CSC 471 Spring 2024 Lab 4

Dr. Si Chen

Kernel Mode Rootkit

The goals of this lab:

- Understanding the concepts of Kernel Mode Rootkit.
- Know how to use WinDBG with VirtualBox to debug Windows kernels.

Experiment Setup

Setting Up Kernel-Mode Debugging of a Virtual Machine Manually using a Virtual COM Port

1. In your host machine (must be either Windows 10 or Windows 11), go to Microsoft Store and download WinDBG preview

   ```
   https://www.microsoft.com/en-us/p/windbg-preview/9pgjgd53tn86
   ```

2. Open VirtualBox, Go to "Settings" for our virtual machine "xpxp", select "Serial Ports," and input the following information (shown in Fig.1) to enable Serial Port 1.
3. Boot up windows XP inside VirtualBox.
4. Inside Windows XP, Open "My Computer" and go to C:
5. On the top menu, click "Tools" – "Folder Options" and then select the tab "View". Uncheck the option "Hide protected operating system files (Recommended)" (shown in Fig.2)
6. Open the boot.ini (under C:) with notepad, in Notepad, copy the existing boot line, paste it at the end of the file, and add these switches to the end of the line, as shown in Fig.3:

   ```
   /debug /debugport=COM1 /baudrate=115200
   ```

7. Power off the TARGET virtual machine. You cannot make this change while the virtual machine is running or suspended.
8. Open WinDBG preview, click "Home," and select "start debugging" – "Attach to the kernel." Select "COM" and fill the information as shown in Fig.4

