Information Security (CP3404)
Chapter 2 practical

- This practical consists of some quick quiz questions, tutorial type questions, and hands-on projects relevant to (chosen from) Chapter 2 of the textbook (i.e., Mark Ciampa, *CompTIA® Security + Guide to Network Security Fundamentals, Fifth Edition*, USA, 2015).
- You may not be able to complete this practical within the scheduled one-hour practical session for this subject. You are strongly recommended to complete it in your own time (note that you are expected to work 10 hours per week on this subject, including 3 hours of contact time).

Section A – Quick-Quiz/Multiple-Choice Questions:

- Each week, complete the test on LearnJCU within the time allocated, which is before the next practical session.
- These on-line tests are worth 20% of the total marks for this subject.

Section B – Short Answer (Tutorial-Type) Questions:

- Answers to this set of questions are available at the end of this document (Section D).
- Effective learning implies you answer the questions before seeing the answer.

1. What is malware?
   Discuss malware classification based on their primary objectives.
2. Explain how an appender infection works.
3. What are some (at least 3) of the functions performed by viruses?
4. Describe a macro virus.
5. What is a worm?
6. How does a rootkit work?
7. What is a backdoor and what is it used for?
8. What are botnets?
9. Describe adware.
10. Due to the prevalence of text filters for filtering spam, how have spammers modified their attacks?

Section C – Hands-On Projects:

Due to security issues, you may not be allowed to practise hands-on projects with university's computers. Interested students are encouraged to do these projects on their own computers (if available). You will not be assessed for utilities/commands that cannot be practised on university computers. Note that you may still be assessed for descriptions/definitions that are provided in this section.

Write-Protecting and Disabling a USB Flash Drive[1]

Viruses and other malware are often spread from one computer to another by infected USBflash drives. This can be controlled by either disabling the USB port or by write-protecting the drives so that no malware can be copied to it. Disabling the port can be accomplished through changing a Windows registry setting while write-protecting the drive can be done through third-party software that can control USB device permissions. In this project, you will download and install a software-based USB write blocker to prevent data from being written to a USB device and also disable the USB port. You will need a USB flash drive for this project.

1. Open a web browser and enter the URL www.irongeek.com/i.php?page=security/thumbscrew-software-usb-write-blocker
2. Click **Download**[2].
3. If the File Download dialog box appears, click **Save** and follow the instructions to save this file in a location such as your desktop or a folder of your choice.
4. When the file finishes downloading, extract the files in a location of your own choice. Navigate to that location and double-click **thumbscrew.exe** and follow the default installation procedures.
5. After installation, notice that a new icon appears in the system tray in the lower right corner of the screen.
6. Insert a USB flash drive into the computer.
7. Navigate to a document on the computer.
8. Right-click the document and then select **Send to**.
9. Click the appropriate **Removable Disk** icon of the USB flash drive to copy the file to the flash drive.
10. Now make the USB flash drive write protected so it cannot be written to.Click the icon in the system tray.
11. Click **Make USB Read Only**. Notice that the red circle now appears over the icon to indicate that the flash drive is write protected.
12. Navigate to a document on the computer.
13. Right-click the document and then select **Send to**.
14. Click the appropriate **Removable Disk** icon on the USB flash drive to copy the file to the flash drive. What Happens?
15. Click the icon in the system tray to change the permissions so that the USB drive is no longer read only.

[1]If you are concern about installing any of the software in this project on your regular computer, you can instead instal the software in the Windows virtual machine created in practical-1. Software installed within the virtual machine will not impact the host computer.

[2]The location of content on the Internet may change without warning. If you are no longer able to access the site through the above web address, use a search engine to search for "Irongeek Thumbscrew".

16. No disable the USB port entirely. First remove the flash drive fromn the USB port.
17. In the Windows **Run** dialog box enter **regedit**.
18. In the left pane double-click **HKEY_LOCAL_Machine** to expand it.
19. Double-click **SYSTEM**.
20. Double-click **ControlSet001**.
21. Double-click **USBSTOR** as shown in Figure 2-10.
22. In the right pane double-click **Start**.
23. In **Value data:** change the number of **3** to **4**. Be sure that **Hexadecimal** under **Base** is selected.
24. Click **OK**.
25. Now insert a USB flash drive into the USB port. What happens?
26. To reactivate the port, Change the **Value data:** back to **3** and click **OK**.
27. Close all windows.

