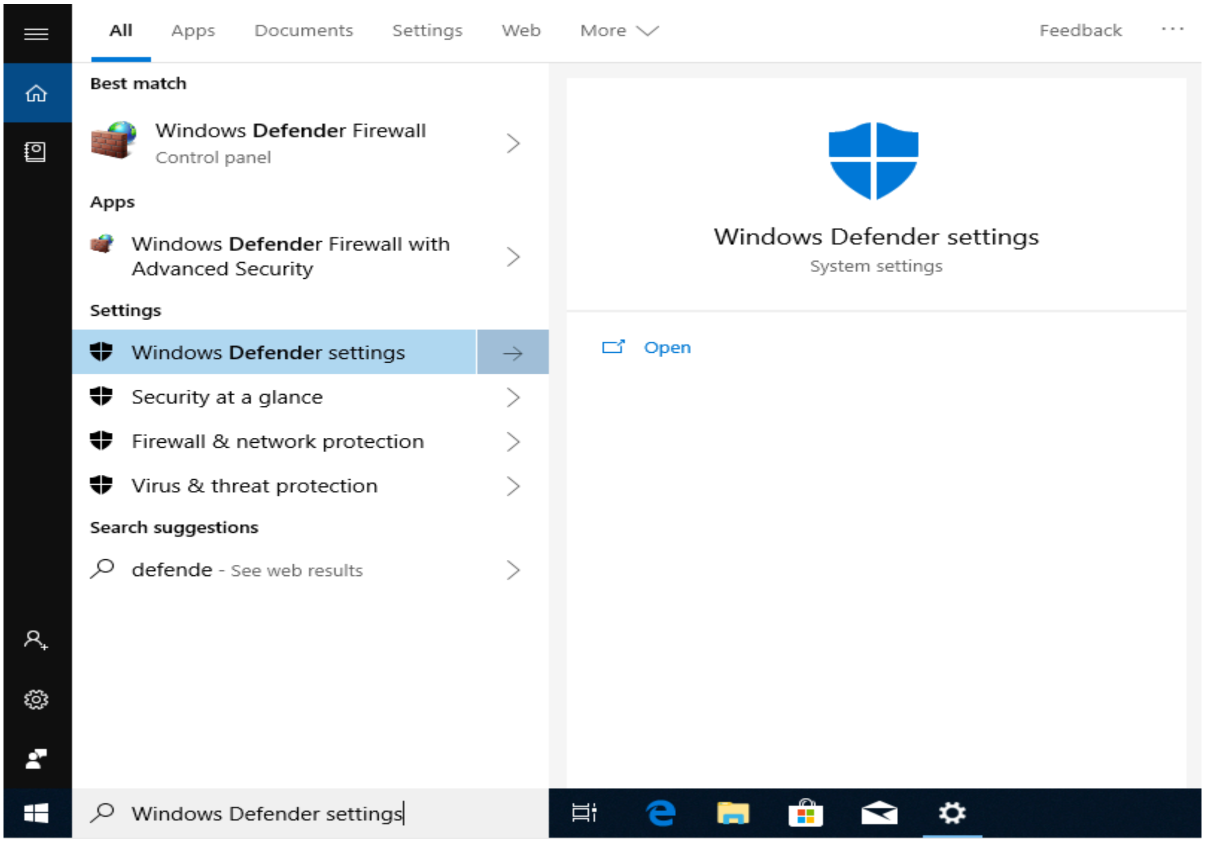
Instructions to access the VM machine for the assignment:

