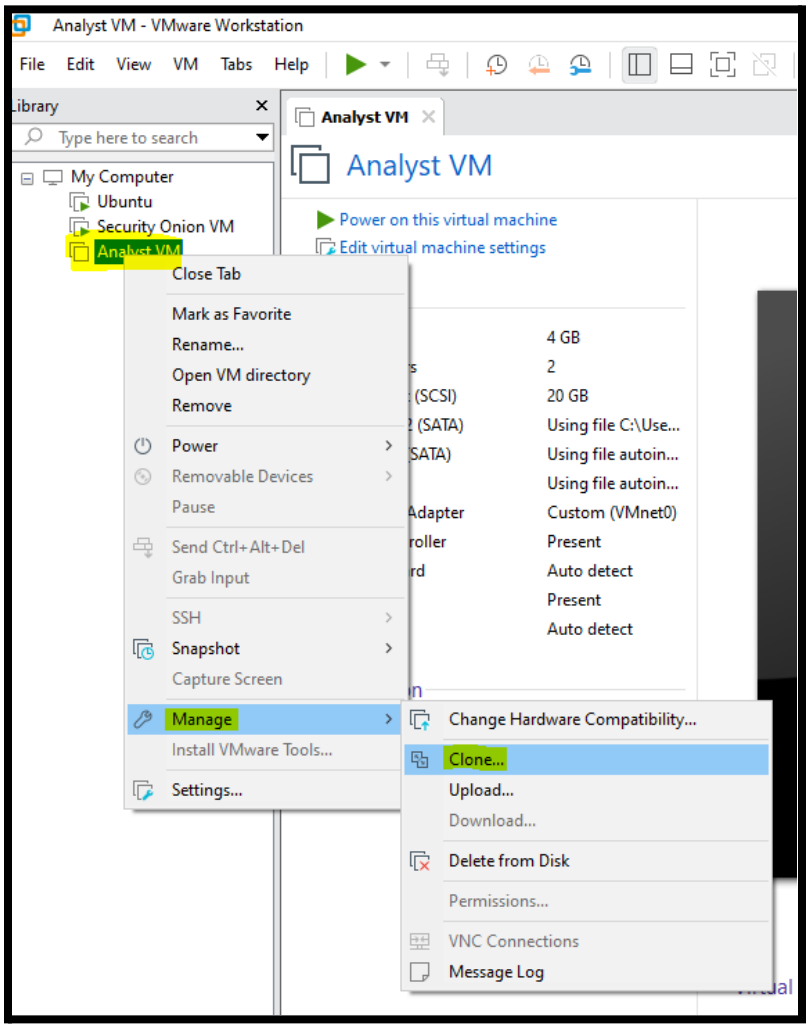
Task 3: Setting up other VMs

After importing the Analyst VM and installing Security onion VM we will set up three additional VMs. As specified in the setup environment of this lab, those additional VMs are the Attacker, Server and User VM. All these machines are connected to the monitoring network only [VMnet2], which will be monitored by Security Onion.

