Information Security (CP3404)
Chapter 1 Practical

- This practical consists of some quick quiz questions, tutorial type questions, and hands-on projects relevant to (chosen from) Chapter 1 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. Why is the speed of attacks making the challenge of keeping computers secure more difficult?
2. Why are there delays in updating products such as anti-virus to resist attacks?
3. List and describe three of the characteristics of information (a.k.a CIA characteristics) that must be protected by information security?
4. Information security is achieved through a combination of what three entities?
   Provide at least one example of each entity.
5. What is a hacker? Describe white hat and black hat hackers.
6. Describe script kiddies.
7. Describe the security principle of simplicity.
8. What is a state sponsored attacker?

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.

Create a Virtual Machine of Windows 8.1 for Security Testing[1]

Part 1

Many users are reluctant to use their normal *production* computer for installing and testing new security applications. As an alternative, a virtual machine can be created on the *host* computer that runs a *guest* operating system. Security programs and testing can be conducted within this host operating system without any impact on the regular host operating system. In this project you will create a virtual machine using Oracle VirtualBox.

1. Open a web browser and enter the URL www.virtualbox.org
2. Click **Download**[2].
3. Under **VirtualBox platform packages** select the latest version of Virtual Box for your host operating system to download that program.For example, if you are running Windows 7, select the version for "VirtualBox x.x.x.for Windows hosts".
4. Under **VirtualBox x.x.x Oracle VM VirtualBox Extension Pack** click **All supported platforms** to download the extension package.
5. Navigate to the folder that contains the downloads and launch the VirtualBox installation program **VirtualBox-xxx-nnnn-hhh.exe**.
6. Accept the default configurations from the installation Wizard to install the program.
7. If you are asked "Would you like to install this device software?" on one or more occasions, click **Install**.
8. When completed click **Finish** to launch VirtualBox, as seen in Figure 1-7.
9. now install the VirtualBox extensions. Click **File** and **Preferences**.
10. Click **Extensions**.
11. Click the **Add a package** icon on the right side of the screen.
12. Navigate to the folder that contains the extension pack downloaded earlier to select that file. Click —bf Open.
13. Click **Install**. Follow the necessary steps to complete the default installation.
14. Click **File** and **Close** to close VirtualBox. Complete the next project to configure VirtualBox and install the guest operating system.

[1]The operating system of the host computer is not required to be different from that of the new guest operating system. That is, a Computer that already has installed Windows 8.1 as its host operating system can still create a virtual machine of Windows 8.1 that is used for testing.

[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, then use a search engine to search for "Oracle VirtualBox download".