1. Download the OVA using the following commands within the IITK network (iitk-sec will not work)

   wget http://172.29.232.18/CS668/CS668.ova

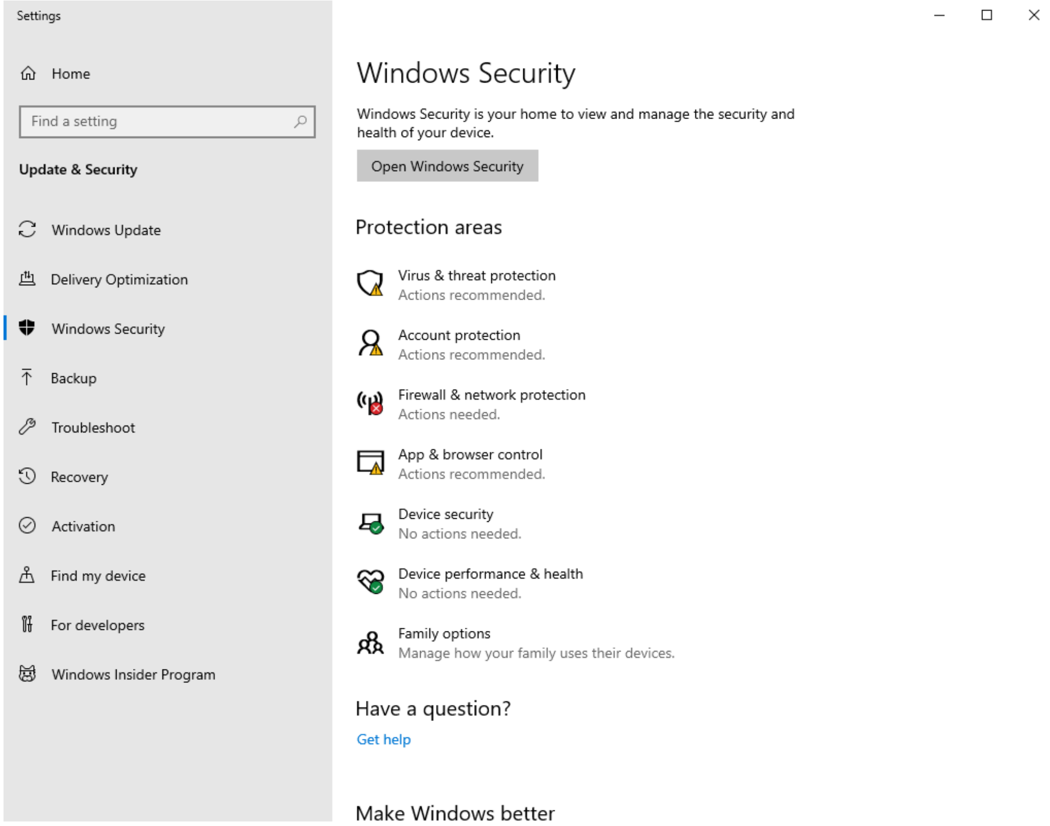
   Or

   copy the URL (http://172.29.232.18/CS668/CS668.ova) and paste it into the browser to download
2. You will be given an OVA file with the Win10 virtual machine.
3. **Prerequisites:** You need to download and install Oracle VirtualBox (https://www.virtualbox.org/)
4. After installing Oracle VirtualBox, double-click on the downloaded OVA file and click on the import option from the dialogue box appearing in the Oracle VirtualBox. **DO NOT alter any configuration settings while importing the OVA file.**
5. Use the following password to login to the Virtual Machine: **Passw0rd!**
6. Go to "**Windows Defender Settings**" by typing it from the search bar as given below:


All
Apps
Documents
Settings
Web
More
Feedback
Best match
Windows Defender Firewall
Control panel
Apps
Windows Defender Firewall with Advanced Security
Settings
Windows Defender settings
Security at a glance
Firewall & network protection
Virus & threat protection
Search suggestions
defende - See web results
Windows Defender settings
System settings
Open

Windows Defender settings

7. Click on ***Virus and Threat Protection*** as given below snippets and go to "**manage settings**" to turn off the "**Real-Time Protection**".
   Note: This real-time protection setting must be turned off manually if you power on the system after a shutdown. ***Ensure this setting is "off" all the time before proceeding to do anything regarding the assignment.***



Windows Security

Windows Security is your home to view and manage the security and health of your device.

Protection areas

Virus & threat protection
Actions recommended.

Account protection
Actions recommended.

Firewall & network protection
Actions needed.

App & browser control
Actions recommended.