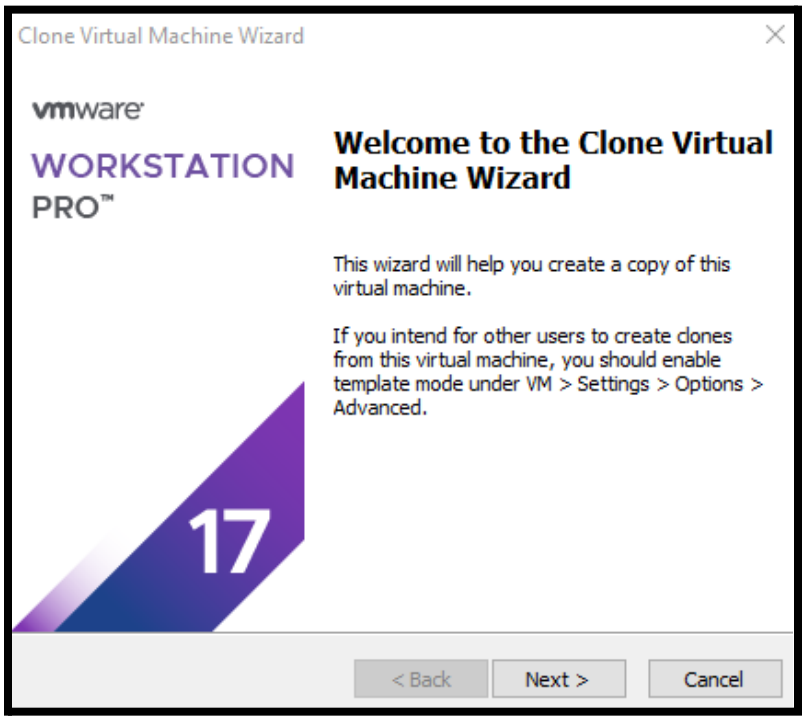
1. Set up the Attacker VM

1.1. Power off the Analyst VM

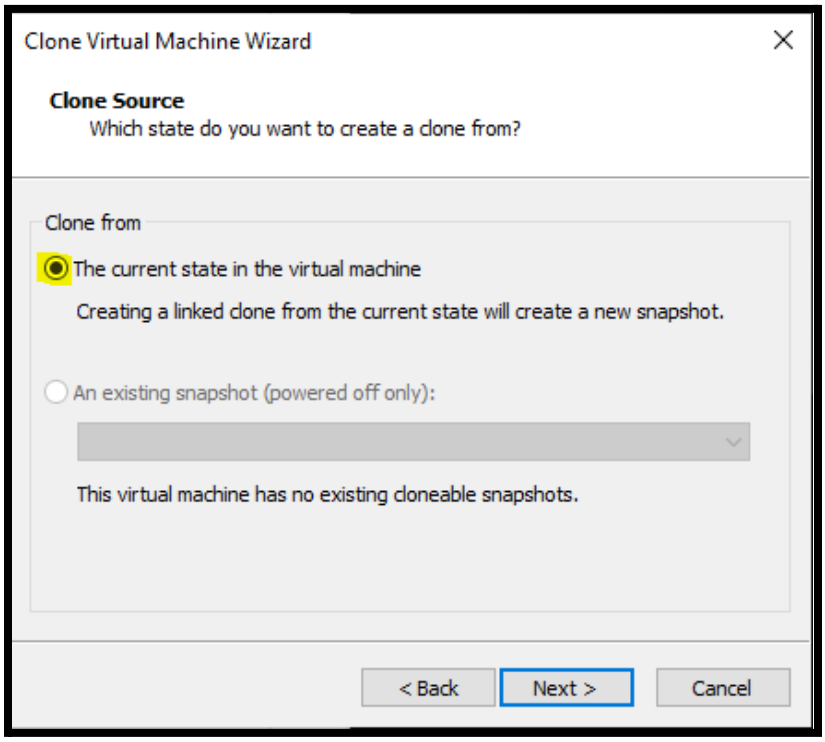
1.2. Clone the Analyst VM by right clicking on [**Analyst VM**] on the left side of the VMware Workstation. Then select [**Manage**] and click on [**Clone**]



