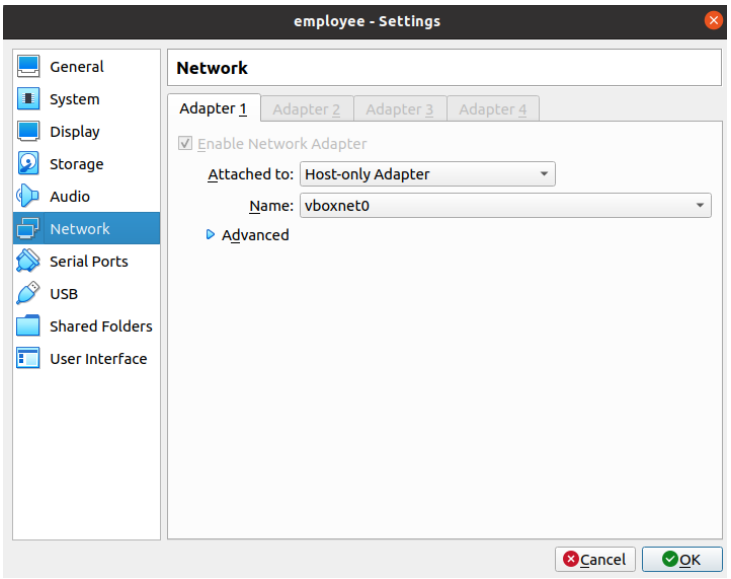
Windows Forensics for Beginners

Windows-10 image:
https://www.microsoft.com/en-us/software-download/windows10ISO

Step 1: Install Windows 10 into LAN

- Import the Windows-10 image into VirtualBox [identical to how you handle the Linux ones]
- Follow the instructions to complete the installation process
- Attach the Windows VM to the LAN, namely attaching the network adapter to the "Host-only Adapter" [identical to how you handle the Linux ones]



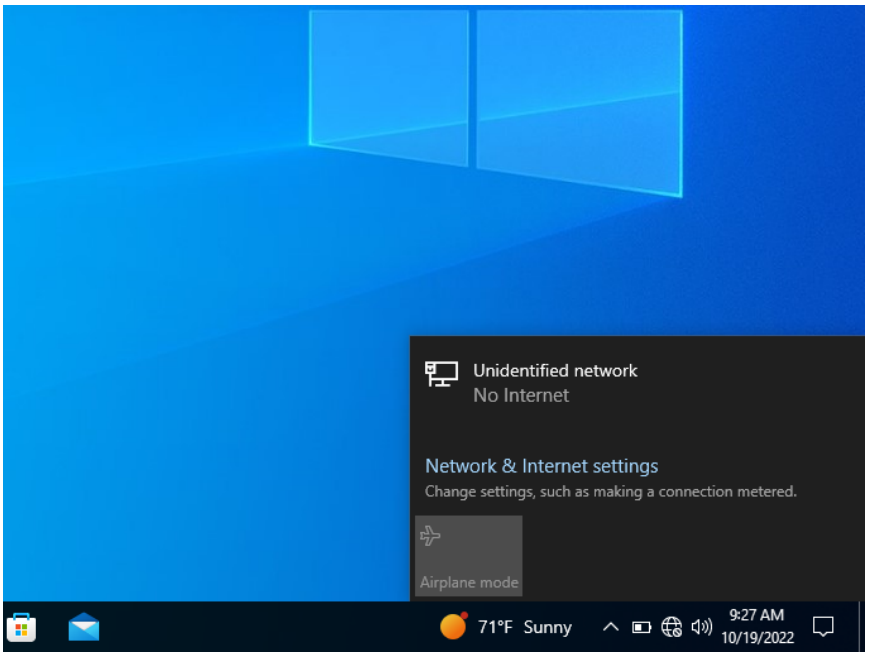
- Now start the VM if it is not running

Test 1: Open the terminal of the Windows VM, run "ipconfig /all":
Requirement: Screenshot the result that contains "IPv4 Address"
Expected results: The VM should have an IPv4 Address in the form of "192.168.56.*"

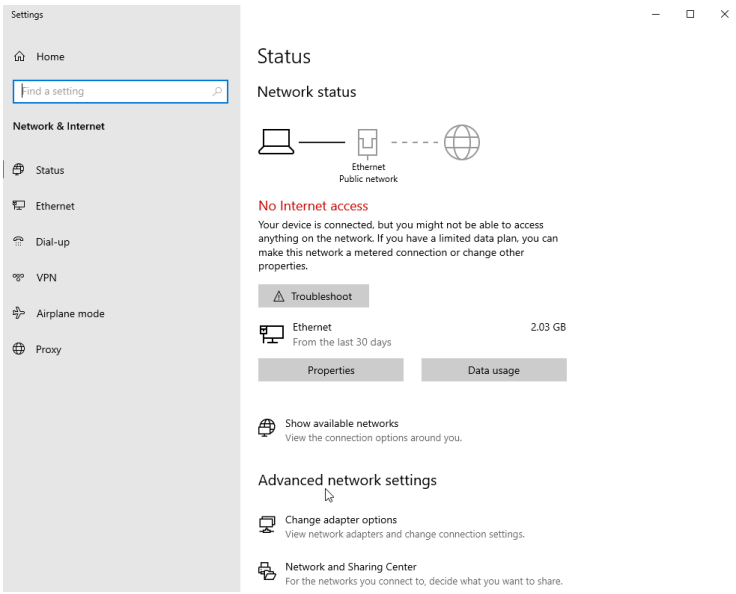
Step 2: Connect Windows 10 to the Internet