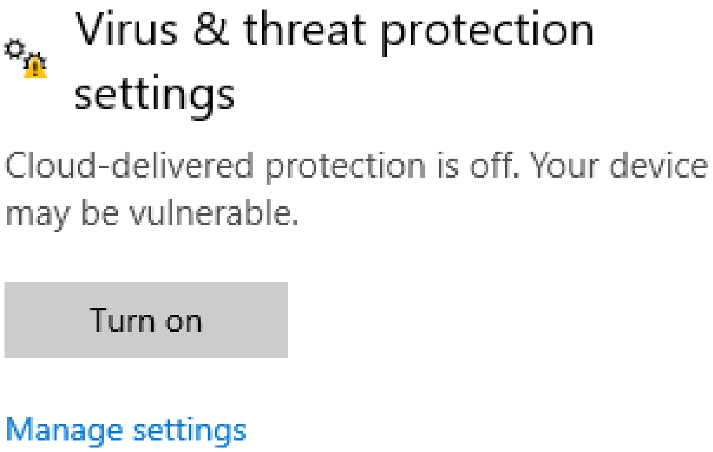
Device security
No actions needed.

Device performance & health
No actions needed.

Family options
Manage how your family uses their devices.

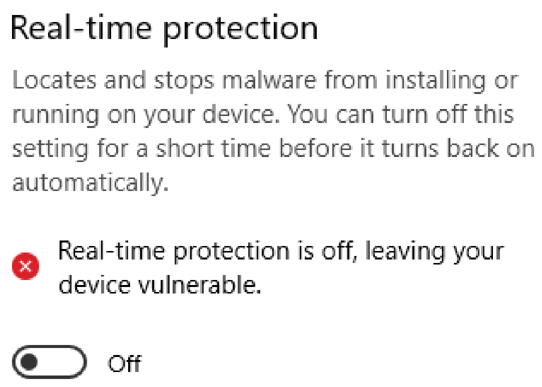
Have a question?

Make Windows better



Virus & threat protection settings

Cloud-delivered protection is off. Your device may be vulnerable.



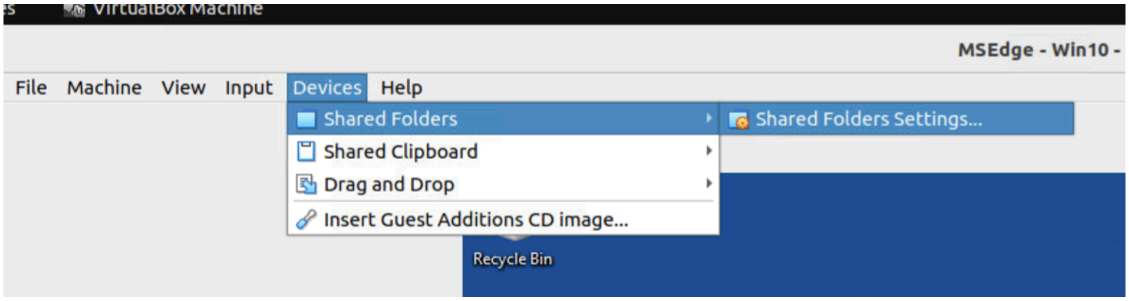
Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

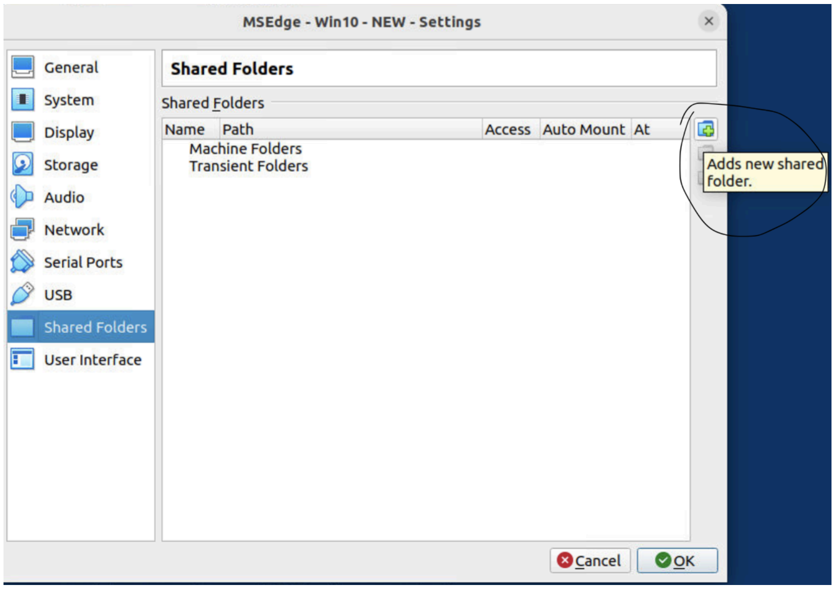
Real-time protection is off, leaving your device vulnerable.