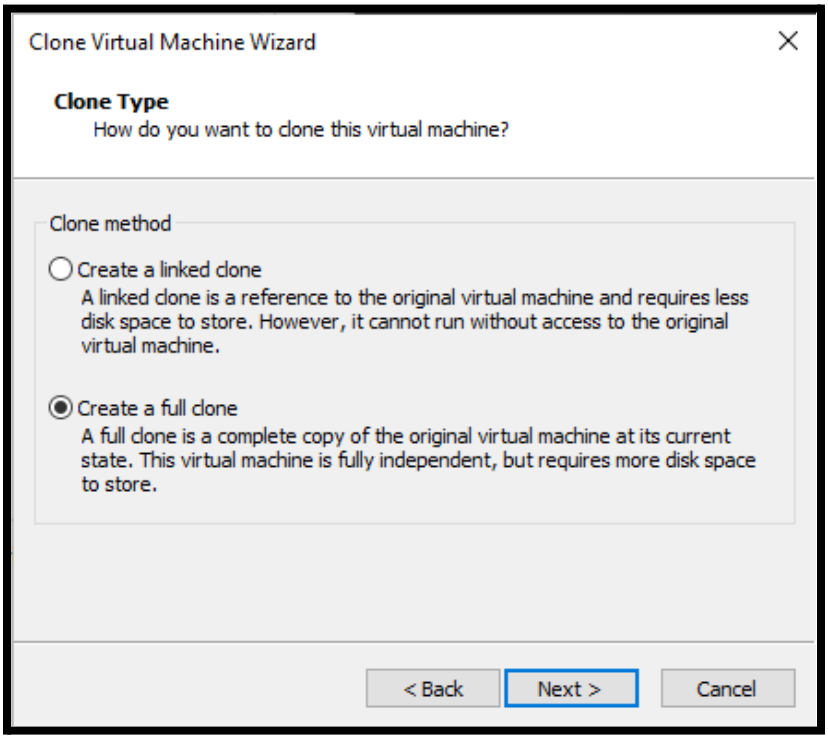
1.3. Then the Clone Virtual Machine Wizard will pop up, Click on **[Next]**



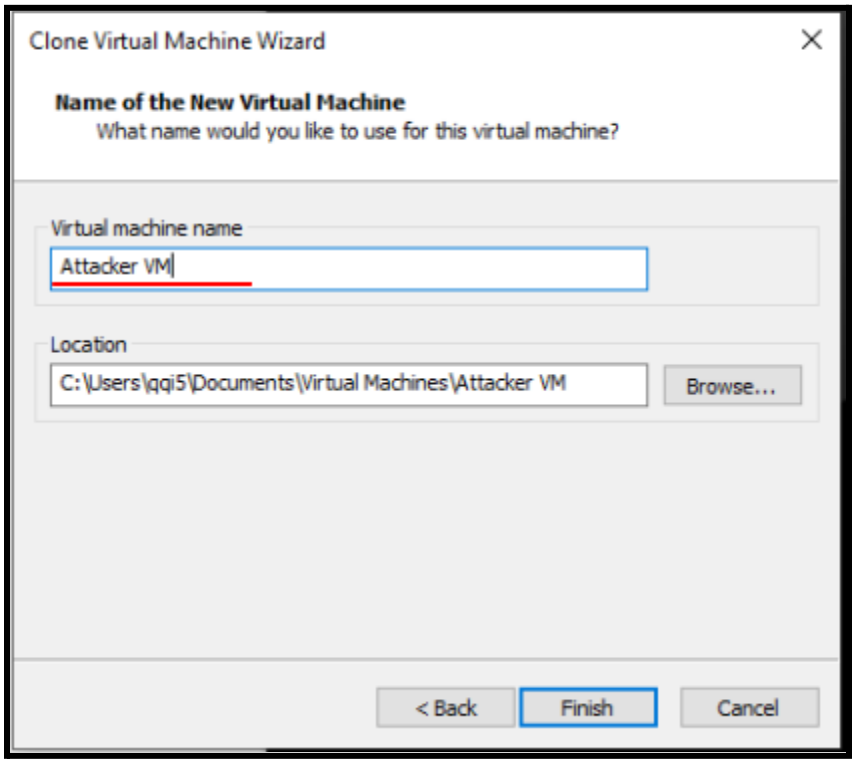
1.4. Select the **[Current State in the VM]** option



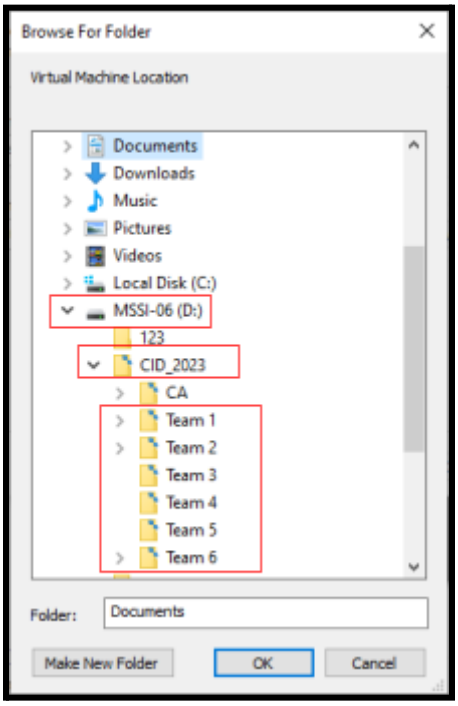
1.5. Choose the clone method as **[Create a full clone]**



