

Lab 1A

Windows Basics

ITSC205: Operating Systems Internals

NAME: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Table of Contents

[Lab Outcome(s) 3](#_Toc472025633)

[Reading 3](#_Toc472025634)

[Introduction 3](#_Toc472025635)

[1.0 Virtual Machine 4](#_Toc472025636)

[2.0 System Information 6](#_Toc472025637)

[3.0 Windows Services 7](#_Toc472025638)

[4.0 Command-Line Interface 8](#_Toc472025639)

[5.0 The Sysinternals Suite 10](#_Toc472025640)

Lab Outcome(s)

* Set up virtual environment for course lab exercise.
* Examine the Windows environment provided by the system user interface and the Sysinternals suite of advanced system utilities.

Reading

* Textbook Chapter 21- Windows 10 –Sections: 21.1 History and 21.4.

Introduction

In this lab, we will set up the virtual machine environment that is used as the basis for studying the Windows operating system in detail for this course. We will study some of the tools, provided by the operating system and external, to examine various information regarding the system itself.

1. Virtual Machine \_\_\_/10

In this course, we study operating systems in a safe environment that allows us to experiment without ruining the configuration of the computers we use for everyday work. The safe environment is a *virtual machine*: a program that **acts like** a physically separate computer. Virtual machine (VM) software is installed on and run on a *host* system. A *guest* operating system is installed onto the VM, and the VM runs programs just as if they were running on a separate computer. We will use the Oracle VM VirtualBox virtual machine system.

1. Obtain the files you will need:

* The latest version of “VirtualBox platform package” virtual machine software from <http://www.virtualbox.org/wiki/Downloads>. Select the host suitable for your machine. (E.g. if your machine is running Windows, select “Windows hosts”.)
* A pre-configured “image” of Windows 10 to run in the virtual machine (obtain from instructor).

1. Run the VirtualBox installer you downloaded. Install the program using the defaults provided.
2. Unzip the image file. (The 7-Zip program should be installed on your computer. If it is not, then get it from <http://www.7-zip.org/>.)
3. Configure the Windows 10 virtual machine:
4. Create a new virtual machine (click the “New” button).
5. Name the machine “Win10” or something similar and specify operating system “Microsoft Windows” and version “Windows 10 64-bit”.
6. Select a base memory size of 4096 MB.
7. Configure the Virtual Hard Disk. Select “Use an existing virtual hard drive file” and click the folder icon. Browse to the Windows 10 hard disk image directory you extracted in step 3. Select “Windows10.vdi”.
8. Click “Create”.
9. View the various system settings.
10. Start the Windows 10 virtual machine. Log in to the user account using the password “P@ssW0rd”.
11. The Windows system will take quite a while to configure itself including the automatic installation of needed device driver code and updates to the operating system. The process may require multiple restarts.
12. Restart the Windows virtual machine and configure the VirtualBox virtual display. “VirtualBox Guest Additions” allows the guest OS to resize the display **plus** adds other features used in **later** labs.
    1. Under Windows 10 guest virtual machine window select: Devices 🡪 Insert Guest Additions CD Image; The system should mount the CD with the image
    2. Login into Windows 10 virtual machine and under This PC click twice on the CD image to install the tools. Install using defaults; restart; resize guest window as desired.

|  |  |
| --- | --- |
| **ASK THE INSTRUCTOR TO SIGN OFF** |  |

**Note:** Rt-Ctrl is the default “Host” key to communicate with VirtualBox on the Host (e.g., Rt-Ctrl-F switches back and forth between full screen and windowed mode).

2.0 System Information \_\_\_\_/10

1. Use the Start Menu 🡪 Windows Administrative Tools 🡪 System Information utility to find the following values:
2. OS name:
3. OS version:
4. System name:
5. Windows directory:
6. Boot device:
7. Total physical memory:
8. Open Task Manager and click on “More details. What is the program (executable) for the System Information application?
9. How can you launch the System Information application using your answer from the previous question?

3.0 Windows Services \_\_\_\_/10

Services on Windows are usually non-interactive (does not directly accept user input) and run consistently in the background. Examples of services include event-logging and the firewall. Many antivirus products run as services as well. Malicious code often leverages services for persistence (to survive reboots), to load kernel drivers and to blend in with legitimate components of the system.

1. Use the Start Menu 🡪 Windows Administrative Tools 🡪 Services utility to view the services installed on the virtual machine.

What is the difference between automatically started and manually started services?

1. Research and briefly describe the purpose of the following services:
2. Security Center:
3. Windows Firewall:
4. Windows Defender Service:
5. Windows Event Log:

4.0 Command-Line Interface \_\_\_\_/10

The command-line interface of Windows has similarities to and differences from that of Linux. Some commands are the same. Some commands are similar, but with subtle syntax differences.

1. The command-line interface is started by Start Menu 🡪 Windows System 🡪 Command Prompt. To save keystrokes, attach (pin) the Command Prompt to the taskbar.

What is the program (executable) for the command prompt application?

1. Execute the following commands, research and explain the results of each.
2. hostname
3. cd \
4. dir /ah
5. The SET command displays all system variables at one time. Use SET to find the value of the following environment variables:
   1. ALLUSERSPROFILE
   2. NUMBER\_OF\_PROCESSORS
   3. windir
6. Use ECHO to display the value of the PATH environment variable (Hint: a special character is required), what is the command you used?

Research and briefly explain the purpose of the PATH variable:

5.0 The Sysinternals Suite \_\_\_\_/10

The utilities provided by the Windows operating system is sufficient for everyday use but as an IT security professional, you need more advanced tools to diagnose and troubleshoot your system.

1. Download the **Sysinternals Suite** from [www.sysinternals.com](http://www.sysinternals.com) (which will redirect you to <http://technet.microsoft.com/en-US/sysinternals> since Microsoft’s acquisition of Sysinternals in 2006).
2. Before you extract the tools from the zip file, you can remove the marker that tells Windows to treat the content of the file as coming from the internet and is untrusted. This will get rid of the security warnings when you run any of the tools or display content errors when viewing the help files.

To do this, right-click on the SysinternalsSuite.zip file in folder what you have downloaded it in the previous step. Go to the Properties dialog box, on the General tab near the bottom – select the Unblock checkbox and click OK.

1. Extract the tools from the zipped file to a location where you will be able to locate easily in the future as we will be using many of these tools for all the lab exercises in the course.
2. Open a command prompt and navigate to the directory where you have extracted the sysinternals tools.

*Pro-tip: Type “cmd” in the address bar of file explorer and the command prompt will start in the same directory location.*

1. In the command prompt window, execute the PsInfo tool by simply typing “psinfo”.

*Pro-tip: Each sysinternals utility requires acceptance of an End User License Agreement (EULA) and will display a dialog box the first time a user runs a particular tool, even in console mode. The /accepteula switch can be used as a valid assertion of the agreement with the license terms.*

1. View all the options by using the /? switch. Demonstrate to the instructor how to append disk volumes information to the PsInfo results.

|  |  |
| --- | --- |
| **ASK THE INSTRUCTOR TO SIGN OFF** |  |

**EVALUATION**:

|  |  |  |
| --- | --- | --- |
| Configure Windows virtual machine | 10 |  |
| Explore Windows basic settings using System Information tool | 10 |  |
| Explore Windows Services | 10 |  |
| Window Command Line Interface | 10 |  |
| Download and explore System internals tools | 10 |  |
| TOTAL MARK | 50 |  |