8. Now, Download the **CS668A_AssignPer.zip** onto your **host machine** from the link using the IITK network (iitk-sec will not work): http://172.29.232.18/CS668/CS668A_AssignPer.zip
9. Create a shared folder for the VM to copy the CS668A_AssignPer.zip from the host machine to the VM. Here are the steps to do it.

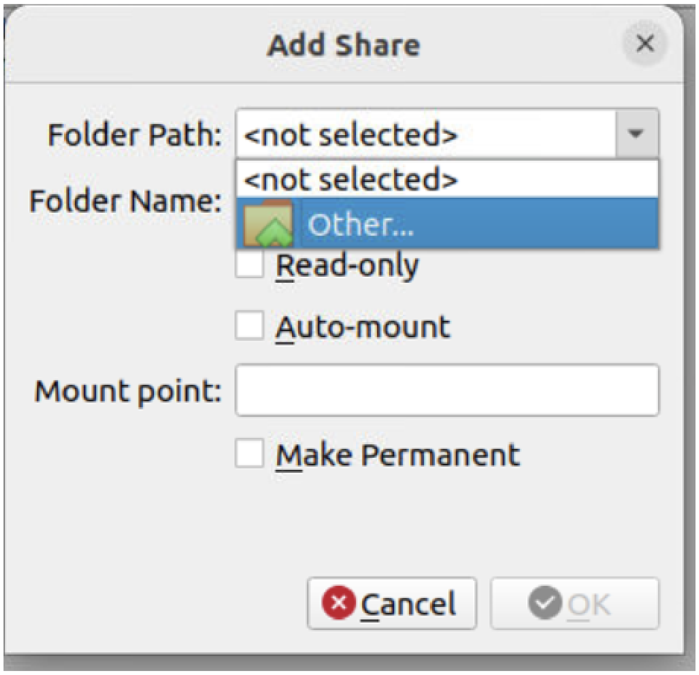
Step 1:



Step 2:



Step 3: Select "Other" from the drop-down and select the folder containing the zip file "**CS668A_AssignPer.zip.**"



Folder Path: <not selected>

<not selected>

Folder Name:

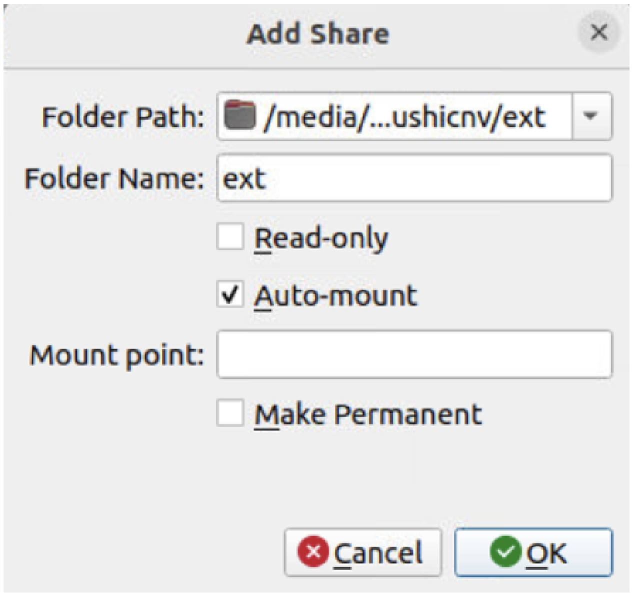
□ Read-only

□ Auto-mount

Mount point:

□ Make Permanent

Step 4: Select the "Auto-mount" option and click on "OK" Twice, and you can see the shared folder added as shown below:



Folder Path: /media/...ushicnv/ext

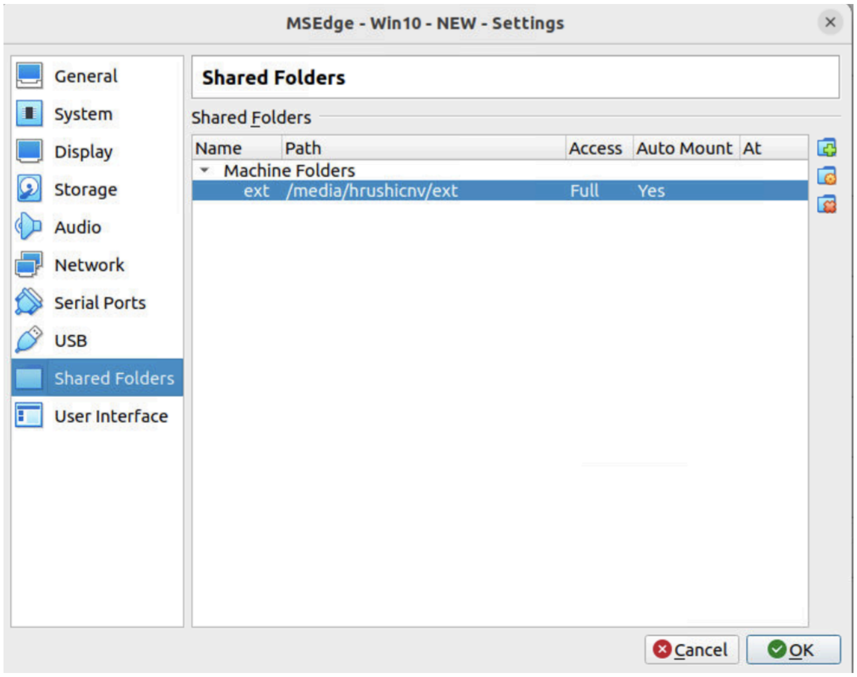
Folder Name: ext

□ Read-only

☑ Auto-mount

Mount point:

□ Make Permanent



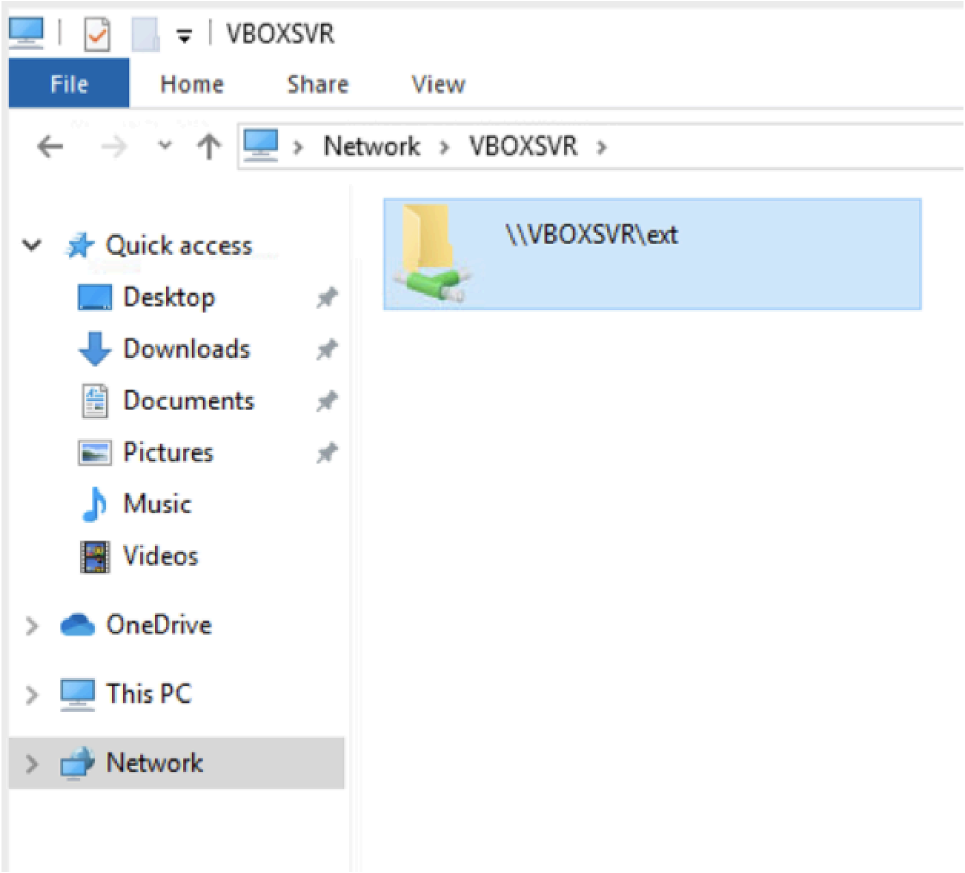
MSEdge - Win10 - NEW - Settings

Shared Folders

Shared Folders

Name	Path	Access	Auto Mount	At
Machine Folders				
ext	/media/hrushicnv/ext	Full	Yes	