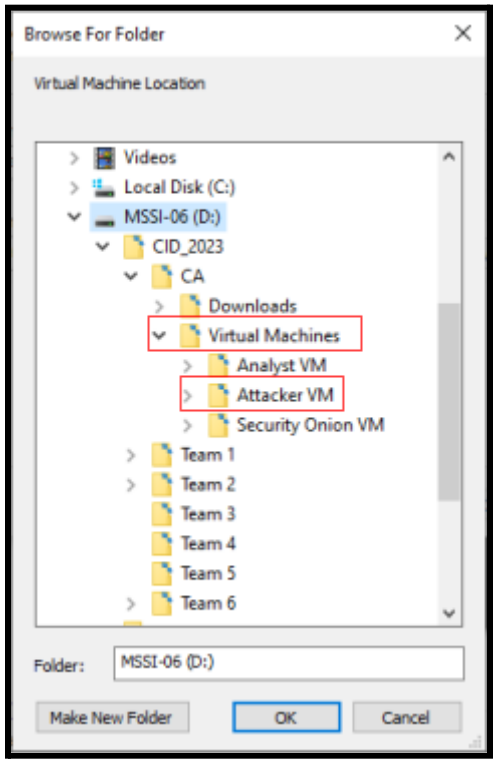
1.6. Change the VM name to **[Attacker VM]**



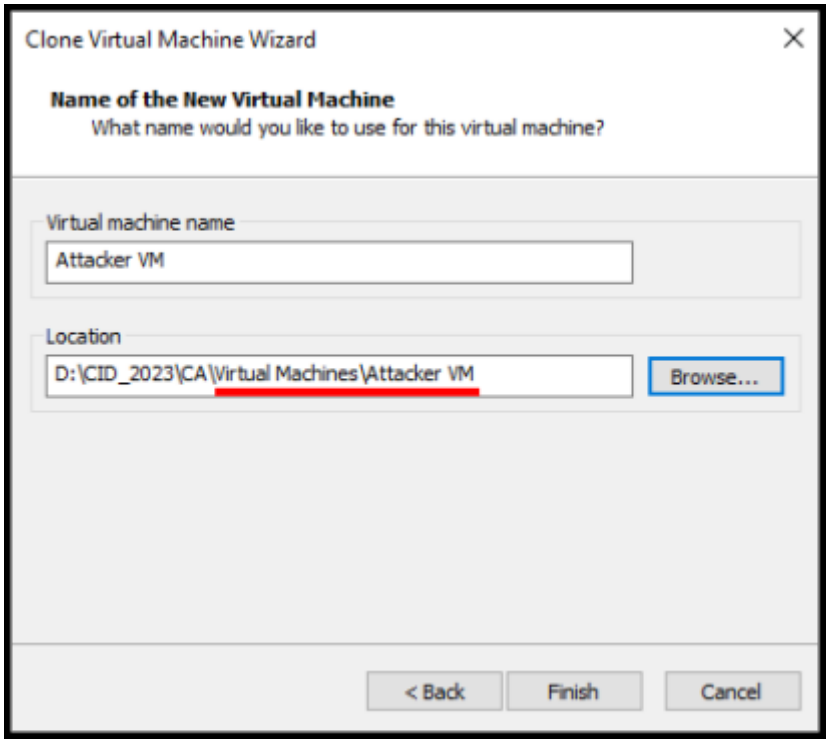
1.7. Change the location to the D drive. Click on **[Browse…]** then navigate to **[D:\CID_2023\TeamX\Virtual Machines]**.



