**Lab 17: Kernel Debugging with WinDbg (PC version)**

**Course Name**: Malware Analysis and Reverse Engineering (IAM302)

**Student Name**: Nguyễn Trần Vinh – SE160258

**Instructor Name**: Mai Hoàng Đỉnh

**Lab Due Date**: 18/3/2023

**Purpose**

Introduction to WinDbg and kernel debugging

**What You Need**

* A Windows 8 machine with VMware Player installed.
* A Windows XPSP3 virtual machine to examine.

**The Two Machines**

You need two Windows machines to do this project: One is the TARGET machine, which is a virtual machine running Win XP SP3. The other is the WINDBG machine, which is the Windows 8 host.

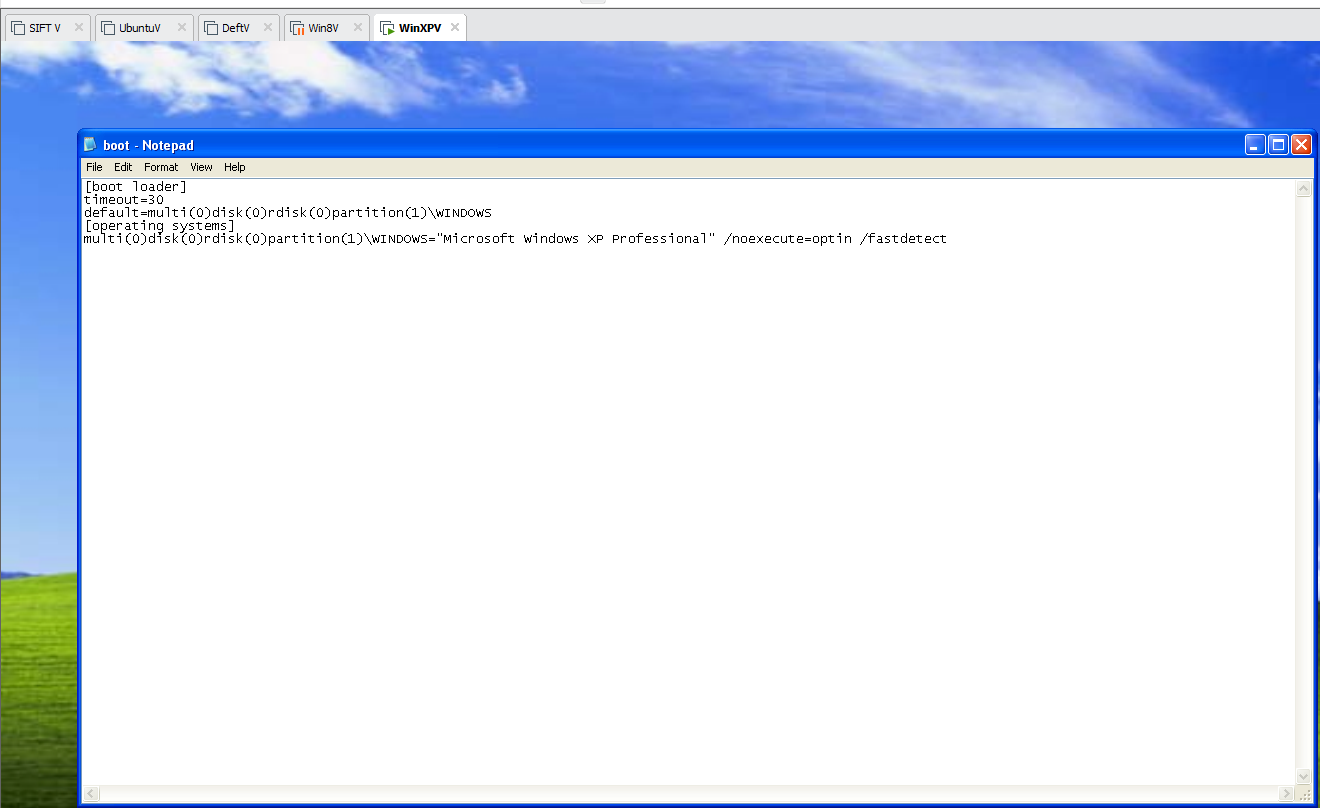
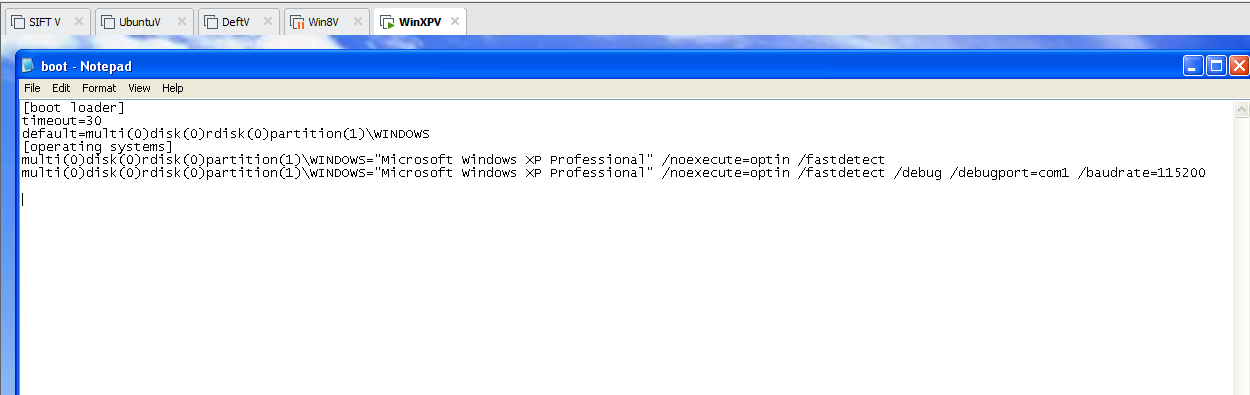
**Adding a Boot Menu Item to the TARGET machine**