- Start your OpenWrt VM if it is not running

- Open “Network & Internet Settings” by clicking on the earth symbol in the bottom-right corner of the desktop



- Select “Network & Internet settings” and you will see the network configuration panel like the following:



  - Go to “Change adapter options” under “Advanced network settings”
  - Select “Ethernet” → Select “Properties” → Select “Internet Protocol Version 4 (TCP/IPv4)” [Just highlight the item with “blue”; DO NOT uncheck the box] → Select “Properties” → Select “Advanced” → Go to “Default gateways” and select “Add” —> Type the IP address of your OpenWrt VM [192.168.56.10 by default] →

Click “add”, then “OK”, then “OK”, then “Close”. At this point, the Windows should be connected to the Internet if your host does

Test 2: Open the terminal of the Windows VM, run “ping 8.8.8.8”:

Requirement: Screenshot the result of the command

Expected results: The result should show that “ping” can get a reply from “8.8.8.8” [assuming your host machine is connected to the internet]

Step 3: Configure the Windows VM to audit file access

- The folder we are going to audit is:
  `C:\Users\%s\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`

Note 1: “%s” is a wild card; Please replace it with your username of the Windows VM

Note 2: “C:\Users\%s\AppData” is hidden by default. You will need to enable view of hidden files on Windows. For that, please refer to https://support.microsoft.com/en-us/windows/view-hidden-files-and-folders-in-windows-97fbc472-c603-9d90-91d0-1166d1d9f4b5

- How to set up auditing on the above folder:

https://www.lepide.com/how-to/track-who-read-files-on-your-windows-file-servers.html#:~:text=To%20audit%20file%20accesses%2C%20you,displayed%20in%20the%20right%20panel

Note 1: In the above link, it says [Launch “Group Policy Management” console. For that, on the primary “Domain Controller”, or on the system where “Administration Tools” is installed, type “gpmc.msc” in the “Run” dialog box, and click “OK”.]

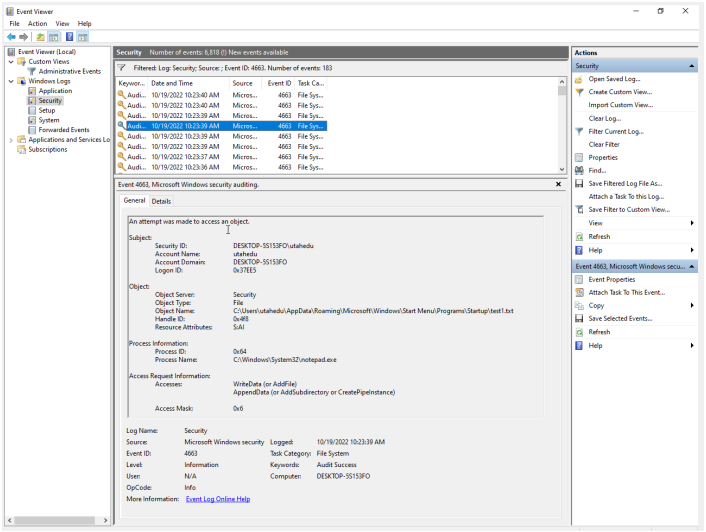
This may not work on your Windows VM. **Instead, open the menu of your Windows VM [click on the “windows” icon on the bottom-left corner], type “group”, and select “Edit group policy”.**

Note 2: In the above link, it says [For that, navigate to “Computer Configuration”]. **In your Windows VM, “Computer Configuration” is under “Local Computer Policy”**

Note 3: When discussing [“Permissions” section] on the target folder, the link says [select “Traverse Folder/Execute File”, “List Folder/Read data”, “Read attributes”, and “Read extended attributes” permissions]. **In your Windows VM, select EVERYTHING**

Test 3: Create a file “test.txt” in the above folder [`C:\Users\%s\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`]; Check the auditing log as explained in the above link

[https://www.lepide.com/how-to/track-who-read-files-on-your-windows-file-servers.html#:~:text=To%20audit%20file%20accesses%2C%20you,displayed%20in%20the%20right%20panel]
Requirement: Find the log for writing data into the “test.txt” and screenshot the log
Expected results: The log should look like this:



- Remove file “test.txt” in the above folder once the above steps are completed

Step 4: Configure SSH Server on the Windows VM

- Install OpenSSH for Windows
  - Open Settings, select Apps, then select Optional Features.
  - Scan the list to see if the OpenSSH is already installed. If not, at the top of the page, select Add a feature, then:
  - Find OpenSSH Client, then select Install
  - Find OpenSSH Server, then select Install
  - Once setup completes, return to Apps and Optional Features and you should see OpenSSH listed.

