Information Security (CP3404)
Chapter 12 practical

- This practical consists of some quick quiz questions, tutorial type questions, and hands-on projects relevant to (chosen from) Chapter 12 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. What are the three broad categories on which authentication can be based?
2. Why do passwords place a heavy load on human memory?
3. Discuss the types of shortcuts that users take to help them recall their passwords.
4. Explain how an attacker can use a resetting attack.
5. Describe how rainbow tables work.
6. What are the three advantages of a rainbow table over other password attacks?
7. List and describe three of the common password setting objects.
8. What is the difference between multifactor authentication and single-factor authentication?
9. Explain why the LAN Manager (LM) hash is vulnerable.

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.

Use an Online Rainbow Table Cracker[1]

Although brute force and dictionary attacks were once the primary tools used by attackers to crack stolen passwords, more recently attackers have used rainbow tables. Rainbow tables make password attacks easier by creating a large pregenerated data set of candidate digests.

In this project, you will create a hash on a password and then crack it with an online rainbow table cracker to demonstrate the speed of using rainbow tables.

1. The first step is to use a general-purpose hash algorithm to create a password hash. Use your web browser to go to www.fileformat.info/tool/hash.htm.[2].
2. Under **String hash**, enter the simple password **apple123** in the **Text:** line.
3. Click **Hash**.
4. Scroll down the page and copy the MD4 hash of this password to your Clipboard by selecting the text, right-clicking, and choosing **Copy**.
5. Open a new tab on your web browser
6. Go to **http://crackstation.net/**.
7. Paste the MD4 hash of *apple123* into the text box beneath **Enter up to 10 non-salted hashes:**.
8. In the RECAPTCHA box, enter the current value being displayed in the box that says **Type the text**.
9. Click **Crack Hashes**.
10. How long did it take this online rainbow table to crack this hash?
11. Click the bowser tab to return to FileFormat.Info.
12. Under **String hash**, enter the longer password **12applesauce** in the **Text:** line.
13. Click **Hash**.
14. Scroll down the page and copy the MD4 hash of this password to your Clipboard.
15. Click to bowser tab to return to CrackStation site.
16. Paste the MD4 hash of *12applesauce* into the text box beneath **Enter up to 10 non-salted hashes:**.
17. In the RECAPTCHA box, enter the current value being displayed in the box that says **Type the text**.
18. Click **Crack Hashes**.

[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 ”Fileformat.info”

19. How long did it take this online rainbow table to crack this stronger password hash?

20. Click the bowser tab to return to FileFormat.Info and experiment by entering new passwords, computing their hash, and testing them in the CrackStation site. If you are bold, enter a string hash that is similar to a real password that you use.

21. What does this tell you about the speed of rainbow tables? What does it tell you about how easy it is for attackers to crack weak passwords?

22. Close all windows.

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

1. What are the three broad categories on which authentication can be based?

   Answer:
   Authentication can be based on:

   (i) What a user knows (such as a password)
   (ii) What a user has (like a token or a card)
   (iii) What a user is (biometrics)

2. Why do passwords place a heavy load on human memory?

   Answer:
   First, long and complex passwords (the most effective ones) can be difficult to memorize and can strain our ability to accurately recall them. Most users have difficulty remembering these types of strong passwords.

   Second, users today must remember passwords for many different accounts. Most users have accounts for different computers at work, school, and home, multiple e-mail accounts, plus online banking and Internet site accounts, to name a few. Each account ideally has its own password. In one study, 28 percent of a group of users had over 13 passwords each, while in another study, a group of 144 users had an average of 16 passwords per user.

3. Discuss the types of shortcuts that users take to help them recall their passwords.

   Answer:
   Because of the burdens that passwords place on human memory, users often take shortcuts to help them recall their passwords.

   The first shortcut is to use a weak password. This may include using a common word as a password (such as January), a short password (such as ABCDE), or personal information (such as the name of a child or pet) in a password.

   The second shortcut is to reuse the same password for multiple accounts. Although this makes it easier for the user, it also makes it easier for an attacker who compromises one account to access other accounts.

4. Explain how an attacker can use a resetting attack.

   Answer:
   If an attacker can gain physical access to a user's computer, then she can erase the existing password and reset it to a new password. Password reset programs require that the computer be rebooted from a CD or USB flash drive that usually contains a version of a different operating system along with the password reset program. For example, to reset a password on a Microsoft Windows computer, a USB flash drive with Linux and the password reset program would be used. The disadvantage of resetting is that it is immediately obvious that the computer has been compromised.

5. Describe how rainbow tables work.

   Answer:
   Rainbow tables make password attacks easier by creating a large pregenerated data set of encrypted passwords. There are two steps to using rainbow tables.

   First is creating the table itself. Next, that table is used to crack a password. A rainbow table is a compressed representation of plaintext passwords that are related and organized in a sequence (called a chain). To create a rainbow table, each chain begins with an initial password that is encrypted, and then that is fed into a function that produces a different plaintext password. This process is repeated for a set number of rounds. The initial password and the last encrypted value of the chain comprise a rainbow table entry.

6. What are the three advantages of a rainbow table over other password attacks?

   Answer:
   Three advantages of a rainbow table are:

   (i) A rainbow table can be used repeatedly for attacks on other passwords.

   (ii) Rainbow tables are much faster than dictionary attacks.

   (iii) The amount of memory needed on the attacking machine is greatly reduced

7. List and describe three of the common password setting objects.

   Answer:
   Any three items of the following is fine:

   (i) *Enforce password history* – determines the number of unique new passwords a user must use before an old password can be reused (from 0 to 24)

   (ii) *Maximum password age* – determines how many days a password can be used before the user is required to change it; the value of this setting can be between 0 and 999

   (iii) *Minimum password age* – determines how many days a new password must be kept before the user can change it (from 0 to 999); this setting is designed to work with the Enforce password history setting so that users cannot quickly reset their passwords the required number of times, and then change back to their old passwords

   (iv) *Minimum password length* – determines the minimum number of characters a password can have (0 to 28)

   (v) *Passwords must meet complexity requirements* – determines whether the following are used in creating a password: Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters; must contain characters from three of the following four categories: English uppercase characters (A through Z), English lowercase characters (a through z), digits (0 through 9), and nonalphabetic characters (!, $, #, %)

   (vi) *Store passwords using reversible encryption* – provides support for applications that use protocols that require knowledge of the user's password for authentication purposes; storing passwords using reversible encryption is essentially the same as storing plaintext versions of the passwords

8. What is the difference between multifactor authentication and single-factor authentication?

   Answer:
   Multifactor authentication uses multiple types of authentication credentials, such as what a user knows and what a user has, whereas single-factor authentication uses only one type of authentication.

9. Explain why the LAN Manager (LM) hash is vulnerable.

   Answer:
   LM hash is not case sensitive, meaning that there is no difference between uppercase (A) and lowercase (a). This significantly reduces the character set that an attacker must use.

Second, the LM hash splits all passwords into two 7-character parts. If the original password is fewer than 14 characters, it simply pads the parts; if it is longer, the extra characters are dropped