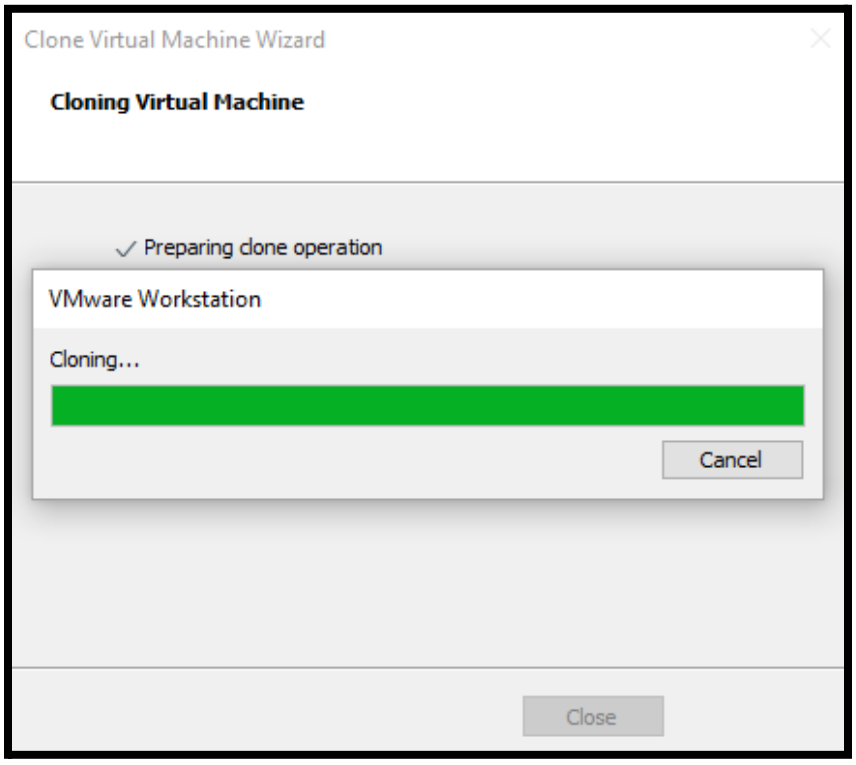
1.8. Inside the [**Virtual Machines]** folder create a new folder and name it **[Attacker VM]**. Select this folder as the location where the VM files should be stored.



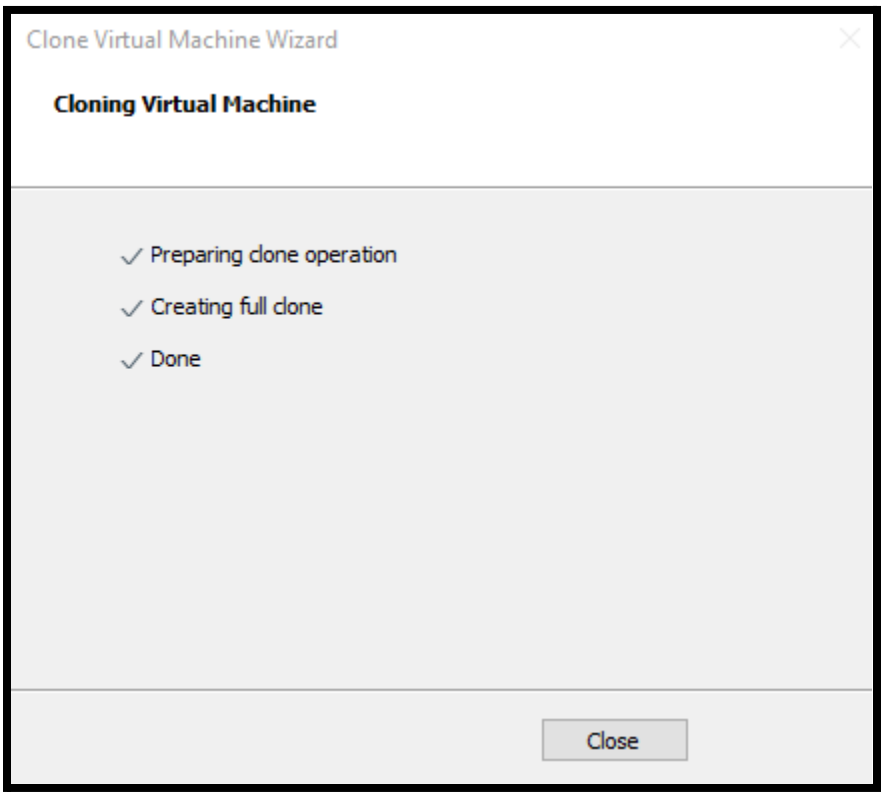
1.9. After you have specified the location correctly, click on **[Finish]**