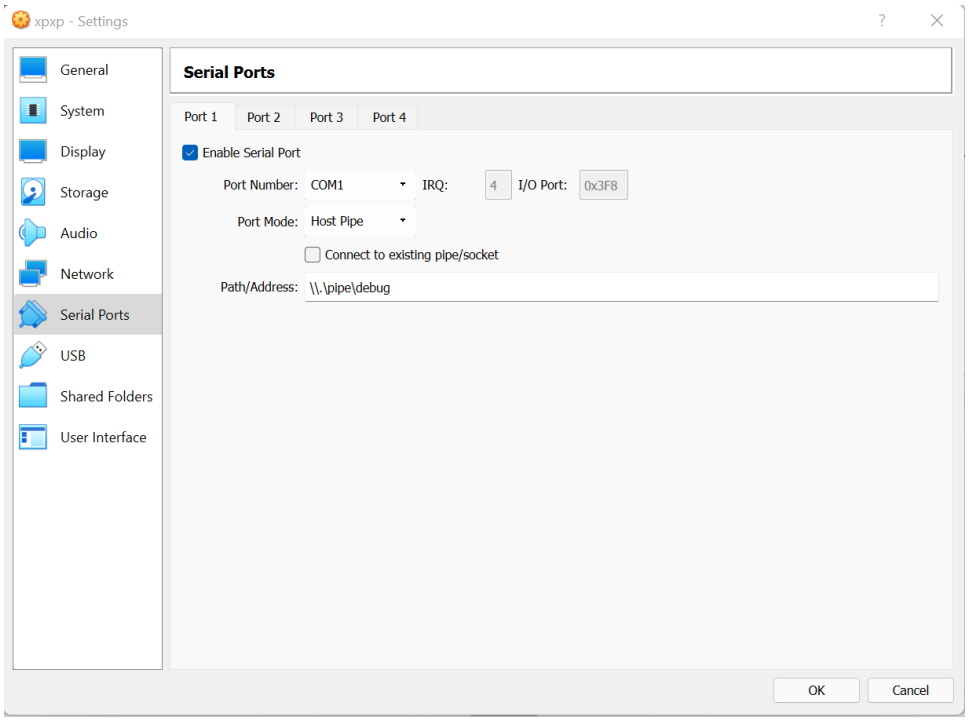

Figure 1: Serial Ports Settings

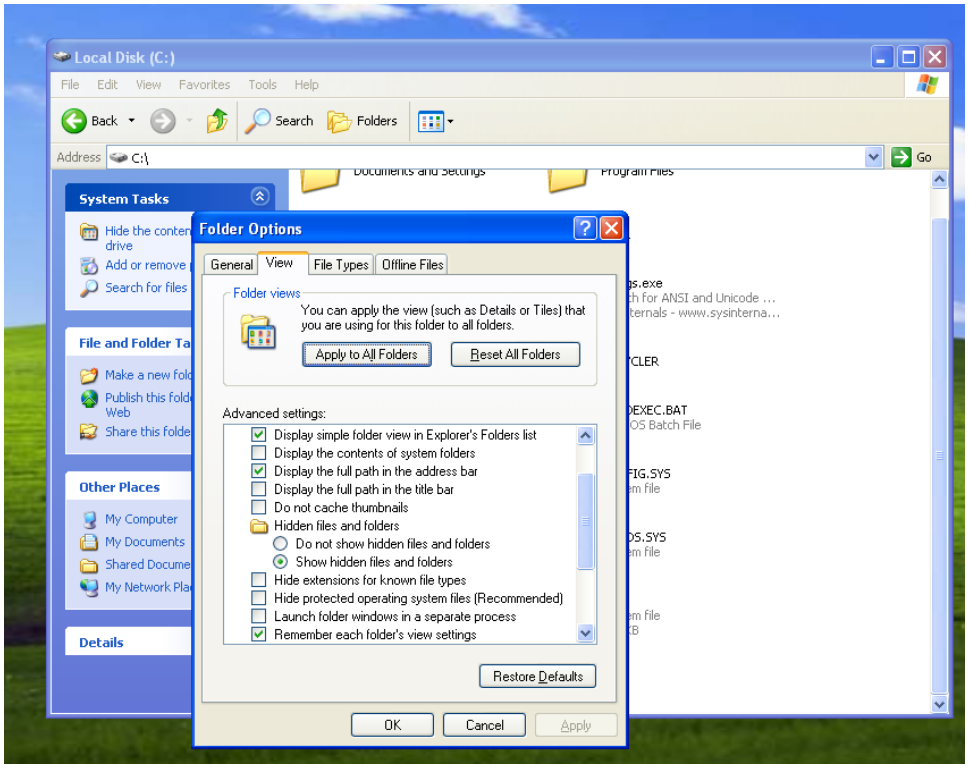

Figure 2: Tweak Folder Settings

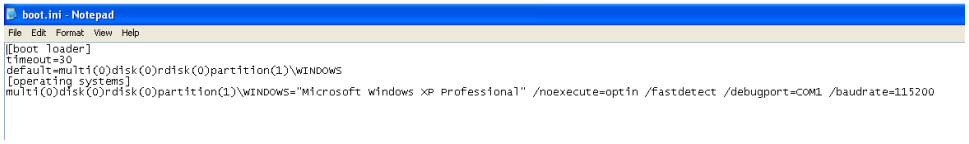

Figure 3: Change boot.ini settings

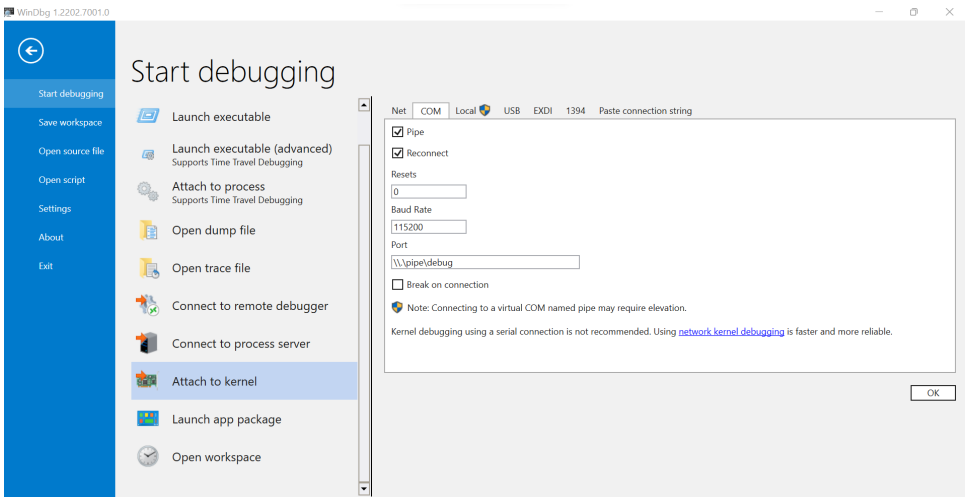

Figure 4: Connect WinDBG with VirtualBox via COM

9. Boot up Windows XP VM, and you should be able to see that WinDBG is outputting some debug information of the VM kernel.

10. Click the "Break" button on the top of the WinDBG; the Windows XP VM should freeze. And you should be able to enter the command (shown in Fig.5).

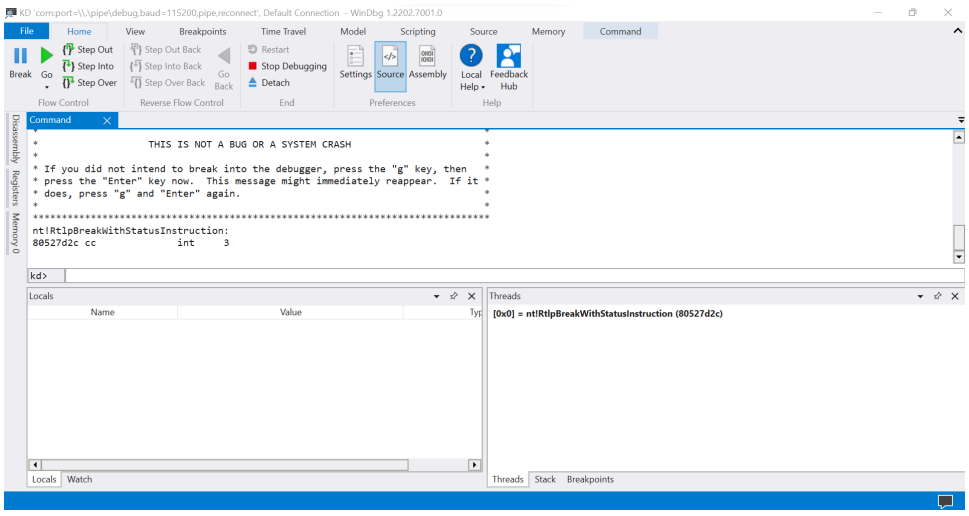

Figure 5: Use WinDBG to break the windows xp VM

11. Read the following questions (in the next section) and answer them in your report.

Lab Questions

Q1. What is a SSDT?

Q2. Please use WinDBG and type the following command:

```
dds KiServiceTable L 12a
```

Please take a screenshot of the output result. What's the meaning of each column?

On your host machine, please open Notepad and copy all your output results into it and save the file (we need to use it after running the malware).

Then, please resume the Windows XP VM by clicking the "GO" button on top of the WinDBG. Inside Windows XP VM, please download Lab4.zip from our class website. Unzip it and double-click the "loader.exe" to run the SSDT hook malware.

Next, switch back to WinDBG and click the "Break" button to pause the VM. Type the same command again:

```
dds KiServiceTable L 12a
```

Q3: Comparing the two outputs (before hook and after hook), can you tell which functions have been hooked?

Q4: Can you take a guess of what is this malware trying to do (based on the hooked functions)?

Hint

Please check the lecture slides – Class 18 Kernel Mode Rootkit (SSDT Hook Example).

Submission

- The lab due date is available on our course website. Late submission will not be accepted;
- The assignment should be submitted to D2L directly.
- Your submission should include: A **detailed project report in PDF format** to describe what you have done, including screenshots of the final result
- **No copy or cheating is tolerated**. If your work is based on others', please give clear attribution. Otherwise, you **WILL FAIL** this course.