- Start “PowerShell” as the “Admin” [Click the “windows” menu on the bottom-left corner, type “power”, right-click “Windows PowerShell”, click on “Run as an administrator”]

- In PowerShell, run
  - `Start-Service sshd`
  - `Set-Service -Name sshd -StartupType 'Automatic'`
  - ~~`Start-Service 'ssh-agent'`~~

~~- Set-Service -Name 'ssh-agent' -StartupType 'Automatic'~~

- `netsh advfirewall firewall add rule name="SSHD service" dir=in action=allow protocol=TCP localport=22`

Test 4: SSH into your Windows VM

- If your Kali Linux VM is running, turn it off
- Attach the Kali Linux to LAN [by switching its network adapter to "Host-only Adapter"]
- Start your Kali Linux
- In the terminal, run: ssh -p 22 windwosusername@windows.vm.ip [Replace "windowsusername" with your real user name in the Windows VM; Replace "windows.vm.ip" with the real IP address of your Windows VM]

Requirement: Screenshot the SSH connection results
Expected results: You should be able to SSH into the Windows VM from Kali Linux

Step 5: **Snapshot your Windows VM!!!** Give it a name like "CleanWindows"

Step 6: Get infected by a malware

- Download a sample from [https://tinyurl.com/4w89easj] to your **Windows VM [please never put it on your host machine]**
- Unzip the downloaded zip file using password "123456" to extract the sample into a new folder [watever folder you would like]
- Run the sample via "Run as administrator" [Windows defender may prevent you from doing that; Just pick "more info" and then "run anyway"; You will also see a question asking "Yes" or "No", pick "Yes"]

Test 5: Observe what happens after you run the sample

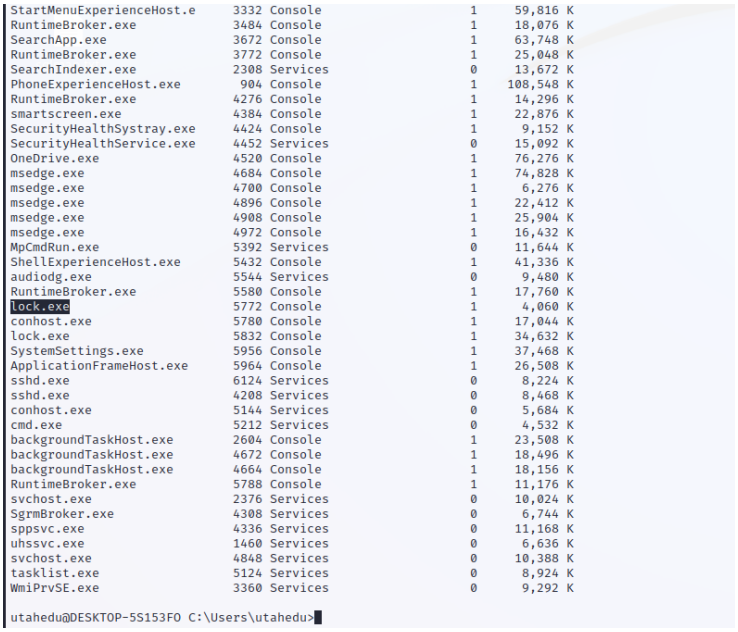
Requirement: Screenshot your observations [you can try to give some passwords except for right answer "123"]
Expected results: You should be able to see that the screenshot is locked [similar to the following]

After the above test, try to restart the Windows VM using VirtualBox; Wait for a couple of seconds and you should see the malware takes the control again

Step 7: Gain access to the Windows VM via SSH

- Repeat what you did for **Test 4**
- Assuming now you SSHed into the Windows VM, then do the following

Test 6: Find the suspicious process by running "tasklist" and look for a process named "lock.exe" [in the ssh terminal on the Kali Linux]
Requirement: Screenshot the list of processes running on your machine
Expected results: The list should contain an item called "lock.exe"



Test 7: Find out where is the malicious program by running "wmic process where "name='lock.exe'" get ProcessID, ExecutablePath" [in the ssh terminal on the Kali Linux]
Requirement: Screenshot the results
Expected results: The list should tell you where is "lock.exe"

Test 8: Kill the malicious process by running "taskkill /IM lock.exe /F"and then check your Windows VM again
Requirement: Screenshot the desktop of your Windows VM
Expected results: You should be able to get your Windows back

Step 9: Clean up the infection

- Delete the sample at the path you found in **Test 7**

Test 9: Check the file auditing logs following what you did in **Test 3.** Check if the sample adds anything to the folder [`C:\Users\%s\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`] [Note: replace "%s" with your username]
Requirement: Screenshot the log recording the action by the sample
Expected results: You should be able to see that the sample adds a file called "open.bat" into the above folder

The Last step: remove "open.bat" in the above folder. Now you have a clean Windows VM [if you are curious, you can check the contents in the file]

Submission:

Please create a PDF document to include the results of **Test 1** - **Test 9**, and submit the PDF document to GradeScope:
https://www.gradescope.com/courses/411636/assignments/2365358/submissions