**Day1**

**1.Laptop Setup**

**2.Installation of Chrome**

**3.Installation Of Bitwarden**

**4.Installation of Virtual Box.**

**5.Installation of Virtual Machine.**

**6.Installation of Putty**

**7.Connecting Windows(local machine) to Remote Server(Ubuntu){Virtual Machine}**

**MVP**(minimum viable product)

**Bitwarden**

Bitwarden download-> selected os(windows)

After download & installed, created account.

It is an open-source password manager that helps individuals and businesses securely store, manage, and share passwords and other sensitive information.

**Virtual Box(S/W)**

It enables users to create and run multiple operating systems on a single physical machine

Here physical machine is windows. So, downloaded the Windows hosts Virtual box.

**Virtual Machine**

The purpose of a virtual machine (VM) is to create a simulated computer environment within a physical computer.

Downloading & Installing the Virtual box images.(website used-->osboxes.org)

Ubuntu Server-->Ubuntu Server 20.04.4(Focal Fossa)-->VirtualBox-->Download.

It will download a 64bit zip file--->Extract it--->inside it we will contain the image.

Followed the steps in( Osboxes.org-->support--->Guide) to attach the image with VirtualBox.

Once the image is attached awe will start the VM.

**Commands to install SSH**

sudo apt update

sudo apt install openssh-server

**Putty**

It is used to connect the local machine to the remote server using SSH(Secure Shell).

Download and install msi file.

To connect to remote server using putty. We need the port of the remote server.

As the remote server will not allow direct connect we will be using port forwarding to establish connection.

Steps followed for port forwarding

Settings in Virtual Box-->Network-->advanced-->setup-->port forwarding

Add rule-->Guest port(2222) Host Port(22).

The default port of SSH is **22**. So, we create one guest port(eg:-2222) in VM and reuse it in putty to establish connection between putty and the Virtual machine.

**SSH(**Secure Shell)

it's a network protocol used for secure communication between two devices. It provides a secure channel over which you can remotely access and control another device or server.

If we want to connect to other device or server via SSH . we first need to authenticate.

It can be through username and password or Cryptographic keys.(public and private keys).

Using Cryptographic key is more secure.

Each Party generates a pair of cryptographic keys:

Public key: This key is shared openly with others and is used to verify the identity of the party.

Private Key: This key is kept secret and is used to digitally sign messages or data.