* In the Run box, execute this command:

**notepad c:\boot.ini**

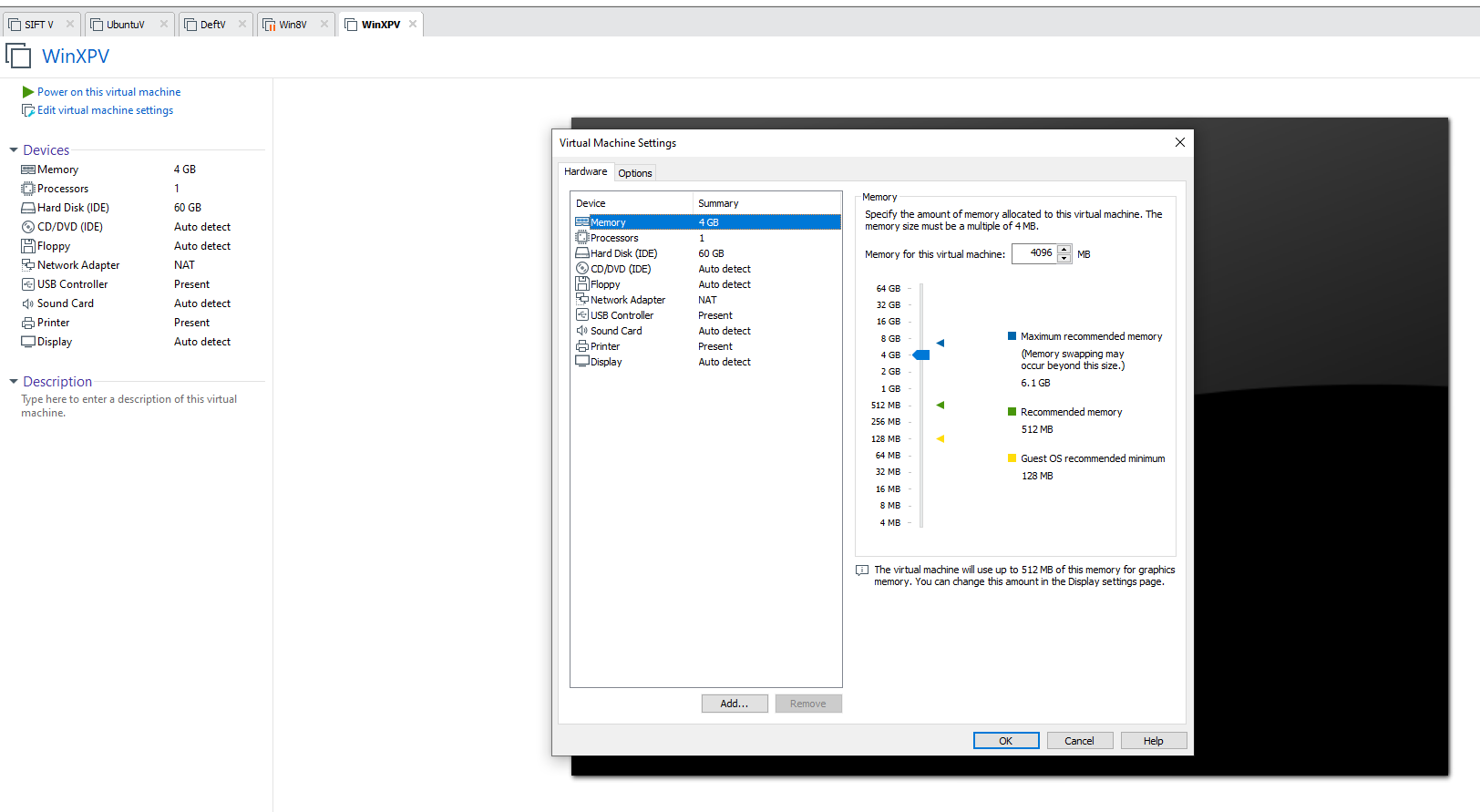
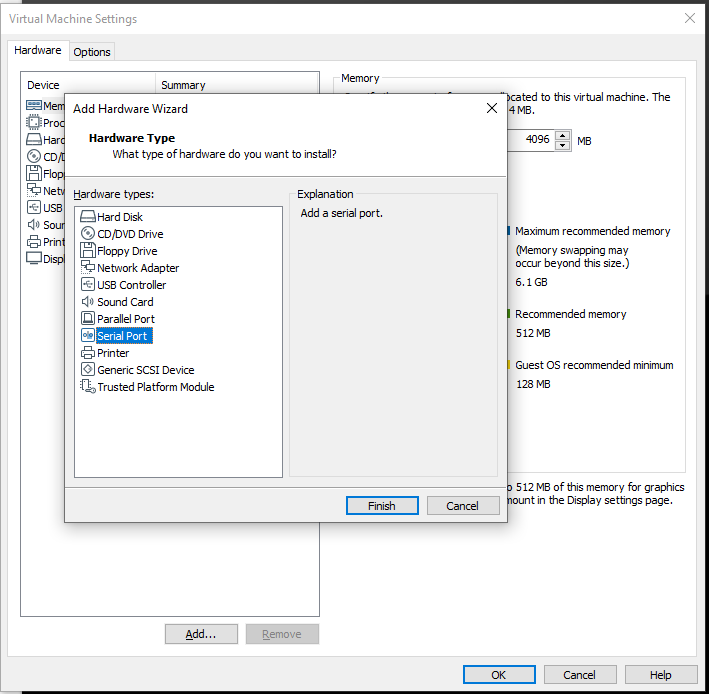
