Information Security (CP3404)

Chapter 10 practical

- This practical consists of some quick quiz questions, tutorial type questions, and hands-on projects relevant to (chosen from) Chapter 10 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. List three things that can be done in order to reduce the risk of theft or loss of a mobile device.
2. How might an attacker misuse a QR (Quick Response) code?
3. Describe three of the risks associated with BYOD.
4. What are the two options for using encryption with mobile devices?
5. How does BYOD increase employee performance?
6. What are the three sizes of Secure Digital (SD) cards available, and how are they typically used?
7. What is the difference between a feature phone and a smartphone?
8. Describe a subnotebook computer

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.

Software to Locate a Missing Laptop[1]

If a mobile device is lost or stolen, there are several different security features that can be used to locate the device or limit the damage. Many of these can be used through an installed third-party app. In this project you will download and install software that can locate a missing laptop computer. Note that for this project a portable computer or desktop computer can be used.

1. Open your web browser and enter URL preyproject.com.[2].
2. Click **FAQ**.
3. Read through the questions so you will understand what Prey does.
4. Click **Download**
5. Select the latest version for your computer.
6. When the file finishes downloading, run the program and follow the default installation procedure.
7. Click **Finish** to configure the Prey settings.
8. Be sure that **New user** is selected. Click **Next**.
9. Enter your information to create an account and click **Create**.
10. Go to **panel.preproject,com**.
11. Enter your login information, and on the **All your devices** page, click the name of your recently added device.
12. You will then receive in your email a link to go to the Prey control panel. Save this link for future reference.
13. Click the question mark next to **Get active connections** to change the setting from **NO** to **YES**.
14. Do the same with each of the other settings that by default are set to **NO** and change them to **YES**.
15. Click **Save changes**.
16. Click the **Hardware** tab to review the hardware settings from this device.
17. Click **Main**.
18. Under **actions to perform**, click the question mark next to **Alarm** to change from **Off** to **On**. What does this function perform?
19. Click the question mark next to **Alert** to change from **Off** to **On**. What does this function perform?
20. Click **save Changes**.
21. Move the slider from **OK** to **MISSING** to begin the tracking process.
22. It may take up to 10 minutes for the alarm to sound depending how frequently the device checks into Prey.

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

[2] It is not unusual for websites to change the location of files. If the URL above no longer functions, open a search engine and search for "Prey Project"

23. When a report is generated, click **Reports** and read the information about the location of the device. Would this be sufficient information to find the missing device?

24. Click **Main**.

25. Move the slider from **MISSING** to **OK**.

26. Click **Save changes**.

27. Close all windows.

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

1. List three things that can be done in order to reduce the risk of theft or loss of a mobile device.

   Answer:
   Any three of the following is fine:

   (i) Keep the mobile device out of sight when traveling in a high-risk area.

   (ii) Avoid becoming distracted by what is on the device. Always maintain an awareness of your surroundings.

   (iii) When holding a device, use both hands to make it more difficult for a thief to snatch.

   (iv) Do not use the device on escalators or near transit train doors.

   (v) White or red headphone cords may indicate they are connected to an expensive device. Consider changing the cord to a less conspicuous color.

   Vi) If a theft does occur, do not resist or chase the thief. Instead, take note of the suspect's description, including any identifying characteristics and clothing, and then call the authorities. Also contact the organization or wireless carrier and change all passwords for accounts accessed on the device.

2. How might an attacker misuse a QR (Quick Response) code?

   Answer:
   An attacker could create an advertisement for a reputable website, such as a bank, and then include a QR code that contains a malicious URL that redirects an unsuspecting user to an imposter website.

3. Describe three of the risks associated with BYOD (Bring Your Own Device).

   Answer:
   Any three of the following is fine.

   (i) Users may erase the installed built-in limitations on their smartphone (called jailbreaking on Apple iOS devices or rooting on Android devices) to provide additional functionality. However, this also disables the built-in operating system security features on the phone.

   (ii) Personal mobile devices are often shared among family members and friends, subjecting sensitive corporate data installed on a users device to outsiders.

   (iii) Different mobile devices have different hardware and different versions of operating systems, all of which contain different levels and types of security features. Technical support staff may be called upon to support hundreds of different mobile devices, creating a nightmare for establishing a security baseline.

   (iv) Mobile devices may be connected to a user's personal desktop computer that is infected, thus infecting the mobile device and increasing the risk of the organization's network becoming infected when the mobile device connects to it.

(v) There may be difficulties in securing the personal smartphone from an employee who was fired so that any corporate data on it can be erased.

4. What are the two options for using encryption with mobile devices?

   Answer:
   Two options for encryption are:

   (i) Full device encryption can be used, where all data on the device is encrypted.

   (ii) Alternatively, data storage can be separated into containers for encryption.

5. How does BYOD (Bring Your Own device) increase employee performance?

   Answer:
   Employees are more likely to be productive while traveling or working away from the office if they are comfortable with their device.

6. What are the three sizes of Secure Digital (SD) cards available, and how are they typically used?

   Answer:
   The three sizes of SD cards are: full SD, miniSD, and microSD. Full SD memory cards are typically used in personal computers, video cameras, digital cameras, and other large consumer electronics devices. The microSD and miniSD cards are commonly used in smaller electronic devices like smartphones and tablets.

7. What is the difference between a feature phone and a smartphone?

   Answer:
   A feature phone is a traditional cell phone, whereas a smartphone has all the tools that a feature phone has, but also includes a mobile operating system that allows for the use of applications and Internet access.

8. Describe a subnotebook computer.

   Answer:
   Sometimes called an ultrabook (Intel/Windows) or air (Apple), these devices are even smaller than standard notebooks and use low-power processors and solid state drives (SSDs). They generally have a high-definition multimedia interface (HDMI) port along with a limited number of USB hardware ports.