Step 5: You can see the shared folder from the "Network" folder in File Explorer as shown below:

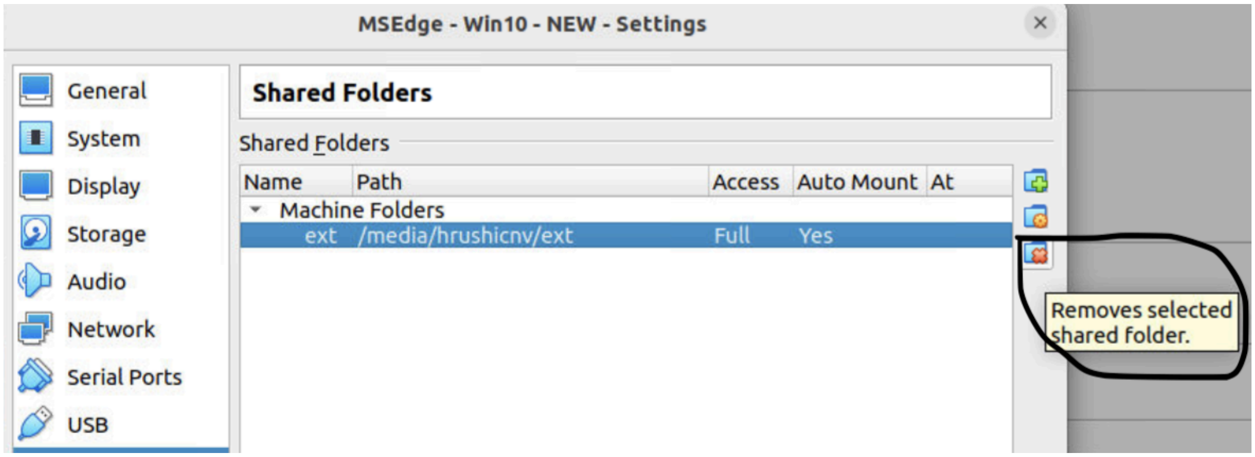


VBOXSVR

Network › VBOXSVR ›

\\VBOXSVR\ext

Step 6: Drag and drop or copy the "CS668A_AssignPer.zip" folder onto your VM (your preferred location) and now delete the shared folder as shown below:



MSEdge - Win10 - NEW - Settings

Shared Folders

Shared Folders

Name	Path	Access	Auto Mount	At
Machine Folders				
ext	/media/hrushicnv/ext	Full	Yes	

Removes selected shared folder.

Important Note:

1. **DO NOT UNZIP** the "**CS668A_AssignPer.zip**" on your host machine, as it contains malware, and your system will be infected.
2. **DO NOT UNZIP** the "**CS668A_AssignPer.zi**p" before deleting the shared folder from the settings. Your host machine can also get affected through a shared folder.

10. Unzip the file named "**CS668A_AssignPer.zip**" on your virtual machine. The password is **infected.**
11. Open your respective group folder to find your two executables to check for persistence.
12. Snapshots will preserve the present state of the VM. Take a snapshot initially before starting the assignment. You need to restore the VM to its initial snapshot taken after executing and analysing every executable. For instructions on taking a snapshot of the VM, refer to https://onlinecomputertips.com/support-categories/software/775-virtualbox-snapshots/

Summary:

1. Download the OVA file and mount it on your Oracle VirtualBox
2. After mounting the VM, disable the real-time protection setting as mentioned in the above steps.

3. Download the “CS668A_AssignPer.zip” on your host machine.
4. Create a shared folder to the VM, copy the zip file onto the VM, and delete the shared folder, as it is dangerous to the safety of your host machine.
5. Take a snapshot of the VM to preserve the above-configured settings
6. Now, go to your corresponding group folder and work on the executables and the tools.
7. After each .exe is executed and analysed, revert the VM to the initial snapshot taken before shutting down the VM.
8. Repeat 6,7 steps for each exe file and cross check for real-time protection status on your VM.

Note: You will be given the necessary tools for this task inside the VM to check persistence.