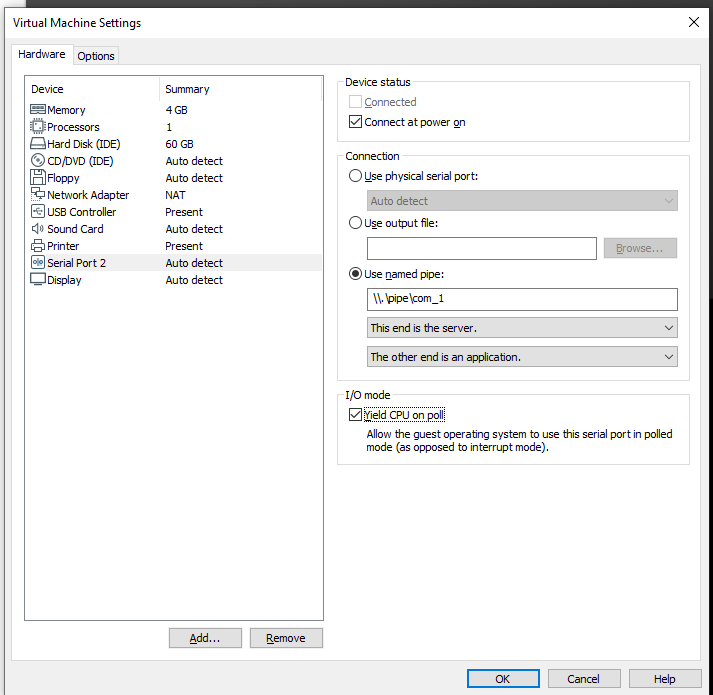
* In Notepad, copy the existing boot line, paste it at the end of the file, and add these switches to the end of the line, as shown below:

**/debug /debugport=com1 /baudrate=115200**

** **

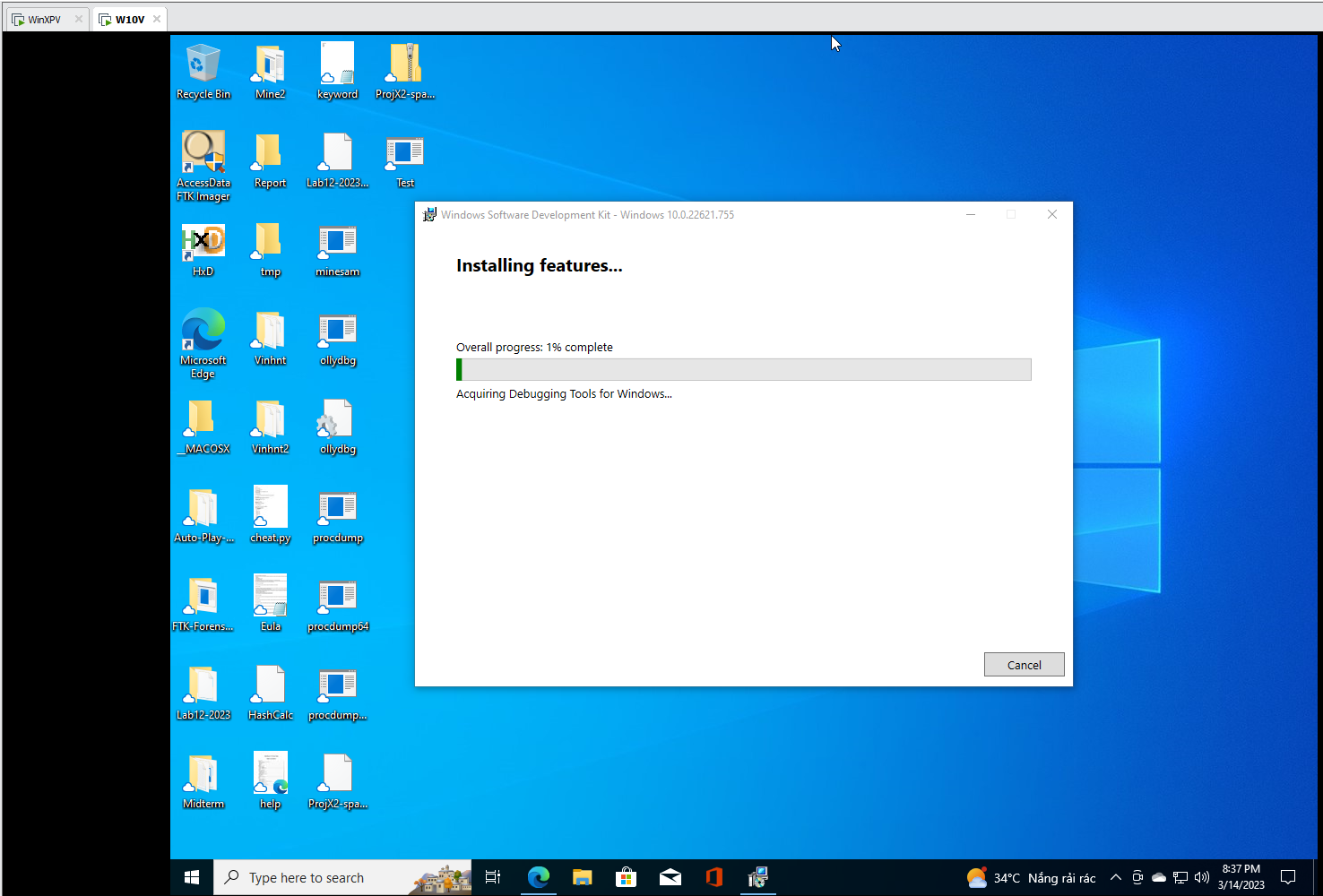
**Adding a Virtual Serial Adapter**

* Power off the TARGET virtual machine.
* On the WINDBG machine, start VMware Player.
* In the left pane of VMware Player, click your TARGET machine.
* At the lower right of VMware Player, click "Edit virtual machine settings".
* In the left side of the "Virtual Machine Settings" box, click the Add... button.
* In the "Hardware Type" box, select "Serial Port", as shown below.

