Information Security (CP3404)
Chapter 11 practical

- This practical consists of some quick quiz questions, tutorial type questions, and hands-on projects relevant to (chosen from) Chapter 11 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 two major access control models.
2. Describe the two key elements of the MAC (Mandatory Access Control) model.
3. Discuss the two significant weaknesses of DAC (Discretionary Access Control).
4. List two of the most common types of authentication and AAA (Authentication, Authorization, and Accounting) servers.
5. List the steps for RADIUS authentication with a wireless device in an IEEE 802.1x network.
6. Describe how Kerberos works.
7. Discuss the differences between DAP (Directory Access Protocol) and LDAP (Lightweight Directory Access Protocol).
8. Describe LDAP (Lightweight Directory Access Protocol) injection 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.

Using Discretionary Access Control to Share Files in Windows[1]

Discretionary Access Control (DAC) can be applied in Microsoft windows. In this project, you will set up file sharing with other users.

You should have a standard user name "Abby Lomax"created in Windows and a Notepad document Sample.txt created by an administrative user in order to complete this assignment.

1. Right-click the file **Sample.txt**.
2. To see the current permissions on this file, click **Properties**, and then click the **security** tab.
3. Click your user name and thern click **Edit**.
4. Under **Permissions for [user]**, click **Deny** for the **Read** attribute.
5. Click **Apply** and **Yes** at the warning dialog box.
6. Click **OK** in the properties dialog box and then click **OK** in the Sample.txt dialog box.
7. Double-click the file **Sample.txt** to open it. What happens?
8. Now give permissions to Abby Lomax to open the file. Right-click the file **Sample.txt**.
9. Click **Share with** and then click **Specific people**.
10. Click the drop-down arrow and select **Abby Lomax**. Click **Add**.
11. Click **Share**.
12. Click **Done** when the sharing process is completed.
13. Now log in as Abby Lomax. Click **Start** and the **right arrow** and then **Switch User**.
14. Log in as Abby Lomax.
15. Right-click **Start** and then click **Explore**.
16. Navigate to your account name and locate the file Sample.txt.
17. Double-click **Sample.txt** to open the file. Using DAC, permissions have been granted to another user.
18. Close all windows.

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

[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.

1. List two major access control models.

   Answer:
   Any two of the following is fine:

   (i) Mandatory Access Control (MAC)

   (ii) Discretionary Access Control (DAC)

   (iii) Role Based Access Control (RBAC)

   (iv) Rule Based Access Control (RBAC)

2. Describe the two key elements of the MAC (Mandatory Access Control) model.

   Answer:
   Two key elements of Mac model are:

   (i) *Labels:* In a system using MAC, every entity is an object (laptops, files, projects, and so on) and is assigned a classification label. These labels represent the relative importance of the object, such as confidential, secret, and top secret. Subjects (users, processes, and so on) are assigned a privilege label (sometimes called a clearance).

   (ii) *Levels:* A hierarchy based on the labels is also used, both for objects and subjects. Top secret has a higher level than secret, which has a higher level than confidential.

3. Discuss the two significant weaknesses of DAC (Discretionary Access Control).

   Answer:
   DAC has two significant weaknesses.

   (i) First, although it gives a degree of freedom to the subject, DAC poses risks in that it relies on decisions by the end user to set the proper level of security. As a result, incorrect permissions might be granted to a subject or permissions might be given to an unauthorized subject.

   (ii) A second weakness is that a subject's permissions will be *inherited* by any programs that the subject executes. Attackers often take advantage of this inheritance because end users in the DAC model often have a high level of privileges. Malware that is downloaded onto a user's computer would then run in the same context as the user's high privileges. Trojans are a particular problem with DAC.

4. List two of the most common types of authentication and AAA (Authentication, Authorization, and Accounting) servers.

   Answer:
   Any two of the followings are fine:

   (i) RADIUS

   (ii) Kerberos

   (iii) Terminal Access Control Access Control Systems (TACACS)

   (iv) generic servers built on the Lightweight Directory Access Protocol (LDAP)

5. List the steps for RADIUS authentication with a wireless device in an IEEE 802.1x network.

   Answer:
   Steps for RADIUS authentication with a wireless device in an IEEE 802.1x network are:

   (i) A wireless device, called the supplicant (it makes an *appeal* for access), sends a request to an AP (Access Point) requesting permission to join the WLAN. The AP prompts the user for the user ID and password.

   (ii) The AP, serving as the authenticator that will accept or reject the wireless device, creates a data packet from this information called the authentication request.

(iii) When an authentication request is received, the RADIUS server validates that the request is from an approved AP and then decrypts the data packet to access the username and password information. This information is passed on to the appropriate security user database.

(iv) If the username and password are correct, the RADIUS server sends an authentication acknowledgment that includes information on the user's network system and service requirements.

(v) If accounting is also supported by the RADIUS server, an entry is started in the accounting database.

(vi) Once the server information is received and verified by the AP, it enables the necessary configuration to deliver the wireless services to the user.

6. Describe how Kerberos works.

   Answer:
   Kerberos is typically used when a user attempts to access a network service and that service requires authentication. The user is provided a ticket that is issued by the Kerberos authentication server, much as a driver's license is issued by the DMV (Department of Motor Vehicles). This ticket contains information linking it to the user. The user presents this ticket to the network for a service. The service then examines the ticket to verify the identity of the user. If the user is verified, they are then accepted. Kerberos tickets share some of the same characteristics as a driver's license: tickets are difficult to copy (because they are encrypted), they contain specific user information, they restrict what a user can do, and they expire after a few hours or a day. Issuing and submitting tickets in a Kerberos system is handled internally and is transparent to the user.

7. Discuss the differences between DAP (Directory Access Protocol) and LDAP (Lightweight Directory Access Protocol).

   Answer:
   Unlike X.500 DAP, LDAP was designed to run over TCP/IP, making it ideal for Internet and intranet applications. X.500 DAP requires special software to access the network.

   LDAP has simpler functions, making it easier and less expensive to implement.

   LDAP encodes its protocol elements in a less complex way than X.500 that enables it to streamline requests

8. Describe LDAP (Lightweight Directory Access Protocol) injection attacks.

   Answer:
   A weakness of LDAP is that it can be subject to LDAP injection attacks. These attacks, similar to SQL injection attacks, can occur when user input is not properly filtered. This may allow an attacker to construct LDAP statements based on user input statements. The attacker could then retrieve information from the LDAP database or modify its content. The defense against LDAP injection attacks is to examine all user input before processing.