Information Security (CP3404)
Chapter 14 practical

- This practical consists of some quick quiz questions, tutorial type questions, and hands-on projects relevant to (chosen from) Chapter 14 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 and describe four (4) of the seven risk categories.
2. What are the typical classification designations of government documents?
3. What are the four (4) duties of the Change management team (CMT)?
4. List three (3) characteristics of a policy.
5. List two (2) reasons why social networking sites are popular with attackers.
6. What is a general security tip for using a social networking site?
7. Identify three (3) opportunities for security education and training.

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 Your Annual Credit Report[1]

Security experts recommend that consumers receive a copy of their credit report at least once per year and check its accuracy to protect their identity.

In this project you will access your free credit report online.

1. Use your web browser to go to www.annualcreditreport.com. Although you could send a request individually to one of the three credit agencies, this website acts as a central source for ordering free credit reports.
2. Click **Request your free credit reports**.
3. Read through the three steps and click **Request your credit reports**.
4. Enter the requested information and click **Continue** and then **Next**.
5. Click **TransUnion**. Click **Next**.
6. After the brief processing completes, click **Continue**.
7. You may then be asked personal information about your transaction history in order to verify your identity. Answer the requested questions and click **Next**.
8. Follow the instructions to print your report.
9. Review it carefully, particularly the sections of ''Potentially negative items" and ''Requests for your credit history." If you see anything that might be incorrect, follow the instructions on that website to enter a dispute.
10. Follow the instructions to exit from the website.
11. Close all windows.

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

1. List and describe four (4) of the seven risk categories.

   Answer:
   Any four items from the followings is fine:

   (i) *Strategic* – Action that affects the long-term goals of the organization
   (ii) *Compliance* – Following a regulation or standard
   (iii) *Financial* – Impact of financial decisions or market factors
   (iv) *Operational* – Events that impact the daily business of the organization
   (v) *Environmental* – Actions related to the surroundings
   (vi) *Technical* – Events that affect information technology systems
   (vii) *Managerial* – Actions that are related to the management of the organization

[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. What are the typical classification designations of government documents?

   Answer:
   The classification designations of government documents are typically Top Secret, Secret, Confidential, and Unclassified.

3. What are the four (4) duties of the Change management team (CMT)?

   Answer:

   (i) Review proposed changes.
   (ii) Ensure that the risk and impact of the planned change are clearly understood.
   (iii) Recommend approval, disapproval, deferral, or withdrawal of a requested change.
   (iv) Communicate proposed and approved changes to coworkers.

4. List three (3) characteristics of a policy.

   Answer:
   Any three os the followings is fine:

   (i) Policies communicate a consensus of judgment.
   (ii) Policies define appropriate behavior for users.
   (iii) Policies identify what tools and procedures are needed.
   (Iv) Policies provide directives for Human Resource action in response to inappropriate behavior.
   (v) Policies may be helpful in the event that it is necessary to prosecute violators.

5. List two (2) reasons why social networking sites are popular with attackers.

   Answer:
   Any two (2) items from the followings is fine:

   (i) They provide a treasure trove of personal data. Users often include personal information in their profiles for others to read, such as birthdays, where they live, and their employment history. Attackers may steal this data and use it for malicious purposes.
   - Users are generally trusting. Attackers often join a social networking site and pretend to be part of the network of users. After several days or weeks, users begin to feel they know the attackers and may start to provide personal information or click embedded links provided by the attacker that load malware onto the user's computer.
   - Social networking Web sites are vulnerable. Because social networking sites have only recently become the target of attackers, many of these sites have lax security measures and it is easy for attackers to break into the sites to steal user information.

6. What is a general security tip for using a social networking site?

   Answer:
   any of the following is fine:

   (i) Consider carefully who is accepted as a friend. Once a person has been accepted as a friend, that person will be able to access any personal information or photographs.
   (ii) Show *limited friends* a reduced version of your profile. Individuals can be designated *limited friends* who only have access to a smaller version of the user's profile. This can be useful for casual acquaintances or business associates.
   (iii) Disable options and then reopen them only as necessary. Users should disable options until it becomes apparent that option is needed, instead of making everything accessible and restricting access after it is too late.

7. Identify three (3) opportunities for security education and training.

Answer:
Any three of the followings is fine:

(i) When a new employee is hired

(ii) After a computer attack has occurred

(iii) When an employee is promoted or given new responsibilities

(iv) During an annual departmental retreat

(v) When new user software is installed

(vi) When user hardware is upgraded