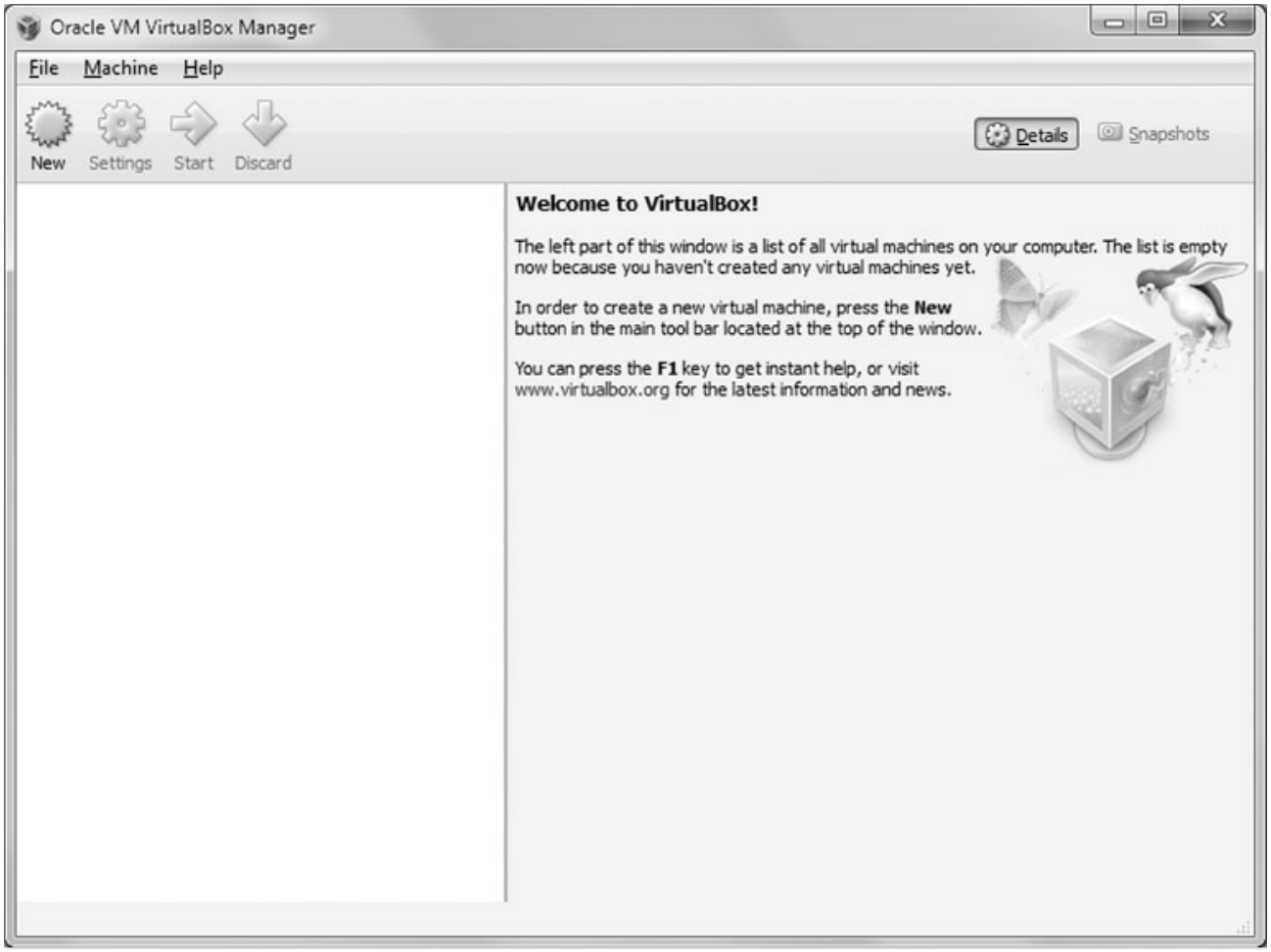

Figure 1-7 VirtualBox
Source: VirtualBox software developed by Oracle Corporation

Create a Virtual Machine of Windows 8.1 for Security Testing Part 2

After installing VirtualBox the next step is to create the guest operating system. For this project Windows 8.1 will be installed. Different options are available for obtaining a copy of Windows 8.1:

- A retail version of the software can be purchased
- If your school is a member of the Microsoft DreamSpark program the operating system software and a license can be downloaded (www.dreamspark.com).
- A 90-day evaluation copy can be downloaded and installed from the Microsoft TechNet Evaluation Center (technet.microsoft.com/en-us/evalcenter/hh699156.aspx).

1. Obtain the ISO image of Windows 8.1 using one of the options above and save it on the hard drive of the computer.
2. Launch VirtualBox.
3. Click **New**.
4. In **Name:** enter **Windows 8.1** as the name of the virtual machine.

5. Be sure that **Type:** changes to **Microsoft Windows** and **Version:** changes to **Windows 8.1**. Click **Next**.

6. Under **Memory size** accept the recommended size or increase the allocation if you have sufficient RAM on your computer. Click **Next**.