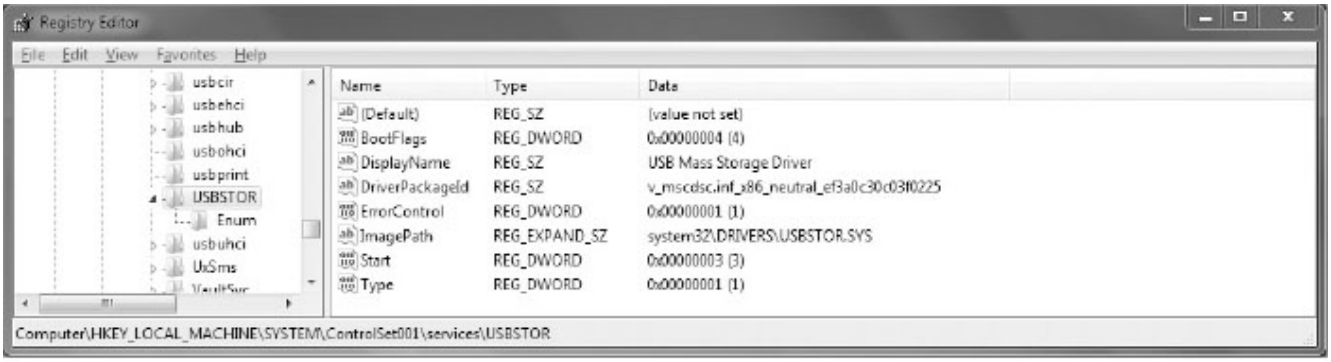

Figure 2-10 Windows Registry Editor
Source: Microsoft Windows

Section D – Answers to Short Answer (Tutorial-Type) Questions:

1. What is malware?
   Discuss malware classification based on their primary objectives.

   Answer:
   Malware is software that enters a computer system without the user's knowledge or consent and then performs an unwanted —and usually harmful— action.

   Malware is a general term that refers to a wide variety of damaging or annoying software programs. One way to classify malware is by its primary objective. Some malware has the primary goal of rapidly spreading its infection, while other malware has the goal of concealing its purpose. Another category of malware has the goal of making a profit for its creators.

2. Explain how an appender infection works.

   Answer:
   The virus first appends itself to the end of a file. It then moves the first three bytes of the original file to the virus code and replaces them with a *jump* instruction pointing to the virus code. When the program is launched, the jump instruction redirects control to the virus.

3. What are some (at least 3) of the functions performed by viruses?

   Answer:
   Viruses have performed the following functions:

   (i) Caused a computer to crash repeatedly
   (ii) Erased files from a hard drive
   (iii) Made multiple copies of itself and consumed all of the free space in a hard drive
   (iv) Turned off the computer's security settings
   (v) Reformatted the hard disk drive

4. Describe a macro virus.

   Answer: A macro virus is written in a script known as a macro. A macro is a series of commands and instructions that can be grouped together as a single command. Macros often are used to automate a complex set of tasks or a repeated series of tasks.

5. What is a worm?

   Answer:
   A worm is a malicious program that uses a computer network to replicate, and is designed to enter a computer through the network then take advantage of vulnerability in an application or an operating system on the host computer.

6. How does a rootkit work?

   Answer:
   One approach used by rootkits is to alter or replace operating system files with modified versions that are specifically designed to ignore malicious activity. For example, on a computer the anti-malware software may be instructed to scan all files in a specific directory and in order to do this, the software will receive a list of those files from the operating system. A rootkit will replace the operating system's ability to retrieve a list of files with its own modified version that ignores specific malicious files. The anti-malware software assumes that the computer will willingly carry out those instructions and retrieve all files; it does not know that the computer is only displaying files that the rootkit has approved.

7. What is a backdoor and what is it used for?

   Answer:
   A backdoor gives access to a computer, program, or service that circumvents any normal security protections. Backdoors that are installed on a computer allow the attacker to return at a later time and bypass security settings.

8. What are botnets?

   Answer:
   Botnets are collections of thousands or even hundreds of thousands of zombie computers are gathered into a logical computer network under the control of an attacker, or bot herder.

9. Describe adware.

   Answer:
   Adware delivers advertising content in a manner that is unexpected and unwanted by the user. Once it becomes installed, it typically displays advertising banners, popup ads, or opens new web browser windows at random intervals.

10. Due to the prevalence of text filters for filtering spam, how have spammers modified their attacks?

    Answer:
    Spammers have turned to image spam, which uses graphical images of text in order to circumvent text-based filters.