1.10. Wait for the clone process to complete



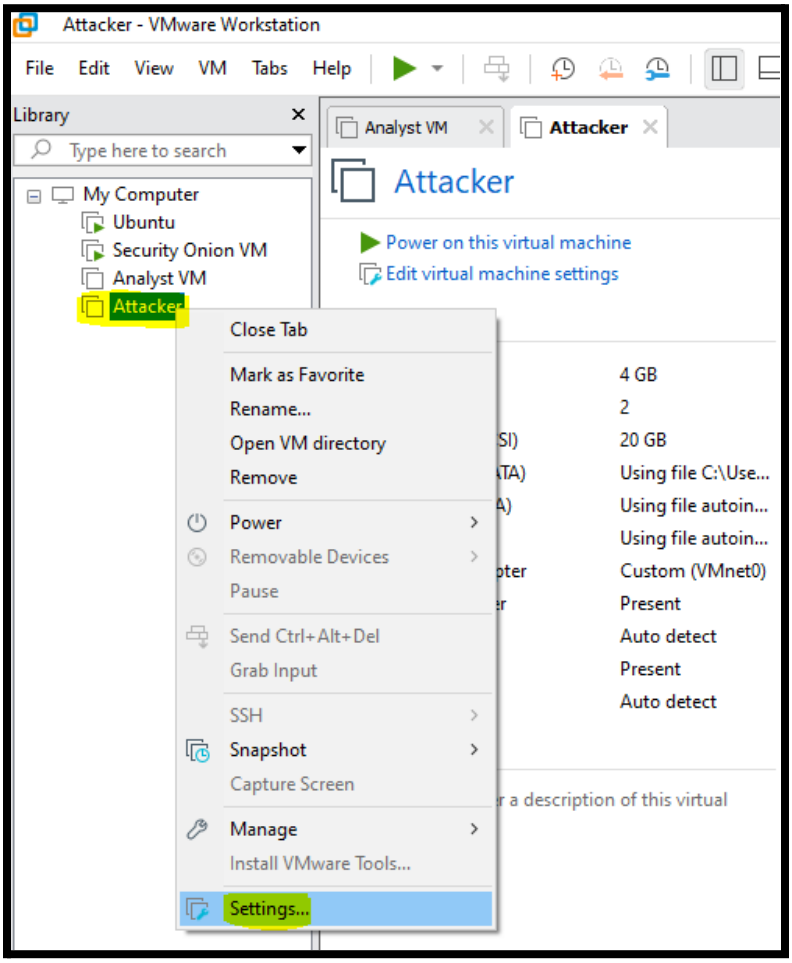
1.11. You have successfully cloned the Analyst VM to create the Attacker VM. click on **[Close]**



