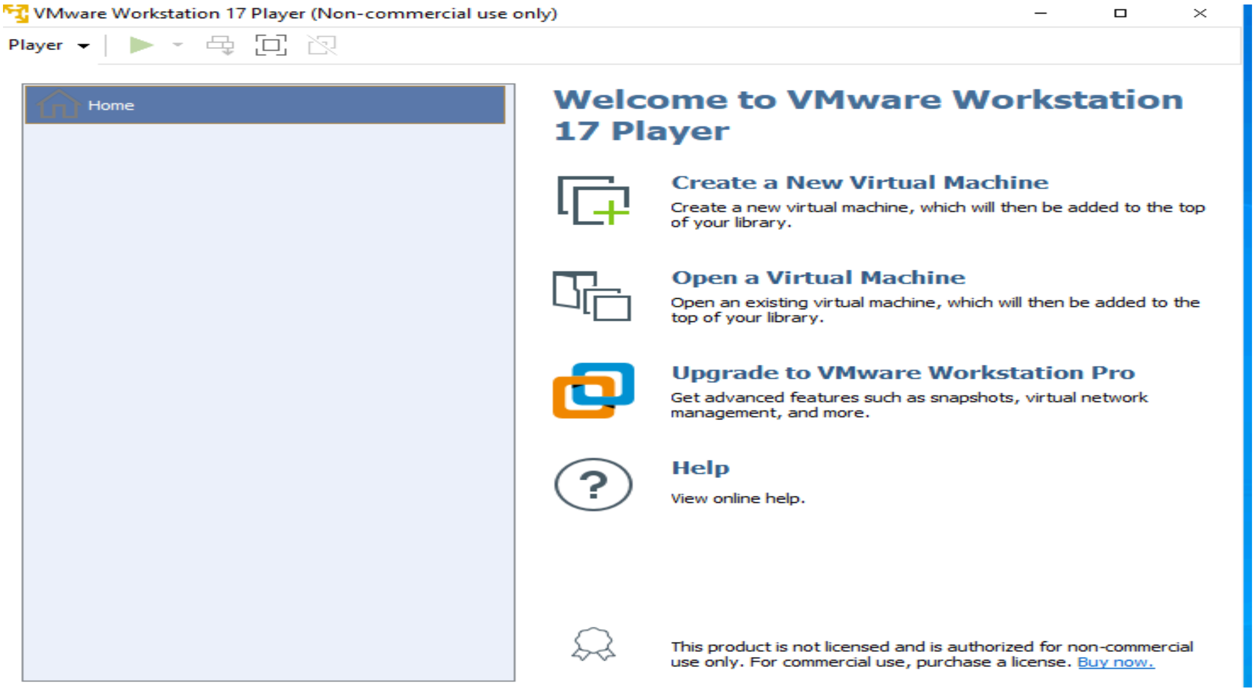
Click on Open Virtual Machine, browse for metaspoiltable.vmx file and click on play virtual machine, then I moved it.

Login into metaspoiltable vm by using msfadmin/msfadmin as username/password

4. Download and Install Windows 11 Virtual Machine on VM ware(Target Machine)

https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/

Select VMWare option in the above link and download and extract files.



Welcome to VMware Workstation 17 Player

Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.

Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.