7. Under **Hard drive** accept **Create a virtual hard drive now**. Click **Create**.

8. Under **Hard drive file type** accept the default **VID (VirtualBox Disk Image)**. Click **Next**.

9. Under **Storage on physical hard drive3** accept the default **Dynamically allocated**. Click **Next**.

10. Under **File location and size** accept **Windows 8.1**. Click **Create**.

11. Now2 the configuration settings for the virtual machine are set as seen in Figure 1-8.

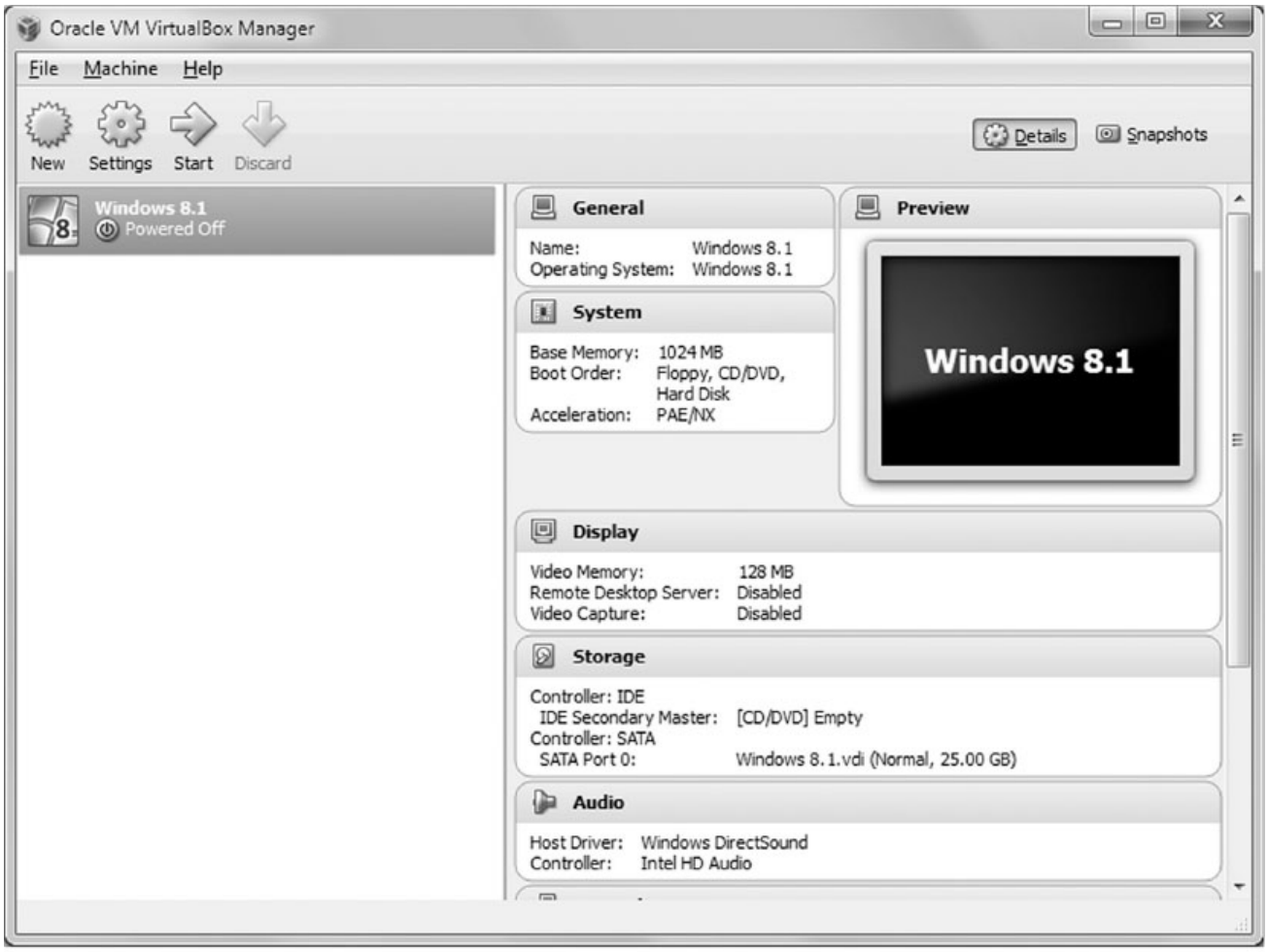

Figure 1-8 VirtualBox virtual machine settings
Source: VirtualBox software developed by Oracle Corporation

