# Windows 7 and Browser Security

## Instructions

You are required to submit a written report of how you accomplished the tasks in this laboratory. The report should consist of a series of screenshots and a written account of your observations. The report must be submitted to Blackboard within a week of completing the laboratory session. Standard CIT penalties for late submission will apply.

## Learning Objectives

Upon completion of this lab, you will be able to:

- Launch a virtual Windows 7 virtual machine on a laboratory computer
- Update this computer with the latest Operating system Patches.
- Secure the Administration account with a password
- Add a non-privileged account to the operating system
- Install and test two types of Antivirus software
- Check configuration of the Windows 7 Firewall
- Modify and test Windows 7 Firewall settings
- Install and test third-party firewall software
- Install and test the CCleaner package for computer maintenance.
- Install the KeepassX password manager application
- Install and test a range of browser extensions to help safeguard your online browsing.

## Background

The Microsoft Windows Operating System is extensively deployed in both domestic and business computing environments. It is essential that both the operating system is kept up to date with the latest OS software patches and anti-malware software to combat the latest cyber threats.

Malware and privacy issues are also of concern to users when browsing the internet. A number of browser extensions can safeguard a user's computer from malicious drive-by downloads and spying activity. We will investigate the use of some of these extensions to the Chrome browser.

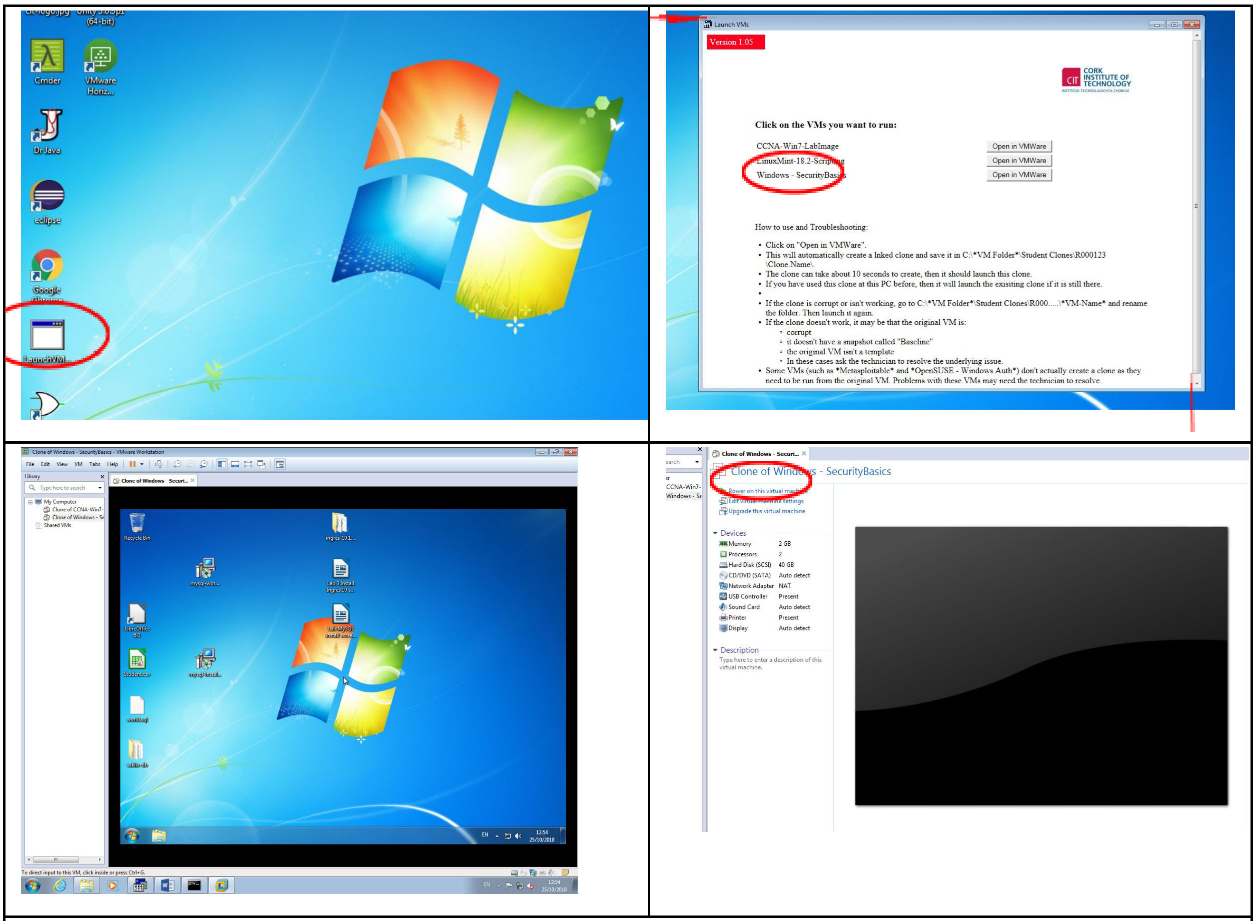
## PART 1: Operating System Security (performed on the Virtual Machine)

Task 1: Start up a Windows 7 Virtual Machine on a laboratory desktop computer.