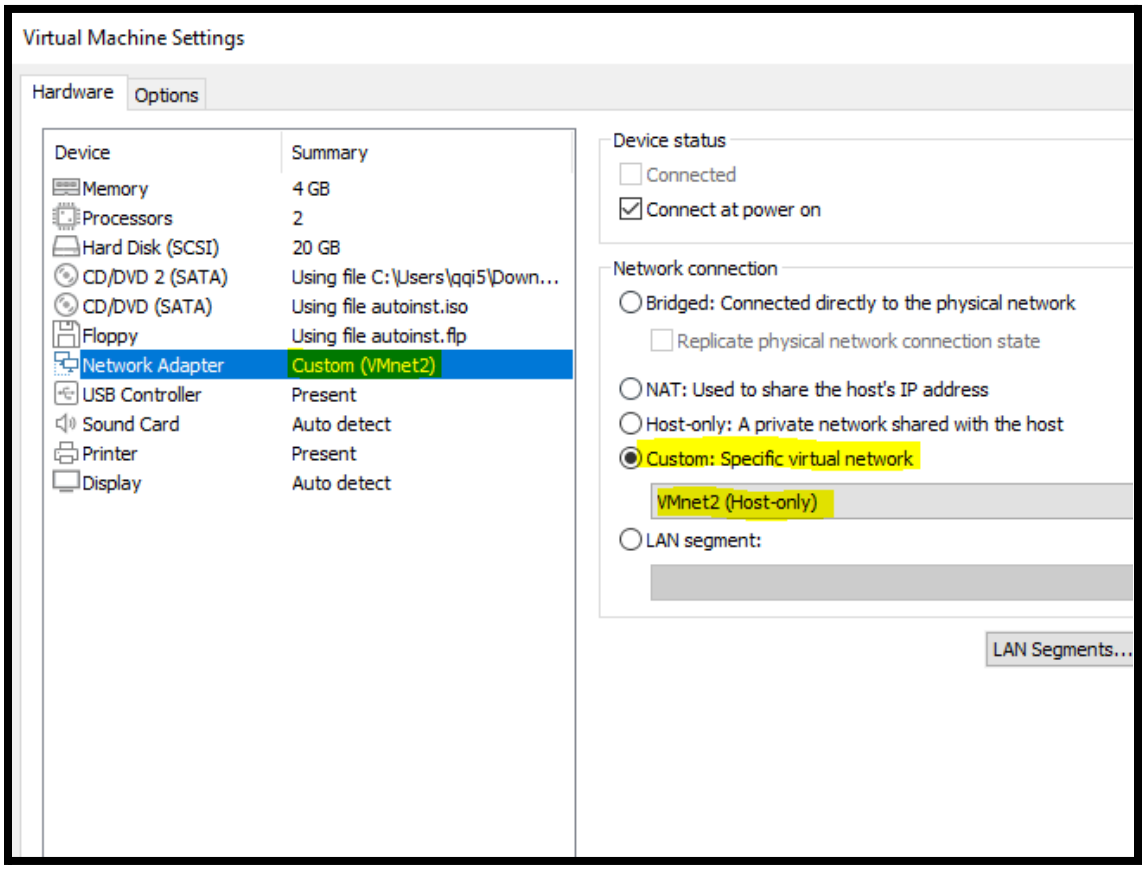
2. Configure the Attacker VM

As mentioned previously, the Attacker VM along with the User and the Server VMs, are all connected to the Monitor Network **[VMnet2]**. Therefore we must configure each one of these VM to be connected to **[VMnet2]** only.

2.1. On the left side of the VMware Workstation, right click on **[Attacker VM]**. Then select **[Setting]**



2.2. Click on **[Network Adapter]** then change the network type to **[Custom]**, and select **[VMnet2]**



You have successfully created and configured the Attacker VM.

3. Create the Server and the User VMs

3.1. Clone the **[Attacker VM]** and create two additional VMs, one as the **[Server VM]** and one as the **[User VM]**

Note: if you cloned the **[Attacker VM]**, you won't need to reconfigure the network for Serve VM and User VM. However, if you cloned the **[Analyst VM]**, make sure that you reconfigure the network setting. Keep in mind, all three VMs **(Attacker, User, Server)** are connected to [**VMnet2]** only, whereas, the **Analyst VM** is connected to **[VMnet0]** only. At the same time **Security Onion VM** is connected to both Networks.

Tasks

Task 3.1: List the IP Address for each virtual machine: Analyst, Security Onion, Attacker, Server, and User VM.

Task 3.2: Provide a screenshot that shows the setting of each VM. You could just take a screenshot of the setting summary in VMware, see the picture below.