Information Security (CP3404)
Chapter 4 practical

- This practical consists of some quick quiz questions, tutorial type questions, and hands-on projects relevant to (chosen from) Chapter 4 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. Explain how tailgate sensors work.
2. Describe a mantrap.
3. What are the three states of data that DLP (Data Loss Prevention) typically examines?
4. Describe how a DLP (Data Loss Prevention) can be configured.
5. What can be a time consuming drawback to the use of traditional ID badges? How can this issue be avoided?
6. How does an RFID (Radio Frequency IDentification) tag embedded into an ID badge function without a power supply?
7. What is the difference between deterrent controls and preventive controls?
8. How can cable conduits that run between two secure areas be protected?
9. What are the five steps that can be used to ensure the security of an OS (Operating System)?
10. How does DLP (Data Loss Prevention) index matching work?

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.

Viewing Windows Firewall Settings[1]

In this project, you will view the settings on Windows Firewall.

1. Click **Start** and then click **Control Panel**.
2. Click **System and Security**, then **Windows Firewall**.
3. In the lefty pane, click **Change notification settings**. Notice that you can either block all incoming connections or be notified when Windows Firewall block a program at the firewall. What would be the difference? Which setting is more secure?
4. Now click **Turn off Windows Firewall (not recommended)** –there may be multiple instances of this setting depending on your network.
5. Click **OK**. What warning appears? Are these sufficient to alert a user?
6. In the left pane, click **Change notification settings**. Click **Turn on Windows Firewall** —there may be multiple instances of this setting depending on your network)
7. Click **OK**.
8. In the left pane, click **Advanced Settings**.
9. Click **Inbound Rules**.
10. Double-click a rule to open the dialog box associated with that rule. Click through the tabs and notice the control that can be configuration firewall rules. Click **Cancel**.
11. Now create a rule that will open a specific port on the computer so that a web server will run and traffic will go through the firewall. Click **New Rule . . .** in the right pane to open the New Inbound Rule Wizard dialog box.
12. Click **Port** as the rule type and then click **Next**.
13. If necessary select **TCP** as the protocol.
14. Enter **80**[2] in the **Specific local ports** text box. Click **Next**.
15. You are asked what to do when the firewall sees inbound traffic on TCP Port 80. Because you want this traffic to reach your web server, click **Allow the connection**.
16. Click **Next**.

[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] You can open a single port by typing its number, or multiple ports by separating them with a comma, or a port range (such as 80-86).

17. You are then asked the type of connections to which this rule will apply. To run a web server only for the local computers in your home network, the *Private* option would be selected while deselecting *Public* and *Domain*. For this project, deselect **Private** and —bf Domain.

18. Click **Next**.

19. Enter the rule name **Web Server Port 80**.

20. To implement this rule cliock **Finish**, otherwise click **Cancel**.

21. Close all windows.

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

1. Explain how tailgate sensors work.

   Answer:
   Tailgate sensors use multiple infrared beams that are aimed across a doorway and positioned so that as a person walks through the doorway some beams are activated; the other beams are then activated a fraction of a second later. The beams are monitored and can determine which direction the person is walking. In addition, the number of persons walking through the beam array can also be determined. If only one person is allowed to walk through the beam for a valid set of credentials, an alarm can sound when a second person walks through the beam array immediately behind (*tailgates*) the first person without presenting credentials.

2. Describe a mantrap.

   Answer:
   A mantrap is designed to separate a non-secured area from a secured area. A mantrap device monitors and controls two interlocking doors to a small room (a vestibule). When in operation, only one door is able to be open at any time. Mantraps are used at high-security areas where only authorized persons are allowed to enter, such as sensitive data-processing rooms, cash-handling areas, and research laboratories.

3. What are the three states of data that DLP (Data Loss Prevention) typically examines?

   Answer:
   DLP typically examines data as it resides in any of three states: data in use (actions being performed by *endpoint devices* such as printing a report from a desktop computer), data in transit (actions that transmit the data across a network like a file being retrieved from a server), and data at rest (data that is stored on a DVD or other media). Data that is considered critical to the organization or needs to be confidential can be tagged as such. A user who then attempts to access the data to disclose it to another unauthorized user will be prevented from doing so.

4. Describe how a DLP (Data Loss Prevention) can be configured.

   Answer: DLPs can be configured to look for specific data (such as Social Security and credit card numbers), lines of computer software source code, words in a sequence (to prevent a report from leaving the network), maximum file sizes, and file types. Because it can be difficult to distinguish a Social Security number from a mistyped phone number or a nine-digit on-line order number, DLP can use fingerprinting to more closely identify important data. A fingerprint may consist of a Social Security number along with a name to trigger an alarm. In addition, white-lists and blacklists can be created to prevent specific files from being scanned

5. What can be a time consuming drawback to the use of traditional ID badges? How can this issue be avoided?

   Answer:
   If verifying more than a few users at a time, a bottleneck can occur while each user is processed. The use of a proximity reader and radio frequency identification (RFID) tags can be used to speed up identification.

6. How does an RFID (Radio Frequency IDentification) tag embedded into an ID badge function without a power supply?

   Answer:
   The passive RFID uses the tiny electrical current induced in the antenna by an incoming signal from the transceiver, which then produces enough power for the tag to send a response.

7. What is the difference between deterrent controls and preventive controls?

   Answer:
   Deterrent controls attempt to discourage security violations before they occur, whereas preventive controls focus on prevention of a threat from coming into contact with a vulnerability.

8. How can cable conduits that run between two secure areas be protected?

   Answer:
   A protected distribution system (PDS) can be used to protect conduit cables between two locations. This can consist of a hardened carrier PDS, in which the conduit is constructed of special electrical metallic tubing or similar material, or an alarmed carrier PDS, which uses optical fibers and acoustic sensors that can detect vibrations from a potential intruder.

9. What are the five steps that can be used to ensure the security of an OS (Operating System)?

   Answer:
   The five steps that can be used to ensure the security of an OS (Operating System) are:

   (i) Develop the security policy.

   (ii) Perform host software baselining.

   (iii) Configure operating system security settings.

   (iv) Deploy and manage security settings.

   (v) Implement patch management.

10. How does DLP (Data Loss Prevention) index matching work?

    Answer:
    Index matching involves analyzing documents that have been identified as needing protection, and makes use of complex computations that are later used to identify parts of the document, and prevent the document from being leaked.