12. Next you will load the Windows 8.1 ISO image. Click **Settings**.

13. In the left pane click **Storage**.

14. Under **Controller: IDE** click **Empty**.

15. In the right page under **Attributes** click the icon of the optical disc.

16. Click **Choose a virtual CD/DVD disc file...**.

17. Navigate to the location of the Windows 8.1 ISO file and click **Open**.
18. Click **OK.**
19. Click **start** to launch the Windows 8.1 ISO.
20. Follow the Windows 8.1 installation wizard to complete the installation.
21. To close the Windows 8.1 guest operating system in VirtualBox click **File** and then **Exit**.
22. Close all windows.

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

1. Why is the speed of attacks making the challenge of keeping computers secure more difficult?

   Answer:
   With modern tools at their disposal, attackers can quickly scan systems to find weaknesses and launch attacks with unprecedented speed. Many tools can even initiate new attacks without any human participation, thus increasing the speed at which systems are attacked.

2. Why are there delays in updating products such as anti-virus to resist attacks?

   Answer:
   At the current rate of submissions of potential malware on a daily basis, updates for anti-virus software would need to be released every few seconds.

3. List and describe three of the characteristics of information (a.k.a CIA characteristics) that must be protected by information security?

   Answer:
   Three of the characteristics of information that must be protected by information security are:

   (i) *Confidentiality* – Confidentiality ensures that only authorized parties can view the information.

   (ii) *Integrity* – Integrity ensures that the information is correct and no unauthorized person or malicious software has altered that data.

   (iii) *Availability* – Availability ensures that data is accessible to authorized users.

4. Information security is achieved through a combination of what three entities?
   Provide at least one example of each entity.

   Answer:

   (i) *Products (physical security)* – The physical security around the data. May be as basic as door locks or as complicated as intrusion-detection systems and firewalls.

   (ii) *People (personnel security)* – Those who implement and properly use security products to protect data.

   (iii) *Procedures (organizational security)* – Plans and policies established by an organization to ensure that people correctly use the products.

5. What is a hacker? Describe white hat and black hat hackers.

   Answer:
   In the past, the term hacker was commonly used to refer to a person who uses advanced computer skills to attack computers.

   White hat hackers said that their goal was only to expose security flaws and not steal or corrupt data. Although breaking into another computer system is illegal, they considered it acceptable as long as they did not commit theft, vandalism, or breach any confidentiality while trying to improve security by seeking out vulnerabilities.

   In contrast, the term black hat hackers was used to refer to attackers whose motive was malicious and destructive.

   However, today the term hacker has been replaced with the more generic term attacker, without any attempt to distinguish between the motives. Although *hacker* is often used by the mainstream media to refer to an attacker, this term is no longer commonly used by the security community.

6. Describe script kiddies.

   Answer:
   Script kiddies are individuals who want to break into computers to create damage yet lack the advanced knowledge of computers and networks needed to do so. Instead, script kiddies do their work by downloading automated attack software (scripts) from Web sites and using it to perform malicious acts.

7. Describe the security principle of simplicity.

   Answer:
   Because attacks can come from a variety of sources and in many ways, information security is by its very nature complex. The more complex something becomes, the more difficult it is to understand. A security guard who does not understand how motion detectors interact with infrared trip lights may not know what to do when one system alarm shows an intruder but the other does not. In addition, complex systems allow many opportunities for something to go wrong. In short, complex systems can be a thief's ally.

   The same is true with information security. Complex security systems can be hard to understand, troubleshoot, and feel secure about. As much as possible, a secure system should be simple for those on the inside to understand and use. Complex security schemes are often compromised to make them easier for trusted users to work with –yet this can also make it easier for the attackers. In short, keeping a system simple from the inside but complex on the outside can sometimes be difficult but reaps a major benefit.

8. What is a state sponsored attacker?

   Answer:
   A state-sponsored attacker is a government supported attacker that attacks foreign governments or citizens who are considered hostile or threatening.