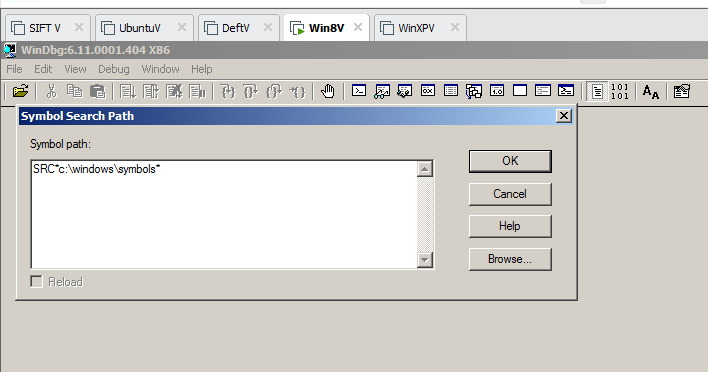
**  **

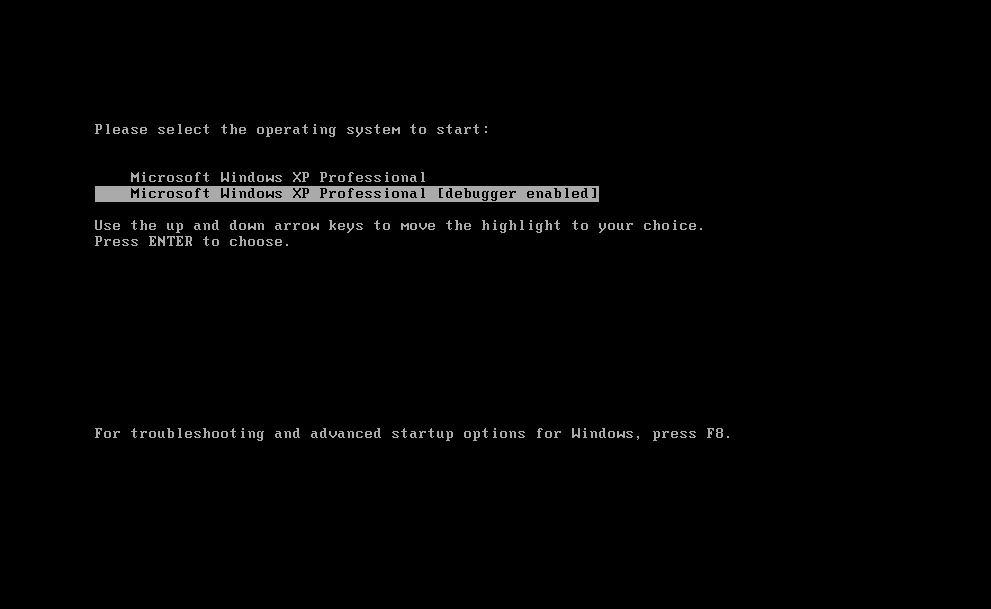
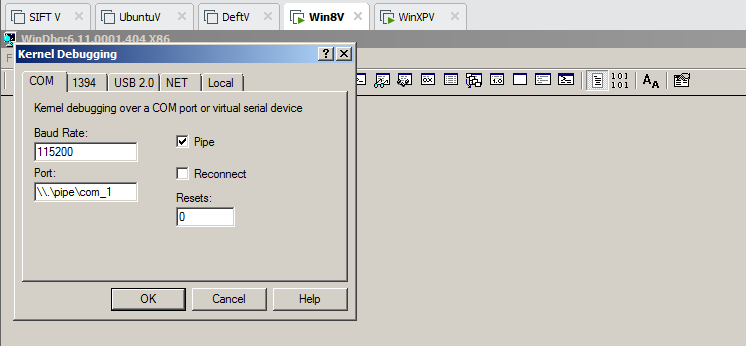
**Downloading Microsoft Symbols**

**Installing WinDbg on the WINDBG Machine**

****

**Configuring Symbols in WinDbg**

****

** **