> -> "double-click" the "Launch VMware" icon on your desktop and you should see "Windows - SecurityBasics" as an OS that you can "launch"

A virtual machine is a computer running inside another computer. Virtual machines in the laboratory to allow students change parameters (network configuration etc.) in a computer without affecting the physical computer.

To start up the virtual machine click on the icons indicated in red in the diagram below: we will be using the “Windows SecurityBasics” virtual machine.


Cmder
VMware Horiz...
Dr Java
eclipse
Google Chrome
LaunchVM
Launch VMs
Version 1.05
CORK INSTITUTE OF TECHNOLOGY
Open in VMWare
Open in VMWare
Open in VMWare
Clone of Windows - SecurityBasics - VMware Workstation
Library
My Computer
Clone of Windows - Securi...
Recycle Bin
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine
Devices
Description

Click on the VMs you want to run:

CCNA-Win7-LabImage
LinuxMint-18.2-Scripting
Windows - SecurityBasics

How to use and Troubleshooting:

- Click on "Open in VMWare".
- This will automatically create a lnked clone and save it in C:\*VM Folder*\Student Clones\R000123\Clone.Name\.
- The clone can take about 10 seconds to create, then it should launch this clone.
- If you have used this clone at this PC before, then it will launch the exisiting clone if it is still there.
-
- If the clone is corrupt or isn't working, go to C:\*VM Folder*\Student Clones\R000.....\*VM-Name* and rename the folder. Then launch it again.
- If the clone doesn't work, it may be that the original VM is:
  - corrupt
  - it doesn't have a snapshot called "Baseline"
  - the original VM isn't a template
  - In these cases ask the technician to resolve the underlying issue.
- Some VMs (such as *Metasploitable* and *OpenSUSE - Windows Auth*) don't actually create a clone as they need to be run from the original VM. Problems with these VMs may need the technician to resolve.

Clone of Windows - SecurityBasics

| | |
|---|---|
| Memory | 2 GB |
| Processors | 2 |
| Hard Disk (SCSI) | 40 GB |
| CD/DVD (SATA) | Auto detect |
| Network Adapter | NAT |
| USB Controller | Present |
| Sound Card | Auto detect |
| Printer | Present |
| Display | Auto detect |

Type here to enter a description of this virtual machine.

To direct input to this VM, click inside or press Ctrl+G.

**Starting up the Windows SecurityBasics Virtual machine**

**Task 2:** Install Google Chrome using Internet Explorer on the Virtual Machine

*Note: Chrome is to be used for all subsequent internet-related tasks.*

**Task 3:** Check the Operating system for updates (don't install as it will take a LONG time)

**Task 4:** Secure the administrator login with the password "CSPismyfavouritemodule!"

**Task 5:** Add a non-privileged user josh with password "+CITistheBestIoT"

**Task 6:** Install Microsoft Security Essentials (32 bit version)

**Task 7:** Install free version of Malwarebytes anti-malware software

**Task 8:** Test the software by creating a text file on the desktop and pasting in the EICAR virus test string available on the internet.

**Task 9:** Check on the status of the Windows Firewall – turn on for all profiles (public etc.)

**Task 10**: Create a new rule that will block all outgoing http traffic (destination port 80 –perfect for those paranoid about unencrypted web traffic). Test to see that it works. Reset when done.

**Task 11:** Install the third-party firewall program Zonealarm and test its configuration

**Task 12:** Install and test KeePassX password manager

**Task 13**: Install and test CCleaner software (do not alter the default configurations unless you know exactly what you are doing – there is a danger you may damage the computer!).

## PART 2: Chrome Browser Security (can be performed outside the lab)

**Task 1:** Investigate, install and test WebofTrust browser extension

**Task 2:** Investigate, install and test ScriptSafe browser extension

**Task 3:** Investigate, install and test AdblockPlus browser extension

**Task 4:** Investigate, install and test Ghostery browser extension

Note: Youtube and Facebook are reasonable sites to test the action of the browser extensions – find others