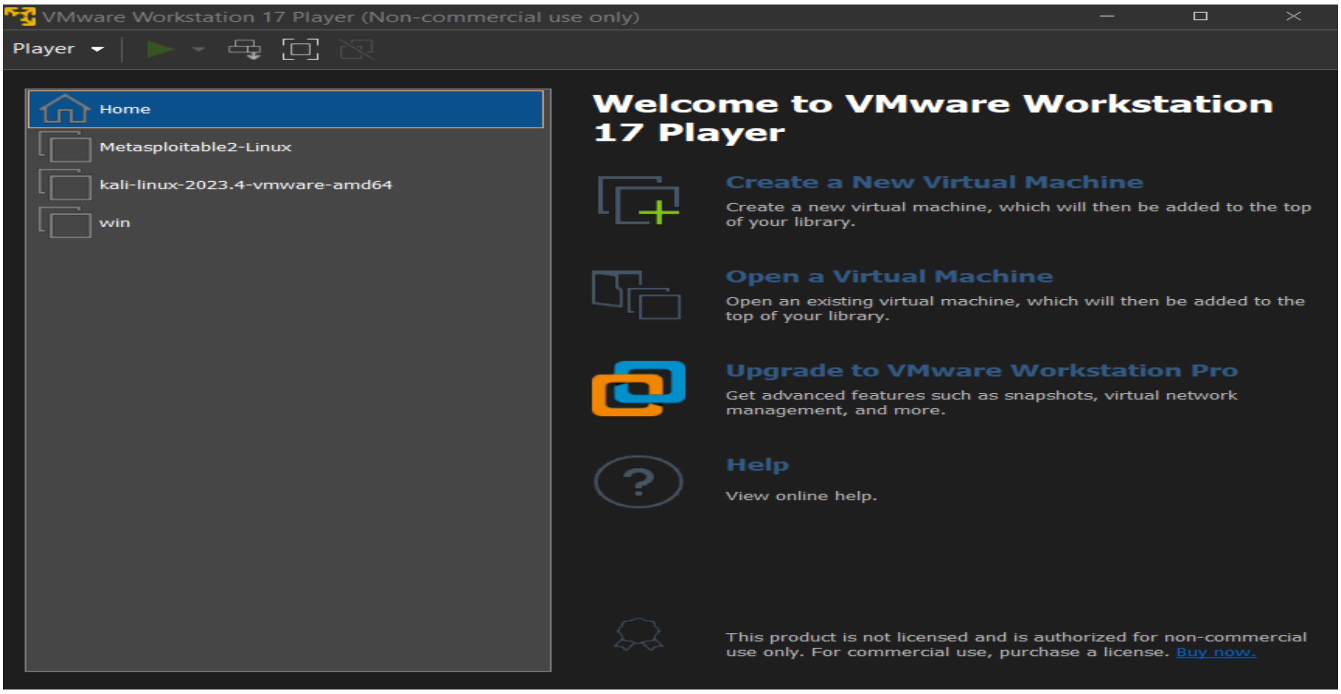
Upgrade to VMware Workstation Pro
Get advanced features such as snapshots, virtual network management, and more.

Help
View online help.

This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.

Click on Open Virtual Machine, browse for winDev2401Eval file and click on play virtual machine.

Now VMware is having kali linux, metaspoiltable2 and windows virtual machine.


VMware Workstation 17 Player (Non-commercial use only)
Player
Home
Metasploitable2-Linux
kali-linux-2023.4-vmware-amd64
win

Welcome to VMware Workstation 17 Player

Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.

Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.

Upgrade to VMware Workstation Pro
Get advanced features such as snapshots, virtual network management, and more.

Help
View online help.

This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.

# VAPT Lab Exercises

1. Imagine you are working as a cybersecurity analyst for a financial institution, you are tasked with conducting a Nessus vulnerability analysis on a critical host system (windows, Linux) in the local network hosting sensitive customer data. Detail your step-step approach, including pre-scan preparations, specific Nessus configurations for maximum efficacy in an environment, scan the targets, prioritize and analyse the results and generate reports.

   Nessus, developed by Tenable Inc, is a widely-used open-source vulnerability scanner.
   Nessus provides a range of services, including vulnerability assessments, network scans, web scans, asset discovery, and more, to aid security professionals, penetration testers, and other cybersecurity enthusiasts in proactively identifying and mitigating vulnerabilities in their networks.

   Search for Nessus Essentials, register for the activation code and download Linux-Debian-amd64.

   https://www.tenable.com/products/nessus/nessus-essentials

   **Installing Nessus on Kali Linux**

1. Download the Nessus package for Debian on the Nessus website and make sure you set the Platform to Linux-Debian-amd64.

2. When it's finished downloading, open your Linux terminal and navigate to the location you downloaded the Nessus file to.

3. Install Nessus using this command:

```
sudo dpkg -i Nessus-10.4.1-debian9_amd64.deb
```

4. Start the Nessus service with this command:

```
sudo systemctl start nessusd.service
```

5. On your browser, go to https://kali:8834/. It would show a warning page.

6. Click on Advanced. Then, click on Accept Risk and Continue.

7. Choose the Nessus Product you prefer. If you want the free version of Nessus, click on Nessus Essentials.

8. Enter your name and email address to receive an activation code by email. Paste the activation code into the space provided and choose a username and password.

9. Allow Nessus to download the necessary plugins.

10. Once the plugin downloads have completed, you can start using the Nessus service.